



# **ORAN SIM CE ATI Security Release Notes**

ORAN SIM CE 3.0 Security - Content

*10-July-2024*

## **Notices Copyright Notice ©**

Keysight Technologies 2005 – 2024

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. [Full Content List](#)

- [173 Precanned Attacks](#)
- [2764 Exploits](#)
- [5122 Malware Samples](#)

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

# Full Content List

## All Precanned Attacks (173)

Name	Description
All Encrypted Attacks	This precanned attack contains a collection of attacks against applications that run by default over SSL. The effects of a successful attack include access to protected data, disclosure of legally protected, highly sensitive information, even system compromise. It will run through each of the strikes one-by-one in order to test how well your implemented security controls protect your assets against these attacks. If these strikes are not blocked, they could compromise your web application and/or put your customers and data at risk.
Apple Browser Attacks	This is a precanned attack, containing a list of web browser attacks targeting Apple Safari software. Attacks may exploit flaws found in Apple Safari's browser engine (WebKit), JavaScript engine (JavaScriptCore) and other browser features (i.e. XSS filter) to perform actions on behalf of an attacker. The strikes found in this precanned attack are known to be used in attacks, being able to block or detect these attacks is an important aspect of your corporate security posture.
Auth Bypass Attacks	Authentication Bypass refers to an attacker gaining access to application, service, or device with the privileges of an authorized or privileged user by evading or circumventing an authentication mechanism. This precanned attack contains a collection of Authentication Bypass attacks. The effects of a successful attack include access to protected data, disclosure of legally protected, highly sensitive information, even system compromise. It will run through each of the strikes one-by-one in order to test how well your implemented security controls protect your assets against these attacks. If these strikes are not blocked, they could compromise your web application and/or put your customers and data at risk.
Brute Force Attack Top Usernames And Passwords	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
CSRF Attacks	Cross-Site Request Forgery (CSRF) is an attack that tricks an user into submitting malicious requests or unwanted actions on a web application in which they're currently authenticated. The effects of a successful CSRF attack consist in performing state-changing requests, like transferring funds, changing the user's email address or even compromise the entire web application. The strikes found in this precanned attack are known to be used in attacks, being able to block or detect these attacks is an important aspect of your corporate security posture.
Chrome Browser Attacks	This is a precanned attack, containing a list of web browser attacks targeting Google Chrome software. Attacks may exploit flaws found in Chrome's browser engine (Blink), JavaScript engine (V8) and other browser features (i.e. XSS filter) to perform actions on behalf of an attacker. The strikes found in this precanned attack are known to be used in attacks, being able to block or detect these attacks is an important aspect of your corporate security posture.

<b>Name</b>	<b>Description</b>
Critical Strikes	This precanned attack contains critical strikes which have a CVSS v3.0 score between 9 and 10.
DoS Attacks	Denial of Service is a type of attack where resources are made unavailable for their legitimate users, by temporarily or indefinitely disrupting services of a host connected to the Internet. DoS can be achieved in multiple ways: flooding or crashing services or by sending an input that takes advantage of bugs in the target that subsequently crash or severely destabilize the system. The strikes found in this precanned attack are known to be used in attacks, being able to block or detect these attacks is an important aspect of your corporate security posture.
Firefox Browser Attacks	This is a precanned attack, containing a list of web browser attacks targeting Mozilla Firefox software. Attacks may exploit flaws found in Firefox's browser engine (Gecko), JavaScript engine (SpiderMonkey) and other browser features (i.e. XSS filter) to perform actions on behalf of an attacker. The strikes found in this precanned attack are known to be used in attacks, being able to block or detect these attacks is an important aspect of your corporate security posture.
Generic Attacks Batch1	This is a precanned attack, containing a list of a wide range of attacks with different exploit capabilities. These attacks may exploit flaws ranging from memory corruption and information leaking to database security.
Generic Attacks Batch2	This is a precanned attack, containing a list of a wide range of attacks with different exploit capabilities. These attacks may exploit flaws ranging from memory corruption and information leaking to database security.
Generic Attacks Batch3	This is a precanned attack, containing a list of a wide range of attacks with different exploit capabilities. These attacks may exploit flaws ranging from memory corruption and information leaking to database security.
Generic Malware	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network.
Insecure Deserialization Attacks	Deserialization is the process of taking data structured for a format and rebuilding it into an object. The features of the native deserialization mechanism can be repurposed for malicious effect when operating on untrusted data. Attacks against deserializers have been found to allow denial-of-service, access control, and remote code execution attacks. This precanned attack contains a collection of Insecure Deserialization attacks. It will run through each of the strikes one-by-one in order to test how well your implemented security controls protect your assets against these attacks. If these strikes are not blocked, they could compromise your application and/or put your customers and data at risk.

<b>Name</b>	<b>Description</b>
LFI Attacks	This is a precanned attack containing a list of Local File Inclusion attacks. These attacks occur when web applications use the path to a file as input. In this manner, an attacker can trick the application into including local files and revealing its content. A successful attack can lead to information disclosure and/or remote code execution. Being able to block or detect these attacks is an important aspect of your corporate security posture.
Microsoft Browser Attacks	This is a precanned attack, containing a list of web browser attacks targeting Microsoft Edge and Internet Explorer. Attacks may exploit flaws found in the browser engine (Blink), the JavaScript engine (ChakraCore and V8) and other browser features (i.e. XSS filter) to perform actions on behalf of an attacker. The strikes found in this precanned attack are known to be used in attacks, being able to block or detect these attacks is an important aspect of your corporate security posture.
Misc Browser Attacks	This is a precanned attack containing a list of web attacks targeting various technologies used in browser software, such as Flash Player or Java applets. The strikes found in this precanned attack are known to be used in attacks, being able to block or detect these attacks is an important aspect of your corporate security posture.
Monthly Malware April 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware April 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware April 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.

<b>Name</b>	<b>Description</b>
Monthly Malware April 2024	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware August 2020	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware August 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware August 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware August 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.

<b>Name</b>	<b>Description</b>
Monthly Malware December 2020	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware December 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware December 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware December 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware February 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.

<b>Name</b>	<b>Description</b>
Monthly Malware February 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware February 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware February 2024	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware January 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware January 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.

<b>Name</b>	<b>Description</b>
Monthly Malware January 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware January 2024	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware July 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware July 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware July 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.

<b>Name</b>	<b>Description</b>
Monthly Malware June 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware June 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware June 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware March 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware March 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.

<b>Name</b>	<b>Description</b>
Monthly Malware March 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware March 2024	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware May 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware May 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware May 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.

<b>Name</b>	<b>Description</b>
Monthly Malware May 2024	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware November 2020	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware November 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware November 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware November 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.

<b>Name</b>	<b>Description</b>
Monthly Malware October 2020	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware October 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware October 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware October 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware September 2020	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.

<b>Name</b>	<b>Description</b>
Monthly Malware September 2021	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware September 2022	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
Monthly Malware September 2023	A malware campaign is a chain-of-events that starts with an external attacker gaining access to your network and ends with the attacker achieving an objective (usually resulting in significant financial or reputational damage to the business). Each stage successfully completed by the attacker gets them one step closer to their ultimate objective - so the sooner the attack chain is disrupted the better. This precanned attack contains different stages from different malware campaigns. Detection is an important aspect, and correlation of events may be the most important way to determine if an Advanced Persistent Threat (APT) is within your network. This precanned attack contains malware strikes often encountered in this month.
OS Command Injection Attacks	OS Command Injection attacks send operating system commands to be executed by the web application. The effects of a successful attack can include compromising web application integrity and arbitrary execution of commands in the context of the running application. This precanned attack contains a collection of known OS Command Injection attacks. It will run through each of the strikes one-by-one in order to test how well your implemented security controls protect your assets against these attacks. If these strikes are not blocked, they could compromise your web application and/or put your customers and data at risk.
RFI Attacks	This is a precanned attack containing a list of Remote File Inclusion attacks. These attacks occur when web applications dynamically include scripts or files. In this manner, an attacker can trick the application into executing the malicious code. A successful attack can lead to information disclosure and/or remote code execution. Being able to block or detect these attacks is an important aspect of your corporate security posture.

Name	Description
SQL Injection Attacks	SQL Injection (SQLi) is a type of computer security vulnerability commonly found in web applications that enables attackers to inject code targeting the backend database. These scripts will typically be used to dump the database contents, attempt to execute shell commands, or modify the database contents. This precanned attack contains a collection of known SQL Injection (SQLi) vulnerabilities. It will run through each of the strikes one-by-one in order to test how well your implemented security controls protect your assets against these attacks. If these strikes are not blocked, they could compromise your web application and/or put your customers and data at risk.
SQLi Vector Attack Blind	Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response. These attacks take advantage of unsanitized data to subvert the query executed on the database by inserting SQL statement into HTTP request. This precanned attack contains a collection of SQL Injection payloads coming from multiple public sources and private resources.
SQLi Vector Attack Detect	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. This precanned attack contains a collection of SQL Injection payloads coming from multiple public sources and private resources.
SQLi Vector Attack Exploit	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. This precanned attack contains a collection of SQL Injection payloads coming from multiple public sources and private resources.
Script Injection Attacks	Script Injection attacks send script code to be executed by the web application. The effects of a successful attack can include compromising web application integrity and arbitrary execution of commands in the context of the running application. This precanned attack contains a collection of known Script Injection attacks. It will run through each of the strikes one-by-one in order to test how well your implemented security controls protect your assets against these attacks. If these strikes are not blocked, they could compromise your web application and/or put your customers and data at risk.
Social Network Attack on Chrome browser	This attack simulates a Chrome browser vulnerability in the context of a social network web application with Google Chrome browser connecting to an Apache web server.
Social Network Attack on Firefox browser	This attack simulates a Firefox browser vulnerability in the context of a social network web application with Mozilla Firefox browser connecting to an IIS web server.
Social Network Attack on Internet Explorer browser	This attack simulates an Internet Explorer browser vulnerability in the context of a social network web application with Internet Explorer browser connecting to a Nginx web server.
Social Network Attack on Microsoft Edge browser	This attack simulates a Microsoft Edge browser vulnerability in the context of a social network web application with Microsoft Edge browser connecting to an Apache web server.

<b>Name</b>	<b>Description</b>
Strike Adobe Acrobat JBIG2 Stream Indexing Overflow (SMTP Quoted Printable)	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)	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)	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)	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)	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)	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)	This strike exploits a denial of service condition in Apple's Mac OS X when opening a malformed PICT file.
Strike Easy FTP Server v1.7.0.11 LIST Command Remote Buffer Overflow	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	This strike exploits a buffer overflow in the Easy FTP server's processing of the MKD command.
Strike Flip4Mac Memory Corruption (SMTP)	This strike exploits a memory corruption flaw in Telestream Flip4Mac when handling WMF files.
Strike GDIPlus JPEG Processing Buffer Overrun - SMTP Message	This strike exploits a vulnerability in the processing of JPEG images in multiple Microsoft products based on the GDIPlus image library. This strike simulates attaching a JPEG to an SMTP message.
Strike Golden FTP PASS Buffer Overflow	This strike exploits a stack overflow in Golden FTP in the parsing of the PASS command.
Strike Internet Explorer EMF File Rendering Denial of Service (SMTP)	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)	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.

<b>Name</b>	<b>Description</b>
Strike Mac OS X DMG UFS ffs_mountfs() Integer Overflow (SMTP)	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)	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 ColorMatchToTargetW (SMTP Quoted Printable)	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 Microsoft Excel BIFF Record Parsing Vulnerability (SMTP Base64)	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)	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)	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)	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing an embedded object.
Strike Microsoft Excel NULL Pointer DoS (A) (SMTP)	This strike exploits a denial of service flaw in Microsoft Excel using a corrupted XLS document.
Strike Microsoft Excel NULL Pointer DoS (B) (SMTP)	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)	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing an embedded object with an invalid subtype record.
Strike Microsoft Excel Obj Record Invalid Subtype Vulnerability (SMTP Quoted Printable)	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)	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)	This strike exploits a vulnerability in Microsoft Excel when evaluating a REPT() formula with a long number_times parameter.

<b>Name</b>	<b>Description</b>
Strike Microsoft Office Memory Corruption (PowerPoint) (SMTP Base64)	This strike exploits a memory corruption vulnerability in the Microsoft Office XP PowerPoint component.
Strike Microsoft Office Memory Corruption (PowerPoint) (SMTP Quoted Printable)	This strike exploits a memory corruption vulnerability in the Microsoft Office XP PowerPoint component.
Strike Microsoft Office Smart Tag WordCount Memory Corruption (SMTP Base64)	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)	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 Text Converter Integer Underflow Code Execution (SMTP Direct Quoted Printable)	This strike exploits an integer underflow code execution vulnerability in Microsoft Office's text convertor.
Strike Microsoft PowerPoint Master Style Integer Overflow (SMTP Base64)	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)	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)	This strike exploits a heap memory corruption vulnerability in Microsoft Office's PowerPoint.
Strike Microsoft PowerPoint TextHeaderAtom Freed Memory Heap Corruption (SMTP Quoted Printable)	This strike exploits a heap memory corruption vulnerability in Microsoft Office's PowerPoint.
Strike Microsoft PowerPoint Viewer 2003 MSODRAWING Property Heap Overflow (SMTP Base64)	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)	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 Picture Array Index (SMTP Base64)	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)	This strike exploits an out-of-bounds array index vulnerability in Microsoft PowerPoint Viewer 2003 when reading malformed PowerPoint files.

<b>Name</b>	<b>Description</b>
Strike Microsoft Windows Color Management Module ICC Profile Buffer Overflow (SMTP)	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 Polyline (SMTP Quoted Printable)	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)	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)	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)	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.
Strike Microsoft Word 2000 Malformed Function Code Execution (SMTP)	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)	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)	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)	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)	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)	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)	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) (SMTP Quoted Printable)	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\dpPENDGROUP' directives.

<b>Name</b>	<b>Description</b>
Strike Microsoft Word RTF Object Parsing Vulnerability (dpolycount) (SMTP Quoted Printable)	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) (SMTP Quoted Printable)	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)	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)	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)	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)	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 RUDY POST Attack	Simulates an HTTP RUDY DDoS attack.
Strike Squid Reverse Proxy Host Header Buffer Overflow Attack	
Strike VLC Ogg Vorbis Comment Header Format String (SMTP)	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)	This strike exploits a denial of service condition in Microsoft Windows explorer.exe when right-clicking on a malformed AVI file.

<b>Name</b>	<b>Description</b>
Strike Windows GDI Malformed Image Denial of Service (SMTP)	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)	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)	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)	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 Wu-FTPd File Globbing Heap Corruption	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 libpng png_handle_sBIT() Local Overflow (SMTP)	This strike exploits a vulnerability in the processing of PNG images by libpng. This strike simulates sending a PNG via SMTP.
Top Google Chrome browser attacks	Simulates most important attacks on Google Chrome browser.
Top Internet Explorer browser attacks	Simulates most important attacks on Internet Explorer browser.
Top Microsoft Edge browser attacks	Simulates most important attacks on Microsoft Edge browser.
Top Mozilla Firefox browser attacks	Simulates most important attacks on Mozilla Firefox browser.
Top RCE attacks	Simulates most important webshell attacks.
Top Safari browser attacks	Simulates most important attacks on Safari browser.
Top browser attacks	Simulates most important attacks on browsers.
Top webshell attacks	Simulates most important webshell attacks.
URL Filtering Malware	Precanned attack which can be used in order to test the URL filtering capabilities of different devices. Makes use of common malware URLs.
URL Filtering Malware and Phishing	Precanned attack which can be used in order to test the URL filtering capabilities of different devices. Makes use of common malware and phishing URLs.
URL Filtering Phishing	Precanned attack which can be used in order to test the URL filtering capabilities of different devices. Makes use of common phishing URLs.

<b>Name</b>	<b>Description</b>
Video Platform Exploit Attack with JSP file upload on Apache server	This attack simulates an exploit sent through a JSP file uploaded on an Apache server in the context of a video platform web application with Microsoft Edge browser connecting to an Apache web server.
Video Platform Exploit Attack with JSP file upload on Nginx server	This attack simulates an exploit sent through a JSP file uploaded on a Nginx server in the context of a video platform web application with Internet Explorer browser connecting to a Nginx web server.
Video Platform Exploit Attack with PHP file upload on Apache server	This attack simulates an exploit sent through a PHP file uploaded on an Apache server in the context of a video platform web application with Google Chrome browser connecting to an Apache web server.
Video Platform Exploit Attack with PHP file upload on IIS server	This attack simulates an exploit sent through a PHP file uploaded on an IIS server in the context of a video platform web application with Mozilla Firefox browser connecting to an IIS web server.
Web Server Attacks	This validation precanned attack contains attacks targeting web server applications, sourced from both public and private sources. The result of successful exploitation depends on the vulnerability being target, payload used by exploit and configuration of the targeted system, but range from information disclosure to full-system compromise.
XSS Attacks	This precanned attack contains a collection of known Cross-Site Scripting (XSS) vulnerabilities. Cross-Site Scripting is a type of computer security vulnerability found in websites that enables attackers to inject script code into web pages viewed by other users. This style of attack usually impacts data integrity, user privacy, and user security, however server integrity is typically unaffected. When the injected scripts are viewed and executed by other users, they can steal credentials, sensitive data, or modify values or settings on the target website. This precanned attack will run each of the strikes one-by-one in order to test how well your implemented security controls protects your assets against these attacks. If these strikes are not blocked, they could compromise your web application and/or put your customers and data at risk.
XSS Vector Attack Reflected Fuzzers	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 Cross-Site Scripting payloads coming from multiple public sources and private resources. This attack includes only payloads listed in XSS Cheat Sheets.
XSS Vector Attack Reflected Grouped	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 Cross-Site Scripting payloads sourced from <a href="https://gist.github.com/kurobeats/9a613c9ab68914312cbb415134795b45">https://gist.github.com/kurobeats/9a613c9ab68914312cbb415134795b45</a>

<b>Name</b>	<b>Description</b>
XSS Vector Attack Reflected HTML5	<p>This attack contains a collection of Cross-Site Scripting 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. This style of attack usually impacts data integrity, user privacy, and user security, however server integrity is typically unaffected. If these audits are not blocked, they could compromise your web application and/or put your customers and data at risk. This attack includes only HTML5 payloads using various exploitation techniques. This attack will run each payload sequentially, attempting to deliver a malicious attack.</p>
XSS Vector Attack Reflected Rsnake	<p>This attack contains a collection of known Cross-Site Scripting 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. This style of attack usually impacts data integrity, user privacy, and user security, however server integrity is typically unaffected. If these attacks are not blocked, they could compromise a web application and/or put customers and data at risk. This attack includes only payloads issued by famous hacker RSnake using various exploitation techniques.</p>
XSS Vector Attack Reflected Sample	<p>This attack contains a collection of known Cross-Site Scripting 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. This style of attack usually impacts data integrity, user privacy, and user security, however server integrity is typically unaffected. If these attacks are not blocked, they could compromise a web application and/or put customers and data at risk. This is a lightweight attack, as it includes only a few XSS exploit samples.</p>
eShop Attack on Chrome browser	<p>This attack simulates a Chrome browser vulnerability in the context of an online shop web application with the Google Chrome browser connecting to an Apache web server.</p>
eShop Attack on Firefox browser	<p>This attack simulates a Firefox browser vulnerability in the context of an online shop web application with the Mozilla Firefox browser connecting to an IIS web server.</p>

Name	Description
eShop Attack on Internet Explorer browser	This attack simulates an Internet Explorer browser vulnerability in the context of an online shop web application with the Internet Explorer browser connecting to a Nginx web server.
eShop Attack on Microsoft Edge browser	This attack simulates a Microsoft Edge browser vulnerability in the context of an online shop web application with the Microsoft Edge browser connecting to an Apache web server.

## All Exploits (2764)

Name	References	Description
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 Linksys PlayerPT ActiveX control base64 string Buffer Overflow	CWE: 119 CVE: 2012-0284 BID: 54588	This strike identifies a buffer overflow vulnerability in Linksys' ActiveX control, PlayerPT. Improper validation occurs when handling the base64string parameter, and an overly large user supplied value will overflow the 0x2E buffer that is allocated on the stack for the parameter.
Strike CuteFlow pre-authenticated Admin Account Creation		This strike exploits the webbased open source document circulation and workflow system CuteFlow. Without Authentication, a user can create an admin account directly from a remote system.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Dell Webcam Software ActiveX Control Buffer Overflow		This strike exploits a vulnerability within Dell's SX2210 Webcam Monitor Software. When handling the properties BackImage, ScriptName, ModelName, and SRC, a buffer can be exploited and overrun by supplying a value larger than 260 bytes.
Strike Novell Remote Manager Host Header Denial of Service		This strike identifies a vulnerability in Novell's Remote Manager. If a HTTP request is sent to the LOGIN SERVER URI, with a HOST header of exactly 64 bytes, the code will overwrite 1 byte of the stack cookie which leads to a denial of service.
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 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 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 customDictionaryOpen Memory Corruption (HTTP)	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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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
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 ActivePerl perlIS.dll Filename Overflow Variant 2	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 '.plx'.
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

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 Flash Player newfunction Invalid Pointer Code Execution (HTTP)	CVE: 2010-1297 BID: 40586	This strike exploits a flaw in Adobe's Flash Player that can result in the execution of arbitrary code.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 AJ Dating view_profile.php user_id Parameter SQL Injection	CVE: 2007-1297 BID: 22808	This strike exploits a SQL injection flaw in the AJ Dating 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 Aladdin ChooseFilePath ActiveX Method Buffer Overflow	BID: 56297	This strike identifies a vulnerability in Aladdin Knowledge System's ActiveX component. If an overly large string is supplied to the ChooseFilePath method a buffer is overflowed which can result in remote code execution.
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.

Name	References	Description
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.
Strike Aloaha PDF Crypter ActiveX Control File Overwrite		This strike exploits a vulnerability in Aloaha Pdf Crypter's ActiveX control EbCrypt.eb_c_PRNGenerator.1. When calling the SaveToFile method the argument passed is not properly validated, and allows for any file on the remote machine to be overwritten.
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 Amadey Bot July 2022 Campaign - Additional Malware Download		This strike simulates the 'Amadey Bot July 2022 Campaign - Additional Malware Download' traffic that occurs once the Amadey malware has been executed. This strike sends 3 HTTP GET requests to the attacker to download additional malware to the victim's machine. The first GET request downloads the xyz named binary that serves as a downloader and only retrieves the next binary named bin. The second GET request downloads the bin binary from the same location. This binary will make requests to download both the Redline Stealer malware as well as another version of Amadey Bot padded with Null bytes. The third and final GET request downloads the Redline stealer malware.
Strike Amlibweb Library Management System Request Buffer Overflow	BID: 42293	This strike exploits a stack buffer overflow vulnerability in Amlib's NetOpacs. If a large value is passed to the app parameter registers can be overwritten allowing for the execution of directed code.
Strike Android AndroidKungFu Malware Command and Control		This strike simulates command and control communication for the AndroidKungFu malware (also known as ANDROIDOS_LENA.B, Android.Gonfu.C, DroidKrungFu.E). The infected device sends a GET request to a Command and Control server, which responds with various commands. The infected device then does other actions based on the command.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Cookie Buffer Overflow		This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the Cookie function.
Strike AOL 9.5 ActiveX CropDimensions Buffer Overflow		This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the CropDimensions 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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 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 ap_escape_html Memory Allocation Denial Of Service	CVE: 2004-0493 BID: 10619	This strike exploits a denial of service bug in the processing of long headers starting with tab or space in the Apache Web Server.
Strike Apache Tomcat mod_jk Arbitrary Code Execution	CVE: 2007-0774 BID: 22791	This strike exploits a stack overflow in Apache Tomcat's mod_jk.so via an overly long URL request.
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 strust2. The attacker can excute command by sending crafted HTTP request.

Name	References	Description
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.
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 iOS 5-5.1 URL bar spoofing	CWE: 20 CVE: 2012-0674	This strike sends a webpage with a click button that will appear open a valid URL, however the content is still being controlled by a malicious server.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 Mutilbyte 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 if 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 Beta feed --URL DoS Variant 10	BID: 24460	This strike exploits a denial if 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 Beta feed --URL DoS Variant 2	BID: 24460	This strike exploits a denial if 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 Beta feed --URL DoS Variant 3	BID: 24460	This strike exploits a denial if 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 Beta feed --URL DoS Variant 4	BID: 24460	This strike exploits a denial if service flaw in Apple Safari for Windows Beta. This flaw is triggered when the browser attempts to open feed:// urls with special characters.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apple Safari for Windows Beta feed --URL DoS Variant 5	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 Beta feed --URL DoS Variant 6	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 Beta feed --URL DoS Variant 7	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 Beta feed --URL DoS Variant 8	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 Beta feed --URL DoS Variant 9	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.
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.

Name	References	Description
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 Ask.com Browser Toolbar ActiveX Exploit		This strike exploits a flaw in the Ask Jeeves browser toolbar for Internet Explorer.
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 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 ATI Data Exfiltration Mar 2021 Campaign - Trojan Command and Control		This strike simulates the 'ATI Data Exfiltration Mar 2021 Campaign - Trojan Command and Control' traffic that occurs after executing the Trojan malware.
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 AVS Media Player 4.2.2.104 EIP Control		This strike identifies a vulnerability in AVS Media Player. This attack is against version 4.2.2.104 of the software, and when the proof of concept is executed a denial of service is observed. The vulnerable method setsource does not properly validate its arguments and we are able to point EIP to the address filled with our Shellcode.
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 Bad Blue Web Server Directory Traversal Variant 1	CVE: 2002-0325 BID: 4179	This strike exploits a directory traversal flaw in the Bad Blue web server.
Strike Bad Blue Web Server Directory Traversal Variant 2	CVE: 2002-0325 BID: 4179	This strike exploits a directory traversal flaw in the Bad Blue web server.
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 Bulldog Web Service HTTP Request Buffer Overflow	BID: 34033	This strike exploits a buffer overflow vulnerability in Belkin Bulldog Web Service. If an HTTP request with an overly long URI string is received, a stack buffer will overflow causing the service to crash.
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 Benders Calendar index.php this_day Parameter SQL Injection	CVE: 2006-0252 BID: 16242	This strike exploits a SQL injection flaw in the Benders Calendar web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 TimesTen HTTP Request Denial of Service	BID: 38019	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 IBM Lotus Web Access ActiveX Control URL BO	CWE: 119  CVE: 2010-0919  BID: 38457	This strike exploits buffer overflow vulnerability within the IBM Lotus Web Access ActiveX Control. This vulnerability is due to lack of boundary checking in the IBM Lotus Web Access ActiveX Control. Remote unauthenticated attackers could exploit this vulnerability to execute arbitrary code on the target system.
Strike Oracle AutoVue SaveViewStateToFile ActiveX Control Arbitrary File Creation	BID: 50321	This strike exploits a vulnerable ActiveX control in Oracle AutoVue. The SaveViewStateToFile can be used to create arbitrary files in arbitrary locations. Successful exploitation can result in the creation of arbitrary files or the overwriting of existing files, including system files.
Strike Oracle AutoVue AutoVueX ActiveX Control Export3DBom Remote File	BID: 50333	This strike exploits the an Activex control flaw associated with Oracle Autovue software. The Export3DBom function does not perform proper input validation and permits the creation of a file anywhere on the system. By manipulating a user to access a specially crafted web page arbitrary file creation may take place which could lead to code execution whith local priviledges. All systems runing versions of Oracle AutoVue prior to 20.0.1 are vulnerable.
Strike McAfee Virtual Technician ActiveX Control Code Execution	BID: 53304	This strike exploits a code execution vulnerability within McAfee Virtual Technician ActiveX Control. This vulnerability is due to lack of confirmation of object type. 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 Oracle Business Transaction Management Server writeToFile handle Directory Traversal	BID: 54839	This strike exploits a directory traversal vulnerability in Oracle Business Transaction Management Server. The writeToFile handle in SOAP requests is not validated for directory traversal characters. Exploitation allows for writing or overwriting of arbitrary files.
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 Siemens Solid Edge SEListCtrlX ActiveX Memory Corruption Vulnerability	BID: 60161	This strike exploits a remote code-execution vulnerability in SIEMENS Solid Edge. The vulnerability is due to the lack of validation on user input to the NumChildren and DeleteItem methods in the SEListCtrlX 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 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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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
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

<b>Name</b>	<b>References</b>	<b>Description</b>
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
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 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 7 HTML Dynamic Page Reloading Memory Corruption	CVE: 2007-0946  BID: 23770	This strike exploits a vulnerability within Microsoft Internet Explorer 7 when dealing with dynamic HTML pages. Application level events are not properly reloaded during a page reload which results in memory corruption.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike IncrediMail ActiveX control Memory Corruption	BID: 23674  CVE: 2007-1683	This strike exploits a vulnerability within IncrediMail's ActiveX control ImShExtU.dll. Memory Corruption occurs when the DoWebMenuAction method is passed an overly long string as an argument.
Strike Microsoft Whale Intelligent Gateway Buffer Overflow	CWE: 119  CVE: 2007-2238  BID: 34532	This strike exploits a vulnerability within Microsoft Whale's Intelligent Application Gateway client. If an overly long string is passed to the CheckForUpdates method a buffer overflows, which can allow for remote code execution.
Strike Microsoft Internet Explorer Expression Objects Memory Corruption	CWE: 189  CVE: 2007-3902  BID: 26506	This strike exploits a vulnerability in Microsoft Internet Explorer. If an object used for expressions is given a value or assignment to a property multiple times and then later freed only one of the references is removed. This use after free condition can cause memory corruption when trying to call the property later because of the invalid pointer dereferencing.
Strike SAP GUI EAI WebViewer3D ActiveX Control Buffer Overflow	BID: 34310  CWE: 119  CVE: 2007-4475	This strike exploits a vulnerability in the SAP GUI's ActiveX control EAI WebViewer3D. The vulnerable parameter is the filePath string. Because it is not properly validated, an overly long value supplied for the filePath string, will overflow a stack buffer of 0x108, overwriting critical memory.
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 Symantec Backup Exec ActiveX control BUffer Overflow	CWE: 119  CVE: 2007-6016  BID: 26904	This strike exploits a vulnerability in Symantec's Backup Exec ActiveX control PVATLCalendar.PVCalendar. If a large string is passed to the _DOWText0 or _MonthText0 methods and then saved with the Save method a stack buffer is overrun.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Opera Browser URI String Buffer Overflow	CWE: 119 CVE: 2008-5178 BID: 32323	This strike exploits a vulnerability within the Opera Browser. The browser does not properly validate the file scheme URI string parameter. If the string is greater than 8192 bytes the data will overwrite memory on buffer.
Strike EasyMail Quicksoft 6.0.2 ActiveX Control Buffer Overflow	CWE: 119 CVE: 2008-6447 BID: 32722	This strike exploits a vulnerability in an EasyMail Quicksoft ActiveX control. Because it is not properly validated, a large amount of data is passed to the CreateStore method causes a buffer to overflow.
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.
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 IBM Access Support ActiveX GetXMLValue Method Buffer Overflow	CWE: 119 CVE: 2009-0215 BID: 34228	This strike exploits a vulnerability in IBM Access Support's IbmEgath.dll control. When handling the element_list parameter inside the GetXMLValue method. If the value inside this parameter is not valid, the message gets printed into the allocated buffer.
Strike MW6 Technologies Barcode ActiveX Control Memory Corruption	BID: 33451 CWE: 119 CVE: 2009-0298	This strike exploits a vulnerability in MW6 Technologies ActiveX Control barcode.dll. Specifically the vuln is due to the way in which the Supplement property of this control is handled. If this property is assigned a value of greater than 0x90 and less than 0xCF8, the code will overwrite a pointer resulting in memory corruption.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Blackberry Web Loader ActiveX Control Buffer Overflow	CWE: 119 CVE: 2009-0305 BID: 33663	This strike exploits a vulnerability in BlackBerry Application Web Loader. Specifically the vulnerability resides in the activeX control RIM.AxLoader. The vulnerable methods load and loadJad do not properly validate their one argument, the URL, and if the input provided is too large, an error message along with the data provided is copied to a fixed heap buffer. If the combination of both is greater than the size of the buffer it will overflow overwriting critical memory, and potentially allowing for 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 XUL _moveToEdgeShift() Memory Corruption Vulnerability	CWE: 399 CVE: 2009-1044 BID: 34181	This strike exploits a memory corruption vulnerability in Mozilla Firefox. The vulnerability is due to a dangling pointer that remains after improper garbage collection in the _moveToEdgeShift() XUL tree method. An attacker could exploit this vulnerability by enticing a user to open a specially crafted web page.
Strike Dawningsoft PowerCHM URL Buffer Overflow	CWE: 119 CVE: 2009-1352 BID: 34517	This strike exploits a vulnerability inside Dawningsoft's PowerCHM. If an overly long string is passed as part of the URL, a buffer will overflow causing a denial of service condition to occur.
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 target-frame Parameter Buffer Overflow	BID: 37242 CWE: 119 CVE: 2009-1568	This strike exploits a vulnerability that exists in Novell's iPrint Client Browser Plugin. The code does not properly validate the input for the target-frame parameter. Any value greater than 128 will overwrite stack data.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Internet Explorer Memory Corruption Upon HTML Object Deletion	BID: 35831 CWE: 399 CVE: 2009-1917	This strike identifies a vulnerability in Microsoft Internet Explorer. The CollectGarbage method is used to release all memory from the IMG object in the code below, and when that object is called later, memory corruption will occur.
Strike Internet Explorer Memory Corruption with New Row Insertion inside Nested Tables	BID: 35826 CWE: 94 CVE: 2009-1918	This strike identifies a vulnerability in Microsoft Internet Explorer. When an html table is found nested inside another table, and a row is inserted into that table, memory corruption occurs.
Strike Microsoft Internet Explorer styleSheet Memory Corruption	CWE: 94 CVE: 2009-1919	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. When the cssText property of a styleSheet is given a new value, the previous value is not disposed of, and all calls made to the object will reference it overwriting memory.
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 Microsoft Internet Explorer DIV with No Reference Script Element Denial of Service	CVE: 2009-2764 BID: 35941	This strike exploits a vulnerability in Microsoft Internet Explorer. When a DIV element is used in conjunction with a script element that does not contain a valid reference to an external script location, then a denial of service condition can occur.
Strike Microsoft Internet Explorer LI Element Denial of Service	CWE: 94 CVE: 2009-3019	This strike exploits a vulnerability in Microsoft Internet Explorer. When creating an LI element by using createElement inside javascript, and then setting the value attribute a denial of service condition can occur.
Strike Symantec Altiris Deployment Solution Arbitrary File Download and Execution	CVE: 2009-3028 BID: 36346	This strike exploits a vulnerability within Symantec's Altiris Deployment Solution, whereby the DownloadAndInstall method is not properly validated, and can be pointed to a remote executable to download and install.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Symantec Altiris Deployment Solution ActiveX control BrowseAndSaveFile Buffer Overflow	CWE: 119 CVE: 2009-3031 BID: 36698	This strike exploits a vulnerability within the ActiveX control AeXNSConsoleUtilities.dll method BrowseAndSaveFile in Symantec Altiris Deployment Solution software. When passed an overly long string to BrowseAndSaveFile it gets copied into a stack buffer without proper validation. Anything larger than 500 bytes will overflow the buffer.
Strike Symantec Altiris Deployment Solution ActiveX control AeXNSConsoleUtilities.dll Buffer Overflow	BID: 37092 CWE: 119 CVE: 2009-3033	This strike exploits a vulnerability within the ActiveX control AeXNSConsoleUtilities.dll method RunCmd in Symantec Altiris Deployment Solution software. When passed an overly long string RunCmd will copy it into a stack buffer without proper validation. Anything larger than 512 bytes will overflow the buffer.
Strike Lotus Notes RIM connector for Blackberry Desktop Manager ActiveX Denial of Service	CVE: 2009-3038	This strike exploits a vulnerability in the Lotus Notes connector(RIM) for Blackberry Desktop Manager. If the vulnerable activeX control's classid is instantiated inside an object element, a denial of service condition occurs.
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 Internet Explorer nested Element Use After Free Memory Corruption	CWE: 399 CVE: 2009-3671 BID: 37188	This strike identifies a vulnerability in Microsoft Internet Explorer. Within an HTML document that contains nested elements, a vulnerability exists when a child node is removed from its parent. The code frees the nested elements pointer, and later if the pointer is accessed, memory corruption occurs.
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 Novell Groupwise Client 7.0.3 ActiveX Control Denial of Service	CWE: 119 CVE: 2009-3863	This strike exploits a vulnerability in a Groupwise 7.0.3 activeX control. If the SetFontFace method is called with an argument that has a large value, a denial of service condition can occur.
Strike Google Chrome SVG Security Bypass	CWE: 20 CVE: 2009-3931 BID: 36947	This strike exploits a security bypass vulnerability in Google Chrome. This vulnerability is due to google chrome will not check the content of SVG document. An attacker can craft malicious SVG file, which may lead to arbitrary code execution.
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 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.

Name	References	Description
Strike Ca eTrust PestPatrol Antispyware ActiveX Buffer Overflow	CWE: 119 CVE: 2009-4225 BID: 37133	This strike exploits a buffer overflow vulnerability inside Ca eTrust PesPatrol Antispyware's ActiveX control. When passing an large value to the intialize method a buffer is overrun allowing for the possibility of remote code execution.
Strike AwingSoft Web3D Player ActiveX Control Buffer Overflow	CWE: 119 CVE: 2009-4588	This strike identifies a buffer overflow vulnerability in Winds3D Viewer. An activeX control does not properly validate the value passed to the SceneURL parameter. An overly long value passed to SceneURL will overflow the buffer.
Strike Safari v4.0.5 Webkit Memory Exhaustion Denial of Service	CWE: 399 CVE: 2010-0050 BID: 38671	This strike exploits a vulnerability within Safari Webkit v4.0.5 of Safari. A blink tag written to the document in a repetitive loop will immediately consume resources resulting in memory exhaustion when the proof of concept is executed.
Strike Symantec Products cliproxy ActiveX Control Buffer Overflow	CWE: 119 CVE: 2010-0108 BID: 38222	This strike exploits a vulnerability in Symatec's cliproxy ActiveX control. If the SetRemoteComputerName method is passed an overly long value a heap buffer of 0x34 bytes is overwritten.
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 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 Hyleos ChemView ActiveX Control Buffer Overflow	CWE: 119 CVE: 2010-0679 BID: 38225	This strike exploits a stack buffer overflow vulnerability in Hyleos ChemView. The ActiveX control methods SaveAsMolFile and ReadMolFile are not properly validated, and if an overly long first argument is passed to them, a buffer will be overrun.
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 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 Safari webkit memory corruption	CWE: 399 CVE: 2010-1119 BID: 40642	This strike exploits a remote code execution vulnerability in Apple Safari. The flaw occurs when handling reference to objects in DOM.
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 toStaticHTML Information Disclosure	CWE: 79 CVE: 2010-1257 BID: 40409	This strike exploits a cross-site scripting vulnerability in Internet Explorer. The vulnerability is due to a lack of input validation of html code. Remote attackers can exploit this vulnerability by enticing a user to open a malicious web page using the toStaticHTML method, leading to information disclosure and execution of arbitrary browser script code.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Tembria Server Monitor Denial of Service	CWE: 119 CVE: 2010-1316	This strike identifies a vulnerability that exists in Tembria Server Monitor. If an overly large URI request is received a denial of service condition occurs.
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.
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 Apple Safari WebKit Option Element Code Execution	CWE: 399 CVE: 2010-1396 BID: 40647 BID: 40620	This strike identifies a vulnerability in Apple Safari Webkit. Specifically, memory corruption occurs when a DOM object that has been freed is referenced improperly. If this object is a container element with the contentediable attribute, or if this container element utilizes this attribute inherently, and it contains an option element, when the parent container is then deleted any reference to the freed element will cause invalid memory to be accessed.
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 Brower 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 MaxAge Parameter Buffer Overflow	CWE: 119 CVE: 2010-1553 BID: 40070	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.
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.

Name	References	Description
Strike Safari webkit CSS memory corruption	CWE: 94 CVE: 2010-1770 BID: 40620	This strike exploits a remote code execution vulnerability in Apple Safari. The flaw occurs when handling CSS text object.
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 Apple Safari WebKit CSS Styling Property Memory Corruption	CWE: 399 CVE: 2010-1806 BID: 43049	This strike identifies a vulnerability in Apple Safari Webkit. Specifically, memory corruption can occur when rendering elements with the CSS display property set to "run-in". Upon adding a sibling block box as a child of a run-in display element, the run-in box will become the first inline box, and then it gets deleted. Invalid memory can be accessed if this element is later referenced.
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 Safari Webkit Menu Onchange Property Memory Corruption	CWE: 119 CVE: 2010-1814 BID: 43083	This strike identifies a vulnerability in Apple Safari Webkit. Specifically, if different methods are used to reference the same object, and that object has not been initialized by the function selectedIndex(), the vulnerable function didSetselectedIndex() does not recognize the object has not been initialized, and an uninitialized function pointer is accessed. This access of an invalid memory location can lead to memory corruption.
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 Novell iManager login Tree Name Denial of Service	CWE: 189 CVE: 2010-1930 BID: 40485	This strike exploits a vulnerability in Novell's iManager. During the login process, the Tree Name parameter is not properly validated, and if a period character does not exist before and after the string it is added upon conversion to a wide character string. This code plus a Null Terminator is copied to a 516 byte stack buffer. So if a string of 256 bytes is supplied, 259 chars will be copied overflowing the buffer.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 HP OpenView Arg Parameter Buffer Overflow	BID: 40873 CVE: 2010-1964	This strike exploits a stack buffer overflow in HP OpenView's Network Node Manager application ovwebsnmpsrv.exe. If a value of more than 1024 bytes is supplied for the arg parameter, a stack buffer is overrun.
Strike EvoLogical EvoCam webserver GET Request Buffer Overflow	CWE: 119 CVE: 2010-2309 BID: 40489	This strike exploits a stack buffer overflow vulnerability in the EvoLogical EvoCam software when handling an overly long GET request.
Strike Weborf HTTP Server Denial of Service	BID: 41064 CWE: 20 CVE: 2010-2435	This strike identifies a vulnerability that exists in Weborf HTTP Server. If unicode characters are supplied in the Connection header, a denial of service condition will occur on the server.
Strike Microsoft Internet Explorer DOM Objet 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SAP Crystal Reports PrintControl Buffer Overflow	CWE: 119 CVE: 2010-2590 BID: 45387	This strike exploits a vulnerability in the SAP Crystal Reports ActiveX control printcontrol.dll. The ServerResourceVersion property is not properly validated, and if it exceeds a size 0x40C the string overflows a heap buffer.
Strike HP OpenView Network Node Manager ov.dll execvp_nc() Function Overflow	BID: 41829 CWE: 119 CVE: 2010-2703	This strike exploits a stack buffer overflow vulnerability in HP OpenView Network Node Manager (NNM). The vulnerability is caused by lack of input validation by webappmon.exe when handling HTTP requests. This vulnerability can be exploited by an unauthenticated attacker to inject and execute arbitrary code on target system.
Strike HP OpenView NNM OvJavaLocale Buffer Overflow	CWE: 119 CVE: 2010-2709 BID: 42154	This strike identifies a vulnerability in the webappmon.exe service of HP OpenView's Network Node Manager. A buffer overflow exists when parsing the OvJavaLocale parameter in the HTTP Cookie header. When passed a string greater than 5107 characters the buffer is overflowed.
Strike Microsoft IIS HTTP Request Header Buffer Overflow	CWE: 119 CVE: 2010-2730 BID: 43138	This strike identifies a vulnerability in Microsoft Internet Information Services. If FastCGI is enabled then a buffer of 944 bytes is allocated to store the pointer and size values of HTTP header fields. This code calculates enough space for 59 headers and re-sizes the buffer accordingly. The code does not properly take into consideration pre-defined headers, so those parameters are added to the same buffer. Therefore supplying more than 16 HTTP headers can overflow the heap buffer.
Strike Mozilla Firefox plugin Array Pointer Heap Corruption	CWE: 399 CVE: 2010-2755 BID: 41933	This strike exploits a vulnerability that exists in Mozilla Firefox. This happens when handling an object tag with the data parameter not set. Two arrays are allocated, and the data parameter is assigned a name value pair. A dangling pointer is then assigned to the array's associated element. When the plugin is unloaded each element in the array is freed causing random heap pointers to free when freeing the data attribute, thereby corrupting memory.
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 Barcodewiz v3.29 Barcode ActiveX Control Buffer Overflow	CWE: 119 CVE: 2010-2932 BID: 42097	This strike exploits a buffer overflow vulnerability in Barcodewiz v3.29 when calling the LoadProperties function. The argument passed is not properly validated, and an overly large value can overflow the buffer causing a denial of service condition, as well as allowing for remote code to possibly be executed.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 Brower 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 Trend Micro extSetOwner Method Remote Code Execution	CWE: 94 CVE: 2010-3189	This strike exploits a vulnerability in Trend Micro's Internet Security Pro 2010. When calling the extSetOwner method, a user can use memory at a specific address. This value can then later be used as a function pointer to access arbitrary memory addresses or execute code.
Strike Microsoft Internet Explorer and Sharepoint Information Disclosure	CWE: 79 CVE: 2010-3243 BID: 43703	This strike exploits a vulnerability that exists in Microsoft Internet Explorer and Sharepoint. An information disclosure exists because of the lack of input validation of the toStaticHTML method when handling CSS content. A single quote allows for the parser to read beyond the CSS definition, allowing for the code to bypass the validation. In this example, 3 necessary components are needed. First a valid CSS section is defined. Second a javascript array with at least 3 elements is used, with an odd number of single quotes, and lastly another CSS section is defined.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Document Capture EasyMail ActiveX Remote Filesystem Access	CVE: 2010-3595 BID: 45849	This strike exploits a vulnerability in the Oracle Document Capture EasyMail ActiveX control. Improper validation within ImportBodyTextEx(), ImportBodyText() and ImportBodyTextAlternative() methods allows for arbitrary file system read.
Strike Oracle Document Capture WriteJPG Buffer Overflow	CVE: 2010-3599 BID: 45856	This strike exploits a vulnerability in Oracle's Document Capture where a malformed request to an ActiveX / Javascript function, WriteJPG, will clobber a stack buffer.
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Novell iPrint Client printerURI Parameter Buffer Overflow	CWE: 119 CVE: 2010-4321 BID: 44966	This strike identifies an stack buffer overflow in Novell's iPrint Client. Due to improper validation on the printerURI String parameter, a user supplied input of greater than 0x800 bytes will overflow a fixed stack buffer.
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.
Strike Moxa MediaDBPlayback ActiveX Buffer Overflow	CWE: 119 CVE: 2010-4742	This strike exploits a buffer overflow vulnerability inside MOXA_ActiveX_SDK. If a long string is passed to the PlayFileName method of MediaDBPlayback.DLL a buffer gets overwritten and remote code execution may be possible.
Strike Image Viewer CP Pro Gold ActiveX Buffer Overflow	CWE: 119 CVE: 2010-5193	This strike exploits a vulnerability inside an ActiveX control within Image Viewer. If an overly long string is passed to the TIFMergeMultiFiles method, a buffer can overflow allowing for remote code execution.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Apple Safari WebKit Range Object Code Execution	CWE: 119 CVE: 2011-0115 BID: 46746	This strike identifies a vulnerability in Apple Safari Webkit. Specifically, when a Range object is removed from the DOM using an event listener, and another Range object is used to access that same freed object, memory corruption can occur potentially allowing for remote code execution.
Strike HP OpenView CGI displayWidth Stack Overflow	CVE: 2011-0261 CVE: 2011-0262 BID: 45762	This strike identifies a vulnerability in HP Openview's Network Node Manager. Specifically the CGI graph application jovgraph.exe provides an interface to NNM by using GET requests to pass parameters. The vulnerability exists within ovutil.dll, and fails to correctly validate the displayWidth parameter passed by jovgraph.exe. A function stringToSeconds converts this displayWidth to seconds and is allocated a buffer size of 0x80. Any user supplied string beginning with a number and greater than 128 bytes will overflow this buffer.
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 HP OpenView Insight Server Backdoor Access	CVE: 2011-0276 BID: 46079	This strike demonstrates the ability to access an HP OpenView Insight Server Account through a backdoor. Default credentials can be used to gain access to admin privelages on the server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Novell GWIA Stack Overflow	CWE: 119 CVE: 2011-0334 BID: 49779	This strike identifies a vulnerability in Novell's GroupWise Internet Agent. If a GET or POST request is sent to gwia.css or gwagents.css with a size of greater than 0xEF, then the request is copied without validation into a stack 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.
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 a 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 Cisco Secure Desktop CSDWebInstaller Code Execution	CWE: 20 CVE: 2011-0926 BID: 46536	This strike exploits a vulnerability in the Cisco Secure Desktop software suite. Due to improper validation inside and ActiveX control, instantiated upon web based executable downloads arbitrary code may be executed inside user machines when redirected to malicious websites. All versions of Cisco Systems Secured Desktop below 3.5 are affected.
Strike Cisco Unified Operations Manager Common Services Framework Cross Site Scripting	CWE: 79 CVE: 2011-0962 BID: 47903	This strike exploits a cross-site scripting vulnerability in Cisco Unified Operations Manager Common Services Framework. Certain parameters passed in the URL are not sanitized properly. These values will be used later, and can be used to execute scripting code.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Windows Messenger ActiveX Control Code Execution	CWE: 119 CVE: 2011-1243 BID: 47197	This strike demonstrates the vulnerability within Windows Messenger's ActiveX control. When using VBscript and Javascript to pass a string to the LaunchIMUI control, the object that references the string is left uninitialized. A pointer inside that object is then used as a function pointer. It should be noted, that in this strike the termination of iexplore.exe,msmsgsgs.exe, and drwtsn32.exe services can be observed.
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.
Strike CA Total Defense Suite UnassignFunctional Users 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.

Name	References	Description
Strike Google Chrome Webkit Stale Pointer in Float	BID: 47965 CWE: 20 CVE: 2011-1804	This strike exploits a vulnerability that exists in Google Chrome's WebKit. The parentBlock is not verified when DHTML is used to remove a float child node from a block list. This causes the chain header to become uninitialized, and later this header is used as a pointer.
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.
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 Network Registrar Default Credentials Backdoor Access	CWE: 255 CVE: 2011-2024 BID: 48076	This strike identifies an authentication vulnerability in Cisco Network Registrar, when Logging in. Default login credentials for username and password allow for unrestricted access.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 GlassFish Server malicious username XSS	CVE: 2011-2260	This strike exploits a XSS vulnerability in the Oracle GlassFish Server. Remote attackers can exploit this vulnerability by sending crafted username in the HTTP request to the server which can lead to script code execution.
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 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.
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.

Name	References	Description
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 Simple HTTPD 1.42 Denial of Service	BID: 48980 CWE: 119 CVE: 2011-2900	This strike identifies a vulnerability in Simple Httpd as well as Mongoose Httpd. If a PUT request is sent to the target service with an overly large amount of data a buffer will overflow causing a denial of service condition to occur.
Strike Mozilla Multiple Products ThinkPadSensor Startup Insecure Library Loading	CVE: 2011-2980 BID: 49217	This strike exploits the insecure way that libraries are searched for by Mozilla Firefox and Mozilla Thunderbird that could result in the loading of a malicious file.
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 HP Data Protector dpnepolicieservice Component LogClientInstallation SQL Injection	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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP OpenView webappmon.exe Stack Buffer Overflow	CVE: 2011-3166	This strike identifies a vulnerability in the webappmon.exe service of HP OpenView's Network Node Manager. When the sel,app,act, and cache parameters are used a stack buffer of 0x400 bytes can potentially be overrun due to insufficient bounds checking. The limit is at most 5 bytes more than the buffer and is equal to each of the previously mentioned parameters added together.
Strike Novell iPrint client ActiveX control Stack Overflow	CWE: 119 CVE: 2011-3173 BID: 50367	This strike identifies a vulnerability in the Novell iPrint client library nipplib.dll. This vulnerability is due to improper handling of the printerUri string parameter. printerUri creates a string by calling wsprintfA() and its output is a stack buffer of size 0x100 (256 bytes), supplying a longer string will overwrite data on the stack.
Strike Flexera Install Shield Buffer Overflow	CWE: 119 CVE: 2011-3174	This strike exploits the heap overflow vulnerability found in the ISGrid2.dll shared library of the Flexera InstallShield software. Specifically, the exploit code targets the SGrid.Grid2 ActiveX control associated with the vulnerable software. By manipulating a user, who's host has the vulnerable version of the software, into accessing a malicious page, a heap overflow is generated and critical in-memory data structures could be corrupted. All versions of 2011 Flexera Admin Studio as well as ZenWors Admin Studios versions 10 and 11 are also affected.
Strike Novell Groupwise Messenger Server Process Memory Information Disclosure	CWE: 200 CVE: 2011-3179 BID: 50443	This strike exploits an error in the Novell Groupwise Messenger Server process, which leads to the disclosure of arbitrary content in memory
Strike Apache HTTPD mod_proxy Security Bypass	CWE: 20 CVE: 2011-3368 BID: 49957	This strike exploits a security bypass vulnerability in Apache HTTP Server module mod_proxy. The vulnerability is due to an input validation error in mod_proxy when handling certain directives in the configuration. This vulnerability could be exploited by an attacker to bypass proxy configuration settings.
Strike Mozilla Firefox DOMAttrModified nsSVGValue Observer Vulnerability	CWE: 399 CVE: 2011-3658 BID: 51138	This strike exploits an out-of-bounds access flaw in Mozilla Firefox. The vulnerability is due to lack of index validation while manipulating 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 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.

Name	References	Description
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 Novell iPrint Client Realm Parameter Buffer Overflow	CWE: 119 CVE: 2011-4187	This strike identifies an stack buffer overflow in Novell's iPrint Client. Due to improper validation on the Realm String parameter, a user supplied input of greater than 129 bytes will overflow a fixed stack buffer.
Strike Novell iManager EnteredAttrName Parameter Buffer Overflow	CWE: 119 CVE: 2011-4188 BID: 40480	This strike exploits a stack overflow in Novell's iManager. The code does not validate the EnteredAttrName parameter properly upon creation, and if it is greater than 0x204 bytes, it will overwrite critical memory on the stack buffer.
Strike Novell iPrint Server natural languages Buffer Overflow	CWE: 119 CVE: 2011-4194 BID: 51791	This strike identifies a buffer overflow vulnerability in Novell's iPrint server. The overflow is due to improper checking of the IPP request's attributes-natural-languages field. A user supplied string is checked be to greater than 32 and less than 63, however, it is later copied into a stack of 0x20 bytes overflowing the stack.
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 Oracle Hyperion Financial ActiveX Control Buffer Overflow	CWE: 119 CVE: 2011-5167 BID: 50565	This strike exploits a vulnerability in Oracle Hyperion's ActiveX control TTF161.TTF1.6. When using the SetDevNames method, a heap buffer is allocated for based on the size of each of the arguments DriverName DeviceName and Port. The arguments' values are converted to unicode before getting stored in the buffer.
Strike Microsoft SharePoint Reflected List Parameter Cross Site Scripting Vulnerability	CWE: 79 CVE: 2012-0017 BID: 51928	Microsoft Office Sharepoint Foundation contains a cross-site scripting (XSS) vulnerability. The vulnerability is due to insufficient validation of parameters passed to the inplnview.aspx page.
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 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 Advantech Studio NTWebServer.exe CreateFileW Absolute Path Arbitrary File Access	CWE: 200 CVE: 2012-0236 BID: 56871	This strike exploits a directory traversal vulnerability in Advantech Studio. The vulnerability is due to lack of proper access control by the web service. Remote, unauthenticated users can exploit this vulnerability to read arbitrary system files.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Broadwin WebAccess Client Bwocxrun 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 Novell Groupwise Internet Agent Content Length Buffer Overflow	CWE: 189 CVE: 2012-0271 BID: 55551	This strike exploits a vulnerability in the Novell GWIA service. If a request is sent to this service with a Content-Length Header of a negative value and enough data to overwrite the stack buffer of 0x504 bytes, a denial of service condition can occur.
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 Novell Groupwise WebAccess Directory Traversal	CWE: 22 CVE: 2012-0410 BID: 54253	This strike exploits a directory traversal vulnerability in Novell Groupwise WebAccess.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Novell GroupWise HTTP Read of Arbitrary File	CWE: 22 CVE: 2012-0419	This strike exploits a flaw in Novell GroupWise where the HTTP interface allows an attacker to download an arbitrary file.
Strike Novell Groupwise Client ActiveX Memory Corruption	CWE: 94 CVE: 2012-0439 BID: 57658	This strike exploits a vulnerability within Novell Groupwise Client. Many functions inside of gwcls1.dll utilize pXPItem parameters, however, they are not properly validated. This user supplied value is later used as an object pointer which can cause invalid memory access.
Strike Oracle Java AtomicReferenceArray Sandbox Escape	CVE: 2012-0507 BID: 52161	This strike exploits a remote code execution vulnerability in Oracle Java. The vulnerability is due to a design weakness within the AtomicReferenceArray class. Successful exploitation of this vulnerability could result in the execution of arbitrary Java code 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 Apple Safari Webkit Button and Column Type Confusion	CVE: 2012-1520 BID: 54680	This strike exploits a vulnerability within Apple Safari's WebKit. If buttons are enclosed within a multi-column layout the code will take any created child objects as children of the button itself instead of the inside object. The code will then try to access the column block object which leads to a type confusion and results in memory corruption.
Strike Microsoft Internet Explorer Loop Counter Memory Corruption	CWE: 94 CVE: 2012-1522	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer (IE). The vulnerability is due to the manner in which IE accesses nested lists. By creating a malicious web page an attacker could cause an access violation, which could lead to remote code execution.
Strike Internet Explorer Remote Code Execution With The center Tag	CWE: 94 CVE: 2012-1523	This strike exploits an index boundary error in Internet Explorer (6, 7 and 8) when handling dhtml related to a center tag.
Strike Microsoft Internet Explorer	CWE: 94 CVE: 2012-1524 BID: 54294	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer (IE). The vulnerability is due to the manner in which IE accesses nested lists. By creating a malicious web page an attacker could cause the application to deference a pointer, resulting in an access violation, which could lead to remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Oracle Java Runtime Bytecode Verifier Cache Code Execution	CVE: 2012-1723 BID: 53960	This strike exploits a remote code execution vulnerability in Oracle Java. The vulnerability is due to an incorrect optimization in the HotSpot bytecode verifier. Successful exploitation of this vulnerability could result in the execution of arbitrary Java code on the target system.
Strike PHP CGI Command Execution	CWE: 20 CVE: 2012-1823	This strike exploits a vulnerability in PHP framework, more specifically how CGI scripts is handeled. 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 Developer Toolbar Use After Free Error	CWE: 94 CVE: 2012-1874	This strike exploits a vulnerability that exists in Microsoft Internet Explorer. When user assigns the console object to a local variable, the object gets released. When using console methods with the assigned variable, a reference is kept to the console object, and a use after free condition occurs.
Strike Microsoft Internet Explorer 2 Element Same id Use After Free Error	CWE: 94 CVE: 2012-1875	This strike exploits a vulnerability that exists in Microsoft Internet Explorer. When two elements contain the same id attribute, a use after free condition occurs if one element is deleted. The object is removed, but a reference is still retained, and if the id is called later, the deleted object may be accessed.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer title Element User After Free Condition	CWE: 94 CVE: 2012-1877	This strike exploits a vulnerability that exists in Microsoft Internet Explorer. If the onpropertychange event handler deletes the DOM and is run when the document.title property is modified, a use after free error is observed.
Strike Microsoft Internet Explorer Use After Free Condition for Multiple Events	CWE: 94 CVE: 2012-1878	This strike exploits a vulnerability that exists in Microsoft Internet Explorer. A use after free condition occurs when an element is removed by an event, and then later accessed.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

Name	References	Description
Strike Symantec Web Gateway ldap_latest.php Blind SQLi Injection	CWE: 89 CVE: 2012-2961 BID: 54425	This Strike exploits Symantec Web Gateway with a blind SQLi injection in ldap_latest.php via a MySQL trigger. The strike will attempt to create a new user in the database.
Strike Dell SonicWALL Scrutinizer statusFilter.php SQL Injection	CWE: 89 CVE: 2012-2962 BID: 54625	This trike exploits statusFilter.php to SQL inject Dell SonicWALL Scrutinizer.
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, 11.1.16 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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Mozilla Firefox XCS Code Execution	CVE: 2012-3993  BID: 56119	This strike exploits a vulnerability in Mozilla Firefox. Due to improper exception handling on objects that don't have the exposedProps property set, it is possible to overwrite functions that get called from a privileged context and silently invoke the AddonManager to install a malicious plugin. All version of Firefox up to 15.0.0.1 are vulnerable to this attack.
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 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 Microsoft Internet Explorer Use After Free Vulnerability	CWE: 399 CVE: 2012-4792 BID: 57070	This strike exploits a use-after-free vulnerability in Internet Explorer. The vulnerability is caused by an attempt to access a dereferenced memory pointer while making use of the applyElement method. By specially crafting a malicious web page, an attacker could exploit this vulnerability to execute arbitrary code with the permissions of the current user.
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 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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Firefly Media Server Multiple Denial of Service Vulnerabilities	CVE: 2012-5875	This strike exploits a multiple denial of service vulnerabilities in Firefly MediaServer when sending an specifically crafted HTTP request with modified headers to the server.
Strike Nero MediaHome Multiple Vulnerabilities Denial of Service	BID: 57253 CWE: 189 CVE: 2012-5876	This strike exploits multiple denial of service vulnerabilities in Nero MediaHome. By sending requests to the server that contain either an overly large URI or maliciously crafted headers, the attacker can cause a stack buffer to overflow causing a denial of service condition to occur.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 XML Core Services Memory Corruption	CWE: 189 CVE: 2013-0006 BID: 57116	This strike exploits an integer truncation in Microsoft's Core Services where an overly large string is mishandled on the 32 bit boundary and an undersized memory buffer is clobbered.
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.
Strike Microsoft Internet Explorer InsertElement Use After Free Condition	CWE: 399 CVE: 2013-0026	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. When a sub or sup element calls the Justify* commands multiple times, a use-after-free can occur.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Silverlight Pointer Dereference Code Execution	CVE: 2013-0074 BID: 58327	This strike exploits a vulnerability in Microsoft Silverlight. The vulnerability is due to improper verification of a pointer when rendering an html object. 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 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 SharePoint OSSSearchResults Cross Site Scripting	CWE: 79 CVE: 2013-0083 BID: 58367	This strike exploits a cross site scripting vulnerability in Microsoft SharePoint. The k parameter of OSSSearchResults.aspx is not sanitized for JavaScript. If a user clicks a link with JavaScript contained in this parameter, the JavaScript will execute with browser privileges. Successful exploitation can result in execution of SharePoint commands with user privileges.
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.
Strike Microsoft Internet Explorer saveHistory Object Use After Free Vulnerability	CWE: 399 CVE: 2013-0092 BID: 58344	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 CMarkup 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 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 Schneider Electric Accutech Manager URI Buffer Overflow	CWE: 119 CVE: 2013-0658	This strike exploits a vulnerability in Schneider Electric's Accutech Manager. An HTTP request URI value is not properly validated, and if a size over more than 128 bytes is received, a buffer is overflowed causing a denial of service condition.
Strike Siemens SIMATIC RegReader ActiveX Buffer Overflow	CWE: 119 CVE: 2013-0674	This strike exploits a vulnerability in Siemens' SIMATIC RegReader where a malformed parameter inside an ActiveX control can clobber a buffer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Mozilla Firefox XMLSerializer serializeToStream Use After Free	CWE: 416 CVE: 2013-0753 BID: 57209	This strike exploits a Use-After-Free vulnerability in Mozilla Firefox. The vulnerability is due to modification of the Document Object Model (DOM) while serializing an object. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
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 Novel ZENworks Mobile Management MDM.php language Param Code Execution	CWE: 22 CVE: 2013-1081 BID: 58402	This strike exploits an arbitrary code execution vulnerability in Novel ZENworks Mobile Management. A crafted HEAD message to download.php can be sent to store arbitrary PHP code in a temporary file. A crafted POST message to MDM.php can then be sent to execute the code in the file.
Strike Novel ZENworks Mobile Management DUSAP.php language Param Code Execution	CWE: 22 CVE: 2013-1082 BID: 60179	This strike exploits an arbitrary code execution vulnerability in Novel ZENworks Mobile Management. A crafted HEAD message to download.php can be sent to store arbitrary PHP code in a temporary file. A crafted POST message to DUSAP.php can then be sent to execute the code in the file.
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 Sanitization Library Cross Site Scripting	CWE: 79 CVE: 2013-1289 BID: 58883	This strike exploits a flaw in Microsoft's HTML Sanitization library which is vulnerable to a cross site scripting attack.

Name	References	Description
Strike Microsoft Windows Remote Desktop Client ActiveX Control Use After Free	CWE: 94 CVE: 2013-1296 BID: 58874	This strike exploits a code execution vulnerability in Microsoft Windows Remote Desktop Client. The vulnerability lies in the ActiveX control and a use-after-free error when handling HTML web pages. 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 Microsoft HTTP Denial of Service	CWE: 399 CVE: 2013-1305	This strike exploits a denial of service in Microsoft's handling of malformed HTTP requests.
Strike Microsoft Internet Explorer EnsureDispNode Use After Free Vulnerability	CWE: 416 CVE: 2013-1309 BID: 59748	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 Internet Explorer .ipsum Construct Layout Memory Corruption	CWE: 416 CVE: 2013-1310 BID: 59751	This strike exploits a Memory Corruption vulnerability in Internet 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.
Strike Microsoft Internet Explorer CSS first-line Use After Free	CWE: 416 CVE: 2013-1311 BID: 59752	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. When the CSS first-line function processes specially crafted content, heap buffer is freed twice, resulting in a use after free condition. Successful exploitation could result in the execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Microsoft Internet Explorer CDOMTextNode Use After Free	CWE: 416 CVE: 2013-1312 BID: 59753	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. If a CDOMTextNode is created and not properly deleted references to this object result in a memory access error causing a use-after-free condition to occur.
Strike Microsoft IE VML TextBox Handling Use-After-Free Vulnerability	CWE: 399 CVE: 2013-1338 BID: 59633	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability lies in the handling of VML TextBox objects. 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 8 CGenericElement Use-After-Free Vulnerability	CWE: 94 CVE: 2013-1347 BID: 59641	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability is due to the manner in which IE8 handles the creation of unsupported objects. By enticing a user to open a malicious web page an attacker could execute arbitrary code in the context of the user.
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 Fortinet Fortigate Firewalls Cross Site Request Forgery	CWE: 352 CVE: 2013-1414 BID: 60861	This strike exploits a Cross Site Request Forgery vulnerability within Fortinet FortiGate Firewalls. Due to improper validation, attackers trick the target into changing system settings, firewall policies or granting control of the firewall to the attacker.
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 Java Font Processing Memory Corruption	CWE: 94 CVE: 2013-1491	This strike exploits a code execution vulnerability in Oracle Java. The vulnerability is caused by an incorrect and insufficient CFF table validation when loading OTF fonts. The vulnerability may be exploited by a remote attacker by directing the user to request and process a maliciously crafted web page containing a Java applet.
Strike Oracle WebCenter Satellite HTTP Server Header Injection	CVE: 2013-1509	This Strike identifies a vulnerability in Oracle Web Center Satellite Server. Because user requests are not properly validated, it is possible to maliciously modify the Servers Response by injecting HTTP headers. These headers allow for session fixation and redirection attacks by utilizing the Refresh and Set-Cookie parameters.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Oracle WebCenter CheckOutAndOpen openWebDav ActiveX Control Code Execution	CVE: 2013-1559 BID: 59122	This strike exploits a vulnerable ActiveX control in Oracle WebCenter. The openWebDav and caco methods in the CheckOutAndOpen ActiveX Control will request, download, and execute the file in the webdavurl parameter. Successful exploitation may result in execution of arbitrary code.
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 Dlink IP Camera Video Stream Authentication Bypass	CVE: 2013-1600	This strike exploits authentication bypass vulnerability in DLINK IP Cameras which allows remote unauthenticated access to video streams
Strike Dlink IP Camera Luminance Information Disclosure	CVE: 2013-1601	This strike exploits an information disclosure vulnerability inside Dlink's IP Cameras, which offers direct unauthenticated access to the ascii luminance image for the item currently captured by the camera. The vulnerability is accessible through accessing a resource that does not properly request authentication.
Strike Mozilla Firefox onreadystatechange Use After Free	CWE: 119 CVE: 2013-1690 BID: 60778	This strike exploits a Use-After-Free vulnerability in Mozilla Firefox. The vulnerability is due to error handling onreadystatechange events. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
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 Nginx HTTP Server Chunked Buffer Overflow	BID: 59699 CWE: 189 CVE: 2013-2028	This strike exploits a buffer overflow vulnerability in the Nginx HTTP Server. If the chunk size is more than 1024 bytes those bytes are copied to a buffer with the following bytes interpreted as a hex-encoded integer that will be copied to a stack buffer of 4096 bytes. If this integer is negative, a stack buffer overflow can occur.
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Web Start ActiveX Memory Access Error	CVE: 2013-2416	This strike exploits an invalid memory access vulnerability in Oracle Java Web Start. When the method processes the unicode parameters, it takes each the 16-bit character and uses it as an index in the Base64 lookup table. It does not perform bounds-checking properly on the index against the lookup table size which allows for an out-of-bounds read access causing the javaws.exe process to crash.
Strike Oracle Java sun.tracing.Provider Skeleton Sandbox Bypass	CVE: 2013-2460 BID: 60635	This strike exploits a sandbox bypass vulnerability that exists in Oracle Java. The vulnerability is due to an insecure invoke() method of the sun.tracing.ProviderSkeleton class. A remote unauthenticated attacker can exploit this vulnerability by eliciting a user to visit a webpage containing a maliciously crafted Java applet. Successful exploitation could result in arbitrary code execution in the context of the currently logged in user.
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 Microsoft Internet Explorer VML Object Integer Underflow	CWE: 416 CVE: 2013-2551 BID: 58570	This strike exploits a integer vulnerability inside Microsoft Internet Explorer. The length field of a dashstyle array is not validated properly, and when this property is passed a negative value an attacker modify data inside the array.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Zavio IP Camera Firmware 1.6.03 Authentication Bypass	CVE: 2013-2567	This strike identifies an authentication vulnerability in Zavio IP Cameras utilizing firmware 1.6.03. Specifically the web interface authentication can be bypassed by using hardcoded admin account found within boa.conf. With this account one of 2 CGI files that are normally not visible, can be accessed
Strike Zavio IP Camera Firmware 1.6.03 User Credentials Disclosure	CVE: 2013-2568	This strike identifies a vulnerability in Zavio IP Cameras utilizing firmware 1.6.03. Specifically the wireless_mft.cgi file is used to copy the user's credentials by means of a OS command injection in the ap parameter.
Strike Zavio IP Camera Firmware 1.6.03 OS Command Injection	CVE: 2013-2570	This strike identifies a vulnerability in Zavio IP Cameras utilizing firmware 1.6.03. Specifically the command injection can be found in sub_C8C8 of /opt/cgi/view/param. The vulnerable parameter is General.Time.NTP.Server, and it can be used to inject malicious commands into the target system.
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 Google Chrome NotifyInstanceWasDeleted User After Free	CWE: 399 CVE: 2013-2912	This strike exploits a use after free vulnerability that is present inside Google Chrome, which gets triggered through actions that are taken by event listeners on an embedded object
Strike IBM Lotus Quickr qp2.cab Activex Control Integere Overflow	CWE: 119 CVE: 2013-3026	This strike exploits the heap overflow vulnerability found in the IBM Lotus Quickr product suite for Domino. The bounds validation flaw is centered around an ActiveX control associated with the qp2.dll library. By manipulating a user to access a specially crafted web page or document a heap overflow vulnerability can be triggered and arbitrary code execution may be achieved using local privileges.
Strike IBM iNotes ActiveX Control Integer Overflow	CWE: 189 CVE: 2013-3027 BID: 60971	This strike exploits a integer overflow vulnerability inside IBM iNotes that can be triggered using an ActiveX Control. The overflow is triggered by passing a large number of files to one of the parameters of the ActiveX Control.
Strike Mitsubishi MX Component ActiveX Control Buffer Overflow	CWE: 119 CVE: 2013-3075	This strike identifies a vulnerability in Mitsubishi's MX Component ActiveX control. This attack is against a vulnerable WzTitle function that takes a string as an argument. If this string size exceeds the limit of the buffer an overflow will occur allowing for remote code to be executed.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer Memory Corruption	CWE: 119 CVE: 2013-3111 BID: 60381	This strike exploits a memory corruption vulnerability in Microsoft Windows Internet Explorer. The vulnerability lies in the handling of DOM node objects. 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 Microsoft Internet Explorer CMarkup Use-After-Free Vulnerability	CWE: 119 CVE: 2013-3112 BID: 60382	This strike exploits a Use-After-Free vulnerability in Microsoft Internet Explorer (IE). The vulnerability occurs when Internet Explorer modifies the DOM using the applyElement method during an onPropertyChange event. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
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.
Strike Microsoft Internet Explorer Node NS Memory Corruption	CWE: 119 CVE: 2013-3118 BID: 60387	This strike exploits a double free memory corruption vulnerability in Microsoft Windows Internet Explorer. The vulnerability lies in the handling of svg element properties. 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 Microsoft Internet Explorer DOM Node Use After Free Memory Corruption	CWE: 119 CVE: 2013-3119 BID: 60388	This strike exploits a use after free vulnerability in Microsoft Windows Internet Explorer. The vulnerability lies in the handling of Document Object Model (DOM) Nodes. 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 Microsoft Internet Explorer setExpression Memory Corruption	CWE: 119 CVE: 2013-3121 BID: 60390	This strike exploits a use after free vulnerability in Microsoft Windows Internet Explorer. The vulnerability lies in the handling of the setExpression function. 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 Microsoft Internet Explorer onScroll Event Memory Corruption	CWE: 119 CVE: 2013-3123 BID: 60392	This strike exploits a use after free vulnerability in Microsoft Windows Internet Explorer. The vulnerability lies in the handling of the Document Object Model (DOM) onScroll event. 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer DOMNodeRemoved Use After Free Condition	CWE: 94 CVE: 2013-3143 BID: 60962	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. If an element is removed such as in this case with removeNode and then later used in the event handler for DOMNodeRemoved, a use-after-free condition will occur when trying to call this object because it has been deleted.
Strike Microsoft Internet Explorer 10 column-count attribute memory corruption	CWE: 94 CVE: 2013-3146 BID: 60965	This strike exploits an integer overflow vulnerability in Microsoft Internet Explorer. The column-count attribute of an html element is used when calculating a heap buffer. If a user supplies an overly large number to this value an integer overflow occurs and the heap size is not properly allocated. When this buffer is later accessed memory corruption occurs.
Strike Microsoft Internet Explorer onbeforereditfocus Memory Corruption	CWE: 94 CVE: 2013-3147 BID: 60966	This strike exploits a Memory Corruption vulnerability in Microsoft Internet Explorer. The vulnerability is due to error while handling the onbeforereditfocus event. 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 MSHTML!CTreePos Memory Corruption	CWE: 94 CVE: 2013-3152 BID: 60971	This strike exploits a memory corruption vulnerability inside IE that resides inside the MSHTML!CTreePos::Release function implementation which leads to a use after free condition
Strike Microsoft Internet Explorer CAnchorElement Use After Free	CWE: 94 CVE: 2013-3163	This strike exploits a vulnerability in Microsoft Internet Explorer when handling a maliciously crafted html file. If an html document contains a table tag with a CPhraseElement located within a table row element but not inside the table body, then an element is created for the tag. If this element is freed later, then all of the children associated with it are also freed. Although, some elements still maintain pointers to memory and any reference or attempt to call these elements will trigger a use after free condition.
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 Internet Explorer CSS StyleSheet Memory Corruption	CWE: 119 CVE: 2013-3191 BID: 61677	This strike exploits a Memory Corruption vulnerability in Internet Explorer. The vulnerability is due to 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 victim machine.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer onbeforeeditfocus Attribute Memory Corruption	CWE: 119 CVE: 2013-3203 BID: 62206	This strike exploits a Memory Corruption vulnerability in Microsoft Internet Explorer. The vulnerability is due to error while handling an on-event attribute of a DOM Element. 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 Explore Memory Corruption	CWE: 119 CVE: 2013-3205 BID: 62208	This strike exploits a use after free error triggered when Microsoft Internet Explorer handles certain objects. If a user opens a specially crafted web page, on a vulnerable machine, a memory corruption is triggered that can lead to arbitrary code execution using local privileges. All versions of Internet Explorer 6,7,8 are vulnerable to this attack.
Strike Microsoft Internet Explorer CBlockElement Handling Use-After-Free	CWE: 119 CVE: 2013-3207 BID: 62211	This strike exploits a Use-After-Free vulnerability in Microsoft Internet Explorer (IE). The vulnerability occurs when Internet Explorer attempts to reuse a deleted object created by a MutationEvent. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
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 usrrgp.cgi parameter in this strike we are able to create users with administrator privileges.
Strike Airlive IP Camera Directory Traversal	CWE: 22 CVE: 2013-3541	This strike identifies a vulnerability in Airlive IP Cameras, where an attacker can perform a directory traversal on the target system allowing him access to confidential or restricted files.
Strike Axis Media ActiveX Control File Creation	CWE: 264 CVE: 2013-3543	This strike identifies a vulnerability within Axis Media Player's ActiveX control methods StartRecord, SaveCurrentImage, and StartRecordMedia. These methods can be used to specify a file by path to create, or possibly overwrite and corrupt.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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	CVE: 2013-3621	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.
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 Airlive IP Camera URI Handling Denial of Service	CWE: 400 CVE: 2013-3691	This strike identifies a vulnerability in Airlive IP Cameras. Specifically an attacker can cause a denial of service condition to occur by sending a malicious request with an overly large URI to the target.
Strike Novell iPrint Client ActiveX Control GetPrinterURLList Denial of Service	CVE: 2013-3708 BID: 64027	This strike exploits a vulnerability in Novell's iPrint Client activeX control. Specifically the GetPrinterURLList method does not properly validate the input of the arguments that it takes. If this argument is passed a value that is out of bounds of the allowed value for the array, an indexing error occurs and invalid memory is referenced resulting in a denial of service condition.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Internet Explorer CTreePos Use After Free	CWE: 119 CVE: 2013-3845	This strike exploits a use after free error triggered when Microsoft Internet Explorer handles DOM rewrites when proccessing certain web pages. If a user opens a specially crafted web page, on a vulnerable machine, a memory corruption is triggered that can lead to arbitrary code execution using local privileges. Internet Explorer
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 Internet Explorer DOM CAnchorElement Use After Free	CWE: 119 CVE: 2013-3871 BID: 62802	This strike exploits a use after free vulnerability in Internet Explorer. The vulnerability in failure to properly delete CAnchorElement objects from the DOM. By enticing a user to view a malicious page a remote attacker could execute arbitrary code on the affected system with the priviledges of the user.
Strike Microsoft Internet Explorer HtmlLayout SmartObject Use After Free	CWE: 119 CVE: 2013-3873	This strike exploits a use after free error triggered when Microsoft Internet Explorer handles DOM rewrites when proccessing certain web pages. If a user opens a specially crafted web page, on a vulnerable machine, a memory corruption is triggered that can lead to arbitrary code execution using local privileges. Only Internet Explorer 10 is affected by this vulnerability
Strike Microsoft Internet Explorer runtimeStyle Handling Memory Corruption	CWE: 119 CVE: 2013-3882	This strike exploits a vulnerability inside Internet Explorer 10 that results in a memory corruption. The vulnerability is triggered through javascript code that manipulates a runtimeStyle object.
Strike Microsoft Internet Explorer onlosecapture Use After Free	CWE: 399 CVE: 2013-3893 BID: 62453	This strike exploits a vulnerability in Microsoft Internet Explorer when handling a maliciously crafted html file. If an html document has an onlosecapture event that contains a document writeln or write, a use after free condition can occur when trying to access that event later after it has been freed and overwritten.
Strike Microsoft Internet Explorer execCommand Memory Corruption	CWE: 399 CVE: 2013-3897	This strikes exploits a memory corruption vulnerability inside IE that gets triggered when an reference to a pointer gets freed by a call to execCommand function with an unselect parameter

Name	References	Description
Strike Microsoft Internet Explorer Print Preview Information Disclosure	CWE: 200 CVE: 2013-3908 BID: 63585	This strike identifies an information disclosure vulnerability in Microsoft Internet Explorer. Specifically a design weakness exists in how pages are parsed when Print Preview is used. By utilizing an html injection method in a script, if an attacker can entice a victim to select print preview, the contents of the page as well as session information can be revealed to the attacker by building a GET request to the attacker's server. This strike delivers the attack method 2 ways, by either clicking a link or automatically when opening a web page the user is directed to the website of their intended destination.
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 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 Apache Tomcat Large Chunked Transfer Denial of Service	BID: 65767 CWE: 20 CVE: 2013-4322	This strike exploits a vulnerability for Apache Tomcat Server. Specifically, the exploit targets how user input in chunked HTTP requests is processed. The flaw allows an unauthenticated remote attacker to craft a special request that utilises a very large amount of resources on the server and might trigger denial of service conditions. All versions prior to Apache Tomcat 6.0.39, 7.0.50 and 8.0.0-RC5 are vulnerable.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Adminstration web interface. The vulnerability allows command injection by passing malicious URL encoded parameters ("other") to php scripts.
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 in failure to properly authenticate HTTP requests by the euAccountSerivce 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

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Samsung PS50C7700TV DOS	CVE: 2013-4890	This strike exploits a Denial of Service vulnerability in Samsung PS50C7700 TV. This vulnerability is due to improper handle large header in HTTP request.
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 Web Gateway XSS	CWE: 79 CVE: 2013-5013 BID: 65405	This strike exploits a vulnerability inside Symantec Web Gateway solution, which allows reflected XSS attacks through the blocklist page. The vulnerability is exploitable through HTTP GET parameters due to improper input validation.
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.
Strike Microsoft Internet Explorer CVE-2013-5049 Memory Corruption	CWE: 119 CVE: 2013-5049 BID: 64123	This strike exploits a vulnerability inside Internet Explorer 6-10 that results in a memory corruption. The vulnerability is triggered through javascript code that manipulates a deprecated tag.
Strike Microsoft Internet Explorer CVE-2013-5052 Memory Corruption	CWE: 119 CVE: 2013-5052 BID: 64126	This strike exploits a vulnerability inside Internet Explorer 7 that results in a memory corruption. The vulnerability is triggered through javascript code that manipulates objects which leads to a use after free condition which can lead to denial of service or arbitrary code execution

<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 Cisco AnyConnect Secure Mobility Client Active Template Library Buffer Overflow	CWE: 119 CVE: 2013-5559	This strike exploits a vulnerability in Cisco AnyConnect's ATL framework. Specifically the Unregister function does not properly validate its parameter and a maliciously crafted value that is out of the range allowed will overflow a buffer causing a denial of service condition to occur, and possibly allowing for remote code execution.
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 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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco EPC3925 goform Quick_setup Cross Site Request Forgery	CWE: 352 CVE: 2013-6976 BID: 64341	This strike exploits a Cross Site Request Forgery vulnerability within goform/Quick_setup on Cisco EPC3925 devices. Due to improper validation, attackers can change a password via the Password and PasswordReEnter parameters of the QuickSetup.
Strike Nagios Core CGI Process_cgivars Off-By-One	CWE: 20 CVE: 2013-7108 BID: 64363	This strike exploits a vulnerability in Nagios open source monitoring solution. Due to improper input handling an unauthenticated attacker can send a specially crafted HTTP request and cause a denial of service condition. All versions of the Nagios Enterprises Core 3.x before Dec 20, 2013 are vulnerable to this attack.
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 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.
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.

Name	References	Description
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 mod_deflate Denial of Service	CWE: 399 CVE: 2014-0118 BID: 68745	This strike exploits a denial of service vulnerability inside Apache web server. The vulnerability exists due to improper processing of HTTP requests when Apache is ran using the mod_deflate module.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft IE CAreaElement Object Handling Use-after-free Vulnerability	CWE: 119 CVE: 2014-0275 BID: 65373	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 during an onfocus event. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
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 Use After Free MS14-010	BID: 65385 CWE: 119 CVE: 2014-0286	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 memory corruption is triggered that can lead to arbitrary code execution using local privileges. All versions of Internet Explorer are vulnerable to this issue.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer Use After Free MS14-012	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 Microsoft Internet Explorer CollectGarbage Use After Free	CWE: 119 CVE: 2014-0312 BID: 66036	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 memory corruption is triggered that can lead to arbitrary code execution using local privileges. All versions of Internet Explorer 8 through 11.
Strike Microsoft Internet Explorer CMarkup Use After Free	CWE: 416 CVE: 2014-0322 BID: 65551	This strike identifies a user after free vulnerability in Internet Explorer 10. When a CMarkup object is created and then destroyed within an onproperty event change the object is freed. Later when it is accessed a user after free condition occurs because it has already been released.
Strike Oracle Java JNDI Sandbox Bypass	CVE: 2014-0422 BID: 64921	This strike exploits a sandbox bypass vulnerability that exists in Oracle Java. The vulnerability is due to a lack of security context validation when loading classes from inside the JNDI package. A remote unauthenticated attacker can exploit this vulnerability by eliciting a user to visit a webpage containing a maliciously crafted Java applet. Successful exploitation could result in loading restricted classes and eventually to code execution with full security privileges. All versions of Java 7 update 45, Java 6 update 65 and java 5 update 55 and prior are vulnerable to this attack.
Strike Oracle Java ServiceLoader Sandbox Bypass	CVE: 2014-0457 BID: 66866	This strike exploits a sandbox bypass vulnerability in Oracle Java. By making use of the ServiceLoader class the ScriptEngine class can be leveraged to execute code with elevated privileges. Successful exploitation of this vulnerability could result in the execution of arbitrary Java code on the target system.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Attachmate Reflection FTP Client ActiveX GetSiteProperties3 Memory Corruption	CVE: 2014-0606 BID: 69156	This strike exploits a memory corruption vulnerability inside Attachmate's FTP Client. The vulnerability can be exploited through calling undocumented methods of ActiveX objects and can lead to remote code execution.
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 ActiveX Control NodeName Parameter Buffer Overflow	CWE: 119 CVE: 2014-0764 BID: 66718	This strike identifies stack buffer overflow in Advantech's WebAccess SCADA software. Specifically the webvact.ocx ActiveX control is not properly validated, and if the NodeName parameter receives a large amount of data the buffer will overflow causing a denial of service.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 SCADA webvact.ocx ActiveX Control Buffer Overflow	CWE: 119 CVE: 2014-0770 BID: 66733	This strike identifies stack buffer overflow in Advantech's WebAccess SCADA software. Specifically the webvact.ocx ActiveX control is not properly validated, and if the UserName parameter receives a large amount of data the buffer will overflow causing a denial of service.
Strike Advantech WebAccess BWOCXRUN.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 bwocxrund.ocx ActiveX Control. By enticing a user to open a crafted web page an attacker could remotely execute arbitrary code.
Strike Indusoft Web Studio Directory Traversal	BID: 67056 CWE: 22 CVE: 2014-0780	The strike exploits a directory traversal vulnerability inside Indusoft Web Studio. The vulnerability is present due to improper sanitization of input parameters and can lead to arbitrary file retrieval.
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 Advantech WebAccess SCADA ProjectName Parameter Buffer Overflow	CWE: 119 CVE: 2014-0991 BID: 69536	This strike exploits a buffer overflow vulnerability inside Advantech's WebAccess SCADA. The exploit targets a parameter of an activeX control and if exploited can result in remote code execution in the context of the currently logged in user
Strike Advantech WebAccess SCADA Password Param Buffer Overflow	CWE: 119 CVE: 2014-0992 BID: 69538	This strike exploits a buffer overflow vulnerability present inside Advantech's Scada ActiveX controls. If exploited, the vulnerability grants the attacker the possibility of running arbitrary code in the context of the currently logged in user.

Name	References	Description
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.
Strike Mozilla Firefox WebIDL Privilege Escalation	CWE: 94 CVE: 2014-1510 BID: 66206	This strike exploits a privilege escalation vulnerability in Mozilla Firefox. The vulnerability is due to a failed security check allowing XUL applications to be loaded within an iframe via a call to window.open(). 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 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 Microsys PROMOTIC NULL pointer dereference	CVE: 2014-1617	This strike exploits a NULL pointer dereference vulnerability within Microsys PROMOTIC ActiveX Control. This vulnerability is due to lack of checking user supplied input to the start method in Microsys PROMOTIC ActiveX Control. Remote unauthenticated attackers could exploit this vulnerability to crash the Brower on the target system.

Name	References	Description
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 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 un-authenticated 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 Google Chrome locationAttributeSetter Use After Free	CWE: 399 CVE: 2014-1713 BID: 66243	This strike exploits a use after free error triggered when Google Chrome handles DOM rewrites when processing AttributeSetter function calls. If a user opens a specially crafted web page, on a vulnerable machine, a memory corruption is triggered that can lead to arbitrary code execution using local privileges. All versions of Google Chrome prior to 33.0.1750.154 are vulnerable

Name	References	Description
Strike Microsoft IE cloneNode Use-After-Free Vulnerability	CWE: 119 CVE: 2014-1753 BID: 66648	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability lies in the handling of CAttrArray objects. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
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.
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.

Name	References	Description
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 CBlockContainerBlock Use After Free	CWE: 119 CVE: 2014-1804 BID: 67835	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 memory corruption is triggered that can lead to arbitrary code execution using local privileges. Only Internet Explorer 8 is affected by this vulnerability.
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.
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.

Name	References	Description
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 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 to conduct denial of service attacks.
Strike Lighttpd Host Header mod_mysql_vhost SQL Injection	CWE: 89 CVE: 2014-2323 BID: 66153	This strike targets a vulnerability inside Lighttpd that is triggered through the host header inside HTTP requests and causes SQL injection.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 LibYAML scanner yasm_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 ame 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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP Network Virtualization storedNtxFile Directory Traversal	CWE: 22 CVE: 2014-2625 BID: 68849	This strike exploits a directory traversal vulnerability in HP Network Virtualization software. The vulnerability is due to a lack of validation of the filename in HTTP requests in "storedNtxFile" method. By sending a specially crafted request using directory traversal patterns, an attacker could access sensitive files.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
Strike Microsoft Internet Explorer CVE-2014-2824 Memory Corruption	CWE: 119 CVE: 2014-2824 BID: 69120	This strike exploits a vulnerability in Microsoft Internet Explorer. The vulnerability is due to the way Internet Explorer processes HTML layout that contains a TextRange object. Enticing a user to access a crafted webpage, an attacker can cause the user's Internet Explorer to terminate abnormally.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Ericom AccessNow Server HTTP GET URI Stack Buffer Overflow	CWE: 119 CVE: 2014-3913 BID: 67777	This strike exploits a buffer overflow vulnerability in Ericom AccessNow. When processing HTTP GET requests, AccessNow copies the URI to a fixed length stack buffer without validating the length. A GET request with an overly long URI can be used to overflow this buffer. Successful exploitation can result in execution of arbitrary code with system privileges or abnormal termination of the AccessNow service.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 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 Oracle Business Intelligence Mobile App Designer Directory Traversal	CVE: 2014-4249 BID: 68605	This strike exploits a Oracle Business Intelligence Mobile App Designer directory traversal vulnerability which is due to improper parameter validation in the toGet function. Sensitive information could be obtained, which could be used in a remote code execution attack.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 OSSIM AlienVault avcenterd 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.
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 Incutio XML-RPC Library Entity Expansion Denial of Service	CWE: 399 CVE: 2014-5265 BID: 69146	This strike exploits a denial of service vulnerability in Incutio XML-RPC Library, a library used by WordPress and Drupal. Incutio XML-RPC Library does not restrict the size of internal entities. XML tags with internal entities will be fully expanded. Successful exploitation can cause CPU and memory exhaustion, causing a denial of service condition.
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 NetFlow Analyzer And IT360 DisplayChartPDF Directory Traversal	CWE: 22 CVE: 2014-5446 BID: 71404	This strike exploits a directory traversal vulnerability in ManageEngine Netflow Analyzer and IT360. The vulnerability is due to failure to sanitize directory traversal patterns in HTTP requests sent to the server. By sending a specially crafted request, an attacker could access confidential information on the server.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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 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 Microsoft Internet Explorer Clipboard Information Disclosure	BID: 70947 CWE: 200 CVE: 2014-6323	This strike exploits a vulnerability in Internet Explorer regarding access restriction to the clipboard. By exploiting this vulnerability, an attacker can use a specially crafted web page and access data copied to the clipboard.
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-After-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 Manage Engine Multiple Products FailOverHelperServlet Information Disclosure	CVE: 2014-7863	This strike exploits an information disclosure vulnerability in multiple ManageEngine products (OpManager, Applications Manager and IT360). An attacker can exploit this vulnerability by sending unauthenticated malicious requests to the server. Successful exploitation can lead to disclosure of file contents from any location on the server or a directory listing of any file path on the server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Manage Engine Multiple Products FailOverHelperServlet Blind SQL Injection	CWE: 89 CVE: 2014-7864	This strike exploits a blind SQL injection vulnerability in multiple ManageEngine products (OpManager and IT360). An attacker can exploit this vulnerability by sending unauthenticated malicious requests to the server, compromising the integrity of the database.
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.
Strike ManageEngine Multiple Products Probename SQL Injection	CWE: 89 CVE: 2014-7867 BID: 71509	This strike exploits a SQL Injection vulnerability in multiple ManageEngine products. The vulnerability is due to insufficient sanitization of parameters in the UpdateProbeUpgradeStatus servlet. By exploiting this vulnerability, an attacker can execute arbitrary SQL queries on the server.
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 Universal CMDB JMX Console Authentication Bypass	CWE: 200 CVE: 2014-7883	This strike exploits a security bypass vulnerability in HP Universal CMDB JMX console. The vulnerability is due to the default authentication configuration file not restricting access using HTTP methods other than GET and POST, such as HEAD or TRACE. Exploitation could allow an attacker to execute arbitrary unrestricted commands on the target server.
Strike HP Point of Sale OPOS Driver opostoneindicator 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 opostoneindicator 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.

Name	References	Description
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.
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 Internet Explorer CInputElement Memory Corruption	CWE: 20 CVE: 2014-8966 BID: 71457	This strike exploits a memory corruption vulnerability in Internet Explorer. The vulnerability is due to a failure to verify the type while processing CInputElement objects. 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.

Name	References	Description
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 <code>wpmp_pp_ajax_call()</code> 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 Trihedral VTScada Web Interface Integer Overflow	CWE: 189 CVE: 2014-9192 BID: 71591	This strike exploits an integer overflow vulnerability in Trihedral VTScada. The flaw is due to insufficient boundary checking of requests by the HTTP server. An attacker could exploit this vulnerability by sending a specially crafted HTTP request to the server in order to crash the HTTP service.
Strike Schneider Electric Multiple Products IsObjectModel RemoveParameter Stack Buffer Overflow	CWE: 119 CVE: 2014-9200 BID: 72335	This strike exploits a stack buffer overflow vulnerability in IsObjectModel ActiveX which is used in multiple Schneider Electric products. The vulnerability is due to improper validation of the supplied parameter in RemoveParameter method. By enticing a user to access a specially crafted web page, an attacker could execute arbitrary code.
Strike Microsys Promotic PmBase64Decode Buffer Overflow	CWE: 119 CVE: 2014-9205 BID: 72874	This strike exploits a remote code execution vulnerability in Microsys Promotic HMI. The vulnerability is due to insufficient validation of user-supplied input by the <code>PmBase64Decode</code> function. A remote, unauthenticated, attacker can exploit this vulnerability by sending a specially crafted HTTP Authorization header, potentially resulting in the execution of arbitrary code on the target system.
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 <code>InterfaceFilter</code> , <code>GetLastTagNbr</code> , <code>UpdateProjec</code> or <code>GetRecipeInfo</code> 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 PTC IsoView ActiveX Control Multiple Methods Buffer Overflow	CWE: 119 CVE: 2014-9267 BID: 71491	This strike exploits multiple vulnerabilities in PTC IsoView ActiveX control. The vulnerabilities are due to improper validation of several properties from the ActiveX control: ViewPort, GetObjectAnimationFlags, GetObjectAnimationSequenceName, CountObjectAnimations. By enticing a user to access a specially crafted web page, an attacker could execute arbitrary code, leading to browser termination.
Strike ManageEngine Desktop Central MSP StatusUpdateServlet fileName Directory Traversal	CVE: 2014-9404 BID: 71910	This strike exploits a directory traversal vulnerability found in ManageEngine Desktop Central MSP. The vulnerability is due to insufficient validation of a parameter in StatusUpdateServlet. An attacker can exploit this vulnerability by sending a specially crafted request, which could allow the attacker to execute arbitrary code in the context of the system user.
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 CTreePos Object Memory Corruption	CWE: 399 CVE: 2015-0041 BID: 72411	This strike exploits a Memory Corruption vulnerability in Internet Explorer. The vulnerability is due to an error while handling CTreePos 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 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 Windows TrueType Font Parsing Remote Code Execution	CWE: 264 CVE: 2015-0059 BID: 72470	This strike exploits a TrueType Font Parsing vulnerability in Windows. The vulnerability is due to an integer underflow that can occur while parsing font files using SHZ instructions. An attacker could exploit this vulnerability by enticing a user to open a file using an embedded, malicious font file. This could potentially lead to remote execution of code with kernel-level privileges.
Strike Microsoft Internet Explorer Policy Bypass	CWE: 264 CVE: 2015-0071 BID: 72455	This strike exploits an information disclosure vulnerability in Internet Explorer that is due to the possibility of overwriting a certain readonly property. By exploiting this vulnerability memory offsets of specific instructions can be viewed by an attacker. This information could be used in a remote code execution attack.
Strike Microsoft Internet Explorer Same Origin Bypass Universal XSS	CWE: 79 CVE: 2015-0072 BID: 72489	This strike exploits a vulnerability in Microsoft's Internet Explorer which allows bypassing the same-origin policy, effectively allowing attackers to access resources from other domains, such as authentication cookies and other private information. The vulnerability is due to the way Internet Explorer handles calls to blocking functions.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.Iwctrl 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 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)
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 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).

<b>Name</b>	<b>References</b>	<b>Description</b>
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 SearchBlox Stored Cross-Site Scripting (XSS)	CWE: 79 CVE: 2015-0967 BID: 74059	This strike exploits a stored cross-site scripting vulnerability inside SearchBlox Web interface. The vulnerability is due to improper validation of user supplied parameters in HTTP requests. By exploiting this vulnerability an attacker could execute malicious scripts on the target machine.
Strike SearchBlox Information Disclosure	CWE: 200 CVE: 2015-0969 BID: 74059	This strike exploits an information disclosure vulnerability inside SearchBlox Web interface. The vulnerability is due to improper access control mechanisms in _cluster/health page. An attacker could exploit this vulnerability in order to gain unauthorized access to information.
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.
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.

Name	References	Description
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 Microsoft Internet Explorer JavaScriptStackWalker Memory Corruption	CWE: 399 CVE: 2015-1730 EXPLOITDB : 40881	This strike exploits a vulnerability in Microsoft Internet Explorer. By creating a pointer to data on the stack that is later referenced after that data has been removed from the stack, an attacker can modify javascript in such a way that causes memory corruption and potentially allowing for remote code execution to occur.
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.

Name	References	Description
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.
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 Eclipse Jetty Web Server 400 Response Information Disclosure	CWE: 200 CVE: 2015-2080 BID: 72768	This strike exploits an information disclosure vulnerability in Eclipse Jetty Web Server versions prior to 9.2.9.v20150224. The vulnerability exists due to improper treatment of HTTP request parsing. Successful exploitation will result in disclosure of information related to previous HTTP requests sent to the server.
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.

Name	References	Description
Strike WebGate WESPPlayback Stack Buffer Overflow	CWE: 119 CVE: 2015-2094 BID: 72841	This strike exploits a WebGate WESPPlaybackCtrl 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 WESPPlayback SiteName Stack Buffer Overflow	CVE: 2015-2098 BID: 72838	This strike exploits a WebGate eDVR Manager WESPPlaybackCtrl 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 Control Center WESPPlayback GetThumbnail Stack Buffer Overflow	CVE: 2015-2099 BID: 72834	This strike exploits a WebGate Control Center WESPPlaybackCtrl ActiveX buffer overflow vulnerability. This vulnerability is due to improper bound validation in the GetThumbnail method. 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 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 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 Microsoft Internet Explorer Use-After-Free Vulnerability	CWE: 119 CVE: 2015-2401	This strike exploits a use-after-free vulnerability inside Microsoft Internet Explorer. The vulnerability is due to accessing an already freed heap buffer. An attacker could exploit this vulnerability in order to remotely execute malicious code.

Name	References	Description
Strike MutationObserver Memory Corruption Vulnerability In Microsoft Internet Explorer	CWE: 119 CVE: 2015-2425 BID: 75745	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 MutationObserver objects. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Internet Explorer JavascriptexcEption 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 CIinput 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 CIinput objects. An attacker could exploit this vulnerability in order to remotely execute malicious code.
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 Microfosft JavaScript Engine RegExp Use After Free	CWE: 119 CVE: 2015-2482 BID: 77007	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically the vulnerability exists in the Microsoft JavaScript engine. If a regexp object is created and its replace method is called on a String object using the regexp object as a parameter, the source param is freed, and the compile method is later called, it attempts to use the cached source property. This results in a use after free condition.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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 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 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 ElasticSearch Site Plugin Directory Traversal	CWE: 22 CVE: 2015-3337 EXPLOITDB : 37054 BID: 74353	This strike exploits a directory traversal vulnerability in Elasticsearch before 1.4.5 and 1.5.x before 1.5.2. The vulnerability allows attackers to read arbitrary files when the site plugin is enabled.
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 F5 BIG-IP iControl Command Execution and Privilege Escalation	CWE: 264 CVE: 2015-3628 BID: 77666 EXPLOITDB : 38764	This strike exploits a command execution and privilege escalation vulnerability in F5 BIG-IP iControl API. A user with Resource Administrator authentication can send a SOAP message with a specially crafted iCall script in order to achieve command execution with root privileges. The attacker could also exploit this vulnerability to achieve a root shell. Successful exploitation may result in arbitrary command execution with root privileges or privilege escalation to root.
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 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).

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Visual Mining Netcharts Server projectContents 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.
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 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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.
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.

Name	References	Description
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 styleSheets Use After Free Vulnerability	CWE: 119 CVE: 2015-6065	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. The vulnerability is due to the way rules array of styleSheets are handled. An attacker could exploit this vulnerability in order to remotely execute malicious code.
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 CElement Use After Free Vulnerability	BID: 77448 CWE: 119 CVE: 2015-6075	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. The vulnerability is due to the way CElement objects deletion is handled. An attacker could exploit this vulnerability in order to remotely execute malicious code.
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 String Object Information Disclosure	BID: 77461 CWE: 200 CVE: 2015-6086	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically the InitFromString method does not handle string objects correctly. When a certain character is processed an out of bounds memory access occurs disclosing memory information to the user.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 overwrote 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Browser TextNode Type Confusion	CWE: 119 CVE: 2016-0003	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically a type confusion vulnerability exists when a child element is re-appended to its parent and then an attempt to access its value is made.
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 Internet Explorer CAttrArray Use After Free	BID: 84014 CWE: 119 CVE: 2016-0106	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically the vulnerability is found when a CAttrArray object is created, deleted, and an event handler is attached to that object. When the event handler attempts to access this object a use-after-free condition occurs, which can lead to memory corruption.
Strike Microsoft Internet Explorer BuildPageLayout Memory Corruption	BID: 84016 CWE: 119 CVE: 2016-0108	This strike exploits a vulnerability in Microsoft Internet Explorer 11. Specifically, a type confusion vulnerability exists in how the vulnerable code treats an arbitrary pointer as a DOM element. This leads to memory corruption, which can result in remote code execution.
Strike Microsoft Browser SVG Attribute Use After Free	BID: 84022 CWE: 119 CVE: 2016-0111	This strike exploits a vulnerability in Microsoft Edge and Internet Explorer. Specifically the vulnerability is found when an attribute is assigned inside an svg element. The object is created, deleted, and an event handler is attached to that object. When the event handler attempts to access this object a use-after-free condition occurs, which can lead to memory corruption.
Strike Microsoft Internet Explorer CTravelEntry Object Use After Free	BID: 84011 CWE: 119 CVE: 2016-0113	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically a use after free vulnerability occurs when a CTravelEntry object is created, and then an attempt to access it is made after it has been deleted. This results in memory corruption, which can lead to code execution.
Strike Microsoft Browser ConvertStringFrom UnicodeEx Memory Corruption	CWE: 119 CVE: 2016-0154	This strike exploits a vulnerability in Microsoft Edge and Internet Explorer. When an HTML document is set to utf-7 encoding, and a form contains an input element, a buffer is allocated allowing space for the input's attributes. It is possible to create a buffer of size zero, allowing for memory corruption to occur when writing to that buffer.
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 Edge Chakra JavaScript Array.unshift Memory Corruption	BID: 90008 CWE: 119 CVE: 2016-0186	This strike exploits a memory corruption vulnerability in the Microsoft Edge Chakra JavaScript engine. Specifically the Array.unshift() function does not properly validate its arguments and will allow an uninitialized pointer to be dereferenced any functions that call it. This results in memory corruption and can potentially lead to remote code execution.

Name	References	Description
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 Microsoft Edge Chakra JavaScript Engine Array.concat Memory Corruption	BID: 90010 CWE: 119 CVE: 2016-0191	This strike exploits a vulnerability in the Microsoft Edge Browser's Chakra JavaScript Engine. Specifically, the Array.concat method does not properly validate the parameters of the Proxy method call. If an uninitialized array is used in a Proxy method call, and concat is called on that proxy object, it is possible to dereference an uninitialized pointer which can lead to memory corruption and potentially remote code execution.
Strike Microsoft Edge Chakra JavaScript typedArray Memory Corruption	BID: 90009 CWE: 119 CVE: 2016-0193	This strike exploits a vulnerability in the Microsoft Edge Chakra JavaScript engine. When writing data to a buffer using the fill method, it is possible for an attacker to specify a value that corrupts memory. When a typedArray object is created, a heap buffer is allocated based on the size of that object. However, due to improper bounds checking the attacker can specify a value that goes beyond the bounds of the created buffer to corrupt memory utilize this fill method.
Strike Microsoft Internet Explorer Attribute Value Type Confusion	CWE: 119 CVE: 2016-0199	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically a type confusion vulnerability exists when the DOM contains certain elements whose attributes are created and have their nodeValue set to an invalid object. If this happens memory corruption will occur causing a denial of service condition and potentially allowing for remote code execution to occur.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 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 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 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.

Name	References	Description
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 <code>escapeshellarg()</code> escaping to prevent this attack. However, this escaping clashes with <code>escapeshellcmd()</code> 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 <code>-X</code> parameter to write out a log with arbitrary php code, which can then be executed.
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 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 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 Apache Struts <code>xslt.location</code> Local File Inclusion	BID: 88826  CWE: 20  CVE: 2016-3082	This strike exploits a local file inclusion vulnerability in Apache Struts. Struts accepts HTTP requests with an <code>xslt.location</code> query parameter which points to a local XSL stylesheet file. The XSL stylesheet can contain an Object-Graph Navigation Language expression allowing Java method execution. An attacker can upload a specially crafted XSL stylesheet and then send a specially crafted HTTP request calling that XSL stylesheet to achieve arbitrary Java method execution, including the <code>exec()</code> method, which could lead to arbitrary command execution.
Strike Shopware <code>getTemplateName</code> 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 <code>getTemplateName</code> function fails to sanitize input when building the file path and name. If a request is made containing the <code>f</code> or <code>file</code> 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.

Name	References	Description
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.
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 Edge normalize Memory Corruption	BID: 92789 CWE: 119 CVE: 2016-3294	This strike exploits a memory corruption vulnerability in the Microsoft Edge Browser. Specifically, when an attacker crafts an html page with an element that makes a call to the insertAdjacentText or insertAdjacentHTML functions, it's possible for type confusion to occur. This can potentially lead to remote code execution within the context of the current user, or a denial of service condition in the browser.

Name	References	Description
Strike Microsoft Internet Explorer and Edge CElement normalize() Function Memory Corruption	BID: 92830 CWE: 119 CVE: 2016-3295	This strike exploits a memory corruption vulnerability in the Microsoft Internet Explorer and Edge Browsers. Specifically, when an attacker crafts an html page with a caption element that contains a doctype declaration a type confusion vulnerability can occur. This can potentially lead to remote code execution within the context of the current user, or a denial of service condition in the browser.
Strike Microsoft Internet Explorer and Edge Font Lang Parameter Use After Free	BID: 92829 CVE: 2016-3297	This strike exploits a use after free vulnerability in Microsoft Internet Explorer and Edge Browsers. Specifically, if a font element's lang attribute is set to a string, and then its node value is set to null, the string is freed. Later a call to reference this lang attribute will result in a user after free condition. An attacker can use this attack to disclose memory information that can potentially lead to an ASLR bypass.
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 CStr Object Use After Free	CWE: 200 CVE: 2016-3326 BID: 92287	This strike exploits a vulnerability in the Microsoft Edge and Internet Explorer browsers. Specifically, it is possible to cause a Use After Free condition by creating many javascript tags that contain a src parameter referencing a non existing resource. When this happens many CStr objects are created. These objects can later be updated or freed when the SetString method is called on them. If an attempt to access these freed objects is then made, a use after free condition will occur. This can cause a denial of service condition in the browser and potentially allow for remote code execution.
Strike Microsoft Internet Explorer and Edge Browser UNC Information Disclosure	CWE: 200 CVE: 2016-3327 BID: 92284	This strike exploits a vulnerability in Microsoft Internet Explorer and Edge browsers. A buffer overrun vulnerability can occur when an invalid UNC URL is processed. When this happens the code enters a loop that iterates through the buffer containing the attacker specified URL. Eventually this will exhaust the memory that was allocoated for the buffer causing a denial of service condition in the browser and potentially allowing for the attacker to disclose memory information that can be used in other types of attacks.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer and Edge MimeType Property Information Disclosure	BID: 92788 CWE: 200 CVE: 2016-3351	This strike exploits a vulnerability in Microsoft Internet Explorer and Edge Browsers. Specifically, an attacker can specify different mime type extensions in javascript that will identify whether or not a certain program is installed on the target machine.
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.
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 Squid Proxy ESI Component Stack Buffer Overflow	CWE: 121 CVE: 2016-4054	This Strike exploits a Stack buffer Overflow in ESI component of squid Proxy. This vulnerability is due to improper handling of ESI Response Packets. The attacker sends an HTTP request to the Squid server with URI as the attacker-controlled origin server. When the vulnerable Squid server sends a request to the attacker controlled origin server and receives the HTTP response containing overly large ESI markup tags, the vulnerability will be triggered when the Squid server parses the HTTP response. Successful exploitation could result in the execution of arbitrary code. *NOTE: We are simulating the exchange of packets between the attacker-controlled server and the squid proxy.
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.

Name	References	Description
Strike Trihedral VTS scada Wap Out of Bounds Indexing Remote Code Execution	CWE: 119 CVE: 2016-4523 BID: 91077	This strike exploits a vulnerability in Trihedral VTS scada. Specifically the program does not properly handle HTTP requests made to the target with directory traversal characters. If several of these characters are sent to the target, an out of bounds indexing error occurs. This will crash the vtscada application, and can potentially lead to remote code execution.
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 VTS scada Wap Directory Traversal	CWE: 22 CVE: 2016-4532 BID: 91077	This strike exploits a directory traversal vulnerability in Trihedral VTS scada. When an un-authenticated user pairs this attack with CVE-2016-4510 ,which allows for a file to be 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 Host Header Cache Poisoning	CWE: 345 CVE: 2016-4553	This strike exploits a cache poisoning vulnerability in Squid Proxy Server. Squid accepts fully qualified domain names in the Request-URI field of HTTP requests. If given a fully qualified domain, it does not ignore the host header. If an attacker places a legitimate fully qualified domain name into the Request-URI field and an attacker-controlled malicious domain into the host field, Squid will access the attacker-controlled domain and cache it as the legitimate domain. Future users who attempt to access the url the attacker provided in the Request-URI field will instead be served the cached malicious website.
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 Webkit Memory Corruption in TypedArray copyWithin and fill Functions	CWE: 119 CVE: 2016-4734 BID: 93057 GOOGLE: 863 GOOGLE: 862	This strike exploits a vulnerability in Webkit. The copyWithin and fill methods both allow for very large values to be written to an absolute pointer within a specified range. It is possible for an attacker to craft javascript in a way that will corrupt memory and may allow for remote code execution to occur.

Name	References	Description
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 HAProxy reqdeny Access Control Denial of Service	CWE: 119 CVE: 2016-5360 BID: 91138	This strike exploits a vulnerability in HAProxy. Specifically, HTTP responses can be configured using the http-request and deny keywords. If a reqdeny rule is configured and then matched, upon receiving an HTTP request, the server will process this match, and send it to lookup any error messages. When this happens the matched data will likely be outside of the errmsg array boundary leading to memory corruption and a segmentation fault causing a denial of service to occur.
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.
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 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.

Name	References	Description
Strike Microsoft Edge Browser Chakra Engine Array.join Type Confusion	CWE: 119 CVE: 2016-7189 BID: 93427	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 Array.join is called on an arry of elements it is possible to reference the array's prototype if it has a getter function. If this function returns an element of a different type to the calling function to assign to the array type confusion can occur. This can lead to a disclosure of memory contents. 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 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 TemplatifiedForEachItemInRange 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 TemplatifiedForEachItemInRange 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer and Edge JavascriptArray Buffer Overflow	CWE: 119 CVE: 2016-7202 BID: 94042	This strike exploits a vulnerability in the Microsoft Edge and Internet Explorer Browsers. Specifically, in the javascript scripting engine when prototype.reverse is called, the EntryReverse function creates an offset to an array using the initial length. If this value is then later modified an integer underflow can occur. The value is then later used in a calculation which results in a heap buffer overflow. This can cause a denial of service condition to occur in the browser, or potentially lead to remote code execution.
Strike Microsoft Edge Array.splice Buffer Overflow	CWE: 119 CVE: 2016-7203 BID: 94039 GOOGLE: 934	This strike exploits a vulnerability in Microsoft Edge. Specifically it is possible to allow for an array with boundaries that will cause integer overflows to be spliced. When this happens a heap overflow will occur which can cause a denial of service in the browser and potentially leading to remote code execution.
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 Internet Explorer and Edge JSON.parse Information Disclosure	CWE: 119 CVE: 2016-7241 BID: 94055	This strike exploits a vulnerability in the Microsoft Edge and Internet Explorer Browsers. Specifically, in the javascript scripting engine when JSON.parse is called in a specific manner, another function gets called on an array object expecting the type to be JavascriptArray. However, if this is changed to a JavascriptNativeIntArray memory pointers can be written to JavascriptNativeIntArray. It is then possible to retrieve and 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 allow for remote code execution to occur.
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 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 Microsoft Edge Browser International Type Confusion	CWE: 119 CVE: 2016-7287 BID: 94722	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically when Object.defineProperty is redefined before Intl is initialized, a user-defined method that defines a Collator can be called during initialization. The getter and setter on the Intl object can change the value of what it was set to. This will then result in type confusion.
Strike Microsoft Edge TypedArray Object sort Method Use After Free	CWE: 119 CVE: 2016-7288 BID: 94749 GOOGLE: 983	This strike exploits a use-after-free vulnerability in the Microsoft Edge Browser. It is possible when an ArrayBuffer is allocated and attached to a TypedArray object, to create a use-after-free-condition. If the toString or valueOf methods are overridden in a function comparison of the sort method by invoking a specific message, the ArrayBuffer is freed and detached from the TypedArray object. However, when the sort method is called, the freed buffer is referenced again triggering the use-after-free condition.
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 ImageMagick TIFF Header Data Type Flag Out-of-Bounds Array Indexing	CWE: 125 CVE: 2016-7799 BID: 93264	This strike exploits an out of bounds array-indexing vulnerability in ImageMagick. When processing TIFF headers, typically found in jpeg or TIFF files, the Data Type Flag value is incorrectly checked as a signed value. Negative values will erroneously pass the check, and are later interpreted as very large unsigned values. These values are later used to access an array, leading to an out-of-bounds array-indexing condition. When this image gets processed on the server, it could cause arbitrary code to be executed.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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 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 URI, 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 Javascript NULL Object Memory Corruption	CVE: 2017-0010 BID: 96059	This strike exploits a vulnerability in Microsoft Edge. Specifically, the vulnerability lies in the CheckModuleReturn function of the AsmJSCompiler method. Due to improper validation, when experimental Javascript features are enabled in the Edge browser and the AsmJSCompiler::CheckModuleReturn function is called on a NULL object, it is possible to corrupt memory. This may result in a denial of service condition in the browser or potentially lead to remote code execution.
Strike Microsoft XML Core Services Information Disclosure	CWE: 200 CVE: 2017-0022 BID: 96069	This strike exploits a vulnerability that exists in Microsoft XML Core Services. Specifically, if the loadXML function is used to reference a portable executable with the res protocol in its URI, the parseError method can return a message up the stack that can be used to identify whether or not the file exists. An attacker can use this method to disclose which portable executables exist on the target's system.

Name	References	Description
Strike Microsoft Internet Explorer and Edge Browser BlockSite Spoofing	CWE: 20 CVE: 2017-0033 BID: 96087	This strike exploits a vulnerability that exists in the Microsoft Internet Explorer and Edge Browsers. If a request to a URL is made, a check to ensure that the page is not a security error page is performed, and if it is, the BlockedSite warning page will be called. A malicious attacker can utilize the ms-appx-web protocol and make a request to this warning page with his or her own data as parameters to spoof the information presented to the user when the page is displayed. This can lead to a social engineering attack.
Strike Microsoft Internet Explorer and Edge HandleColumnBreak OnColumnSpanning Element Function Type Confusion	CWE: 704 CVE: 2017-0037 GOOGLE: 1011 BID: 96088	This strike exploits a vulnerability in the Microsoft Internet Explorer and Edge Browsers. It is possible for an attacker to craft HTML and CSS in such a way that allows for the styleSheet of an object containing the colspan property to be modified causing a type confusion to occur.
Strike Microsoft Internet Explorer CStr Object Use-After-Free	CWE: 200 CVE: 2017-0059 BID: 96645 GOOGLE: 1076	This strike exploits a Use-After-Free vulnerability in Microsoft Internet Explorer. Specifically, when a textarea value is allocated, a CStr object is created and assigned to this value. Later this object is reallocated when a handler method is triggered and the form is reset. It is then possible to call a function that looks for the pointer to the CStr object, but it has already been freed and no longer exists. This results in a Use-After-Free condition, which can lead to a disclosure of memory contents or potentially allow for remote code execution to occur.
Strike Microsoft Edge read URI Scheme Information Disclosure	CWE: 200 CVE: 2017-0065 BID: 96648	This strike exploits an information disclosure vulnerability in Microsoft Edge. Specifically, the vulnerability lies in the _LoadRMHTML function of CReadingModeViewerEdge. A remote attacker can determine, through the read URI scheme, whether or not a file exists on a target system.
Strike Microsoft Edge Frame Elements Security Policy Bypass	CVE: 2017-0066 BID: 96655	This strike exploits a vulnerability that exists in Microsoft Edge. Specifically a newly opened window can modify the frame element on another web page. These web pages may be of different origins, which violates the same origin policy. An attacker can employ this attack to potentially disclose information from a victim.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Edge ProfiledLdElem Function Type Confusion	CWE: 119 CVE: 2017-0071 GOOGLE: 1045 BID: 96681	This strike exploits a vulnerability in Microsoft Edge's Chakra.dll component. Specifically, the vulnerability lies in the ProfiledLdElem function of the JS::ProfilingHelpers method. An attacker can craft javascript that allows for a javascriptArray object to get processed as a javascriptNativeArray or javascriptfloatArray, which leads to type confusion. A successful attack may cause a denial of service condition in the browser or lead to remote code execution.
Strike Microsoft Edge Chakra Javascript Engine asm Type Confusion	CWE: 119 CVE: 2017-0093 BID: 97419	This strike exploits a vulnerability that exists in the Microsoft Edge Chakra Javascript Engine. Specifically, it is possible for an attacker to craft Javascript in such a way that assigns eval to a function that uses the Javascript experimental "use asm" feature. When eval is called in a specific manner, a type confusion error will occur. This will cause a denial of service condition in the browser, and may allow for remote code execution.
Strike Microsoft Edge SetPropertyTrap Method Type Confusion	CWE: 119 CVE: 2017-0094 BID: 96682	This strike exploits a vulnerability in the Microsoft Edge ChakraCore engine. Specifically, if an object that is inherited from proxy is indexed with a symbol, type confusion can occur. The SetPropertyTrap method assumes the returned type to always be a Property String. However, if this object makes calls on symbol object type confusion can occur. This can lead to a denial of service condition in the browser, or potentially allow for remote code execution to occur.
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 Microsoft Edge ChakraCore Type Confusion Information Disclosure	CWE: 119 CVE: 2017-0134 BID: 96687	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 the type JavascriptNativeIntArray to be changed to type JavascriptArray. This later leads to a disclosure of information such as memory addresses and fake object contents.
Strike Microsoft Edge Chakra Array.Reverse Heap Overflow	CVE: 2017-0141 BID: 96685	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 a heap overflow to occur when making a call to the ArrayReverse helper function. This may cause a denial of service condition in the browser, or potentially lead to remote code execution.

Name	References	Description
Strike Microsoft Edge Repeat Method Out of Bounds Memory Read	CWE: 200 CVE: 2017-0208 BID: 97460	This strike exploits a vulnerability that exists in Microsoft Edge. An attacker can craft Javascript in a way that causes an out of bounds buffer to be read when a string object is created by the repeat method. During this process a string replace method is called to replace characters in the string, and a sign extension is performed on the count parameter of the calculation. If this value is too large, it becomes negative, which can potentially lead to an out of bounds memory read, disclosing the memory contents of the buffer.
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 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.
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.

Name	References	Description
Strike Synology Photo Station Information Exposure	CWE: 200 CVE: 2017-11155 EXPLOITDB : 42434	This strike exploits an Information Exposure vulnerability in Synology Photo Station. A remote, unauthenticated attacker can obtain sensitive system information.
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 Internet Explorer Jscript JSONStringifyObject Use After Free	BID: 101141 CWE: 119 CVE: 2017-11793 GOOGLE: 1381 EXPLOITDB : 43368	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. Specifically, the vulnerability exists in Jscript.dll. It is possible to craft Javascript in such a way that a user after free condition can occur in JSONStringifyObject. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
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.
Strike Microsoft Edge Chakra StringReplace Type Confusion	CWE: 119 CVE: 2017-11802 BID: 101130 GOOGLE: 1334 EXPLOITDB : 43000	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 StringReplace function to be used inline with the JIT process. When the replace function is called it fails to check if a user function is called and type confusion can occur. This may cause a denial of service condition in the browser, or potentially lead to remote code execution.
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 Internet Explorer JsErrorToString Buffer Overflow	CWE: 119 CVE: 2017-11810 BID: 101081 GOOGLE: 1340 EXPLOITDB : 43131	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. Specifically, the vulnerability exists in jscript.dll. Javascript can be crafted in such a way that allows for a Use-After-Free to occur in the JsErrorToString function, which can cause a heap buffer overflow. 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 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 ASM.JS ArrayBuffer Use-After-Free	CWE: 119 CVE: 2017-11812 BID: 101139	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 a Use-After-Free condition to occur when processing an ArrayBuffer that has previously been freed. This may cause a denial of service condition in the browser, or potentially lead to remote code execution.
Strike Microsoft Edge Chakra ToDefiniteAnyNumber Type Confusion	CWE: 119 CVE: 2017-11840 BID: 101734 GOOGLE: 1365 EXPLOITDB : 43183	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 setting the value of an object property, and then changing its internal type during optimization. This may cause a denial of service condition in the browser, or potentially lead to remote code execution.
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.

Name	References	Description
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 Edge Chakra	CWE: 119 CVE: 2017-11873 BID: 101728 GOOGLE: 1357 EXPLOITDB : 43154	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 OP_memset is called to change the type of a float array. This may cause a denial of service condition in the browser, or potentially lead to remote code execution.
Strike Microsoft Internet Explorer Jscript RegExpComp Compile 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.

Name	References	Description
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.
Strike Microsoft Internet Explorer Jscript NameTbl GetValDef Use After Free	CWE: 119 CVE: 2017-11903 GOOGLE: 1376 BID: 102047 EXPLOITDB : 43367	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. Specifically, the vulnerability exists in the Javascript Jscript DLL. The NameTbl object is not tracked by the Garbage collector, so if toString deletes its this object a use after free condition can occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.
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 Internet Explorer Jscript Array.Sort Heap Overflow	CWE: 119 CVE: 2017-11907 GOOGLE: 1383 EXPLOITDB : 43370 BID: 102045	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. Specifically, the vulnerability exists in jscript.dll. It is possible to craft Javascript in such a way that will allow for a heap overflow to occur when making calls to the JsArrayStringHeapSort or JsArrayFunctionHeapSort functions. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
Strike Microsoft Edge Chakra Engine RemoveEmptyLoopAfterMemOp Breaks Control Flow	CWE: 119 CVE: 2017-11909 BID: 102085 GOOGLE: 1384 EXPLOITDB : 43467	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 RemoveEmptyLoopAfterMemOp function to remove empty function loops. However, when this is called it may not take all branches into consideration and can potentially break the control flow. 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 JBoss Application Server ReadOnlyAccessFilter Unrestricted Deserialization	CWE: 502 CVE: 2017-12149 BID: 100591	This strike exploits a Java unrestricted Deserialization vulnerability in JBoss application server. The vulnerability is due to the way in which the doFilter method does not restrict classes for which it performs deserialization. Successful exploitation will allow an attacker to execute arbitrary code via crafted serialized data.
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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.

Name	References	Description
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 Wget HTTP Non-200 Negative Chunk Size Buffer Overflow	CWE: 119 CVE: 2017-13089 BID: 101592	This strike exploits a heap buffer overflow vulnerability in Wget. Wget can accept HTTP responses using chunked encoding. Due to typecasting, very large negative values will result in a heap buffer overflow. An attacker may respond to an HTTP GET request with a response of any type other than HTTP 200 OK, with chunked encoding and a chunk with a very large negative size value to exploit this vulnerability. Successful exploitation may result in arbitrary code execution with privileges of the user running Wget, or abnormal program termination.
Strike Wget Negative Chunk Size Buffer Overflow	CWE: 119 CVE: 2017-13090 BID: 101590	This strike exploits a heap buffer overflow vulnerability in Wget. Wget can accept HTTP responses using chunked encoding. Due to typecasting, very large negative values will result in a heap buffer overflow. An attacker may respond to an HTTP GET request with an HTTP 200 OK Response with chunked encoding and a chunk with a very large negative size value to exploit this vulnerability. Successful exploitation may result in arbitrary code execution with privileges of the user running Wget, or abnormal program termination.
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.

Name	References	Description
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 Node.js 8.5.0 Normalize Directory Traversal	CWE: 22 CVE: 2017-14849 BID: 101056	This strike exploits a directory traversal vulnerability in Node.js 8.5.0. The vulnerability is caused by improper sanitization of the normalize method in a HTTP request. An unauthenticated remote attacker could exploit this vulnerability by sending a crafted HTTP request to the target application, leading to gain unauthorized access to information.
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.
Strike Flexense SyncBreeze Enterprise HTTP Header Stack Buffer Overflow	CWE: 119 CVE: 2017-17099 EXPLOITDB : 42984	A stack buffer overflow has been identified in Flexsense SyncBreeze Enterprise appliance. The vulnerability is caused by the lack of proper bound checking of the URI within HTTP requests processing. The vulnerability can be exploited by sending a specially-crafted HTTP request, allowing the attacker arbitrary code execution with SYSTEM privileges.
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.

Name	References	Description
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.
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 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 XMLHTTP request 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.
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.

Name	References	Description
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.
Strike Google Chrome V8 WebAssembly Module Information Disclosure	CWE: 125 CVE: 2017-5088 BID: 99096	This strike exploits a vulnerability in the Google Chrome. Specifically, the vulnerability exists in the V8 Javascript engine. It is possible to craft Javascript in such a way that will allow for values on the heap to be leaked to the user. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Google Chrome V8 Javascript Use After Free	CWE: 416 CVE: 2017-5098 BID: 99950	This strike exploits a vulnerability in Google Chrome. Specifically, the vulnerability exists in the v8 Javascript engine. It is possible to craft Javascript in such a way that will allow for a use after free condition 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 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 Google Chrome V8 Javascript Engine Turbofan Compiler Type Confusion	CWE: 704 CVE: 2017-5115 BID: 100610	This strike exploits a vulnerability in Google Chrome. Specifically, the vulnerability exists in the v8 Javascript engine. It is possible to craft Javascript in such a way that will allow for out of bounds memory to be accessed. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Google Chrome v8 Web Assembly Type Confusion	CWE: 704 CVE: 2017-5116 GOOGLE: 759624 BID: 100610	This strike exploits a vulnerability in the Google Chrome browser. Specifically, the vulnerability exists in Javascript v8 engine. It is possible to craft Javascript in such a way that when the main thread parses the WebAssembly Code, the worker thread can also modify this code at the same time causing out of bounds memory access. This may lead to a denial of service condition in the browser, or potentially 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.

Name	References	Description
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 createImageBitmap Integer Overflow	CWE: 190 CVE: 2017-5428 BID: 96959	This strike exploits a vulnerability that exists in Mozilla Firefox. Specifically, an integer overflow occurs in the ImageBitmap::Create function that can lead to an out of bounds memory read. A malicious attacker can call the createBitmapImage function with overly large values for arguments triggering this vulnerability. A successful attack can lead to a denial of service condition in the browser, or potentially lead to remote code execution.
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 Mozilla Firefox WebGL Intersect Integer Overflow	CWE: 119 CVE: 2017-5459 BID: 97940	This strike exploits a memory corruption vulnerability in Mozilla Firefox. An integer overflow occurs within the Intersect() function when code containing the WebGL readPixels() method is called. This strike utilizes the copyTexSubImage2D method to demonstrate this vulnerability by causing a denial of service in the browser. Successful exploitation could potentially lead to remote code execution.
Strike Intel AMT Remote PPrivilege 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HPE Intelligent Management Center accessMgrServlet Insecure Java Deserialization	CWE: 502 CVE: 2017-5790 BID: 96755	This strike exploits an insecure java deserialization in Hewlett Packard Enterprise (HPE) Intelligent Management Center (IMC). IMC accepts java serialized objects in the body of HTTP POST requests to accessMgrServlet. It does not validate the objects before deserialization. An attacker could send an HTTP POST request to the vulnerable URI with a specially crafted java serialize object to achieve arbitrary command execution with privileges of the user running the IMC application, often SYSTEM or root.
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
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.
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 Nginx Range Filter Request Integer Overflow	CWE: 190 CVE: 2017-7529 BID: 99534	This strike exploits an integer overflow vulnerability in the way the nginx web server handles range requests. The vulnerability can be exploited by an attacker with a specifically crafted web request. An attacker could exploit this vulnerability to disclose cache key syntax and other interesting private data about the web server's configuration.

Name	References	Description
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 Http2 Null Pointer Dereference	CWE: 476 CVE: 2017-7659 BID: 99132	This strike exploits a null pointer dereference vulnerability in Apache. The vulnerability is due to lack of input validation of HTTP Host parameter in module mod_http2 . A maliciously constructed HTTP/2 request could cause mod_http2 to dereference a NULL pointer and crash the server process.
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 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.
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 Microsoft Edge CAttrArray Object Type Confusion	CWE: 119 CVE: 2017-8496 BID: 98880 GOOGLE: 1254	This strike exploits a type confusion vulnerability in the Microsoft Edge browser. Specifically, if a user sets an event handler with the DOMAttrModified event and the style property clip-path, type confusion can occur when the PrivateFindInl method of the CAttrArray Function is called. This can result in a denial of service condition in the browser or potentially lead to remote code execution on the targeted system.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Edge Chakra TypedArray Type Confusion	CWE: 119 CVE: 2017-8548 GOOGLE: 1290 BID: 98954	<p>This strike exploits a vulnerability in Microsoft Edge. Specifically, the Javascript Chakra engine assumes that the specified array will be a float array, however, it is possible to modify this type with the valueOf handler, which will result in type confusion. This can cause a denial of service in the browser or potentially allow for remote code execution to occur.</p>
Strike Microsoft Internet Explorer Filter Element Type Confusion	CWE: 119 CVE: 2017-8594 BID: 99401 GOOGLE: 1233	<p>This strike exploits a type confusion vulnerability in Microsoft Internet Explorer. If an svg element is created with use and filter elements in a specific way and then those elements are relocated in the DOM, type confusion can occur. When the elements are relocated and the DOM is torn down the MSHTML DestroySplayTree method is called. This method in turn calls another method that attempts to act upon the svg filter element structure, and this leads to the type confusion condition. This can result in a denial of service in the browser or potentially lead to remote code execution on the targeted system.</p>
Strike Microsoft Edge Chakra TypedArray Type Confusion JIT Optimization	CWE: 119 CVE: 2017-8601 GOOGLE: 1316 BID: 99420 EXPLOITDB : 42479	<p>This strike exploits a vulnerability in Microsoft Edge. Specifically, the Javascript Chakra engine assumes that the specified array will be a float array, however, it is possible to modify this type with the valueOf handler, which will result in type confusion. This vulnerability differs from CVE 2017-8548, in that the object replaced is now an empty new object and not an integer. This can cause a denial of service in the browser or potentially allow for remote code execution to occur.</p>
Strike Microsoft Edge AsmJsInterpreter Method Use After Free	CWE: 119 CVE: 2017-8603 BID: 99406	<p>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.</p>
Strike Microsoft Edge Chakra Argument Buffer Overflow	CWE: 119 CVE: 2017-8636 EXPLOITDB : 42466 BID: 100056	<p>This strike exploits a vulnerability in the Microsoft Edge browser. It is possible to cause a stack 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.</p>

Name	References	Description
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.
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 Chakra PushPopFrameHelper DoS	CWE: 119 CVE: 2017-8646 BID: 100053 GOOGLE: 1277 EXPLOITDB : 42470	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 PushPopFrameHelper to be used incorrectly. This results in a denial of service condition in the browser.

Name	References	Description
Strike Microsoft Edge textarea Use After Free	CWE: 200 CVE: 2017-8652 BID: 100047 EXPLOITDB : 42445 GOOGLE: 1255	This strike exploits a vulnerability in Microsoft Edge. Specifically, when a textarea element contained inside a form element is created, an eventhandler modifies the value inside this element, and the form is reset, a heap buffer is freed. Later when this memory is referenced in the function InsertSanitizedTextEx a use after free condition occurs. This may result in a denial of service in the browser or potentially lead to 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 Deferred Parsing Incorrect Scope	CWE: 119  CVE: 2017-8740  GOOGLE: 1310  EXPLOITDB : 42764  BID: 100763	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Chakra Javascript engine. It is possible to craft Javascript in such a way that DeferParse causes an incorrect opcode to be generated. This may lead to a denial of service condition in the browser, or potentially 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.

Name	References	Description
Strike Microsoft Edge Chakra ReparseAsmJs Incorrectly Reparses	CWE: 119 CVE: 2017-8755 BID: 100778 GOOGLE: 1327 EXPLOITDB : 42766	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 an exception to be thrown when re-parsing asmjs modules. By exhausting the stack we can cause an exception to occur. This may cause a denial of service condition in the browser, or potentially lead to 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 Managment Center perfAccessMgrServlet 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 Operations Orchestration central-remoting Remote Code Execution	CWE: 20 CVE: 2017-8994 BID: 100588	This strike exploits a remote code execution vulnerability in Hewlett Packard Operations Orchestration. 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 under the context of the user running the web application.
Strike Subsonic Media Server Cross-Site Scripting	CWE: 352 CVE: 2017-9414 EXPLOITDB : 42120	This strike exploits a cross-site scripting vulnerability in Subsonic media server. This vulnerability is due to improper sanitization of user controlled parameters to different HTTP GET and POST 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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Httpd Options Method Memory Leak	CWE: 416 CVE: 2017-9798 BID: 100872 EXPLOITDB : 42745	This strike exploits a memory leak vulnerability in Apache httpd. Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations.
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 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.

Name	References	Description
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 LowerSetConcatStr MultiItem Integer Overflow	CWE: 119 CVE: 2018-0758 GOOGLE: 1380 EXPLOITDB : 43491 BID: 102405	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in Javascript Chakra engine. Because there is not an Integer Overflow check in place, it is possible to craft Javascript in such a way that causes a bug to occur when LowerSetConcatStrMultiItem is called to concatenate strings. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge AppendLeftOverItemsFromEndSegment Out of Bounds Read	GOOGLE: 1387 CWE: 200 CVE: 2018-0767 BID: 102393 EXPLOITDB : 43522	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 when the AppendLeftOverItemsFromEndSegment method is invoked an out of bounds memory read will occur. This can lead to a denial of service condition in the browser or potentially remote code execution.
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 GlobOpt OptTagChecks fix bypass	CWE: 119 CVE: 2018-0770 BID: 102397 GOOGLE: 1434 EXPLOITDB : 44075	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 cause a denial of service condition in the browser.
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 BoxStackInstance Stack to Heap Copy	CWE: 119 CVE: 2018-0776 GOOGLE: 1420 EXPLOITDB : 43723 BID: 102401	This strike exploits a vulnerability in the Microsoft Edge. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that will allow for access to arguments containing stack-allocated variables where they should not exist. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra Loop Analysis Out Of Bounds Read-Write	CWE: 119 CVE: 2018-0777 GOOGLE: 1429 EXPLOITDB : 43718 BID: 102402	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 will cause an OOB read/write to occur when dealing with loop optimization. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
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 Array.prototype.reverse Type Confusion	CWE: 119 CVE: 2018-0835 BID: 102874 GOOGLE: 1459 EXPLOITDB : 44079	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 a call to Array.prototype.reverse is made. This can allow for a denial of service to occur or potentially remote code execution.
Strike Microsoft Edge Chakra LdThis Type Confusion	CWE: 119 CVE: 2018-0837 GOOGLE: 1464 EXPLOITDB : 44081 BID: 102876	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 type confusion can occur when handling LdThis objects. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
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 <code>__proto__</code> type confusion can occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra ImplicitCallFlags Bypass	CWE: 119 CVE: 2018-0840 GOOGLE: 1438 EXPLOITDB : 44077 BID: 102886	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 will bypass the ImplicitCallFlags check by throwing an exception. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra Escape Analysis	CWE: 119 CVE: 2018-0860 GOOGLE: 1437 EXPLOITDB : 44076 BID: 102883	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 a way that can abuse the <code>Object.prototype.valueOf</code> method to return 'this', and can use it as the getter to return an array object on the stack. This may lead to a denial of service condition in the browser, or potentially remote code execution.
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 <code>lastIndexOf</code> method on <code>String</code> 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.

Name	References	Description
Strike Microsoft Internet Explorer RegExp.lastMatch Memory Disclosure	CWE: 200 CVE: 2018-0891 GOOGLE: 1461 EXPLOITDB : 44312 BID: 103309	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically, the vulnerability exists in the Javascript jscript.dll library. It is possible to craft Javascript in such a way that when making a call to the RegExp.lastMatch function information will be disclosed. In this case memory contents are dumped to the user. It is also possible that this may lead to a denial of service condition in the browser.
Strike Microsoft Edge Chakra InstanceOf Type Confusion	CWE: 119 CVE: 2018-0893 BID: 103288	This strike exploits a vulnerability in Microsoft Edge. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that an object is passed to the InstanceOf method to dereference a pointer value of an assumed type, which can be changed causing type confusion to occur. This may 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 Edge Chakra BoxStackInstance NewError Stack to Heap Copy	CWE: 119 CVE: 2018-0934 GOOGLE: 1503 EXPLOITDB : 44397 BID: 103275	This strike exploits a vulnerability in the Microsoft Edge. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that will allow for access to arguments containing stack-allocated variables where they should not exist. This strike uses the Error constructor to iterate over each function and the arguments on the stack which end up invoking BoxStackInstance with the arguments. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
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 - Cross Context Use-After-Free	CWE: 119 CVE: 2018-0946 EXPLOITDB : 44758 BID: 103989	This strike exploits a vulnerability in the Microsoft Edge Chakra engine. Specifically the vulnerability is under the CrossSite class, which passes Javascript variables across different contexts. An attacker who successfully exploits the vulnerability could trigger a Use-After-Free condition.
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.
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.

Name	References	Description
Strike Electron Protocol Handler Command Injection	CWE: 78 CVE: 2018-100006 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 Squid Proxy Server ESI Null Pointer Dereference	CWE: 476 CVE: 2018-1000027	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: 2018-1000207	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.
Strike GONICUS GOsa WebUI Change Password Form Reflected Cross-Site Scripting	CWE: 79 CVE: 2018-1000528	This strike exploits a cross-site scripting vulnerability in GOsa, a web-based LDAP administration program. This vulnerability is due to inadequate input filtering in the web interface, while changing the password within 'password.php' form. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
Strike GitList searchTree method Remote Code Execution	CWE: 20 CVE: 2018-1000533 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: 2018-1000861 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.

Name	References	Description
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 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.
Strike IPConfigure Orchid Core Video Management System Unauthenticated Directory Traversal	CWE: 22 CVE: 2018-10956 EXPLOITDB : 44916	This strike exploits a directory traversal vulnerability within the IPConfigure Orchid Core Video Management System. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to the target server. Successful exploitation results in the disclosure of arbitrary file contents from the target server.
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 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 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.

Name	References	Description
Strike Samsung Web Viewer Cross Site Scripting	CWE: 79 CVE: 2018-11689	This strike exploits a reflected XSS vulnerability inside the Samsung DVR Web Viewer. Web Viewer is vulnerable to a cross-site scripting attack that will allow remote attackers to inject code.
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 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.

Name	References	Description
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 Apache HTTP Server Empty Headers Denial of Service	BID: 103522 CWE: 125 CVE: 2018-1303	This strike exploits a denial of service vulnerability in Apache HTTP Server configured with mod_cache_socache. An error in handling empty HTTP headers may lead to abnormal termination of the httpd process, resulting in a denial of service condition. An attacker can send specially crafted HTTP messages with empty HTTP header to trigger the vulnerability.
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.

Name	References	Description
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 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 MyBB New Threads Cross Site Scripting	CWE: 79 CVE: 2018-14392	This strike exploits a reflected cross-site scripting vulnerability found in MyBB open source PHP forum platform. This vulnerability is due to inadequate input filtering in the web interface, while parsing input passed to 'subject' parameter within newthread.php. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
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 Responsive FileManager Directory Traversal	CWE: 22 CVE: 2018-15535 EXPLOITDB : 45271	This strike simulates a directory traversal attack on Responsive FileManager. The vulnerability can be exploited by issuing requests to the endpoint that handles AJAX calls. By exploiting it, an attacker may read arbitrary files from the filesystem.
Strike Supervene RazDC User Reset Password CGI Form OS Command Injection	CVE: 2018-15549	This strike exploits a command injection vulnerability in Supervene RazDC. The vulnerability is due to improper validation of input passed to 'User Reset Password' CGI script. By exploiting this vulnerability, a remote, unauthenticated attacker can execute arbitrary OS commands on the target server.
Strike Supervene RazDC WebUI Edit User CGI Form Stored XSS	CVE: 2018-15550	This strike exploits a stored cross site scripting vulnerability in Supervene RazDC. The vulnerability is due to the lack of user-supplied input sanitization within 'save_user.cgi' form, while parsing input passed to various HTTP parameters. By exploiting this vulnerability, a remote, unauthenticated attacker can execute arbitrary OS commands on the target server.
Strike Supervene RazDC Create User CGI Form OS Command Injection	CVE: 2018-15551	This strike exploits a command injection vulnerability in Supervene RazDC. The vulnerability is due to the lack of user-supplied input sanitization while parsing input passed to 'password' (Password) and 'password2' (Confirm Password) HTTP parameters within 'create_user.cgi' form. By exploiting this vulnerability, a remote, unauthenticated attacker can execute arbitrary OS commands on the target server.
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.

Name	References	Description
Strike Argus Surveillance DVR Directory Traversal	CWE: 22 CVE: 2018-15745 EXPLOITDB : 45296	This strike exploits a directory traversal found in Argus Surveillance DVR. The vulnerability is due to insufficient user input sanitization passed to the 'RESULTPAGE' parameter. A specially crafted HTTP request could allow an attacker to read arbitrary files from the file system.
Strike D-Link Authorization HTTP Header Buffer Overflow	CWE: 119 CVE: 2018-15839	This strike exploits a buffer overflow vulnerability inside D-Link DIR-615 devices. The vulnerability is due do insufficient user input validation passed to SessionID parameter. By crafting a malicious HTTP request, an attacker can cause DoS conditions or achieve code execution on the target device.
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 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.
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.

Name	References	Description
Strike ManageEngine OpManager SetManaged API SQL Injection	CWE: 89 CVE: 2018-17283	This strike exploits a blind SQL injection vulnerability in ManageEngine's OpManager application. The vulnerability is present in a API parameter for managing devices 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.
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 CentOS Web Panel Authenticated Directory Traversal	CWE: 22 CVE: 2018-18323 EXPLOITDB : 45610	This strike exploits a directory traversal vulnerability in CentOS Web Panel. The vulnerability is due to lack of parameter sanitization while executing service-related operations, with the service name passed as a GET parameter. Successful exploitation results in the disclosure of arbitrary file contents from the target server.
Strike ACME mini_httpd Arbitrary File Read	CWE: 200 CVE: 2018-18778	An arbitrary file read vulnerability has been reported in ACME mini_httpd. This vulnerability is due to the way mini_httpd process HTTP requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a maliciously crafted HTTP request to the affected server. Successful exploitation of this vulnerability can lead to disclosure of the content of arbitrary file on the target system.

Name	References	Description
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 Zoho ManageEngine OpManager DataMigrationServlet Insecure Deserialization	CVE: 2018-19403	This strike exploits a remote code execution in Zoho ManageEngine OpManager. The vulnerability is due to deserialization of untrusted data by the DataMigrationServlet 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 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 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.
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.

Name	References	Description
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 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.
Strike Apple Safari Webkit WebAssembly Compilation Info Leak	GOOGLE: 1545 CWE: 125 CVE: 2018-4222 EXPLOITDB : 44859	This strike exploits a vulnerability in the Apple Safari browser. Specifically the vulnerability exists when compiling WebAssembly source buffers in WebKit. The source buffer is copied to a read only buffer, and if this buffer is a view, the offset is added to the buffer which can potentially allow for heap memory to be read off of the source. This can result in a denial of service condition in the browser or possibly remote code execution.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apple Safari WebKit WebCore SVGAnimateElementBase resetAnimatedType Use After Free	CVE: 2018-4314 CWE: 416 GOOGLE: 1596	This strike exploits a vulnerability in Apple Webkit. Specifically, an attacker can craft JavaScript in such a way that when the Webcore SVGAnimateElementBase::resetAnimatedType method is invoked a Use After Free condition can occur . 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 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 updateMinimumColumnHeight Use After Free	CWE: 119 CVE: 2018-4323 GOOGLE: 1609	This strike exploits a vulnerability in Apple Safari Webkit. Specifically the vulnerability exists in the WebCore::RenderMultiColumnSet::updateMinimumColumnHeight method. It is possible to craft Javascript in such a way that allows for a use-after-free condition to occur when invoking the updateMinimumColumnHeight method. 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 WebCore InlineTextBox paint Out of Bounds Read	CWE: 119 CVE: 2018-4328 GOOGLE: 1610	This strike exploits a vulnerability in Apple Safari Webkit. Specifically, the vulnerability exists when making a call to the InlineTextBox::paint method. It is possible to craft Javascript in such a way that when invoking this method memory corruption will occur leading to an out of bounds memory read. This can lead to a denial of service or potentially allow for remote code execution to occur.
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.

Name	References	Description
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.
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 Apple Webkit GetIndexedProperty Storage GC Use After Free	CWE: 119 CVE: 2018-4442 GOOGLE: 1699	This strike exploits a vulnerability in Apple Webkit. Specifically, an attacker can craft javascript that takes advantage of a vulnerability that exists in how the GetIndexedPropertyStorage can cause garbage collection via rope strings, which can lead to a use after free condition. This can cause a denial of service in the browser or potentially allow for remote code execution to occur.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.
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.

Name	References	Description
Strike Google Chrome V8 CollectValuesOrEntriesImpl Type Confusion	CWE: 704 CVE: 2018-6064 GOOGLE: 1498 EXPLOITDB : 44394 BID: 103297	This strike exploits a vulnerability in the Google Chrome browser. Specifically, the vulnerability exists in the Google Chrome V8 javascript engine. It is possible to change the elements kind by getters. This may lead to a denial of service condition in the browser, or potentially remote code execution.
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_nof_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.
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.

Name	References	Description
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! 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.
Strike Easy Hosting Control Panel Cross Site Request Forgery	CWE: 352 CVE: 2018-6458	This strike exploits cross site request forgery vulnerabilities in Easy Hosting Control Panel. This vulnerability is due to lack of CSRF tokens to protect against malicious HTTP requests. By enticing an authenticated user to visit an attacker controlled webpage or click a malicious link, an attacker could delete the entire database or manipulate the availability of different services running on the server.
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 TrendNet AUTHORIZED_GRO UP Information Disclosure	CWE: 20 CVE: 2018-7034	This strike exploits an information disclosure vulnerability in TRENDnet TEW-751DR v1.03B03, TEW-752DRU v1.03B01, and TEW733GR v1.03B01 devices. An attacker can use global variable \$AUTHORIZED_GROUP to bypass security checks and use it to read arbitrary files.

Name	References	Description
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.
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 results 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.

Name	References	Description
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.
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.

Name	References	Description
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 Appear TV Maintenance Centre Directory Traversal	CWE: 22 CVE: 2018-7539	This strike exploits a directory traversal vulnerability within the fuzzd webserver running the Appear TV Maintenance Centre application. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to the target server. Successful exploitation results in the disclosure of arbitrary file contents from the target server.
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.
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 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.

Name	References	Description
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.
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 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 EntrySimpleObjectSlotGetter Type Confusion	CWE: 119 CVE: 2018-8133 GOOGLE: 1542 EXPLOITDB : 44817 BID: 103982	This strike exploits a vulnerability in Microsoft Edge. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that will allow for type confusion to occur when a call to the EntrySimpleObjectSlotGetter method is made. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
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.
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 SetConcatStrMultiItemBE Type Confusion	GOOGLE: 1560 CWE: 119 CVE: 2018-8229 BID: 104369 EXPLOITDB : 45013	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 SetConcatStrMultiItemBE instructions can be hoisted without properly validating its type. 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 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 DictionaryProperty Descriptor 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.
Strike Microsoft Edge Chakra localeCompare Type Confusion	CWE: 119 CVE: 2018-8355 BID: 104978 GOOGLE: 1588 EXPLOITDB : 45432	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 type confusion to occur when utilizing the Javascript localCompare method. This may lead to a denial of service condition in the browser, or potentially remote code execution.
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.

Name	References	Description
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 Chakra JIT BailOutOnInvalidate dArrayHeadSegment Check Bypass	CWE: 119 CVE: 2018-8466 GOOGLE: 1612 EXPLOITDB : 45571 BID: 105243	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to bypass the check whether a given object is an array by wrapping an object with the CrossSite class to replace the vtable of the object. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra JIT Definite Object Type Confusion	CWE: 119 CVE: 2018-8467 GOOGLE: 1613 EXPLOITDB : 45572 BID: 105244	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 illustrates an array type conversion check is not implemented for definite objects. If a native array is processed as a definite object type confusion can occur. This may lead to a denial of service condition in the browser, or potentially 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.

Name	References	Description
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 WSO2 Identity Server Stored Cross-Site Scripting	CWE: 79 CVE: 2018-8716 EXPLOITDB : 44531	This strike exploits a cross-site scripting vulnerability in WSO2 Identity Server. This vulnerability is due to improper sanitization of user input when adding a new workflow engine profile. 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 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.
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 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.

Name	References	Description
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.
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 Configr 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 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 Microsoft Edge Renderer Double Free	CWE: 119 CVE: 2019-0940	This strike exploits a double-free vulnerability in the Microsoft Edge browser. The vulnerability lies within the rendering component. It is possible to partially initialize canvas pattern objects and trigger a double-free. This may lead to arbitrary read-write in the browser or potentially remote code execution.
Strike Jenkins Script Security Plugin Authenticated Remote Command Execution	CWE: 254 CVE: 2019-10030 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 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.

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 PHP FPM init_request_info Buffer Underflow	CWE: 787 CVE: 2019-11043	A buffer underflow vulnerability exists in PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11. The vulnerability resides in 'init_request_info (fpm_main.c)' function and is a side-effect of no string length check when FCGI parameters are received from a nginx server. An unauthenticated remote attacker can exploit the flaw to execute arbitrary code on the target server.
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 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 Pulse Connect Secure tcpdump options Command Injection	CWE: 77 CVE: 2019-11539 BID: 108073	A command injection vulnerability exists in Pulse Connect Secure due to insufficient parameter sanitization. The vulnerability resides in the '/dana-admin/diag/diag.cgi' endpoint and can be exploited by crafting the 'options' parameter in order to create a template file which contains Perl directives. By exploiting the flaw, a remote authenticated attacker may execute arbitrary commands on the target system.

Name	References	Description
Strike Mozilla Firefox Spidermonkey IonMonkey Spidermonkey Array.prototype.pop Type Confusion	CWE: 704 CVE: 2019-11707 GOOGLE: 1820	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 IonMonkey incorrectly predicts the return type of Array.Prototype.pop. This causes type confusion to occur which can result in remote code execution.
Strike HPE Intelligent Management Center IccSelectDevTypeBean an Expression Language Inject	CWE: 287 CVE: 2019-11941	This strike exploits a remote code execution 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.

Name	References	Description
Strike Belkin Wemo UPnP API SmartDevURL OS Command Injection	CWE: 78 CVE: 2019-12780 EXPLOITDB : 46436	This strike exploits a code injection vulnerability in the Belkin Wemo Crock-Pot UPnP API. Specifically it is possible for an attacker to inject code into the SmartDevURL parameter when sending a POST request to the listening basicevent1 service of the Belkin application. The attacker can perform this attack unauthenticated and execute code remotely on the vulnerable device.
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 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 Squid Proxy user_name and auth Reflected Cross-Site Scripting	CWE: 79 CVE: 2019-13345 BID: 109095	This strike exploits a cross-site scripting vulnerability in Squid Proxy. This vulnerability is due to inadequate input filtering of "user_name" 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 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.

Name	References	Description
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 WebAudio OfflineAudioContext Use After Free	CWE: 416 CVE: 2019-13720	This strike exploits a use-after-free vulnerability in the WebAudio component of Google Chrome. The vulnerability is due to incorrect handling of AudioContext objects in memory. A malicious attacker can exploit this vulnerability by creating a specially-crafted HTML page and convince the target user to access it using Chrome. Successful exploitation can potentially lead to remote code execution.
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.
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 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.

Name	References	Description
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.
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 Data Center Network Manager getConfigTemplateFileName 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 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 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 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 EPNM. 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 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.
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.

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 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 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 VMWare Fusion Guest VM Remote Code Execution	CWE: 20 CVE: 2019-5514 BID: 107637	This strike exploits a vulnerability in the VMWare fusion. The vulnerability is due to lack of access control under WebSocket service. An attacker could exploit this vulnerability by enticing the victim to click a malicious link and execute the malicious web page. Successful exploitation may lead to remote command execution on the guest virtual machine.
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 Google Chrome ExtensionsGuestViewMessageFilter Race Condition	CWE: 362 CVE: 2019-5796 GOOGLE: 1748	This strike exploits a vulnerability in Google Chrome. Specifically, the vulnerability exists when ExtensionsGuestViewMessageFilter is destroyed while concurrently modifying ProcessIdToFilterMap. When this happens a race condition will occur which can lead to a denial of service in the browser.

Name	References	Description
Strike Webkit CustomGetterSetter Type Confusion	CWE: 704 CVE: 2019-6215 GOOGLE: 1723 BID: 106691 EXPLOITDB : 46448	This strike exploits a vulnerability in Apple Safari Webkit. It is possible to craft Javascript in such a way that will cause type confusion to occur when using a CustomGetterSetter object linked to regExpConstructorInput. This can lead to a denial of service in the browser or potentially allow for remote code execution to occur.
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 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 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.
Strike Apple JavaScriptCore Out of Bounds Memory Access in FTL JIT	CWE: 119 CVE: 2019-8518 GOOGLE: 1775	This strike exploits a vulnerability in Apple Webkit JavaScriptCore. Specifically, the vulnerability exists during JIT compilation in FTL. It occurs when a loop-invariant code motion moves access to an array before a bounds check occurs. When this happens a denial of service condition, or potentially remote code execution, may occur.

Name	References	Description
Strike Apple JavaScriptCore CodeBlock Use-After-Free	CWE: 119 CVE: 2019-8558 GOOGLE: 1783	This strike exploits a vulnerability in Apple Webkit JavaScriptCore. Specifically, the vulnerability exists when a Watchpoint jettisons code that has already been freed. This causes a Use-After-Free condition to occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.
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.
Strike Apple Safari WebKit HTMLFrameElement Base isURLAllowed Subframe Overflow and Cross Origin Page Load	CVE: 2019-8762 GOOGLE: 1916	This strike exploits a vulnerability that exists inside Apple Safari Webkit. An attacker can insert frame elements with an empty URL into a node to overflow the subframe counter. When this node is later removed, the subframes won't be detached. The attacker can also make a subframe "survive" a cross-origin page load. It is possible for the new document to inherit the security context of its parent document, which can be an arbitrary cross-origin page, while the contents will be attacker-controlled.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apple Safari WebKit putInlineSlow and putToPrimitive Universal XSS	CWE: 79 CVE: 2019-8764 GOOGLE: 1914	This strike exploits a vulnerability in Apple Webkit. Specifically, an attacker can craft JavaScript in such a way that a cross-origin object can be placed into the prototype chain of a regular object and trigger the invocation of a cross-origin setter. If this causes an exception it can be potentially leaked allowing access to another window's function constructor and turning it into a UXSS attack.
Strike Apple Safari WebKit JavaScriptCore GetterSetter Type Confusion	CWE: 119 CVE: 2019-8765 GOOGLE: 1915	This strike exploits a vulnerability in Apple WebKit. Specifically, an attacker can craft JavaScript in such a way that when modifying the GetterSetter type confusion can occur leading to a denial of service in the browser.
Strike Apple Safari WebKit JavaScriptCore Argument Object Type Confusion	CWE: 119 CVE: 2019-8820 GOOGLE: 1924	This strike exploits a vulnerability in Apple WebKit. Specifically, an attacker can craft JavaScript in such a way that when reconstructing arguments objects type confusion can occur leading to a denial of service in the browser.
Strike Apple Safari WebKit Integer Overflow in NodeRareData m_connectedFrameCount	CWE: 119 CVE: 2019-8822 GOOGLE: 1919	This strike exploits a vulnerability in Apple Webkit. Specifically, an attacker can cause an integer overflow in NodeRareData::m_connectedFrameCount by inserting a large number of iframe elements into a DOM node that already has cached subframes. Doing this can cause type confusion to occur leading to a denial of service in the browser, and it can also lead to a UXSS attack.
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 strikes 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.

Name	References	Description
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.
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 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 SpiderMonkey IonMonkey Type Confusion	CWE: 704 CVE: 2019-9813 GOOGLE: 1810	This strike exploits a vulnerability in Mozilla Firefox. Specifically the vulnerability exists in the Javascript engine Spidermonkey. Inside SpiderMonkey, IonMonkey fails to detect changes properly when the ObjGroup is modified during a prototype change. This can lead to a denial of service or potentially allow for remote code execution to occur.

Name	References	Description
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 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 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 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 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.

Name	References	Description
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 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 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 Atlassian Jira Server and Data Center User Enumeration	CWE: 200 CVE: 2020-14181	This strike exploits an information disclosure vulnerability in Atlassian Jira Server and Data Center. The affected versions are before version 7.13.6, from version 8.0.0 before 8.5.7, and from version 8.6.0 before 8.12.0. An unauthenticated attacker could enumerate users using the /ViewUserHover.jspa endpoint, leading to information disclosure.
Strike Oracle WebLogic Server Remote Code Execution	CWE: 20 CVE: 2020-14882 EXPLOITDB : 48971	This strike exploits a remote code execution vulnerability in Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). The vulnerability is due to improper sanitization of user-supplied data sent via HTTP. 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.

Name	References	Description
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 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 Google Chrome JSPromise Fulfill Use After Free	CWE: 416 CVE: 2020-15994	This strike exploits a vulnerability in Google Chrome. Specifically, javascript can be crafted in such a way that when the JSPromise::Fulfill function is invoked it is possible that the FinishStream is not able to finish fulfilling the promise correctly allowing for memory corruption to occur. When this happens a denial of service condition, or potentially remote code execution, may occur.
Strike Google Chrome V8 Map Deprecation Leads to Type Confusion	CWE: 787 CVE: 2020-16009 GOOGLE: 2106	This strike exploits a vulnerability in Google Chrome. Specifically, javascript can be crafted in such a way that when several maps are created and type tagged, if one of the maps is deprecated when transitioning from the first tagged map to the second, type confusion can occur. When this happens a denial of service condition, or potentially remote code execution, may occur.
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.
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 vBulletin widget_tabbedcontent_iner_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.

Name	References	Description
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 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).
Strike Apache Subversion mod_authz_svn AuthzSVNReposRelativeAccessFile Null Pointer Dereference	CWE: 476 CVE: 2020-17525	This strike exploits a NULL Pointer Dereference vulnerability in the mod_authz_svn Apache HTTPD module of Apache Subversion. The vulnerability is due to improper handling of requests for non-existing repository URLs when the server is using in-repository authz rules with the AuthzSVNReposRelativeAccessFile option. A remote, unauthenticated attacker can exploit this vulnerability by sending a request to a non-existing repository which results in a crash of the HTTPD worker handling the request, leading to denial of service conditions. *NOTE: When running this strike in OneArm mode, the exploit will trigger only if the repository to which the request is sent to doesn't exist on the server. In the false-positive evasion, the strike sends a request to a repository named 'repo1' which is assumed to be pre-existing on the server.
Strike Apache Struts OGNL 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 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 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.

Name	References	Description
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 PHPMyAdmin SearchController SQL Injection	CWE: 89 CVE: 2020-26935	This strike exploits an sql injection vulnerability in phpMyAdmin. The vulnerability is due to a lack of escaping or input validation on the user-supplied input. A remote, authenticated attacker can exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could result in the execution of arbitrary SQL statement, potentially leading to the disclosure of sensitive information.
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.
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 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.

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 Apple Safari WebKit WebCore AudioArray Allocate Data Race	CWE: 362 CVE: 2020-3894 GOOGLE: 1999	This strike exploits a vulnerability in Apple Webkit. 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 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 Smtplib 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 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 Grandstream UCM6202 Remote SQL Injection	CWE: 89 CVE: 2020-5722 EXPLOITDB : 48247	Grandstream UCM6200 series is vulnerable to an unauthenticated remote SQL injection via a crafted HTTP request. A remote attacker can use this vulnerability to either execute shell commands under root privileges (on versions before 1.0.19.20) or inject HTML in password recovery emails (on versions before 1.0.20.17).
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.

Name	References	Description
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 ReadableStream Close Out of Bounds Memory Access	CWE: 119 CVE: 2020-6390 GOOGLE: 2001	This strike exploits a vulnerability in Google Chrome. Specifically, an attacker can craft JavaScript in such a way that when read_requests are modified from inside the accessor, the loop's iterator becomes invalid, and continuing to iterate through will cause out of bounds memory to be accessed. This can cause a denial of service condition in the browser or potentially lead to remote code execution.
Strike Google Chrome kJSCreate Type Confusion Code Execution	CWE: 843 CVE: 2020-6418	A type confusion vulnerability exists in V8 JavaScript engine in Google Chrome prior to 80.0.3987.122. The vulnerability may be triggered by changing array elements types (e.g. from SmallInteger to Double) after optimization takes place. By successfully exploiting this flaw, an attacker can execute arbitrary code in the context of the Chrome's 'renderer' process.
Strike Google Chrome USB OnServiceConnectio nError 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 Google Chrome WebIDBGetDBName sCallbacksImpl SuccessNamesAndVersionsList Use After Free	CWE: 416 CVE: 2020-6550 GOOGLE: 2067	This strike exploits a vulnerability in Google Chrome. Specifically, javascript can be crafted in such a way that an attacker can synchronously destroy the 'WebIDBGetDBNamesCallbacksImpl' object which can result in the access of freed memory. When this happens a denial of service condition, or potentially remote code execution, may occur.
Strike Google Chrome FocusedFrameChanged and NotifyFocusChange dObservers Use After Free	CWE: 416 CVE: 2020-6551 GOOGLE: 2069	This strike exploits a vulnerability in Google Chrome. Specifically, javascript can be crafted in such a way that the FocusedFrameChanged and NotifyFocusChangedObservers functions may invoke a user defined listener, which can cause an element to be added to sessions_ during iteration. This will invalidate the iterator, and can allow for a use after free condition to occur upon the next iteration. When this happens a denial of service condition, or potentially remote code execution, may occur.
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 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.
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.

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 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 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.
Strike Oracle iPlanet Web Server Information Disclosure	CWE: 326 CVE: 2020-9315	An information disclosure vulnerability exists in Oracle iPlanet Web Server versions 7.x and prior. By accessing specific paths related to the admin panel, a remote unauthenticated attacker may obtain sensitive information regarding server's configuration.
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 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.

Name	References	Description
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 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 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.
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 AttachmentUploadServer 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 random data in the "C://" directory depending on the variant.

Name	References	Description
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.
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 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 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 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.

Name	References	Description
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.
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.

Name	References	Description
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 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 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 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 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 Google Chrome V8 Remote Code Execution	CVE: 2021-30551 CWE: 843	This strike exploits a memory corruption vulnerability in Google Chrome browsers. The vulnerability is due to type confusion in the V8 engine. The vulnerability can be found in the SetPropertyInternal function due to an interceptor. 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 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.

Name	References	Description
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 Windows 10 MSHTML CTreePos Remote Code Execution	CVE: 2021-33742 CWE: 787	This strike exploits a remote code execution vulnerability in the Microsoft Internet Explorer. The vulnerability is due to insufficient input validation in the MSHTML CTreePos structure. An attacker could exploit this vulnerability by convincing a user to open a malformed HTML page, which could lead to remote code execution.
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.
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.

Name	References	Description
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 Nagios XI Post-auth command injection in watchguard wizard	CWE: 78 CVE: 2021-37346	This strike exploits an Command Injection vulnerability in Nagios XI versions prior to 5.8.5. This vulnerability is due to improper validation of the ip_address parameter in the watchguard wizard component. A remote authenticated 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: When running in one-arm mode file will be created in the /tmp/, in the directory specific to the apache service.
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 Google Chrome V8 Garbage Collector Remote Code Execution	CVE: 2021-37975 CWE: 416	This strike exploits a use-after-free vulnerability in Google Chrome browsers and causes the browser to crash. The vulnerability is due to a logic bug in the V8 garbage collector while handling ephemeralons. An attacker could exploit this vulnerability by convincing a user to open a malicious HTML page, which could lead to remote code execution.
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 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.

Name	References	Description
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.
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 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.
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 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.

Name	References	Description
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 StructuredDataMessage 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.
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 Google Chrome Safe Browsing OnReceivedThreatD OMDetails Use After Free	CWE: 416 CVE: 2022-0289 GOOGLE: 2251	This strike exploits a vulnerability in Google Chrome. Specifically, javascript can be crafted in such a way that when Safe Browsing flags a page the user visits and the DOM is processed a frame belonging to WebContents can be removed without notifying the object causing a Use After Free condition to occur. When this happens a denial of service condition, or potentially remote code execution, may occur.
Strike Google Chrome RequestThumbnail Buffer Overflow	CWE: 787 CVE: 2022-0306 GOOGLE: 2250	This strike exploits a vulnerability in Google Chrome. Specifically, the RequestThumbnail function does not properly validate the page_index parameter, which is used as an index within the pages_vector. Javascript can be crafted in such a way that when getThumbnail messages are called from an embedding page a buffer overflow will happen. When this happens a denial of service condition, or potentially remote code execution, may occur.
Strike Google Chrome UpdateAnimationTimingForAnimationFrame Use After Free	CWE: 416 CVE: 2022-0609 GOOGLE: 1296150	This strike exploits a vulnerability in Google Chrome. Specifically, in the anim0.finished.then() callback a new DocumentTimeline gets added to the current animation which has already been released, and when a document is scheduled in the UpdateAnimationTimingForAnimationFrame function a Use after Free condition occurs. When this happens a denial of service condition, or potentially remote code execution, may occur.
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.

Name	References	Description
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 OpenSSL c_rehash Command Injection	CVE: 2022-1292 CWE: 78	This strike exploits a vulnerability in OpenSSL. A vulnerability exists due to improper validation of shell metacharacters and will be triggered when the attacker entices the target user to parse malicious files, which allows command execution to occur in the context of the OpenSSL service.
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.
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 Cisco RV Series Routers Remote Code Execution	CWE: 787 CVE: 2022-20699	This strike exploits a remote code execution vulnerability in Cisco RV Series Routers. The vulnerability is due to Stack based buffer overflow in sslvpnd binary. A remote attacker can exploit this vulnerability by sending a crafted query to the target server. Successful exploitation could lead to remote code execution on the server. *NOTE: The strike attempts to create a reverse shell connection to a random IP and PORT.
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.

Name	References	Description
Strike Microsoft Windows http.sys HTTP protocol stack DOS	CWE: 119 CVE: 2022-21907	This strike exploits a vulnerability in the HTTP stack of Microsoft Windows in http.sys. The vulnerability is due to a logic flaw in the same. A remote unauthenticated attacker on the same network segment can exploit this vulnerability by sending a crafted HTTP packet. Successful exploitation can result in a crash of the target Windows Operating System.
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 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 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.

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 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 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 Google Chrome OnItemRemoved Heap Buffer Overflow	CWE: 787 CVE: 2022-2853 GOOGLE: 2342	This strike exploits a type confusion vulnerability in Google Chrome. Specifically, it is possible to cause a heap buffer overflow in the OnItemremoved function. When this happens a denial of service condition, or potentially remote code execution, may occur in the context of the browser process.
Strike Google Chrome LinkToTextMenuObserver CompleteWithError Use After Free	CWE: 416 CVE: 2022-2998 GOOGLE: 2300	This strike exploits a vulnerability in Google Chrome. Specifically, LinkToTextMenuObserver holds a pointer to a RenderFrameHost object, but does not properly observe when FrameHost destruction events occur. Because of this, if an attacker manages to craft javascript in such a way that will destroy the frame host at the right time, a use after free condition can occur in LinkToTextMenuObserver::CompleteWithError. When this happens a denial of service condition, or potentially remote code execution, may occur.
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.

Name	References	Description
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.
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 Sophos Firewall User Portal and Webadmin Code Injection Vulnerability	CWE: 74 CVE: 2022-3236	This strike exploits a Code Injection Vulnerability in Sophos Firewall. This vulnerability is due to improper validation of JSON keys submitted 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 remote code execution with privileges of the root user. *NOTE: While running this strike in one-arm mode, four files Test1, Test2, Test3 and Test4 will be created in the /tmp/ directory of the server.
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 vulnerability in Django. The vulnerabilities are due to insufficient sanitization of user input to kind and lookup_name parameter 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.

Name	References	Description
Strike Teclib GLPI Remote Code Execution Vulnerability	CVE: 2022-35914 CWE: 74	This strike exploits a code injection vulnerability in GLPI. The vulnerability is due to improper validation of user configuration data sent to the endpoint htmLawedTest.php. 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 in the security context of the web server process. *NOTE: While running this strike in OneArm mode, a file /tmp/poc is created on the server.
Strike Google Chrome PerformLayout Use After Free	CWE: 416 CVE: 2022-3654	This strike exploits a vulnerability in Google Chrome. Specifically, it is possible when placing elements into a container and making a call to PerformLayout to trigger a use after free condition. When this happens a denial of service or potentially remote code execution, may occur.
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 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.
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 an attacker bypassing authentication and executing commands as an admin user on the target system.
Strike Google Chrome Synchronous Mojo Messages Use After Free	CWE: 416 CVE: 2022-4178	This strike exploits a vulnerability in Google Chrome. Specifically a message handler called from a synchronous message might destroy an object referenced by a local variable somewhere up the stack. When the reply to the outbound message is received, the execution returns to the stack \${frame} with the dangling pointer and a UAF will occur. This can potentially allow for remote code execution to occur in the context of the browser.
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.

Name	References	Description
Strike Apple Safari Webkit RenderMathML Use After Free	CWE: 416 CVE: 2022-42867 GOOGLE: 2362	This strike exploits a vulnerability in Apple Safari Webkit. Specifically, a vulnerability inside Webkit allows for a dangling pointer to the RenderMathML object to exist. It is possible to craft javascript in such a way that when the crossfadeChanged function is accessed a use after free condition can occur. When this happens a denial of service condition, or potentially remote code execution, may occur.
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 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 Cacti remote_agent php Command Injection	CWE: 78 CVE: 2022-46169	This strike exploits a command injection and IP restriction bypass vulnerability in Cacti. The vulnerability is due to an access control weakness and insufficient validation of user data when receiving requests from Cacti pollers. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could lead to arbitrary command execution in the security context of the web server running the application. *NOTE: In one-arm mode, the strike creates a random file in the /tmp folder of the server.
Strike Zoho ManageEngine Multiple Products SAMLResponse Remote Code Execution	CWE: 94 CVE: 2022-47966	This strike exploits a remote code execution vulnerability in multiple Zoho ManageEngine products. The vulnerability is due to an outdated version of Apache Santuario in the impacted products allowing an attacker to execute XSLT in SAML response messages. 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 SYSTEM. *NOTE: Although the strike simulates the attack on endpoints /SamlResponseServlet, /saml2 running on server port 7272, it can vary depending on the ManageEngine product under attack.
Strike Google Chrome BuildElementAccess copy-on-write Safety Bypass	CWE: 787 CVE: 2022-4906	This strike exploits a vulnerability in Google Chrome. Specifically, javascript can be crafted in such a way that the V8 engine's copy-on-write safety can be bypassed when making a call to BuildElementAccess. When this happens a denial of service condition, or potentially remote code execution, may occur.

Name	References	Description
Strike Fortra Goanywhere MFT LicenseResponseServlet Insecure Deserialization	CWE: 502 CVE: 2023-0669	This strike exploits an insecure deserialization vulnerability in Fortra GoAnywhere MFT. The vulnerability is due to insufficient validation of user-supplied data sent to the License Response Servlet exposed on the administrative interface. The attacker submits a request to the License Response Servlet running on the target server containing an encoded and encrypted crafted serialized object. A remote, unauthenticated attacker could exploit the vulnerability by sending crafted requests to the target server. Successful exploitation can result in arbitrary code execution under the security context of SYSTEM or 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 Samsung Galaxy AppStore Javascript Execution	CWE: 20 CVE: 2023-21434	This strike exploits a JavaScript execution vulnerability in the Samsung Galaxy App store. The vulnerability is due to insufficient input validation in the 'com.sec.android.app.samsungapps.deeplink.CloudGameDeepLink' class of the app. This can be exploited both remotely and locally. A remote attacker can serve a malicious web page containing the malicious Intent URI call which if the victim clicks leads to opening of the galaxy store app which can then lead to execution of arbitrary JavaScript pulled from an attacker controlled domain. Locally any installed rogue application can do the same by triggering the same intent call from within the app. *NOTE : This strike covers the remote version of the attack where a server sends a HTML file containing the malicious intent call.
Strike Google Chrome JObject Origin Trials Access	CWE: 843 CVE: 2023-2724 GOOGLE: 2444	This strike exploits a vulnerability in Google Chrome. Specifically, it is possible to extend a non configurable JObject via an Origin Trial. When this happens a denial of service condition, or potentially remote code execution, may occur in the context of the browser process.
Strike Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	CVE: 2023-27997 CWE: 787	This strike exploits a heap based buffer overflow vulnerability in Fortinet FortiOS and FortiProxy. The vulnerability exploits the possibility of redirecting the execution flow in FortiGate SSL-VPN by sending a specially crafted payload whose size is not properly checked and which would corrupt the heap memory area of the device. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation of this vulnerability could result in remote code execution or denial of service.

Name	References	Description
Strike Gitlab Arbitrary File Read Directory Traversal	CWE: 22 CVE: 2023-2825	This strike exploits a directory traversal vulnerability in GitLab Community and Enterprise Editions. The vulnerability is due to improper validation of file names requested by users on the server. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to a vulnerable public Gitlab server hosting projects with nested subgroups. Successful exploitation results in the disclosure of files on the target server. The number of directories traversed by the attacker depends on the number of subgroups of the project. *NOTE: In one-arm mode, the strike sends a malicious request with the project name 'sampleproject' to a specific path and fetches the file /etc/passwd from the server.
Strike Google Chrome SetPropertyWithAccessor Type Confusion	CWE: 843 CVE: 2023-2935 GOOGLE: 2448	This strike exploits a vulnerability in Google Chrome. It is possible to craft Javascript in such a way that an attacker can control the value of an AccessorPair object. When this happens a denial of service condition, or potentially remote code execution, may occur in the context of the browser process.
Strike Google Chrome Non-Extensible Object Type Confusion	CWE: 843 CVE: 2023-2936 GOOGLE: 2450	This strike exploits a type confusion vulnerability in Google Chrome. Specifically, in v8 JSObject doesn't check if the receiver is extensible before adding a new property. This may allow an attacker to extend a non-extensible object. When this happens a denial of service condition, or potentially remote code execution, may occur in the context of the browser process.
Strike Google Chrome OpenXrApiWrapper Use After Free	CWE: 416 CVE: 2023-3217 GOOGLE: 2458	This strike exploits a type confusion vulnerability in Google Chrome. Specifically, when using an attached VR headset it is possible to trigger a use after free condition by requesting two immersive VR sessions. When this happens a denial of service condition, or potentially remote code execution, may occur in the context of the browser process.
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.
Strike Ivanti Endpoint Manager Mobile Authentication Bypass	CWE: 287 CVE: 2023-35078	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 restricted functionality or resources without proper authentication, including creating an administrative account that can make further changes to the target server.

Name	References	Description
Strike Citrix ADC formsso Remote Code Execution	CWE: 94 CVE: 2023-3519	A remote code execution vulnerability exists in Citrix Application Delivery Controller (ADC). The remote code execution is possible using a buffer overflow vulnerability, due to improper sanitization of HTTP request path. The flaw may be exploited by an unauthenticated attacker to execute arbitrary commands on the target server.
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	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 Cacti Group graph_view.php SQL Injection Vulnerability	CWE: 89 CVE: 2023-39361	This strike exploits a directory traversal vulnerability in VMware Aria Operations for Networks. 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 Google Chrome Read-Only TruboFan Property Overwrite	CWE: 843 CVE: 2023-4352 GOOGLE: 2460	This strike exploits a type confusion vulnerability in Google Chrome. Specifically, it is possible to overwrite read-only properties that can then be compiled by Turbofan. When this happens a denial of service condition, or potentially remote code execution, may occur in the context of the browser process.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cybozu grn.exe-todo-view tid Parameter SQL Injection	CVE: 2006-4444 BID: 19731	This strike exploits a SQL injection flaw in the Cybozu web application.
Strike Cybozu grn.exe-todo-modify tid Parameter SQL Injection	CVE: 2006-4444 BID: 19731	This strike exploits a SQL injection flaw in the Cybozu web application.
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.
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 Cyme ChartFX ActiveX Control Array Indexing Vulnerability		This strike exploits an indexing vulnerability in Cyme ChartFX activeX control Cfx62ClientServer.Chart. The page number parameter of the ShowPropertiesDialog method is not properly validated, and it gets used in a pointer calculation which is then later used in a memory write operation.
Strike Darkside Ransomware May 2021 Campaign - Darkside Command and Control		This strike simulates the 'Darkside Ransomware May 2021 Campaign - Darkside Command and Control' traffic that occurs after executing the Darkside Ransomware.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
Strike Dell KACE K1000 krashrpt 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/krashrpt.php', a remote unauthenticated attacker may execute arbitrary OS commands as the user 'www'.
Strike DivX Plus Web Player Buffer Overflow		This strike exploits a vulnerability in DivX Plus Web Player. The vulnerable object does not properly validate the length of the sourced media parameter. If this value is too large a buffer will overflow potentially allowing for remote code execution.
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 http://IP_ADDR/tools_firmw.htm. 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).

<b>Name</b>	<b>References</b>	<b>Description</b>
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 D-link Wireless N300 Router CAPCHA Code Execution		This strike exploits a vulnerability in D-Link Wireless N300 Router's web interface which listens on port 80. A buffer overflow in CAPCHA processing allows for remote code execution (note: processor is MIPS-based)
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Doms Httpd Denial of Service		This Strike exploits a denial of service vulnerability in Doms Httpd when sending a crafted POST request with an overly large amount of data in the referer header.
Strike Dridex May 2020 Malware Campaign - Command and Control		This strike simulates the 'Dridex May 2020 Malware Campaign - Command and Control' traffic that occurs after executing the Dridex malware executable. 1. The victim sends an HTTP GET request, and the attacker replies with base64 encoded data and some unknown data. The base64 encoded data includes the CNC IP address and a future file to retrieve. 2. The victim sends an HTTP GET request with only the base64 encoded data, and the attacker replies with a ZIP file that includes a malicious VBS file. 3. The victim sends an HTTP POST request with binary data, and the attacker replies with an HTTP code 502. This sequence occurs 2 times.
Strike Easy File Sharing HTTP Server Buffer Overflow	EXPLOITDB : 39661 EXPLOITDB : 39008	This strike exploits a vulnerability in Easy File Sharing Server v7.2. Specifically a buffer overflow occurs when sending a large amount of data in an http request to the target server allowing us to overwrite the SEH record. This strike chooses between 2 different attack vectors that both target the same vulnerable web server. This is an unauthenticated attack that leads to remote code execution for both attack vectors.
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 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 EBCRYPT Active X Denial of Service	BID: 25787 CWE: 22 CVE: 2007-5110	This strike exploits an arbitrary file write flaw in the EBCrypt ActiveX control.
Strike FLIR AX8 Thermal Camera Arbitrary File Disclosure	EXPLOITDB : 45597	This strike exploits a directory traversal vulnerability in FLIR AX8 Thermal Camera. The vulnerability is due to lack of input sanitization while downloading config files using the 'file' parameter in download.php. Successful exploitation results in the disclosure of arbitrary file contents from the target server.
Strike Edraw Diagram Component ActiveX control Buffer Overflow		This strike exploits a buffer overflow vulnerability in Edraw Diagram's activeX controla EDBoardLib.EDBoard. If an overly large value is passed to the LicenseName method a buffer will overflow allowing for the possiblity of remote code execution.
Strike Eir D1000 Modem CWMP Command Injection	EXPLOITDB : 40740	This strike exploits a code-injection vulnerability in Eir D1000 Modems. The vulnerability is due to failure to sanitize supplied values inside SOAP requests. By crafting a SOAP message, a remote unauthenticated attacker could execute arbitrary code on the target system.
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 EMC ApplicationXtender ActiveX control Buffer Overflow	CWE: 119 CVE: 2012-2515 BID: 36546	This strike exploits a stack buffer overflow vulnerability inside KeyWorks KeyHelp Activex control which comes with EMC's ApplicationXtender. If the JumpURL method is passed an overly large string a buffer is overrun.
Strike Emotet Dec 2021 Campaign - Emotet Command and Control		This strike simulates the Command and Control traffic that occurs after executing the Emotet malware.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Exodesk PHP Desk faq.php id Parameter SQL Injection (Default)	CVE: 2007-0676 BID: 22338	This strike exploits a SQL injection vulnerability in the Exodesk PHP Desk web application.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Explorer WMF Unspecified DoS	BID: 22715  CVE: 2007-1090	This strike exploits a denial of service flaw in the Windows Explorer using a corrupted WMF file.
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.
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.

Name	References	Description
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 nsTextFrame ClearTextRun() Remote Memory Corruption	CWE: 399 CVE: 2009-1313 BID: 34743	This strike exploits a flaw in Mozilla Firefox's handling of certain types of text objects.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 Foxit Reader Plugin URL Buffer Overflow		This strike identifies a vulnerability in the latest version of the foxit reader plugin available for mozilla firefox. The software does not properly validate the input into the url field. A 260 byte buffer is allocated, and any input over this amount will overflow the buffer. To observe this exploit you must create a pdf named test, and store it in the same directory as the html page.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Hyphenated URL Exploit	BID: 14784  CVE: 2005-2871	This strike exploits a flaw in Firefox that is triggered by a hostname in a URL that is all soft hyphens.
Strike Mozilla Firefox-Thunderbird- SeaMonkey Javscript 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 Memory Corruption (Array.toSource)	CWE: 189  CVE: 2006-3806  BID: 19181	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript code that calls toSource() on a javascript array.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
Strike Mozilla Firefox Javascript Engine Memory Corruption (Object.toSource)	CWE: 189 CVE: 2006-3806 BID: 19181	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript code that calls toSource() on a javascript object.
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 Javascript Engine Memory Corruption (String.toSource)	CWE: 189 CVE: 2006-3806 BID: 19181	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript code that calls toSource() on a javascript string.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Mozilla Firefox Event Handler Privilege Escalation	CVE: 2007-3737 BID: 24946	This strike exploits a priviledge 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.
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.method.eval Variant 2	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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Mozilla Firefox Javascript XBL Compilation Scope Access Variant 3	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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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
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

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.
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 programmatically 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Flexense DiskPulse Enterprise Server Stack Buffer Overflow	EXPLOITDB : 42560	This strike exploits a Stack Buffer Overflow vulnerability in Flexense DiskPulse Enterprise Server. The vulnerability is due improper length validation of user controlled request URI. By exploiting this vulnerability, an attacker could execute arbitrary code in the security context of SYSTEM. NOTE: Strike will launch calc.exe when run in OneArm mode. Verified against Flexense DiskPulse Enterprise v9.9.16 32bit running on Windows 7 x86 with DEP disabled.
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.
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 Forum Livre info_user.asp user Parameter SQL Injection	CVE: 2007-0589 BID: 22246	This strike exploits a SQL injection 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
Strike GDIPlus 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 GDIPlus image library. This strike simulates downloading a JPEG via HTTP.
Strike Microsoft GdiPlus.dll EMF GpFont SetData Stack Overflow (HTTP)		This strike triggers a denial of service flaw in Microsoft Windows GdiPlus.dll when rendering malformed EMF files.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike geoBlog viewcat.php cat Parameter SQL Injection	CWE: 89 CVE: 2006-0249 BID: 16249	This strike exploits a SQL injection flaw in the geoBlog web application.
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 Goahead Webserver HTTP Request Denial of Service		This strike identifies a vulnerability in Embedthis Goahead Webserver. When receiving a malformed HTTP GET request a denial of service condition can be forced.
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 Google Chrome NewFixedDoubleArray Integer Overflow		This strike replicates an integer overflow exploit for Chrome browser engine. The vulnerability can be triggered via the Array JS API by using the 'ArrayConcat' or 'ArrayPrototypeFill' as entry points. By successfully exploiting this flaw, an attacker can execute arbitrary code in the context of the Chrome's 'renderer' process.
Strike XSS Filter Bypass Vulnerability In Google Chrome		This strike exploits a cross-site scripting (XSS) vulnerability in Google Chrome. The vulnerability is due to improper filtering of script tags. An attacker could exploit this vulnerability in order to obtain sensitive information.
Strike XSSAuditor Policy ByPass Vulnerability Inside Google Chrome		This strike exploits a policy bypass vulnerability inside Google Chrome. The vulnerability is due to improper filtering of script tags inside svg tags. An attacker could exploit this vulnerability in order to obtain sensitive information.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 July 2021 Campaign - Cobalt Strike Command and Control		This strike simulates the 'Hancitor July 2021 Campaign - Cobalt Strike Command and Control' traffic that occurs after executing the Cobalt Strike stagers.
Strike Hancitor July 2021 Campaign - Hancitor Command and Control		This strike simulates the 'Hancitor July 2021 Campaign - Hancitor Command and Control' traffic that occurs after executing the Hancitor malware.
Strike Hancitor Malware April 2020 Campaign Command and Control Data Exfiltration		This strikes 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 ALM ActiveX Overwrite		This strike exploits a HP ALM's XGO ActiveX control arbitrary file overwrite vulnerability which is due to bad input sanitization. Remote attackers may do arbitrary code execution on the target system.
Strike HP data protector signinname Denial of service	BID: 44381	This strike exploits a DOS vulnerability in HP datai protector media operations. This vulnerability is due to bad check the length of the signinname. Remote attackers may do denial of service attack on the target system.
Strike HP Intelligent Management Center disclosure information		This strike exploits a policy bypass vulnerability presents in the HP Intelligent Management Center. The vulnerability is due to insufficient validation of configuration files requests The remote attacker may disclosure the information in the target system.
Strike HP Openview Network Node Manager OpenView5.exe Action Parameter Buffer Overflow	CWE: 119 CVE: 2008-0067 BID: 33147	This strike exploits a stack buffer overflow vulnerability in HP OpenView Network Node Manager 7.53 that occurs when processing the CGI parameter Action on an HTTP GET request.
Strike HP OpenView Network Node Manager ovalarm.exe CGI Buffer Overflow	CWE: 119 CVE: 2009-4179 BID: 37347	This strike sends a malicious Accept-Language header value that will trigger a buffer overflow condition in the ovalarm.exe module of vulnerable installations of HP OpenView Network Node Manager web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 de.php 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 fr.php 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 loadcatnews.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 motd.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 mod.news.php3 HPEinc Parameter PHP File Include Variant 1	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 mod.newslog.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 news.htmlnews.php3 HPEinc Parameter PHP File Include Variant 1	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 news.xmlbi.php3 HPEinc Parameter PHP File Include Variant 1	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 news.xmlphp.php3 HPEinc Parameter PHP File Include Variant 1	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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Headline Portal Engine page.dmoz.show.php3 HPEinc Parameter PHP File Include Variant 1	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 1	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 mod.news.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 Headline Portal Engine news.htmlnews.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 Headline Portal Engine news.xmlbi.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 Headline Portal Engine news.xmlphp.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 Headline Portal Engine page.dmoz.show.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 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 page.randnews.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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Headline Portal Engine page.teaser.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 mod.news.php3 HPEinc Parameter PHP File Include Variant 3	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 news.htmlnews.php3 HPEinc Parameter PHP File Include Variant 3	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 news.xmlbi.php3 HPEinc Parameter PHP File Include Variant 24	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 news.xmlphp.php3 HPEinc Parameter PHP File Include Variant 3	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 page.dmoz.show.php3 HPEinc Parameter PHP File Include Variant 3	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 HttpdASM Directory Traversal		A directory traversal vulnerability exists in httpdASM v0.92 that allows a user to bypass restrictions and download arbitrary files outside the context of webroot.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 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 Apr 2021 Campaign - IcedID Command and Control		This strike simulates the 'IcedID Apr 2021 Campaign - IcedID Command and Control' traffic that occurs after executing the IcedID malware.
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 IcedID Command and Control		This strike simulates the 'IcedID Command and Control' traffic that occurs after executing the IcedID malware. The malware sends a GET request to the malicious carismorth C2 server and receives a 401 NOT FOUND HTML page in response. This server can then send further commands such as downloading additional 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike IDAutomation PDF SaveBarcode ActiveX Arbitrary File Write		This strike exploits an arbitrary file write vulnerability in the IDAutomation Aztec ActiveX control.
Strike IDAutomation PDF SaveEnhWMF 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.
Strike Use-after-free vulnerability in the CMshtmlEd Exec function in mshtml.dll in Microsoft Internet Explorer 6-9	CVE: 2012-4969	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer 6, 7, 8 and 9 allowing arbitrary code execution to a remote attacker via a specially-crafted website.
Strike IE6-7 Frame[FrameBorder] Denial Of Service Memory Corruption		This strike exploits stack overflow and memory corruption on IE6/7 due to improper handling of the frame[frameborder] property resulting in denial of service and possible code execution.
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 CSS style memory corruption	CWE: 399 CVE: 2009-0076	This strike exploits a memory corruption vulnerability in Microsoft IE, that is due to improper type checking when handling an object pointer in a CSS strict XHTML mode.
Strike Microsoft Internet Explorer VML use after free	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.

Name	References	Description
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 BGSOUND 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 BGSOUND element with a long local file name specified as the source.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Internet Explorer Object.Microsoft.DX TFilter.Enabled DoS		This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the Object.Microsoft.DXTFilter 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 Microsoft Internet Explorer Event Handler Memory Corruption	CWE: 399 CVE: 2009-1530	This strike exploits a memory corruption vulnerability in the way Microsoft Internet Explorer handles specific DHTML objects. This can be seen when calling an event handler several times while the HTML document is being modified.
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.
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 Microsoft Internet Explorer Get Cell Index Information Disclosure		This strike exploits a vulnerability in Microsoft's Internet Explorer where some contents of memory can be leaked and that leakage can lead to an attacker finding a way around memory protection.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer HtmlDlgSafeHelper. HtmlDlgSafeHelper. f onts 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 ipeers.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 mdauth.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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 JPEG Processing DoS (Random)	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 IE6 MSAgent Memory Corruption	CWE: 189 CVE: 2006-3445 BID: 21034	This strike exploits a flaw in the Character::Speak method contained within Microsoft Agent for Windows 2000
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 Microsoft Internet Explorer onreadystatechange event use after free with iframe	CWE: 94 CVE: 2012-0170 BID: 52904	This strike exploits a user after free vulnerability in Microsoft Internet Explorer. This can be seen when the onreadystatechange event tries to access script from inside an iframe after the object or data has been destroyed.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<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 iLife Photocast XML Title Format String Variant 2	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 sends traffic that differs randomly from the original POC.
Strike Imperva SecureSphere Remote Command Execution		This strike exploits a remote command execution in Imperva SecureSphere Web Application Firewall. The vulnerability resides in the lack of sanitization of the 'installer-address' parameter when the server status is being queried. By exploiting this flaw, an attacker will be able to execute commands as the root user on the host system.
Strike Indusoft ThinClient ActiveX Control Initialize2 Method Buffer Overflow		This strike identifies a vulnerability in an Indusoft ThinClient ActiveX control. The Initialize2 method does not properly validate its arguments. If a malicious or overly large string size is used and exceeds the limit of the buffer, an overflow will occur allowing for remote code to be executed.
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

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer Global Mouse Tracking		This strike exploits a flaw in Internet Explorer 6 - 10 that allows any page (any frame on any tab) to globally track mouse position and certain keys. Affected properties of the Event object are: altKey, altLeft, clientX, clientY, ctrlKey, ctrlLeft, offsetX, offsetY, screenX, screenY, shiftKey, shiftLeft, x and y.
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 Microsoft IIS .httr ISAPI Buffer Overflow	CVE: 2002-0071 BID: 4474	This strike exploits a buffer overflow in the HTR ISAPI filter of Microsoft IIS versions 4.0 and 5.0.
Strike Microsoft IIS .httr 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 URL Access Violation DoS	CVE: 2002-0072 BID: 4479	This strike exploits a DoS bug in Microsoft IIS versions 4.0, 5.0 and 5.1.
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

Name	References	Description
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 iTunes PLS File Remote Code Execution	CWE: 119 CVE: 2009-2817 BID: 36478	This strike exploits a vulnerability in the parsing of PLS files that can result in the execution of arbitrary code
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 Sun Java Plugin JNLP Codebase Buffer Overflow	CWE: 119 CVE: 2007-3655 BID: 24832	This strike exploits a buffer overflow flaw in the Sun Java plugin that allows arbitrary code execution through malicious JNLP files.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 component JE Photo Gallery SQL Injection	EXPLOITDB : 45930	This strike exploits a SQL injection vulnerability in the JE Photo Gallery component 1.1 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 component Jimtawl SQL Injection	EXPLOITDB : 45524	This strike exploits a SQL injection vulnerability in the Jimtawl component 2.2.7 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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Lingxia ICE CMS media.cfm session.user_id Parameter SQL Injection Vulnerability	CWE: 89 CVE: 2011-1055 BID: 46373	This strike exploits a SQL injection flaw in Lingxia's I.C.E CMS 1.0 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.
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

<b>Name</b>	<b>References</b>	<b>Description</b>
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 LokiBot Oct 2017 Malware Campaign - HTA File Transfer		This strike simulates download of a malicious .hta file in the 'LokiBot Oct 2017 Malware Campaign' via an HTTP request. The traffic occurs after executing the Word attachment from the phishing email. .hta file is often downloaded by pre-stage malware, such as embedded-macro word-files or distributed via 'LokiBot malware campaign phishing email'.
Strike LooCipher Nov 2020 Campaign - LooCipher Command and Control		This strike simulates the 'LooCipher Nov 2020 Campaign - LooCipher Command and Control' traffic that occurs after executing the LooCipher ransomware.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Macromedia JRun Remote SYSTEM Buffer Overflow	CVE: 2002-1310 BID: 6122	This strike exploits a remote buffer overflow in the Macromedia JRun 4.0 IIS ISAPI handler.
Strike Macromedia JRun 4 Web Server URL Parsing Stack Overflow	CVE: 2005-4472 BID: 15905 BID: 16026	This strike exploits a stack overflow in Macromedia JRun 4's Web Server Component when handling overly-long request URLs.
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 (PlayerVersion)		This strike exploits a stack overflow in an ActiveX control in Macromedia Shockwave 11.5.1.601'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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

Name	References	Description
Strike Magento Core Mysql.php-synchronize Unauthenticated SQL Injection		This strike emulates a SQL injection attack on Magento e-commerce platform. The vulnerable code resides in 'vendor/magento/framework/DB/Adapter/Pdo/Mysql.php' and the flaw is due to the way the request parameters are parsed. By exploiting the '/catalog/product_frontend_action/synchronize' endpoint, a remote unauthenticated attacker could access the database and even leverage the vulnerability to obtain administrator privileges and remote code execution.
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.
Strike MagnetoSoft NetResources NetFileClose ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft NetResources NetFileClose ActiveX Control.
Strike MagnetoSoft NetResources NetSessionDel ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft NetResources NetSessionDel ActiveX Control.
Strike MagnetoSoft NetResources NetShareEnum ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft NetResources NetShareEnum ActiveX Control.
Strike MagnetoSoft SNTP SntpGetReply ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft SNTP SntpGetReply ActiveX Control.
Strike MagnetoSoft SNTP SntpSendRequest ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft SNTP SntpSendRequest ActiveX Control.
Strike Magniber Ransomware Aug 2021 Campaign - Command and Control		This strike simulates the 'Magniber Ransomware Aug 2021 Campaign - Command and Control' traffic that occurs after executing the Magniber Ransomware.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Malformed AU File Divide-by-Zero Denial of Service (HTTP)		This strike exploits a denial of service flaw in programs that handle .au files without detecting a divide-by-zero condition
Strike Microsoft IIS Malformed File Extension	BID: 1190	This strike attempts to crash IIS by sending a malformed request.
Strike Operation Quicksand Nov 2020 Campaign - PowGoop Malware File Transfer	MD5: 1d6f241798 818e6fdc03 015d01e1e6 80  SHA1: 0984f359c1 f8c85da5a0 662448a4fe dab4c524e5  SHA256: b154d3fd88 767776b1e3 6113c479ef 3487ceda0f 6e4fc80cef8 5ba539a589 555	This strike simulates the download of the PowGoop malware via an HTTP GET request.
Strike Crimson RAT Dec 2020 Campaign - Crimson Malware File Transfer	MD5: 18acd5ebe d316061f88 5f54f82f000 17  SHA1: 0cb5e5d0b9 5589fb59b7 42413e9ac5 610e79a83d  SHA256: 2de20700d9 43981ad1b db2f6b4d03 b7c65633c1 a7e1bc504 ba20ec5f41 7eb69b	This strike simulates the download of the 'Crimson RAT Dec 2020 Campaign - Crimson Malware' via an HTTP GET request.

Name	References	Description
Strike Raccoon Sep 2020 Campaign - Raccoon Malware File Transfer	MD5: 8dbab4018 a4cfb8c40d 67df913fb0 ed5  SHA1: 0db8ab2d54 205ec35a05 8ce312e101 5a0247b2ff  SHA256: 8ee70efcf5 51614fa18b e3b913497 ee9c46fb1f3 d5dcc855c4 1c102f0ea8 db0	This strike simulates the download of the Raccoon malware via an HTTP GET request.
Strike Emotet August 2020 Campaign - Word Document Malware File Transfer	MD5: 9d6025d316 72fc5ee775 9164354c02 ee  SHA1: 876c29a8d d6ceefa063 3a5f651e11 1cbcd13457 d  SHA256: b06fa4a032 74712b0d1 bea0d2a5d1 afc2c71541 acb80b1054 d31b661b67 514ea	This strike simulates the download of the 'Emotet August 2020 Campaign - Word Document' via an HTTP GET request.

Name	References	Description
Strike APT-29 July 2020 Campaign - SoreFang Malware File Transfer	MD5: 967fcf18563 4def5177f74 b0f703bdc0  SHA1: 152189b62 c546d6297 a7083778fb a62dcec576 be  SHA256: 58d8e65976 b53b77645 c248bfa18c 3b87a6ecfb 02f306fe6b a4944db96 a5ede2	This strike simulates the download of the APT-29 SoreFang via an HTTP GET request.
Strike LooCipher Nov 2020 Campaign - Word Malware File Transfer	MD5: 868a06468 b0eb6d5e97 77681a0cb2 afe  SHA1: 2551e34c72 e928f615ae ba3b7c2a09 9b3adcb84e  SHA256: e824650b66 c5cdd8c719 83f4c4fc0e1 ac55cd0480 9d562f3b6b 4790a28521 486	This strike simulates the download of the Word malware via an HTTP GET request.

Name	References	Description
Strike RIG EK GandCrab Oct 2020 Campaign - GandCrab Malware File Transfer	MD5: c3c68834fd 88af33c075 4a6e782124 23  SHA1: 36164eee39 cbb47247c5 fff3e1788f7 e80993943  SHA256: 77bc25af79 82bd07ec40 813ed81f2f3 afb4978e07 cb875efa35 61ff2f4ed34 df	This strike simulates the download of the encrypted GandCrab malware via an HTTP GET request.
Strike IcedID Dec 2020 Campaign - IcedID Malware File Transfer	MD5: 8dccd1c176 f6b855e1a6 0b710d38a9 e4  SHA1: 3b72fecbab d585947cd9 cf4b5d9c37 95ab798d39  SHA256: 6610a12184 a15e0fe2f3 c8d2f730aa 7a4497386 a10487138 cfe1e019ec 3f1f2a	This strike simulates the download of the 'IcedID Dec 2020 Campaign Campaign - IcedID Malware' via an HTTP GET request.

Name	References	Description
Strike Winnti ShadowPad Oct 2020 Campaign - Bisonal Malware File Transfer	MD5: 5e25dfdf79 dfc0542a2d b424b11968 94  SHA1: 3bf3cd0f381 7cf9481944 536c0c65d8 a809e6d4a  SHA256: e114dd78f9 acacf7e93 efe1c9e68a 29e4fe52c4 830431a4a a5457927b ef7c5e	This strike simulates the download of the Bisonal malware via an HTTP GET request.
Strike IcedID Dec 2020 Campaign - PNG First Payload Malware File Transfer	MD5: fb37d9c08f4 0c97c2f715 e2b2ba0f3e 6  SHA1: 452bea5697 110ad1bf86 a3759ff00b0 8603d4a78  SHA256: e0f454e9d9 bae4843a55 bacafdf53a1 131debd9cd 795c489131 71edfb946b 9325	This strike simulates the download of the 'IcedID Dec 2020 Campaign Campaign - PNG First Payload' via an HTTP GET request.

Name	References	Description
Strike Winnti ShadowPad Oct 2020 Campaign - ShadowPad Malware File Transfer	MD5: 82118134e6 74fe403907 c9b93c4dc7 be  SHA1: 5e29d9e4b e79b5d1d7 e606ba59a9 10cdd84020 3b  SHA256: 2c2b1d9b34 df9364fd91 a6551890b0 fdc58a7e68 1713c68222 1a674d1116 089a	This strike simulates the download of the ShadowPad malware via an HTTP GET request.
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.

Name	References	Description
Strike Maze Apr 2020 Campaign - Maze Malware File Transfer	MD5: 21a563f958 b73d453ad9 1e251b1185 5c  SHA1: 64ed4f6b31 5448d518e d003a1d0c7 e56790ef50 d  SHA256: 067f1b8f1e0 b2bfe286f51 69e17834e8 cf7f4266b8 d97f28ea78 995dc81b0 e7b	This strike simulates the download of the Maze ransomware via an HTTP GET request.
Strike IcedID Dec 2020 Campaign - Word Malware File Transfer	MD5: 98ec9df625 4d78b1fc1a bdf7090da3 f7  SHA1: 6642cb5d47 4a9ed788fb 5a33cc5b72 c6f825c1f3  SHA256: 37db367c01 e40ee2f05a 5966d6670 e07fd3292c 01f4da8ffd7 7c0e3c96a7 9464	This strike simulates the download of the 'IcedID Dec 2020 Campaign Campaign - Word Malware' via an HTTP GET request.

Name	References	Description
Strike Crimson RAT Dec 2020 Campaign - Word Malware File Transfer	MD5: 8c58a7d516 b371722f26 d7270a76b5 67  SHA1: 6aa88102bf c2d244ed99 95067a2a97 fcfe7f915f  SHA256: 9e305566f7 d342adc8e af30471aa3 eb95c049ac ffc742ae23 a5830a44f9 6e51d	This strike simulates the download of the 'Crimson RAT Dec 2020 Campaign - Word Malware' via an HTTP GET request.
Strike Emotet August 2020 Campaign - Emotet Malware File Transfer	MD5: 1950966348 02dadd6ac6 5db48b2a5 e9c  SHA1: 6c2d1dd282 98aa0bf7f96 99dbf2351a bd60acadf  SHA256: de06a2c720 90bb6399d6 bf41e76f03 a42ca1ccf4 df2c32cb95 0a032d7408 d45c	This strike simulates the download of the 'Emotet August 2020 Campaign - Emotet Malware' via an HTTP GET request.

Name	References	Description
Strike Winnti ShadowPad Oct 2020 Campaign - xDll Malware File Transfer	MD5: 60ddb540d a1aefee1e1 4f12578eaf da8  SHA1: 8d16bc28ce f6760ecf695 43a14d29b a041307957  SHA256: 87a57f5bb9 76644fce14 6e62ee54f3 e53096f37f2 4884d312a b92198eb1 e6549	<p>This strike simulates the download of the xDll malware via an HTTP GET request.</p>
Strike Raccoon Sep 2020 Campaign - libs.zip Malware File Transfer	MD5: 1117cd347 d09c43c1f2 079439056 ada3  SHA1: 93c2ce5fc49 2431431855 4e131cfbcd 119f01ab6  SHA256: 4cfada7eb5 1a6c0cb262 83f9c86784 b2b2587c59 c46a5d3dc0 f06cad2c55 ee97	<p>This strike simulates the download of the Raccoon libs.zip via an HTTP GET request.</p>

Name	References	Description
Strike Operation Quicksand Nov 2020 Campaign - Excel Malware File Transfer	MD5: 2e6169253 a87a9d6703 7b1a238d46 365  SHA1: 9804af6865 f0ffcc81437 61863160b6 e8a004ee8  SHA256: a1282dde50 3e911d5653 e1d9d1214 e4780e61c9 6d1530c3a1 be22d88a81 dcf5f	This strike simulates the download of the Excel malware via an HTTP GET request.
Strike RigEK Delivers Redline Stealer Campaign Mar 2023 - Redline Stealer Malware Download	MD5: 991129c128 cce33d434 849d79d284 34  SHA1: 27f1eee21b aa75297140 7d5a547920 9b3461ef74  SHA256: 0795128a43 b086cdc6b8 a4036b318 a5ba32762 cc387a86b4 2e7211e6d3 e164ad	This strike simulates the download of the Redline Stealer malware.

Name	References	Description
Strike Raccoon Sep 2020 Campaign - sqlite3.dll Malware File Transfer	MD5: f964811b68 f9f1487c2b4 1e1aef576c e SHA1: b423959793 f14b1416bc 3b7051bed5 8a1034025f SHA256: 83bc57dcf2 82264f2b00 c21ce0339e ac20fcb740 1f7c5472c0 cd0c014844 e5f7	This strike simulates the download of the Racoonn sqlite3.dll file via an HTTP GET request.
Strike RigEK Delivers Redline Stealer Campaign Mar 2023 - Malware Loader	MD5: b457df9a93 68bd321be acf704bf205 d3 SHA1: 01b6ecada b722825b8f bc22d6ab6f 3e05fb0a61 b SHA256: a75a099fae cf07c5cec20 a2223985b5 c5944d9cd8 7600c89254 d5213bb17f 4e3	This strike simulates the RigEK download of a malware loader.

Name	References	Description
Strike IcedID Dec 2020 Campaign - PNG Second Payload Malware File Transfer	MD5: 425cd83776 facc118d6e c3f266b1f86 e  SHA1: c1faa9cb4a a777902800 8375e79320 51ee786a52  SHA256: cc1030c4c7 486f529544 4acb205fa9 c9947ad414 27b6b181d7 4e7e5fe4e6 f8a9	This strike simulates the download of the 'IcedID Dec 2020 Campaign Campaign - PNG Second Payload' via an HTTP GET request.
Strike Winnti ShadowPad Oct 2020 Campaign - SkinnyD Malware File Transfer	MD5: ec2377cbd3 065b4d751 a791a22bd3 02c  SHA1: cdd78ccd27 4705f6c94b 6640c968e9 0972597865  SHA256: 1d59968304 f26651526a 27dabd2780 006ebd1492 5c9e00093 acfa2443a2 23675	This strike simulates the download of the SkinnyD malware via an HTTP GET request.

Name	References	Description
Strike RIG EK GandCrab Oct 2020 Campaign - CVE-2018-4878 Exploit Malware File Transfer	MD5: 92f27fb119 cd67c0ec34 16f501714f ab  SHA1: d11f6dd033 8946828c23 8e62dba3b7 9d8e0b8692  SHA256: a21ca5124 a51eb5633 c51b05e40 ac2f68d536 4af23d64ca 67ff1ee043 b8eb436	This strike simulates the download of the CVE-2018-4878 exploit malware via an HTTP GET request.
Strike APT-29 Sep 2020 Campaign - WellMess Malware File Transfer	MD5: 861879f402 fe3080ab05 8c0c88536b e4  SHA1: db4f07ecef d1e290d727 379ded4f15 a0d4a59f88  SHA256: 14e9b5e214 572cb13ff87 727d680633 f5ee238259 043357c943 02654c546c ad2	This strike simulates the download of the APT-29 WellMess via an HTTP GET request.

Name	References	Description
Strike Operation Quicksand Nov 2020 Campaign - CLI.dll Malware File Transfer	MD5: fbe65cd962 fc97192d95 c40402eee5 94  SHA1: dc7fca6a34 a3a65cf5df6 c17435fc5f2 f1c62b93  SHA256: 61072ae06 a5e25194e7 bf6297026b 54ae52fcfc1 4787ead886 6866d8098 a1fa3	This strike simulates the download of the CLI.dll malware via an HTTP GET request.
Strike RIG EK GandCrab Oct 2020 Campaign - CVE-2016-0189 Exploit Malware File Transfer	MD5: 11500100a8 5f1d8687f3 c652e14164 7c  SHA1: df0fc71b70 cc21caec43 f4f7f495bb4 a1e610249  SHA256: 2ac66dfe47 c1a40f88ce 753cd7d45 ede0976a99 f1c6088049 af4648cb5e f9d93	This strike simulates the download of the CVE-2016-0189 html exploit malware via an HTTP GET request.

Name	References	Description
Strike IcedID Dec 2020 Campaign - IcedID Loader Malware File Transfer	MD5: 9fd1bc2568 60d6a18a9 b1a294b66 dfb3  SHA1: e34c49a332 c42a0c3afd 0e2ff7d9031 1ac01aa3f  SHA256: 1b145cd128 82ab58ddb7 bdb833e11f 9e11b3eb9 ce721d75cc 6197f87ba4 fd341	This strike simulates the download of the 'IcedID Dec 2020 Campaign Campaign - IcedID Loader' via an HTTP GET request.
Strike Maze Apr 2020 Campaign - Word Malware File Transfer	MD5: ad30987a53 b1b0264d80 6805ce1a25 61  SHA1: e7da9cac8f c6a30c2879 ddb1ab9742 2e59979591  SHA256: 9f2139cc7c3 fad7f133c26 015ed33109 81de26d7f1 481355806f 430f9c97e6 39	This strike simulates the download of a Word document containing embedded macros via an HTTP GET request. The macros can be used to download additional malware, like the Maze ransomware seen in the 'Maze Apr 2020 Campaign'.

Name	References	Description
Strike Dridex May 2020 Malware Campaign - Dridex Malware File Transfer	MD5: d6ab8be7b5 a9e59a399 c27c1b8e21 bfc  SHA1: f88f5dfa79 a83aae6c3 a5e4d417d9 e184b4d0c4 c  SHA256: ff8e2e72b12 82b72f1a97 abb30553d2 b8d53366f4 29083f041c 553d2a9087 8f6	This strike simulates the download of the Dridex 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 - base64 Encoded XOR Encrypted Matanbuchus Binary Download		This strike simulates the 'Matanbuchus Jun 2022 Campaign - base64 Encoded XOR Encrypted Matanbuchus Binary Download' traffic that occurs after executing the Matanbuchus MSI package. This binary is the actual Matanbuchus malware that gets loaded into memory and executed, so that it is never dropped onto the disk. It is retrieved via HTTPS.
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.
Strike Matanbuchus Jun 2022 Campaign - Matanbuchus DLL Download		This strike simulates the 'Matanbuchus Jun 2022 Campaign - Matanbuchus DLL Download' traffic that occurs after executing the Matanbuchus MSI package. The malware is retrieved via a GET request over HTTPS.

Name	References	Description
Strike Maze Apr 2020 Campaign - Command and Control		This strike simulates the 'Maze Apr 2020 Campaign - Command and Control' traffic that occurs after executing the 'Maze' ransomware executable. The victim sends an HTTP POST request with binary data containing host information, and the attacker replies with an HTTP code 404. This sequence occurs 2 times.
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 MetaStealer Mar 2022 Malware Campaign - Windows DLL Retrieval		This strike simulates the HTTPS traffic that gets generated after the malware is executed in the 'MetaStealer Mar 2022 Malware Campaign'. Once the persistent executable is run, the malware sends an HTTPS request to download a malicious reverse byte Windows DLL.
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 IIS 5.0, IIS 5.1, IIS 6.0 WebDAV Authentication Bypass Variant 2	BID: 34493 CWE: 287 CVE: 2009-1535	This strike exploits an authentication bypass vulnerability in multiple versions of Microsoft IIS using UTF-8 encoded WebDAV requests. The strike uses a number of encoded characters, not just forward slash ('/') in the request.

<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 MinaliC Webserver v2.0 HTTP Request Buffer Overflow		This Strike exploits a buffer overflow in MinaliC Webserver version 2.0 when sending a GET request with an overly large URI.
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 Monitor-Line Links Management index.php lcnt Parameter SQL Injection	CVE: 2007-1339 BID: 22825	This strike exploits a SQL injection vulnerability in Monitor-Line's Link Management portal
Strike More.groupware PHP Groupware index.php include Parameter PHP File Include	CVE: 2001-1296 BID: 3383	This strike exploits a PHP include flaw in the More.groupware PHP-based Groupware.
Strike More.groupware PHP Groupware index.php include_dir Parameter PHP File Include	CVE: 2001-1296 BID: 3383	This strike exploits a PHP include flaw in the More.groupware PHP-based Groupware.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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

<b>Name</b>	<b>References</b>	<b>Description</b>
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
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 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 nsiilog.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 nsiilog.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 nsiilog.dll, an IIS ISAPI filter, by sending a 5000 byte POST request.

<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 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 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.
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

<b>Name</b>	<b>References</b>	<b>Description</b>
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 2	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 3	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 5	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 7	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 8	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 9	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 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 12	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.
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 15	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 16	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 17	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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 20	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 21	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 22	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 24	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 26	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 27	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 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 29	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 30	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 31	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 32	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 33	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 35	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 ActiveX Arbitrary Code Execution Variant 36	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 Remote Code Execution Variant 37	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.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 39	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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 Internet Explorer Compressed Content URL Heap Overflow (Compress)	CVE: 2006-3869 BID: 19667	This strike targets a heap overflow vulnerability in Microsoft Internet Explorer where the browser attempts to store an overly long URL into a smaller buffer when handling a server response that indicates compressed content.
Strike Internet Explorer Compressed Content URL Heap Overflow (GZIP)	CVE: 2006-3869 BID: 19667	This strike targets a heap overflow vulnerability in Microsoft Internet Explorer where the browser attempts to store an overly long URL into a smaller buffer when handling a server response that indicates compressed content.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer MHTML URI ID Buffer Overflow	CVE: 2006-2766 BID: 18198	This strike exploits a buffer overflow vulnerability in Internet Explorer.
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
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

Name	References	Description
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.
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 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

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.
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 BMP Heap Overflow	BID: 30599 CWE: 399 CVE: 2008-3020	This strike exploits a heap overflow in the Microsoft Office Graphics Image Filter for the BMP file format.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
Strike Microsoft Internet Explorer GDI+ WMF Polygon Memory Corruption	BID: 31021 CWE: 119 CVE: 2008-3014	This strike exploits a memory corruption bug in Microsoft Internet Explorer when processing a WMF file with a large amount of polygon data.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 DataGridView ActiveX Control Text Parameter Memory Corruption	BID: 32591 CWE: 264 CVE: 2008-4252	This strike simulates an attack against the Visual Basic 6.0 DataGridView 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

Name	References	Description
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 Polylines (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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows HTTP Services Integer Underflow Vulnerability	BID: 34435 CWE: 189 CVE: 2009-0086	This strike exploits an integer underflow memory corruption vulnerability present in Microsoft Windows HTTP Services. Due to an issue in reading the length of certain data passed to an affected client application, 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 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 Microsoft Office PowerPoint Legacy File Format Stack Overflow (HTTP)	BID: 34882 CWE: 119 CVE: 2009-0227	This strike exploits a stack overflow vulnerability in Microsoft Office PowerPoint when viewing a crafted PowerPoint legacy format document.
Strike Microsoft PowerPoint CurrentUser 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
Strike Microsoft Internet Explorer Object Tag Information Disclosure	CWE: 200  CVE: 2009-1140  BID: 35200	A vulnerability exists in versions 5, 6, and 7 of Internet Explorer prior to the June 2009 update that allows an attacker to read files on the users computer via the use of the object tag.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 DHTML Editing Component ActiveX Control Denial Of Service	BID: 36280 CWE: 94 CVE: 2009-2519	This strike exploits a denial of service vulnerability in the DHTML Editing ActiveX control's LoadURL() function.
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 Office Art Property Memory Corruption (HTTP)	CWE: 94 CVE: 2009-2528	This strike exploits a remote code execution flaw in Microsoft Office GDI+ Library as used in Office 2000 and Office XP products. This vulnerability is due to MSO.dll improperly handling bad or overflow pointers directly from malicious office files and results in memory corruption and potential code execution. This strike exploits the vulnerability by way of a maliciously crafted excel file.
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 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 Excel SxView Memory Corruption (HTTP)	CWE: 94 CVE: 2009-3128 BID: 36944	This strike exploits a memory corruption vulnerability in Microsoft Office Excel that can be triggered by modifying the cRw field of an SXLI record potentially leading 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 Office Project Parser PropList Mismatched PID Code Execution (HTTP)	CWE: 399 CVE: 2009-0102	This strike exploits a vulnerability in Microsoft Office Project's file parser when it parses a file containing a Properties Stream List where one of the properties is an Odf9 type and does not have a specific PID value associated with the type. This causes the use of an uninitialized variable, resulting in a read access violation by the CDoc9Ser::ReadUidValue function when a value is attempted to be read using the uninitialized variable. In some circumstances, this error can provide an opportunity for arbitrary code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
Strike Microsoft PowerPoint Long Filename Overflow Code Execution (HTTP)	CWE: 119 CVE: 2010-0029	This vulnerability is triggered when PowerPoint attempts to open a non-PowerPoint file with an overly-long filename. PowerPoint attempts to store the filename in a fixed-size stack buffer, resulting in an overflow and potential arbitrary code execution.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 Internet Explorer Dynamic Object Tag Information Disclosure	CWE: 264 CVE: 2010-0255 BID: 38055	A vulnerability exists in Internet Explorer versions 7 and 8 prior to the June 2010 update that allows an attacker to read files on the users computer via the dynamic use of the object tag.
Strike Microsoft Excel RTD Parsing Memory Corruption Vulnerability (HTTP)	CWE: 94 CVE: 2010-1246	This strike exploits an arbitrary program execution flaw in Microsoft Excel 2002. This flaw is triggered when a malformed RTD field is parsed in a malicious XLS file.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
Microsoft Access ImexGrid Denial of Service DOS 1	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.
Microsoft Access ImexGrid Denial of Service DOS 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.
Microsoft Access ImexGrid Denial of Service DOS 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.
Microsoft Access ImexGrid Denial of Service DOS 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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 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.
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.

Name	References	Description
Strike Microsoft Internet Explorer Layouts Handling Memory Corruption	CWE: 399 CVE: 2011-0094 BID: 47190	This strike triggers a memory corruption 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.
Strike Microsoft Internet Explorer toStaticHTML Information Disclosure	CWE: 79 CVE: 2011-1252 BID: 48199	This strike sends an html page that bypasses the XSS protections of IE's toStaticHtml method.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Microsoft .NET Framework OData filter Denial of Service	CWE: 20 CVE: 2013-0005 BID: 57141	This strike exploits a denial of service .NET Framework implementation of the Open Data Protocol. If nested replace functions are used with the \$filter query option a System out of Memory exception will be thrown from the replace function. The OData service will then terminate.
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 Excel XF Record Unchecked Inheritance(HTTP)		This strike triggers a memory corruption vulnerability in Microsoft Excel 2003. This flaw is due to an unchecked inheritance of cell styles in the Flags field (specifically the ixfParent) in XF records, and results in denial of service conditions, effectively killing all instances of Excel by way of a specially crafted malicious XLS file.
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 Agent Crafted URL Stack Buffer Overflow	CWE: 119 CVE: 2007-3040 BID: 25566	There exists a stack-based buffer overflow vulnerability in agentdpv.dll 2.0.0.3425 in Microsoft Agent on Windows 2000 SP4 which may allow remote attackers to execute arbitrary code via a crafted URL to the Agent (Agent.Control) ActiveX control, which triggers an overflow in the Agent Service (agentsrv.exe) process. This strike delivers a payload consistent with triggering this vulnerability and can cause denial of service conditions or remote code execution.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Word 2003 MSO Null Pointer Dereference DoS (HTTP)	CVE: 2010-3200	This strike exploits a null pointer dereference vulnerability in the MSO.dll library and causes a denial of service in Microsoft Word 2003.
Strike Microsoft Core Services Undocumented Object Memory Corruption	BID: 53934 CWE: 119 CVE: 2012-1889	This strike exploits a memory corruption vulnerability in Microsoft XML Core Services that is due to an error when attempting to access an object in memory that is not initialized. Because the vulnerability is found in a core system library any software that uses that library, including Internet Explorer and Microsoft Office, are affected. On top of that, the guys at vupen found a way to use this vulnerability to bypass ASLR in Windows 7, meaning the severity of this exploit is extreme! Affected Windows versions: Microsoft Windows XP Microsoft Windows Vista Microsoft Windows 7 Microsoft Windows Server 2003 Microsoft Windows Server 2008
Strike Opera Canvas Denial Of Service Memory Corruption		This strike exploits stack overflow and memory corruption across all browsers listed due to improper rendering of overly-sized unicode strings resulting in denial of service.
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.
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 MyPhPim calendar.php3 cal_id Parameter SQL Injection	CVE: 2006-0167 BID: 16210	This strike exploits a SQL injection flaw in the MyPhPim web application.
Strike myphpPagetool index.php include Parameter PHP File Include	CVE: 2001-1236 BID: 3394	This strike exploits a PHP include flaw in the myphpPagetool content management system.
Strike myphpPagetool index.php include_dir Parameter PHP File Include	CVE: 2001-1236 BID: 3394	This strike exploits a PHP include flaw in the myphpPagetool content management system.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 (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.
Strike Nokia N95 JPEG File Crash PoC		This strike sends a JPG file that will crash the Nokia N95 smartphone when opened in a browser or in a SMS message.
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 eDirectory Host Header Overflow	CWE: 119  CVE: 2006-5478  BID: 20655	This strike exploits a buffer overflow in a 'Host' header sent to a Novell eDirectory HTTP server

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Novell GroupWise WebAccess Basic Authentication Buffer Overflow	CVE: 2007-2171 BID: 23556	This strike triggers a buffer overflow vulnerability in Novell GroupWise WebAccess by sending a basic authentication value with a decoded length of more than 0x148 bytes.
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 Internet Agent LDAP BIND Buffer Overflow		This strike exploits a buffer overflow vulnerability in the Novell gwia service. If a BIND request is sent to the service with an overly long User Agent field a buffer will overflow.
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
Strike Nvidia Install Application ActiveX Buffer Overflow		This strike exploits a vulnerability in Nvidia Install Application's activeX control NVI2.DLL. If an overly long string is passed to the AddPackages method a buffer will overflow causing a denial of service condition to occur and potentially allowing for remote code execution.

<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 Opera Browser document write Uninitialized Memory Access	BID: 39855	This strike exploits the Opera browser using the asynchronous scripting method setInterval. This strike uses this method to make changes to the DOM using document.writeln. A reference to this uninitialized value can cause a change in the EIP register.
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 Operation Quicksand Nov 2020 Campaign - CLI.dll Command and Control		This strike simulates the 'Operation Quicksand Nov 2020 Campaign - CLI.dll Command and Control' traffic that occurs after executing the CLI.dll malware.
Strike Oracle Web Cache Admin Module Multiple GET Request Method DoS Variant 1	CVE: 2002-0386 BID: 5902	This strike exploits a denial of service bug in the Oracle9i Web cache Administration tool on the Windows platform.
Strike Oracle Application Server Portal XSS		This strike exploits a cross site scripting vulnerability in Oracle application server portal. The vulnerability is due to lack of input sanitation when handling HTTP request. Remote attackers may do arbitrary code execution on the target system.
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 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.
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 Weblogic mod_wl POST Request Buffer Overflow	CWE: 119 CVE: 2008-3257 BID: 30273	This strike triggers a buffer overflow in the Oracle Weblogic mod_wl Apache module by sending a long HTTP POST request.

<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 National Instruments installer ActiveX control file creation		This strike exploits a National Instruments installer 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 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 Webkit XSS Auditor srccdoc policy bypass	BID: 65066	This strike exploits exploits a security-bypass vulnerability in Google Chrome and Apple Safari (Webkit). The vulnerability lies in the handling of the srccdoc attribute. By enticing a user to view a malicious web page, an attacker could inject arbitrary JavaScript code.
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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 RealNetworks RealGames StubbyUtil.Process Mgr ActiveX command execution		This strike exploits a vulnerability in the RealNetworks RealGames framework. Specifically, it targets the insecure methods in StubbyUtil.ProcessMgr ActiveX control. If a user is manipulated into opening a specially crafted web page arbitrary code execution may be achieved. All versions of RealNetworks GameHouse, prior to 3.3.0.0 are affected by this vulnerability.
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 HP SiteScope Default User information	BID: 49345	This strike exploits a default credentials vulnerability in HP SiteScope. Attack can use this vulnerability to bypass the authentication on the target system.
Strike Oracle AutoVue ActiveX Control ExportEdaBom Remote File	BID: 50332	This strike exploits the an Activex control flaw associated with Oracle Autovue software. The ExportEdaBom function does not perform proper input validation and permits the creation of a file anywhere on the system. By manipulating a user to access a specially crafted web page arbitrary file creation may take place which could lead to code execution with local privileges. All systems runing versions of Oracle AutoVue prior to 20.0.1 are vulnerable.
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 Samsung AllShare Null Pointer Defereance		This strike exploits a vulnerability in the Samsung Allshare software to share data across the network . By using a specially crafted Content-Length string, a remote an attacker could generate a crash that could potentially lead to code execution. All versions prior to 2.1.1.0 are vulnerable.
Strike Zenoss 3 showDaemonXMLConfig Remote Code Execution		Zenoss contains a flaw that is triggered when input passed via the 'daemon' parameter to the zport/About/showDaemonXMLConfig script is not properly sanitized. This could allow an authenticated user to execute arbitrary shell commands.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP Application Lifecycle Management ActiveX Control Remote Code Execution	BID: 55272	This strike exploits a remote code-execution vulnerability in HP Application Lifecycle Management. The vulnerability is due to the insecure exposure of the SetShapNodeType method in the XGO.ocx ActiveX control. By enticing a user to open a crafted web page an attacker could remotely execute arbitrary code.
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 OpenFiler NetworkCard Command Execution	BID: 55490	This strike exploits a vulnerability in OpenFiler software solution. Due to improper authorization, a remote authenticated attacker may execute system commands using the system privileges associated with the 'openfiler' user. All versions of the software prior to 2.x 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 PhpTax-File Manipulation Remote Code Execution		This strike exploits a vulnerability inside php tax 0.8 that allows remote code execution through the newvalue parameter supplied to the application's index.php file
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike PineApp Mail-SeCure ldapsyncnow.php shell_command Command Execution		This strike exploits an arbitrary code execution vulnerability in PineApp Mail-SeCure. A specially crafted HTTP request can be sent to ldapsyncnow.php to execute arbitrary commands with root privileges.
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 D-Link MDIR-645 Multiple Buffer Overflow and Cross Site Scripting Vulnerabilities	BID: 61005	This strike exploits multiple buffer overflow and cross site scripting vulnerabilities in D-Link MDIR-645. Specially crafted HTTP messages can be sent to a vulnerable device to achieve arbitrary code execution or abnormal termination.
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 Flip4Mac Memory Corruption (HTTP)	BID: 22286 CVE: 2007-0466	This strike exploits a memory corruption flaw in Telestream Flip4Mac when handling WMF files.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Mac OS X Safari Archive Metadata Command Execution	BID: 16736  CWE: 94  CVE: 2006-0397	This strike exploits a command execution flaw in the Mac OS X operating system via the Safari web browser.
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 Patchwork Jan 2022 Campaign - Patchwork RAT Command and Control		This strike simulates the Command and Control traffic that occurs after executing the Patchwork RAT malware.
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 PDF Viewer ActiveX Method Denial of Service		This strike exploits a vulnerability in PDFViewer's activeX control PDFViewerLib.PDFViewer. If an overly long string is passed to the TitleBarText argument a buffer will overflow causing a denial of service condition to occur.
Strike Personal File Share 1.0 Denial of Service		This Strike exploits a denial of service vulnerability in Personal File Share 1.0 when sending a crafted HTTP request packet with an overly large amount of data in the uri.

<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 Pheap edit.php filename Parameter Directory Traversal		This strike exploits a directory traversal flaw in the Pheap CMS web 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 Phormation PHP Library index.php include_dir 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 PHP5.4 htmlspecialchars- htmlentities heap overflow	BID: 51860	This strike exploits a heap overflow bug in PHP 5.4SVN that exploits an incorrect length calculation for escaping numeric types with htmlentities or htmlspecialchars.
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 htmlspecialchars()- htmlentities() Heap Overflow	BID: 51860	This strike targets a vulnerability in the PHP html special character handling functions whereby a properly crafted string may cause a heap overflow in the PHP processor.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 phpinfo() Cross Site Scripting (POST)		This strike exploits a cross site scripting bug in the PHP interpreter phpinfo() function. This strike simulates an HTTP POST request to a vulnerable page.
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 PHPBB2 Modificat functions.php phpbb_root_path Parameter PHP File Include	CVE: 2007-0656  BID: 22320	This strike exploits a PHP remote file include vulnerability in the PHPBB2 Modificat web application.
Strike phpBook mail Parameter PHP Code Execution	CVE: 2006-0075  BID: 16106	This strike exploits an arbitrary code execution flaw in the phpBook PHP 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.
Strike PHPjournaler index.php readold Parameter SQL Injection	CVE: 2006-0066  BID: 16111	This strike exploits a SQL injection flaw in the PHPJournaler Web Application.

<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 IIS Unicode Exploitation - Powerbot Ping Flood Attack	CVE: 2000-0884  BID: 1806	This strike attempts to launch a ping flood against a random IP address by exploiting the IIS Unicode command execution flaw.
Strike Microsoft Powerpoint 2003 Heap Overflow (HTTP)		This strike exploits a heap overflow vulnerability in Microsoft Office 2005 Powerpoint
Strike Progea Movicon Negative Content Length	CWE: 119  CVE: 2011-3491  CVE: 2011-3498  CVE: 2011-3499  BID: 49605	This strike demonstrates Progea Movicon treating a negative content length as a very large unsigned integer.
Strike pSlash Web Portal index.php include Parameter PHP File Include	CVE: 2001-1235  BID: 3395	This strike exploits a PHP include flaw in the pSlash web portal application.
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 Qakbot Nov 2021 Campaign - Cobalt Strike Command and Control		This strike simulates the Command and Control traffic that occurs after executing the Cobalt Strike malware.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Qakbot Nov 2021 Campaign - Qakbot Command and Control		This strike simulates the Command and Control traffic that occurs after executing the Qakbot malware.
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 Raccoon June 2021 Campaign - Raccoon Command and Control		This strike simulates the 'Raccoon June 2021 Campaign - Raccoon Command and Control' traffic that occurs after executing the Raccoon Stealer.
Strike Raccoon Sep 2020 Campaign - Info Fetch Command and Control		This strike simulates the 'Raccoon Sep 2020 Campaign - Info Fetch Command and Control' traffic that occurs after executing the Raccoon malware.
Strike Raccoon Sep 2020 Campaign - URL Fetch Command and Control		This strike simulates the 'Raccoon Sep 2020 Campaign - URL Fetch Command and Control' traffic that occurs after executing the Raccoon malware.
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.
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.

<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 RigEK Delivers Redline Stealer Campaign Mar 2023 - Landing Page		This strike simulates the retrieval of the RigEK landing page. After visiting the page the targeted system will make outbound HTTP requests to download a follow on malware loader.
Strike RIG EK GandCrab Oct 2020 Campaign - Command and Control		This strike simulates the 'RIG EK GandCrab Oct 2020 Campaign - Command and Control' traffic that occurs after executing the GandCrab malware. The victim sends an HTTP GET request without any HTTP body data to the attacker.
Strike RIG EK GandCrab Oct 2020 Campaign - Gate.php page		This strike simulates the 'RIG EK GandCrab Oct 2020 Campaign - Gate.php page' traffic that occurs when a user visits the exploit kit's page.
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 5.0.5 SVG Memory Corruption Remote Code Execution	CWE: 119 CVE: 2011-0222 BID: 48844	This strike exploits a memory corruption vulnerability in the version of Webkit that ships with Apple Safari 5.0.5 and earlier. The flaw occurs when handling SVG documents and recursively building a tree of member objects.
Strike Apple Safari 4.0.4 XML Parser Infinite Recursion Denial of Service		This strike exploits a denial of service (infinite recursion) vulnerability via an XML document composed of a long series of start-tags followed by backslashes.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SAP DB Webtools 7.4 GET request HTTP_COOKIE Buffer Overflow	CVE: 2007-3614 BID: 24773	This strike exploits a stack buffer overflow in SAP DB Webtools 7.4 when handling long GET requests.
Strike SAP GUI BExGlobal ActiveX control code execution		This strike exploits a SAP GUI BExGlobal ActiveX control code execution vulnerability which is due to no confirmation when executing the command in the ActiveX control. Remote attackers may do arbitrary code execution on the target 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 Information Disclosure	CVE: 2003-0747 BID: 8515	This strike exploits an information disclosure 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 sap netweaver command execution		This strike exploits an arbitrary command execution vulnerability in SAP's NetWeaver via their SOAP interface.
Strike sap netweaver callsystem command execution		This strike exploits an arbitrary command execution vulnerability in SAP's NetWeaver via their SOAP interface.
Strike SAP NetWeaver Arbitrary Command Execution		This strike exploits an arbitrary command execution vulnerability in SAP's NetWeaver via their SOAP interface.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SaPHLesson show.php lessid Parameter SQL Injection	CVE: 2006-2835 BID: 18934	This strike exploits an SQL injection flaw in the SaPHLesson web application.
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 Serva HTTP Server GET Request Denial of Service		This strike exploits a vulnerability in the Serva HTTP Server. By sending a malformed GET HTTP request to the remote machine, a denial of service condition occurs.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Shenzhen TVT Digital Technology API OS Command Injection		A remote OS command injection exists in multiple devices using the Shenzhen TVT Digital Technology API. Due to hardcoded credentials and lack of input sanitization when parsing user supplied data, the vulnerability allows remote attackers to execute arbitrary OS commands with 'root' privileges.
Strike Shlayer May 2021 Campaign - Gatekeeper Bypass Command and Control		This strike simulates the 'Shlayer May 2021 Campaign - Gatekeeper Bypass Command and Control' traffic that occurs after executing the Shlayer malware.
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 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 Snitz Forums 2000 pop_profile.asp id Parameter SQL Injection	CVE: 2007-1023 BID: 22593	This strike exploits an SQL injection vulnerability in Snitz Forums 2000
Strike SolarWinds Orion ActiveX control PEstrarg1 Parameter Buffer Overflow	BID: 62585	This strike exploits a vulnerability in SolarWinds Orion Server and Application Monitor Pepco32c. A heap buffer overflow vulnerability exists within the PEstrarg1 parameter. This parameter does not properly validate input, and concatenates a given string to a 132 bytes fixed heap buffer. If a larger value is supplied the buffer will overflow.

Name	References	Description
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 SourceBans Cross-Site Scripting (XSS)		This strike exploits a cross-site scripting vulnerability in SourceBans 1.4.11. 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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 SquirrelWaffle Oct 2021 Campaign - Cobalt Strike Command and Control		This strike simulates the 'SquirrelWaffle Oct 2021 Campaign - Cobalt Strike Command and Control' traffic that occurs after executing the Cobalt Strike malware.
Strike SquirrelWaffle Oct 2021 Campaign - SquirrelWaffle Command and Control		This strike simulates the 'SquirrelWaffle Oct 2021 Campaign - SquirrelWaffle Command and Control' traffic that occurs after executing the SquirrelWaffle malware.
Strike StrRAT Sep 2021 Campaign - Excel Document Command and Control		This strike simulates the 'StrRAT Sep 2021 Campaign - Excel Document Command and Control' traffic that occurs after executing the macro-embedded Excel file.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 1.6.0 Class Validator Abort Denial of Service		This strike exploits an denial of service vulnerability in the Sun Java 1.6.0 class verifier.
Strike Sun Java 1.6.0 Class Validator strlen() Denial of Service		This strike exploits an denial of service vulnerability in the Sun Java 1.6.0 class verifier.
Strike Sunburst HTTP IoC strikes		This strike simulates the HTTP requests sent by a host infected with Sunburst malware. An infected host may periodically send one or more similar HTTP requests. Requests to these URLs should be considered an Indicator of Compromise (IoC).
Strike Sunburst SUNSHUTTLE GOLDMAX HTTP IoC strikes		This strike simulates the HTTP requests sent by a host infected with Sunshuttle or Goldmax malware. An infected host may periodically send one or more similar HTTP requests. Requests to these URLs should be considered an Indicator of Compromise (IoC).
Strike Sunburst Teardrop Raindrop HTTP IoC strikes		This strike simulates the HTTP requests sent by a host infected with TEARDROP or RAINDROP malware. An infected host may periodically send one or more similar HTTP requests. Requests to these URLs should be considered an Indicator of Compromise (IoC).
Strike SurgeLDAP GET Request Buffer Overflow	BID: 8408	This strike crashes a SurgeLDAP HTTP server by sending a GET request greater than 500 characters
Strike NetWin SurgeMail Webmail Server HTTP Header Overflow	CWE: 119 CVE: 2008-1054 BID: 27992	This strike simulates a buffer overflow attack against the NetWin SurgeMail webmail server by sending a large amount of HTTP headers.

Name	References	Description
Strike SVCReady Jun 2022 Campaign - Redline Stealer File Transfer	MD5: af9b2d811b 8ced789a31 12a0a5cb52 4e  SHA1: 14f9e58466 a566a211af 40045e4039 20dfb40510  SHA256: 6e11374473 76815e733 c74ab67f20 2be0d7c769 837a0aaac0 44a9b2696 a8fa89	This strike simulates the Redline Stealer malware download via an HTTP GET request.
Strike Sybase M-Business Anywhere agSoap.exe SOAP Request Closing Tag Memory Corruption		This strike exploits a memory corruption vulnerability in Sybase M-Business Anywhere when processing malformed SOAP requests.
Strike Symantec WinFax Pro ActiveX Buffer Overflow	BID: 34766	This strike exploits an overflow in Symantec's WinFax Pro Fax Viewer ActiveX control.
Strike Google Ad for Fake Anydesk Campaign Feb 2023 - TA505 DLL Downloads		This strike simulates the download of additional DLL files via a TLS request. After the MSI installer malware is executed, a dll is downloaded to allow the TA505 malware to remain persistent by placing the malware in the same location but randomizing the name and some contents to modify the hash. After this dll is executed with rundll32 an additional dll is downloaded.
Strike TankLogger showInfo.php livestock_id Parameter SQL Injection	CVE: 2006-0209  BID: 16228	This strike exploits a SQL injection flaw in the TankLogger web application.
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 4	CWE: 20 CVE: 2005-4360 BID: 15921	This strike attempts to crash IIS 5.1 by sending a malformed request.
Strike Tiny HTTP Server HEAD Request Denial of Service		This strike exploits a vulnerability in Tiny HTTP Server when handling a HEAD HTTP request. The server is a lightweight http server that was written to only accept GET requests however, it does not properly handle an incoming HEAD requests. If the server receives one a denial of service will occur.
Strike TinyPHPForum action.php txt Parameter XSS	CVE: 2006-0102	This strike exploits a cross site scripting flaw in the TinyPHPForum web application.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Trickbot June 2021 Campaign - Cobalt Strike Command and Control		This strike simulates the "Trickbot June 2021 Campaign - Cobalt Strike Command and Control" traffic that occurs after executing the Cobalt Strike malware.
Strike Trickbot June 2021 Campaign - Trickbot Command and Control		This strike simulates the "Trickbot June 2021 Campaign - Trickbot Command and Control" traffic that occurs after executing the Trickbot malware.
Strike TSEP colorswitch.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 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 Unauthenticated DNS Change Exploit		This strike exploits a vulnerability regarding DNS changes in the D-Link router web interface, which is accessible without authentication. By exploiting this vulnerability an attacker might redirect users to malicious sites.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft IIS Unicode Directory Traversal Command Execution Variant 1	CVE: 2000-0884 BID: 1806	This strike attempts to execute the "dir" command via a directory traversal flaw in Microsoft's IIS web server.
Strike Microsoft IIS Unicode Directory Traversal Command Execution Variant 2	CVE: 2000-0884 BID: 1806	This strike attempts to execute the "dir" command via a directory traversal flaw in Microsoft's IIS web server.
Strike Microsoft IIS Unicode Directory Traversal Command Execution Variant 8	CVE: 2000-0884 BID: 1806	This strike attempts to execute the "dir" command via a directory traversal flaw in Microsoft's IIS web server.
Strike Up.Time Monitoring Server 7.2 File Upload and Code Execution	BID: 64031	This strike identifies a vulnerability in the Up.Time Monitoring Server. Due to a lack of proper validation, an attacker can upload a file remotely that leads to execution.
Strike Ursnif Aug 2021 Campaign - Command and Control		This strike simulates the 'Ursnif Aug 2021 Campaign - Command and Control' traffic that occurs after executing the Ursnif malware.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Vmist Downstat admin.php 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 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 Parameter PHP File Include	CVE: 2006-4827 BID: 20007	This strike exploits a PHP include flaw in the Vmist Downstat web application.
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 Webby Webserver 1.0.1 GET Method Buffer Overflow		This strike exploits a buffer overflow flaw in the GET method implementation of the Webby web server.
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.

Name	References	Description
Strike Webkit handleRunInChild Use After Free	BID: 52913 CWE: 399 CVE: 2011-3068	This strike exploits a use after free vulnerability in Webkit-based browsers. The flaw occurs when handling children of a run-in box, when it changes its display type from block to inline. When handled by RenderBlock::handleRunInChild, webkit fails to delete child nodes to render the box as inline.
Strike WebPageTests Upload Feature resultimage.php Remote File Upload		This strike exploits failure to properly validate input in WebPageTest's resultimage.php, which enables a remote attacker to upload arbitrary files that are then publically accessible through the webserver
Strike WEBrick Directory Traversal	BID: 28123 CWE: 22 CVE: 2008-1145	This strike exploits a directory traversal vulnerability in the WEBrick ruby webserver.
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 heap overflow in Winamp when it is parsed.
Strike Winamp Playlist UNC Path Arbitrary Code Execution	BID: 16410 CVE: 2006-0476	This strike exploits a code execution vulnerability in the Winamp media player.
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.
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.

Name	References	Description
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.
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 Winnti ShadowPad Oct 2020 Campaign - xDll Command and Control		This strike simulates the 'Winnti ShadowPad Oct 2020 Campaign - xDll Command and Control' traffic that occurs after executing the xDll malware.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 strike 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.
Strike Microsoft WordPad Embedded COM Code Execution (AddressBook) (HTTP)		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) (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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Unauthenticated Content Injection	EXPLOITDB : 41223	This strike exploits an unauthenticated content injection in Wordpress. The vulnerability is due to improper input validation for HTTP requests to the REST API url /wp-json/wp/v2/posts/. By exploiting this vulnerability an attacker can change any post on a victim site.
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 Admin Panel - Multiple XSS Vulnerabilities Variant 1	BID: 22738	This strike exploits several XSS vulnerabilities in the Wordpress blogging engine
Strike Wordpress Admin Panel - Multiple XSS Vulnerabilities Variant 2	BID: 22738	This strike exploits several XSS vulnerabilities in the Wordpress blogging engine
Strike Wordpress Admin Panel - Multiple XSS Vulnerabilities Variant 3	BID: 22738	This strike exploits several XSS vulnerabilities in the Wordpress blogging engine
Strike Wordpress Admin Panel - Multiple XSS Vulnerabilities Variant 4	BID: 22738	This strike exploits several XSS vulnerabilities in the Wordpress blogging engine
Strike Wordpress Default Theme Admin XSS Vulnerability		This strike exploits an XSS vulnerability in the Wordpress blogging engine
Strike WordPress DZS Video Gallery Plugin Remote and Local File Disclosure		This strike exploits a vulnerability inside the DZS Video Gallery WordPress plugin which allows remote users to access the contents of local and remote files to which the user under which the webserver is ran, has access.
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.

<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 Tinymce Thumnail Gallery Plugin File Disclosure		This strike identifies a vulnerability in the WordPress Tinymce Thumbnail Gallery Plugin. Due to improper validation, a user can disclose data from a remote location.
Strike Wordpress wp_title() year parameter XSS		Wordpress 2.0, 2.1, and 2.2 are vulnerable to a cross site scripting attack in the wp_title() function using the year parameter.
Strike WordPress xmlrpc Pingback Denial of Service		This strike emulates a large number of requests for pingback calls through the xmlrpc service available by default on wordpress servers. This kind of requests are used as part of a distributed denial of service scenario. The requests generated by this strike are identical to what an attacker would send to reflector and amplifier wordpress servers in order to disrupt service on other servers.
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 X97EmbedAn Excel Document (http)	BID: 18422  CVE: 2006-3059	The X97EmbedAn malware abuses an arbitrary code execution flaw in Microsoft Office.
Strike Xitami Web Server HEAD Denial of Service		This strike exploits the Xitami Web Server which mishandles HEAD requests against directories leading to a denial of service.

Name	References	Description
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 XLatunes Remote SQL Injection	CWE: 89 CVE: 2007-1026 BID: 22602	This strike exploits an SQL injection vulnerability in the XLatunes package
Strike Generic XSS - Failure		This is a generic cross-site scripting attack that fails.
Strike Generic XSS - Success		This is a generic cross-site scripting attack that succeeds.
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 SQL Injection Vulnerability In Multiple ManageEngine Applications		This strike exploits an SQL injection vulnerability in ManageEngine Applications Manager and ManageEngine IT360 MSP Edition. The vulnerability is due to improper validation of customerName HTTP parameter. An attacker could exploit this vulnerability by sending an unauthenticated malicious requests 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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		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 Avira Management Console HTTP Overly Long Header Heap Over Buffer Overflow		This strike exploits a heap buffer overflow vulnerability in Avira Management Console. When performing length calculations on header fields, if no carriage return (0x0d) character is encountered within the first 0x1000 bytes, a miscalculation allows the overly long header to be copied into a fixed length heap buffer, resulting in a buffer overflow. Successful exploitation may result in execution of arbitrary code with system privileges or abnormal termination of the Avira Management Console process.
Strike Trend Micro IWSVA Domain List bdn Paremeter 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)

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike ZebraFeeds aggregator.php zf_path Parameter PHP File Include	CVE: 2007-1010 BID: 22576	This strike exploits a PHP include flaw in ZebraFeeds 1.1.
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 Zebrocy May 2021 Campaign - Wininitiation Command and Control		This strike simulates the 'Zebrocy May 2021 Campaign - Wininitiation Command and Control' traffic that occurs after executing the Wininitiation malware.
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 Zloader July 2021 Campaign - Zloader Command and Control		This strike simulates the 'Zloader July 2021 Campaign - Zloader Command and Control' traffic that occurs after executing the Zloader malware.
Strike ZorbStats index.php include Parameter PHP File Include	CVE: 2001-1299 BID: 3386	This strike exploits a PHP include flaw in the ZorbStats web site traffic stats application.
Strike ZorbStats index.php include_dir Parameter PHP File Include	CVE: 2001-1299 BID: 3386	This strike exploits a PHP include flaw in the ZorbStats web site traffic stats application.
Strike Cybozu Injection	CVE: 2006-4444 BID: 19731	This strike exploits a SQL injection flaw in the Cybozu web application.
Strike ZTE CPE Webshell	CVE: 2014-2321 CWE: 264	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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Elastix SQLi	CVE: 2015-1875 CWE: 89	An SQL injection vulnerability in the Elastix unified communications server which allows remote attackers to execute arbitrary SQL commands via the transactionID parameter, using a specially crafted HTTP GET request.
Strike Magento RCE	CVE: 2016-4010 CWE: 74	This strike exploits a vulnerability of the Magento e-commerce platform that allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via crafted serialized shopping cart data.
Strike McAfee SQLi	CVE: 2016-8027 CWE: 89	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 Tomcat File Upload	CVE: 2017-12615 CWE: 434	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 Jenkins RCE	CVE: 2018-10008 61 CWE: 502	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 Echo Passthru Php	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 Exec Php	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.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Passthru Php	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 System php	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 Shell Exec Php	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 WordPress XSS	CVE: 2019-14470  CWE: 79	The WordPress plug-in 'UserPro' uses a Instagram library (Instagram PHP API V2 by coseenary) that is vulnerable to Reflected Cross-Site Scripting (XSS).
Strike CmdJsp jsp	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 Cmd jsp	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 List jsp	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 Up jsp	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.

Name	References	Description
Strike Waf Webshell Single jsp	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 Denial of Service	CVE: 2019-11287 CWE: 400	RabbitMQ for Pivotal Platform, 1.16.x versions prior to 1.16.7 and 1.17.x versions prior to 1.17.4, contain a web management plugin that is vulnerable to a denial of service attack. The <X-Reason> HTTP Header can be leveraged to insert a malicious string that will expand and consume the memory resulting in a server crash
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 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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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 Polyline (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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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).
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.

<b>Name</b>	<b>References</b>	<b>Description</b>
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.
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 RUDY POST	CWE: 400	'R U Dead Yet?' or R.U.D.Y. is a denial-of-service attack tool that aims to keep a web server tied up by submitting form data at an absurdly slow pace. A R.U.D.Y. exploit is categorized as a low-and-slow attack, since it focuses on creating a few drawn-out requests rather than overwhelming a server with a high volume of quick requests.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Slowloris GET	CWE: 400	Slowloris is a type of denial of service attack, where the attacker tries to keep many connections open and hold them open for as long as possible. The target server will only have so many threads available to handle the concurrent connections, resulting in the overwhelming and slowing down the server.
Strike Slowloris POST	CWE: 400	Slowloris is a type of denial of service attack, where the attacker tries to keep many connections open and hold them open for as long as possible. The target server will only have so many threads available to handle the concurrent connections, resulting in the overwhelming and slowing down the server.
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 (5122)

Name	Description
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike AceCryptor_fe1cfdddb	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 fe1cfdddb7b44cec0b5c37769934a2ee9.
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 ecbe1b1e30a1f4bffaf1d374014c877f.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 dcb287aff31159ff8e4fc6d8b3343036.
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.
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 AhRat_98bb907d	This strike sends a malware sample known as AhRat. It's an android malware which poses as a voice recorder app. It was initially uploaded as a benign app in the google play store and later updated with malicious functionalities like exfiltration of voice recording, screen capture, call log, SMS etc. 'com.tsoft.app.iscreenrecorder' is the package name of the malware sample. The MD5 hash of this AhRat sample is 98bb907d79beaa9aaece8d767d28ddb0.

<b>Name</b>	<b>Description</b>
Strike AhRat_dbe8815b	This strike sends a polymorphic malware sample known as AhRat. It's an android malware which poses as a voice recorder app. It was initially uploaded as a benign app in the google play store and later updated with malicious functionalities like exfiltration of voice recording, screen capture, call log, SMS etc. 'com.tsoft.app.iscreenrecorder' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this AhRat sample is dbe8815b7c2d3be3074570982ed8412d.
Strike AhRat_f3ca8e27	This strike sends a polymorphic malware sample known as AhRat. It's an android malware which poses as a voice recorder app. It was initially uploaded as a benign app in the google play store and later updated with malicious functionalities like exfiltration of voice recording, screen capture, call log, SMS etc. 'com.tsoft.app.iscreenrecorder' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this AhRat sample is f3ca8e27eb9a3f81c85b169a97d8d56c.
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.

<b>Name</b>	<b>Description</b>
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.
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_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.

<b>Name</b>	<b>Description</b>
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.
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 0ac539e23e9befbbc96b874719fcceb50.
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 a0e72ce4f88f7f8dccce31db8ace8a2.

<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_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_61b7507a	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.
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.

<b>Name</b>	<b>Description</b>
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_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 c09266666ee71ade24e0e5f889cc8199.
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.
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 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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 eb5f7076a810e1bcd7797545f05e5664.
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.

<b>Name</b>	<b>Description</b>
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 06d7088ee3d6560a888025a8c28cab0.
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.
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.

<b>Name</b>	<b>Description</b>
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 485274755aeccfc2f3c577eb6aa61cc4.
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.
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.

<b>Name</b>	<b>Description</b>
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_6d1bdaf6	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.
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.

<b>Name</b>	<b>Description</b>
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.
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 94a170cb5beb4d608e23d555333c86ee.
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 95dd67c228fe6339411c6809cebfb96.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 dc2c2460f88c67ba4596bdfb34b2cbc.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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_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.
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.

<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 bf7c42a9d8dc2dcefbcfd3f0d0d3698c.
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.
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.

<b>Name</b>	<b>Description</b>
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 b58d686f1c6c124cccd8d5fab08638ec8.
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.
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.

<b>Name</b>	<b>Description</b>
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 11ac73b0ffdf22b9b329bfdd215ed83.
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike Bifrost_2bcdc1b5	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 2bcdc1b533f88165e5ef0da754517536.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 8b220453ce856f3709cd80beeae503b2.

<b>Name</b>	<b>Description</b>
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.
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 abdcebabc0c8ce3ddc1f1d4f11902b.
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.

<b>Name</b>	<b>Description</b>
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 bb1b81eae69f9128d2ff6dcf5e35c4b.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 fa874b334f0797b3df342966ff5567f.
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.
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.

<b>Name</b>	<b>Description</b>
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 1dd464ccb3fb6881eeff3f05b8b1fdb5.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 a6237d5041d5a178c50bcd6387b405e.
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 b5c9d7c157a3ffd0cab340313f1c5ec.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 470c803b32209fbebe09af80a1b83e6f2.

<b>Name</b>	<b>Description</b>
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 59db7bd22d4ec503b768ecee646205c27.
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.
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.

<b>Name</b>	<b>Description</b>
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 bc95f228b11fa3b4e91c30d98f9f3bff.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

Name	Description
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.
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.

Name	Description
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike Buer_3dcd5f44	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 3dcd5f4471a4f9dd34ac0b61d2f295dc.
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 693df2e2029ed05eb3e7ccd214fb414f.
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.

<b>Name</b>	<b>Description</b>
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.
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.

Name	Description
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.
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_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.
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 25a8caa929eb681e1f75b495e8ddbde.
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.

<b>Name</b>	<b>Description</b>
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.
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 1f954e9fabe22e942d65f42df913829d.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike CLOP_508a671c	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.
Strike CLOP_9ec70a82	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.
Strike CLOP_a04eb443	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.
Strike CLOP_d3ace85c	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.
Strike CLOP_f2114603	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.

<b>Name</b>	<b>Description</b>
Strike CaddyWiper_01fe1c58	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.
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 42e2b6e4fba51ec71235e28dff27a76.

<b>Name</b>	<b>Description</b>
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.
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 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 02a86e7e82925efccb3c63da2b73bbb6.
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.

<b>Name</b>	<b>Description</b>
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_1aaf04ed	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 1aaf04edca15d3323f8cdf31accf7a29.
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.
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 2ecc1dd8dcb81eed88244e714caa65f7.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 70a3a2a8d3c916b2ec01d5d7dc6c3bf.
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.

<b>Name</b>	<b>Description</b>
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.
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 93b1e1dcbe3389af820e092e0890067.
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.

<b>Name</b>	<b>Description</b>
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.
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 a316e70955be20426f5d2a12f5bfea8.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 aed474509baebe1b716d5c65d21a2cfc.
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.
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.

<b>Name</b>	<b>Description</b>
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_bebf0baf	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.
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.

<b>Name</b>	<b>Description</b>
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.
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 binary has the timestamp field updated in the PE file header." 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_d8aad63d	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 d8aad63dd0d7e7a646e8edc7fcc09f87.
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 binary file has one more imports added in the import table." 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.

<b>Name</b>	<b>Description</b>
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 dc82432a6a69957fcc2e326fdbd97924a.
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.
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_efbf48e14	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.

<b>Name</b>	<b>Description</b>
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 f633f7b424983cef70eae8bcfb81ff19.
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.
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 f902f4a5f05146167efeaed2a8f7961c.
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 fce00a14d4542ddada0befb0a40cb7ea.

<b>Name</b>	<b>Description</b>
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.
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 mofifications. 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.
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.

<b>Name</b>	<b>Description</b>
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.
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 7e665259f4178fcf254d809d3acf2b2.

<b>Name</b>	<b>Description</b>
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.
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 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 eda8ab9741ff7b166c04d59e4c778a45.

<b>Name</b>	<b>Description</b>
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.
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 77e19f056443b6dbcccc1336251a7e4.
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.

<b>Name</b>	<b>Description</b>
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.
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 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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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_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.
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.

<b>Name</b>	<b>Description</b>
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_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.
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_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 bfa936de26037dd4693af0f8d69cdcc8.
Strike CoralRaider_ce5fbb5a	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 ce5fbb5af0805ae714563ea936298358.

<b>Name</b>	<b>Description</b>
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.
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_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 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 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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 180f8ee1842a3465cfc9bb2e1fedce8e.
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.

<b>Name</b>	<b>Description</b>
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 215b14ac07078fcf72774efca6bbbfc6.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 5bd6a4959e85dc87e9fc0da98bd36ab.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 6b41728e3ab0def43977ee60eaea6efa.
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.

<b>Name</b>	<b>Description</b>
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 6f2fdbdadd5bc65bcd1a5450aafc7a3.
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.
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.

<b>Name</b>	<b>Description</b>
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 7ada5970aa4eaef202d0e67d872ee2e.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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_afa7e1cf	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 afa7e1cf7d0c1dcf3e55e57590286549.
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.

<b>Name</b>	<b>Description</b>
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 b2a17564d97ec1ca975dcd8ee222a987.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 c288a31269c6d2b85e08603cfe6afe4.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 f1672da40e317021e8e81a73de0aea3.
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.

<b>Name</b>	<b>Description</b>
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 fac38e7afa79375ca964db486879bfeb.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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_8ecfdcd69	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 8ecfd699de69ff65a3cd3f6b6de329b.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 0ed51a595631e9b4d60896ab5573332f.
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.
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.

<b>Name</b>	<b>Description</b>
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 29bcd459f5ddeeefad26fc098304e786.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 e44450150e8683a0add5c686cd4d202.
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 e5ca2d127e7300f28fbeb1e74d6a6858.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 f44695a8feb2a35576a59fa984629d2.

<b>Name</b>	<b>Description</b>
Strike Darkgate DLL_9d82885d	<p>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.</p>
Strike Darkgate Loader_645cc995	<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 645cc995139d0646250eca32683afae1.</p>
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>

<b>Name</b>	<b>Description</b>
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>
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>

Name	Description
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>
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>

Name	Description
Strike Darkgate_bce3f0e9	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.
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5c5d0c1。
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.

<b>Name</b>	<b>Description</b>
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 6821f568afd50383f31ceac886a99ab7.
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.
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 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 391c894616dd0e8b372b801cbbc0a790.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike Dharma_1fdbd39b2	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.
Strike Dharma_272d8ad1	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.
Strike Dharma_2873a268	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 2873a26848097af920b6e6bc9375a48.

<b>Name</b>	<b>Description</b>
Strike Dharma_3752ab93	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.
Strike Dharma_3cdd778b	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.
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 48b09277d82efbcraf25e6dbe5dad3c5c.

<b>Name</b>	<b>Description</b>
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 6b5798035d7d54cfa82271799ddd12ac.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 1aadb27c19050b903a8fcfc63f426db36.
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.

<b>Name</b>	<b>Description</b>
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 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 1301e933ffd26d973e2d92726a5cb165.
Strike Dofoil_17238a77	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 17238a77d4115a153200b352da8667e4.
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 41cbc9f14ba35bc3fb01fa373366684.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike Dofoil_bc8169b8	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 bc8169b8f36da028c90537694d4dedf0.
Strike Dofoil_d6b15dd2	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 d6b15dd2c82446ef06feb78f18ed6435.
Strike Dofoil_e81d1b51	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 e81d1b51ee7a971cbbe4cb91f09a5d90.
Strike Dofoil_f80691f4	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 f80691f47500b11ae90d642583a87781.
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.

<b>Name</b>	<b>Description</b>
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 81f50e95bfbbe7d86229ac9592febfb2f.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 4f2fccaff3b068ee744b80db7474f8043.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 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.

<b>Name</b>	<b>Description</b>
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 1bba771b9a32f0aada6eae64643673a.
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.
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 3cc77c18b4d1629b7658afb4175222c.
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 48c8e8cc189eef04a55ecb021f9e6111.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 6cfec4bdcbc7f99535ee61a0ebae5dc.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 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 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.

<b>Name</b>	<b>Description</b>
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.
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 09a87f23cc5a5459bfb443faffd76f1.
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.

<b>Name</b>	<b>Description</b>
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.
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 1cf9f32e7c95143df2125a20cb8d5ffc.
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.

<b>Name</b>	<b>Description</b>
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.
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 270d4a7cd0cd8f8aa84619dbcfdb13.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 544de53a55edb56db93c07002f7ec0.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 6b8e4dc413f5f537594d193dda39efe9.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 a047e8bc82f34dfffd1748eee7a7160.
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_a6ae4aab	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 a6ae4aab85b21a4b811504d50054bb13.
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.

<b>Name</b>	<b>Description</b>
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 ac1464a7af3438caeccf8d4bc797fc59.
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.
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_bbcbb2ae7	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 bbcbb2ae776fc56d292f741c4de5394fc.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 ce27e41e75ad21b3d7ffbcc40a2e989.
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.

<b>Name</b>	<b>Description</b>
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 d4e7d65bfdedb3a4330bbb70b4ceefef.
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_d9cceea03	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 d9cceea03cd6642af5baaf58e128bb583.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 Decoy_0758c566	This strike sends a malware sample known as ExelaStealer Decoy. 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 decoy document. The MD5 hash of this ExelaStealer Decoy sample is 0758c56672f29aa493d955ced3682239.
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.
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.

<b>Name</b>	<b>Description</b>
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 0d256ab0a8b8b7a3b3d4aa566189ca6.
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 4908a364b1d9467f2c9c3fceccba202.
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.
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.

<b>Name</b>	<b>Description</b>
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 Expiro_006d69c5	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 006d69c55af445e249fa154e4f31e55a.
Strike Expiro_0155baf3	This strike sends a malware sample known as Expiro. Expiro 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 Expiro sample is 0155baf3b793202061b0c43ca7c9cec2.
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.

<b>Name</b>	<b>Description</b>
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.
Strike Expiro_30f54fcac	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.

<b>Name</b>	<b>Description</b>
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_3daea3b8	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 3daea3b8bbb4ead9495ee4aff49b3a83.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 8bb301137c9cf0781df8dc295d904dc.
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 92ee6e8d9fc8083bf2089fbce77c66e.
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.
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.

<b>Name</b>	<b>Description</b>
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 b167581fc856d403e0c2163ced4a080.
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.
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.

<b>Name</b>	<b>Description</b>
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 c5877275ffbfb064142094638cb4dc9.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike FROZEN#SHADOW JS_337504e8	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.
Strike FROZEN#SHADOW JS_50c9e639	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.

<b>Name</b>	<b>Description</b>
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>
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>

<b>Name</b>	<b>Description</b>
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>
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>

<b>Name</b>	<b>Description</b>
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>
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 f85f33e5ce5264618850cc4b9d79fd9.</p>

<b>Name</b>	<b>Description</b>
Strike Fakecalls-BankingTrojan_703b22fce	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 banking trojan. 'com.grn.nbz.ktvhe.xeubdv' is the package name of the malware sample. The MD5 hash of this trojan is 703b22fce432d2c681cebbc150394f1.
Strike Fakecalls-BankingTrojan_821ed14c	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 manifest file of the malware has been randomly rearranged. The MD5 hash of this trojan is 821ed14cd734237b802f520ae0cbc8c2.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 random contents appended in one of the existing sections 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.

<b>Name</b>	<b>Description</b>
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 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 247045753ccb8cccd6a567d00641858b.
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.

<b>Name</b>	<b>Description</b>
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.
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 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 3a0db08d86d3d57ede47d52843f32761.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike ForestTiger_fffe249	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 ffffe24971d48bb8884dee321f93c0f5.
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.

<b>Name</b>	<b>Description</b>
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.
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 random contents appended in one of the existing sections 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.

<b>Name</b>	<b>Description</b>
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.
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 4131d35ec6a865907eddcb8faa8cce33.
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 42e783c3fce37f1ea7eaa89c45b31e6.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 54497e2f3ef331eba62e146a4bbbcf4.
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.
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 79071d4b37fd17e5e1aa6519894631f.

<b>Name</b>	<b>Description</b>
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.
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 8f905d0c1831985db19e53d2b442fb4.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 b0de6a61550374c5e342fda91ee21533.
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.
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 c1930047f21a89ddfb5a2e2db2d5485.
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.

<b>Name</b>	<b>Description</b>
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.
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 d1ef4711e6d940cfbdf343767f94d5f4.
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.

<b>Name</b>	<b>Description</b>
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.
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_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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 1c6b014e86d887ef235adbce8c23a7f.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 eb5f77715eb2a50f1aaf03074f3ad388.

<b>Name</b>	<b>Description</b>
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 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 10733ef18028d94596776413bab9920.
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.
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 2be3fc0fc545426dff818de235b9418f.
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.

<b>Name</b>	<b>Description</b>
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.
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 46fda5099af718be6fec6710916dec8.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 cb1077195da0ed778a3180ab0aaaf4c92.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 ServerV15\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 ServerV15\FrontEnd\HttpProxy\owa\auth\ C:\Exchange\FrontEnd\HttpProxy\owa\auth\ The MD5 hash of this HAFNIUM Webshell sample is 4b3039cf227c611c45d2242d1228a121.

<b>Name</b>	<b>Description</b>
Strike HAFNIUM Webshell_4ef04cba	<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 4ef04cba6bec2c3a164b9b755efbeb1c.</p>
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 Hades_9fa1ba3e	<p>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.</p>
Strike Haron_04ef9ed3	<p>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.</p>
Strike Haron_27757047	<p>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.</p>

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 ed31cc349ffdc64e35ad4b149c06d55.
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 f4274360fefdf50fb219f0ec648bf015e.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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aa34e2.
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 700ab60cd8ea41c959394479d0bafdf5e.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 Hupigon_05fa4098	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.

<b>Name</b>	<b>Description</b>
Strike Hupigon_06f83b6c	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.
Strike Hupigon_07c75bae	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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 689678d733098fafa9138197421f1b25.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike IZ1H9_9fbcd7e	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.
Strike IZ1H9_e06c85ea	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.

<b>Name</b>	<b>Description</b>
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>
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>

<b>Name</b>	<b>Description</b>
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>
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>

<b>Name</b>	<b>Description</b>
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>
Strike InfectedSlurs_d38aacc6	<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 d38aacc6becf788d30d5c709f497b518.</p>

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike JanelaRAT_3870e4a4	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.

<b>Name</b>	<b>Description</b>
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>
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_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>

<b>Name</b>	<b>Description</b>
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>
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>

<b>Name</b>	<b>Description</b>
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>
Strike JanelaRAT_d1684fa8	<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 d1684fa84602a2d560b47dfe0f0779b4.</p>
Strike JanelaRAT_f71471d7	<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 f71471d7e94ef739a8ee44125023b750.</p>
Strike Johnnie_006d8728	<p>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.</p>
Strike Johnnie_00826892	<p>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.</p>
Strike Johnnie_0318ec7b	<p>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.</p>

<b>Name</b>	<b>Description</b>
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.
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 38c0b11fdbfbcc2806cfacb08ecd6ca1.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 b5435acae01e6f182ec43d92e86c73f0.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 f492468be9b84083fc48b102b9ce1efa.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike KandyKorn_015c5d12	<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 015c5d12273dde42fd0a17985ee9a1cd.</p>
Strike KandyKorn_056b1d9c	<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 056b1d9ce628efe6128e17cddab3811e.</p>
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>

<b>Name</b>	<b>Description</b>
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>
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>

<b>Name</b>	<b>Description</b>
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>
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_f8fdb1d	<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 f8fdb1d21eaebaea117b041d42447a.</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>

<b>Name</b>	<b>Description</b>
Strike Kapeka_2bebf05a	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 2bebf05a9607f038f5407248fb075cd6.
Strike Kapeka_3a4c7bbf	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.
Strike Kapeka_50acd887	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.
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.

<b>Name</b>	<b>Description</b>
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 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.
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.

<b>Name</b>	<b>Description</b>
Strike Konni_8ce075e4	<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 8ce075e44ae4ac67862a5024d997161d.</p>
Strike Konni_b6a9f393	<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 b6a9f3933f734f7822da5e7b520ed79d.</p>
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>

<b>Name</b>	<b>Description</b>
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>
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>

Name	Description
Strike Korplug Loader_b1756033	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.
Strike Korplug Loader_d9165591	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.
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.

<b>Name</b>	<b>Description</b>
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.
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 031fce2f46862d4bd7055da4333cfaf66.
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.

<b>Name</b>	<b>Description</b>
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 0616f3c930b80fdb8ed66810c2ea97fc.
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.
Strike Kuluoz_082721c6	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 082721c6a65a2e6f1c9c16db10f5ab9c.
Strike Kuluoz_08a5665e	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 08a5665e588077e5ee093952d7dffcc1c.
Strike Kuluoz_0b0061e5	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 0b0061e58c3626c7a01b5e02c1c46240.
Strike Kuluoz_0fec7e00	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 0fec7e00c7c25b6100c1486bdccc90ae.
Strike Kuluoz_11c108f7	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 11c108f7a7e10c3b8c83b4822bc10a30.
Strike Kuluoz_13186602	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 1318660229c3303b7ca6cc790116c376.

<b>Name</b>	<b>Description</b>
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 1351ebf2a8b179fdb456dc70bc87e891.
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.
Strike Kuluo_17409590	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 174095907aeaffda652d87c33bc6899f.
Strike Kuluo_18ebe58a	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 18ebe58a606b06daac837db615ceb3ae.
Strike Kuluo_19244e86	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 19244e8666f85a39f977c878d4ca17e7.
Strike Kuluo_1ad639e3	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 1ad639e3f520caef6fb25628e9676cca.
Strike Kuluo_1d0da87d	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 1d0da87d04a68d52f9474a50e324e3af.
Strike Kuluo_1d5c1d91	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 1d5c1d91765a64808c6ee8452b3ad55e.

<b>Name</b>	<b>Description</b>
Strike Kuluoz_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 Kuluoz_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 Kuluoz_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 Kuluoz_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.
Strike Kuluoz_22fbf3b7	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 22fbf3b79f80ab0ee9850316a402fa58.
Strike Kuluoz_2470172c	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 2470172c7e9f2ead84917c01bb009992.
Strike Kuluoz_287f6409	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 287f6409bcd54c59c175fce1abb995.
Strike Kuluoz_291eb74d	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 291eb74d506802c09985eefcd7b55f43.
Strike Kuluoz_29ff333d	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 29ff333df9b82790a19b06bce2696586.
Strike Kuluoz_2affda67	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 2affda6728c1e7df9c897ae43f7e4847.

<b>Name</b>	<b>Description</b>
Strike Kuluoz_2ebfec62	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 2ebfec626dce31ca659db6d32b3baabc.
Strike Kuluoz_2f1e72c7	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 2f1e72c7c360157a2842eda8663cae52.
Strike Kuluoz_317767f7	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 317767f77668bbd3f31cf19b7c0fbfb99.
Strike Kuluoz_330ba1d3	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 checksum removed in the PE file format. The MD5 hash of this Kuluoz sample is 330ba1d383004c9ca6dca37fbbea2467.
Strike Kuluoz_351a9389	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 351a938965339a71b890c26f163da37f.
Strike Kuluoz_3531fecd	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 3531fecd47a9757aaa8ec5015380e0fe.
Strike Kuluoz_36b27d3c	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 36b27d3ccb0ff0a08c92098a6f2fa708.
Strike Kuluoz_3d2be4f6	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 3d2be4f6be65738d71e6f84c737d4f59.
Strike Kuluoz_3e015bab	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 3e015bab445cb876363cd4a4c66d801.
Strike Kuluoz_40f9503f	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 40f9503fcdbb866cd1492c494b32c411.

<b>Name</b>	<b>Description</b>
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.
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 4899bfe897fb03d2a59beac556f29c5.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 600b87cfeb2352e0710a32ab9787d9f5.
Strike Kuluo_6302a1e7	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 6302a1e74ad439abe9f38f2d28ff846d.
Strike Kuluo_639147d6	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 639147d6eae567f8d88715bef315905c.
Strike Kuluo_65d19829	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 65d19829875f1513eea13f0bbe2947c8.
Strike Kuluo_678fa6d7	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 678fa6d7254b0ab4ed2f895256f03c17.
Strike Kuluo_681b9704	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 681b97043169c2431ddbbe457e3ab85d.

<b>Name</b>	<b>Description</b>
Strike Kuluo_68dfa31b	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 68dfa31bf8c4a2056cff7f037396a21f.
Strike Kuluo_6aa2aaf7	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 6aa2aaf7d3b701812b6515644d2598d0.
Strike Kuluo_6b3de80c	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 6b3de80c056c5ce27414a16f1b3e0c8b.
Strike Kuluo_6c605ebf	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 6c605ebf5c50898355ad69027897198f.
Strike Kuluo_6fdd6663	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 6fdd666304034cb79543a52aac70f787.
Strike Kuluo_723dc107	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 723dc107a8b1ac080ea3e5ac641dbc68.
Strike Kuluo_7539c94b	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 7539c94b87c2f141589181e77b57d6b5.
Strike Kuluo_770e42fa	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 770e42fa612a899ed1c87a5b46cc466f.
Strike Kuluo_77aca864	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 77aca864bb43d404baa9ecfb97d130d.
Strike Kuluo_77e14aca	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 77e14aca659a6bd06a52e0faad013826.

<b>Name</b>	<b>Description</b>
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.
Strike Kuluoz_86631965	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 866319652a22b4be324d298aefda62b7.
Strike Kuluoz_8c50454c	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 8c50454c2720cd0b8c50aa7977dbc28a.
Strike Kuluoz_8f5c3202	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 8f5c320206923f7e06ff383791843518.
Strike Kuluoz_93793281	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 937932817fad19389760ab3a9880d0fe.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike Kuluo_z_a250b5c8	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 a250b5c892d7c5b73d1d37b5305b1898.
Strike Kuluo_z_a26c6aca	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 a26c6aca229b4012e78497689baac26f.
Strike Kuluo_z_a2afe5d1	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 a2afe5d161efec64eb761c98bd78a778.
Strike Kuluo_z_a2d400fe	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 a2d400fec6cc641a1cbe40e3eda7033.
Strike Kuluo_z_a6584ff4	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 a6584ff407513e6bb84599908b01b78a.
Strike Kuluo_z_a7d2ae19	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 a7d2ae192489f6494346f91efb1bfe83.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike Kuluoz_c5ac8863	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 c5ac8863efddb0bc1dc7781353a4ac06.
Strike Kuluoz_c68b0470	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 c68b0470a04ba3eb2a42ebe8bf04f9ae.
Strike Kuluoz_c6f79921	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 c6f7992199f83d089e6c108b6b0896ff.
Strike Kuluoz_c806314b	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 c806314b2408d24675193f8d57ea13c5.
Strike Kuluoz_c8984053	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 c8984053c52f9c5aa349cc2023d482bb.
Strike Kuluoz_c90925bd	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 c90925bd4346ed71a973b82f63aae70f.
Strike Kuluoz_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 Kuluoz_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 Kuluoz_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 Kuluoz_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.

<b>Name</b>	<b>Description</b>
Strike Kuluoz_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 Kuluoz_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 Kuluoz_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 Kuluoz_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 Kuluoz_db75c1d3	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 db75c1d3275504ef331f667fa7d3b79c.
Strike Kuluoz_dc03588f	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 dc03588f2f3ff5a9797f2ee2e23c1473.
Strike Kuluoz_e0389d5e	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 e0389d5e1468add772d596c39e3f58c.
Strike Kuluoz_e38266f7	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 e38266f7609f8a8038cc707ac3981e5b.
Strike Kuluoz_e41c6689	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 e41c66894d11d3cf4f599785ab6b554b.
Strike Kuluoz_e492fc18	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 e492fc1829fdd76ba7a8a0092f0a8b2a.

<b>Name</b>	<b>Description</b>
Strike Kuluoz_e4c1130b	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 e4c1130b2e0c2b07ddd4ff633be95408.
Strike Kuluoz_e5e03f8f	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 e5e03f8fe42271ebe1c3f93d223cd726.
Strike Kuluoz_e76477e1	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 e76477e155e9b21069f8c7dfb2722cfc.
Strike Kuluoz_e9431443	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 e9431443b0061f5e1ed3ca59bf265c23.
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.

<b>Name</b>	<b>Description</b>
Strike Kuluo_z_f7e2deea	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 f7e2deea538a9efb9e03f2c7750a94f8.
Strike Kuluo_z_f818a873	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 f818a8731476ae4471e348d2b6ecda94.
Strike Kuluo_z_fe82f4f2	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 fe82f4f2854df62c607a4a2a2e053e79.
Strike Kuluo_z_ffdb03de	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 ffdb03defeb3b3edabae49fc1b0c360d.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike Letscall_96c8a39b	<p>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 96c8a39be11aa3e22140bcea6d3a1198.</p>
Strike Letscall_e84d00df	<p>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.</p>
Strike Liberator_5acdd854	<p>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.</p>
Strike Liberator_5c0693ed	<p>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.</p>
Strike Liberator_62b9e5b4	<p>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.</p>
Strike Liberator_876b71d3	<p>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.</p>

<b>Name</b>	<b>Description</b>
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 d60e2151cc438b1c6378d23aed7f3b1.
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.

<b>Name</b>	<b>Description</b>
Strike Lightrail_a5fdf55c	This strike sends a malware sample known as Lightrail. Lightrail is a tunneeler 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 tunneeler 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 tunneeler 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 tunneeler 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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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_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.

<b>Name</b>	<b>Description</b>
Strike Liontail_f0dfb7bf	This strike sends a malware sample known as Liontail. Liontail 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. Liontail 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 Liontail 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 1536ec56d69cc7e9aebb8fdb0d3277c4.
Strike LitterDrifter_1da0bf90	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.
Strike LitterDrifter_2239800b	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 2239800bfc8fdfdd78229f2eb8a7b95.
Strike LitterDrifter_2996a70d	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.

<b>Name</b>	<b>Description</b>
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>
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_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>

<b>Name</b>	<b>Description</b>
Strike LitterDrifter_8096dfa	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 8096dfa954113242011e0d7aaaebffd.
Strike LitterDrifter_83500309	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.
Strike LitterDrifter_96db6240	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.
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.

<b>Name</b>	<b>Description</b>
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_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 0859a78bb06a77e7c6758276eafbef9.
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_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_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.
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 207718c939673a5f674ce51f402cf06.
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_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_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.

<b>Name</b>	<b>Description</b>
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 5cc28691fdcaa505b8f453e3500e3d690.
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_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_83b0fc1	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 83b0fc1bd3190c5badcea4d507b8c95.
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_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_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_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.

<b>Name</b>	<b>Description</b>
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_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_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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 141c2a99ec6c365eebcfe39e8dd84be3.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 2992b0b080ab66fc660f9e1f6db0e6d.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 3f2e92568e3e77e88dc3a0fb6755a79.
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.
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.

<b>Name</b>	<b>Description</b>
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 4d198d9c0564a594ce46be7bce19edde6.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 8caa05af7060f02bab07ccfb6ac42d6.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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_985dc1f	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 985dc1f24eba6bb96148752cc35bd28.
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.

<b>Name</b>	<b>Description</b>
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 9a53b56adecec33768f427031a3e068d.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 c102ca2e4e64d11889524a1b56fcd4ad.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 deeee41bfad6e302d1a7ceeb22f6abb.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 f3821f00986bcfeae38622179fc49f5c.
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.
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.

<b>Name</b>	<b>Description</b>
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 Lydرا_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 Lydرا_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 0af3b3f763055e7c0437e5f0b57eaaf.
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.

<b>Name</b>	<b>Description</b>
Strike Lydra_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 Lydra_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 Lydra_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 Lydra_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 Lydra_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 Lydra_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.
Strike Lydra_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 Lydra_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 Lydra_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 Lydra_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 840710a56264b708f3eb3bbc5c1321d.

<b>Name</b>	<b>Description</b>
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 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.
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.

<b>Name</b>	<b>Description</b>
Strike Lydra_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 Lydra_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.
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.

<b>Name</b>	<b>Description</b>
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.
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 4b9c69fb12988796f94b9bfeaddbb6d.

<b>Name</b>	<b>Description</b>
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.
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 e966bf21c1c69b3dcebdc4da19c08466.

<b>Name</b>	<b>Description</b>
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.
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.

Name	Description
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.
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.

<b>Name</b>	<b>Description</b>
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 b9078b6db33deb83201c8d2cbb3ced4e.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 cf32d73c501d5924b3c98383f53fd451.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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_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.
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 6a449567f353dce7cef5bc10c334655.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 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.
Strike Moqhao_6b3a51e0	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.

Name	Description
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>

<b>Name</b>	<b>Description</b>
Strike MuddyC2Go_db0e68d7	<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 db0e68d7d81f5c21e6e458445fd6e34b.</p>
Strike MuddyC2Go_e07adc4e	<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 e07adc4ee768126dc7c7339f4cb00120.</p>
Strike MuddyC2Go_f08aa714	<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 f08aa714fd59b68924843cbfddac4b15.</p>
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>

<b>Name</b>	<b>Description</b>
Strike MuddyC2Go_fe5f94e5	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.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 5fd23435c94a809ec2351a44137fcfc.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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_fbfbb66e	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 fbfbb66e81bbbd6156f6c62a5b5ee138.
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.

<b>Name</b>	<b>Description</b>
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 659c4b68f2027905def1af9249feebb3.
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.

<b>Name</b>	<b>Description</b>
Strike Neflim_ce3cd1da	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 ce3cd1dab67814f5f153bccdaf502f4c.
Strike Neflim_dc88265c	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 dc88265c361d73540a31c19583271fb0.
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 0b33471bbd9fbff08983eff34ee4ddc9.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 3cf36a72db703e25aec51eb74f0feb.
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.

<b>Name</b>	<b>Description</b>
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.
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 9172586c2f870ab76eb0852d1f4dfaee.
Strike Netwalker_93f91bfcc1bf0c858fc7f3bd4536eba6	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.

<b>Name</b>	<b>Description</b>
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 b49ea17739f484b2cccf79f245186f3.
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.
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.

<b>Name</b>	<b>Description</b>
Strike NineRAT_12e39941	<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 12e399411185e386c863954eaa6f6595.</p>
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>

<b>Name</b>	<b>Description</b>
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>
Strike NineRAT_ea853503	<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 ea853503ca1681e07de3e556604c4af7.</p>
Strike Nood RAT_0a35e06f	<p>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&amp;C server. The MD5 hash of this Nood RAT sample is 0a35e06f53c17ab1c8e18e7e0c0821d8.</p>
Strike Nood RAT_35743db3	<p>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&amp;C server. The MD5 hash of this Nood RAT sample is 35743db3dc333245ef5b69100721ced9.</p>
Strike Nood RAT_4f3afdcf	<p>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&amp;C server. The MD5 hash of this Nood RAT sample is 4f3afdcfff8f7994b7d3d3fbbaa6858b4.</p>

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

Name	Description
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 c1f0c0b7a75e3b39d592fdbd76bb49fc4.
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.

<b>Name</b>	<b>Description</b>
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.
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 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 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 victims 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.

<b>Name</b>	<b>Description</b>
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.
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 has been encrypted. The MD5 hash of this malware sample is 5948461cacbeb2543f52ac0a08161884.

<b>Name</b>	<b>Description</b>
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 has been encrypted. The MD5 hash of this malware sample is 91b14bf2b8c4a588fdf7f37e6c79b3fd.
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.

<b>Name</b>	<b>Description</b>
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.
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_aa03fbbd	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 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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 9f8e8dd6c3b95d095fdd39687b2b6a0b.
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.
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.

<b>Name</b>	<b>Description</b>
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 b2f82fffaf5edbdc741cc7423c54a204.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 cfd7809538b65db8f8d3fb645b93e03.
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.

<b>Name</b>	<b>Description</b>
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 da3b944da04513346d8edeb4304fefc1.
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.
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.

<b>Name</b>	<b>Description</b>
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 e5a95f5f45d3af5f9f3d0f27692def5.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 1ab83ff93da4ce0da0fc706f6bc8228.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 36a4df9b0ab0f2d3af615f775d3dba9c0.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 62db37de46ba0bcc9411ba2a2a35827.

<b>Name</b>	<b>Description</b>
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.
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 7bec66ed971abfbff9b25447a39fcae.
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.

<b>Name</b>	<b>Description</b>
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.
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 99643fddadebf383c3541121edd2d6d7.

<b>Name</b>	<b>Description</b>
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 a242ae568af1fede9d7540da878e817c.
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.
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 ae2833fc5def4beb9797e7694f8208.
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 afae38a2c92cbe37c3ef6b1414e1f4e.
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 b288040040a839a5bff8b5e1dc60a89.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 e48ac0ab19c5b5599c45e9846fffb1de.
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.
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.

<b>Name</b>	<b>Description</b>
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 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.

<b>Name</b>	<b>Description</b>
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.
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 18786bfa1be0ddf23ff94c029ca4d63.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike REvil_b26fb99	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 b26fb999449caad351b18364a17bd6e.
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 b67606d382f50ebf76848d023dece20.
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 cce629db2606ae98ba6e931adbf1aeae.
Strike REvil_ce1eeffe4	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 ce1eeffe48010f4946cf45ffd6c4bebfa.

<b>Name</b>	<b>Description</b>
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.
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 ffedad13fdb2cf0996cf728e8c1b4c11.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 29442acfe82ca85c78134021d6064d37.
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.
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.

<b>Name</b>	<b>Description</b>
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 3703f175acf146e4269949a95dd5aa8.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 68464084c82fb09faebcbf040dfc7c4.

<b>Name</b>	<b>Description</b>
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.
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 7bbe1db690fc36ae9801c66034bb326.
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 7c3272f758022b290addbab3710823a.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 a43b1f59decbaa066b65e4e83f644ed.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 ccbf0c6561f9f4cbd092bbcab0455734.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

Name	Description
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 75181839d4eca01c095f5976cf06f71.
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.

<b>Name</b>	<b>Description</b>
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.
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 e4b3a9f9e5e90ce3912665ffb7e0f6f8.
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.

<b>Name</b>	<b>Description</b>
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.
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 0dd8ba9e4af52d8cf1f12b856f44060.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 408a2d09fdd9ba44cac548bb77173a7.
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 47edd917ab49602626cfe46c6781c87e.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 967d450cda75fad84009f55723311d0.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 faffdf7c523de20379785fdbbef179f0.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 fd1facf3a3fca0fd6108bbbe98f8d5fd.
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 252fd12929535d1f2dff12d7193c021.
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.

<b>Name</b>	<b>Description</b>
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.
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 .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.

<b>Name</b>	<b>Description</b>
Strike Redline_8ed60c6e	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 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 .NET, and it has been packed using upx packer with the default options. 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 .NET, and it has a random section name renamed according to the PE format specification. 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 .NET, and it has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Redline sample is a396d712ef77c30f53b6299bfe4a28d3.
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.

<b>Name</b>	<b>Description</b>
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, and it can be purchased on hacking forums 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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike RemcosRAT_145349bb	<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 145349bbf829a5f9276096963902e4ce.</p>
Strike RemcosRAT_239898c6	<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 239898c682bcb7091aaa57cd6d70f736.</p>
Strike RemcosRAT_2bb1eae8	<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 2bb1eae8d55eb6bb5607065a241622a2.</p>
Strike RemcosRAT_3e1a5431	<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 3e1a54314b67d65e343d7ded3466f8c1.</p>
Strike RemcosRAT_4b724c9c	<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 4b724c9c3ce7abc1612f4f811a01ca96.</p>

<b>Name</b>	<b>Description</b>
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 6ae9e6b744b2779965c89e3bebcefa94.
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.
Strike RemcosRAT_8c080870	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.
Strike RemcosRAT_8f70e913	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.

<b>Name</b>	<b>Description</b>
Strike RemcosRAT_a86a836f	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 MD5 hash of this RemcosRAT sample is a86a836fc04ddabe4d35d3f240051915.
Strike RemcosRAT_a9489436	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.
Strike RemcosRAT_acc101b0	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.
Strike RemcosRAT_bb4891f8	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.

<b>Name</b>	<b>Description</b>
Strike RemcosRAT_ca84ab08	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.
Strike RemcosRAT_d2db8289	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.
Strike RemcosRAT_d60fa5f2	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.
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.

<b>Name</b>	<b>Description</b>
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 f6118a965e44ee55e708edf7adcdc1df.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 31266fefafa52798b306939c3fc169c0ea.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 75923cf648fa5660efe85589465266f9.
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.
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.

<b>Name</b>	<b>Description</b>
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 7f0579cf1e45669bc3308e7c70d8dff.
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.
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.

<b>Name</b>	<b>Description</b>
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 a902c80fc532b5baf357a4b6a6583ec.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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_cbc03f7	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 cbc03f7d4b73b42caf9d613050dc414.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 fbcad086e0b20b839ce4f29362624146.
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.
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.

<b>Name</b>	<b>Description</b>
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 61384796b20744038fee8c26dde1c4e.
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.

<b>Name</b>	<b>Description</b>
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 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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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_7fdbc96e	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 7fdbc96ea01f7c0e4410014ce7b9127e.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 SUBTLE-PAWS_03eacabd	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 & 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.
Strike SUBTLE-PAWS_0df2774f	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 & 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.

<b>Name</b>	<b>Description</b>
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 1950b7fcf347e03505327579a9e98b55.</p>
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>

<b>Name</b>	<b>Description</b>
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>
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>

<b>Name</b>	<b>Description</b>
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>
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_c3e19bfb	<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 c3e19bfb6fc6299dd1e0cba17b1f06c6.</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>

<b>Name</b>	<b>Description</b>
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_d86eede8	<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 d86eede8a5c4d87879a8d2c9ffd44287.</p>
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>

<b>Name</b>	<b>Description</b>
Strike SUBTLE-PAWS_eaae2db7	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 & 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 eaae2db7cf9cf9deb15c70fad26d76d0.
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.

<b>Name</b>	<b>Description</b>
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.
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 36a91fe472d4ddfff1c296a3e798deed.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 9adb6b64a3edebaea039c4f45bee5bef.
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.

<b>Name</b>	<b>Description</b>
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.
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.

Name	Description
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 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.
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.

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_1adbaaa3	<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 1adbaaa352a8366c03faaa44fc5d4687.</p>
Strike SolarPhantom_23807082	<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 23807082358d736404cf935fe7c65b5.</p>
Strike SolarPhantom_38cbe65f	<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 38cbe65f8d2221a6c1b32abd4c96206d.</p>
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>

<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_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>
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>

Name	Description
Strike SolarPhantom_80b2e25a	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.
Strike SolarPhantom_848af416	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.
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.

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_afecc46a	<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 afecc46a346af09f5a9b4c7739986a8d.</p>
Strike SolarPhantom_b3447a64	<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 b3447a648b588d2fc40cdd5b3eb7542e.</p>
Strike SolarPhantom_b62aa586	<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 b62aa5869c43fb9995aed9ec33ce41b.</p>
Strike SolarPhantom_bf55a651	<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 bf55a651364edeb64f2e37ff86a094b8.</p>

Name	Description
Strike SolarPhantom_d3274945	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.
Strike SolarPhantom_e4d1337f	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.
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.

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_fea30627	<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 fea30627a4cdb82aaf9d0d7a47b46115.</p>
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>

<b>Name</b>	<b>Description</b>
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>
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>

<b>Name</b>	<b>Description</b>
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>
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 a4b83ae23cc959f8244060783982bfa.</p>

<b>Name</b>	<b>Description</b>
Strike SpyLoan_cd15f394	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.
Strike SpyLoan_da1580cb	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.
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.

<b>Name</b>	<b>Description</b>
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 fd2750e3be8c5ad625bedbeba8f03b.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike Sunburst_2c4a910a	<p>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.</p>
Strike Sunburst_56ceb6d0	<p>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.</p>
Strike Sunburst_731d724e	<p>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.</p>
Strike Sunburst_846e27a6	<p>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.</p>
Strike Sunburst_b91ce2fa	<p>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.</p>

<b>Name</b>	<b>Description</b>
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 e49aaa9a5933c48fec39f3080a7b94d.
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.

<b>Name</b>	<b>Description</b>
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.
Strike SysJoker_2eafd0c5	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 2eafd0c5c2bf567631e08c999edb17cd.
Strike SysJoker_31c2813c	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.

Name	Description
Strike SysJoker_9416d7dc	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.
Strike SysJoker_c2848b4e	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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike TA402_f321fcf	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.

<b>Name</b>	<b>Description</b>
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 3b417b51e1d7c4289a47fb07cfa309fd.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
Strike Tedy_f07edfcfd	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 f07edfcfd02e0bd17ccfc5c24cbe41466.
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 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 00658cacac94f6d736a67b553302c7980.
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 02689622fffb34c0b816a26f937bc2c8.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 412f4761dcf9e20ad8a05a16663fbcc7e.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 8a5d68384093d008fded0bbcfb29fc42.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 f5c24ce99fc9ff25cf8bdfe7c033.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 04420a52469fa8c3dece0126fdcb7e80.
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.
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.

<b>Name</b>	<b>Description</b>
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_0fbba702a	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 0fbba702ad70f4ad393a2d97c99289a15.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 26b8e67bbcce94745b87a541c867f9ee8.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 5d9d5845db1526c160a1cc0791cfa49c.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 949e4fddcd7de77db26dcdaef532bf79a.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 c7cbc36f31fcf55b87796f18cb009606.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 f35913834ff4b111ee7971561136d185.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 30559fb94b2a673067d6dfbb21d42c0.
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.

<b>Name</b>	<b>Description</b>
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 31a7a4756aeb04493094f0f16eb9f68.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 a73478e7f62a5856aeed787188c8f777.
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.
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.

<b>Name</b>	<b>Description</b>
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 bd704697b8fece91346d861844017808.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 fb1458288b548f5c3c20c4fe985bd969.
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 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.

<b>Name</b>	<b>Description</b>
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.
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 9e75705b4930f50502bcd740fc3ece1.
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.

<b>Name</b>	<b>Description</b>
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.
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 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.

<b>Name</b>	<b>Description</b>
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.
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 2784f9de40228cb4e33fc9087272b61.
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.

<b>Name</b>	<b>Description</b>
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.
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 5954c22bbc31a84fcdb8d2c52cc5e584.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 94badbcde0d0f8c50cca6a841c2eb40.
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.
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 b1de5235a3e3429f25828979ddfd0be7.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

Name	Description
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.
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.

<b>Name</b>	<b>Description</b>
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 1539d1f4c573d787e07ddc605cafa450.
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 1d68af9dc752856b0c403efffacac46c8.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 7818811bb3842ce5cdc17e5143fc947.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 d82397fbb236c86fdd352c86b4871045.
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.

<b>Name</b>	<b>Description</b>
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.
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 e75f00bfbbaa72b44532eae3fcf4fc20.
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.

<b>Name</b>	<b>Description</b>
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.
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 fb8cb8cb1e358d57c0a43cb4cc6f977f.
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.

Name	Description
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 643fbcd0041c2b57a2740bb02e16db0.
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 7031a1138e1892fb09bfbdf518dba07b.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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_b90fb7a	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 b90fb7ae572eca2f64d14c0e0dc4a21.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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_406fce2	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 406fce22aa3fd15b761f2da6cce7bc1.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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_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_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.

<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_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_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 37fdc1d68ff770bd1f1f464c431728f07.
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.

<b>Name</b>	<b>Description</b>
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_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_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_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 5761439abee0c77d907849fe1adc11c.
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.
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_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.

<b>Name</b>	<b>Description</b>
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_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_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_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_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_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_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.
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.

<b>Name</b>	<b>Description</b>
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_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.
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.

<b>Name</b>	<b>Description</b>
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_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.
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_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_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.

<b>Name</b>	<b>Description</b>
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.
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_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_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_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.

<b>Name</b>	<b>Description</b>
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 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.

<b>Name</b>	<b>Description</b>
Strike Vultur_753bf0cd	<p>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 753bf0cd0e154893f8bd36c12740a7ed.</p>
Strike Vultur_8bc072db	<p>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.</p>
Strike Vultur_8e83d178	<p>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.</p>
Strike Vultur_979bd87a	<p>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 979bd87a975a128fe51cd46eaef2123.</p>
Strike Vultur_a02059f5	<p>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.</p>

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
Strike WhisperGate Downloader_bfb1c2c2	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 bfb1c2c22ed861fb7435533378304574.
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.

Name	Description
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 0424b9dca148e291178aca85797b9e3.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 da8e17f6380a617142636b0927abbecf.
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 e194825fe6454a69ff1d74313afdf43d4.
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.

<b>Name</b>	<b>Description</b>
Strike WyrmSpy_f499f7e4	<p>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.</p>
Strike WyrmSpy_feea40f6	<p>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.</p>
Strike Xamalicious_0ffda3a3	<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. '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 0ffda3a31c5f1ff988a9db7d3195d718.</p>
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. '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. '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>

<b>Name</b>	<b>Description</b>
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>
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.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.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>

<b>Name</b>	<b>Description</b>
Strike XenomorphV3_8ce057ff	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 8ce057ff57478e98c0e246355cccd27db.
Strike XenomorphV3_a2efff06	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.
Strike XenomorphV3_dd82858b	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.
Strike XtremeRAT_00656070	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.
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.

<b>Name</b>	<b>Description</b>
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 0df4f4f5d006c793ef0cfa500a3e16d.
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.
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.

<b>Name</b>	<b>Description</b>
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 277609ed83e6f042e185c3d5740feb.
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 58f35ba4608b5371cfecb575026c957af.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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 a344bf734cde979206eefb19372a4acf7.
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.

<b>Name</b>	<b>Description</b>
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_a8502dfe	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 a8502dfeaaf19b633bdf35b0058c95ad.
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 ab115bd7a7ca4c70c3acb81ed682e.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 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.

<b>Name</b>	<b>Description</b>
Strike Zardoor_60d5648d	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 60d5648d35bacf5c7aa713b2a0d267d3.
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.
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.

Name	Description
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.
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 Zardoor_ec956ae1	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 ec956ae1cd30bad3ebd55a984ce3d9ed.
Strike Zardoor_f8b31864	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 f8b318648494128da3b35f659526365b.
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.

<b>Name</b>	<b>Description</b>
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.
Strike Zbot_7fffdd12	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 7fffdd12a34a3016695ee2de18e9d387.
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.

<b>Name</b>	<b>Description</b>
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.
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 fe2e0db42c21c90dcdbde0983ab89276.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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 461c6d648ad38ea49feb08a5f7a34d8.
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 582433da271d3f4c78027bbbeba4e4c.
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 5bde8a697c4ed4b020035278f48ebca.
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.
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.

<b>Name</b>	<b>Description</b>
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.

<b>Name</b>	<b>Description</b>
Strike brokewell_ddbf3a1d	<p>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.</p>
Strike cherryblos_028622ca	<p>This strike sends a polymorphic malware sample known as CherryBlos. It is an android malware which is designed to steal cryptocurrency wallet-related credentials and replace a victim's wallet address when they make withdrawals. The malware is distributed through fake Android apps on Google Play, social media platforms, and phishing sites. The malware makes use of Android's accessibility service which prevents it from being killed and often uses fake user interfaces that look like official apps to steal passwords. CherryBlos can utilize OCR to extract text from images stored on the device. This poses a risk when people store cryptocurrency wallet recovery codes as photos on their devices, as the malware can potentially access and misuse these codes to gain unauthorized access to crypto wallets. 'com.example.walljsdemo' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this CherryBlos sample is 028622cab0efe5df725d9afd9681912d.</p>
Strike cherryblos_718dc1f6	<p>This strike sends a polymorphic malware sample known as CherryBlos. It is an android malware which is designed to steal cryptocurrency wallet-related credentials and replace a victim's wallet address when they make withdrawals. The malware is distributed through fake Android apps on Google Play, social media platforms, and phishing sites. The malware makes use of Android's accessibility service which prevents it from being killed and often uses fake user interfaces that look like official apps to steal passwords. CherryBlos can utilize OCR to extract text from images stored on the device. This poses a risk when people store cryptocurrency wallet recovery codes as photos on their devices, as the malware can potentially access and misuse these codes to gain unauthorized access to crypto wallets. 'com.example.walljsdemo' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this CherryBlos sample is 718dc1f6de73a68d80c07a625f53a732.</p>
Strike cherryblos_e355f014	<p>This strike sends a malware sample known as CherryBlos. It is an android malware which is designed to steal cryptocurrency wallet-related credentials and replace a victim's wallet address when they make withdrawals. The malware is distributed through fake Android apps on Google Play, social media platforms, and phishing sites. The malware makes use of Android's accessibility service which prevents it from being killed and often uses fake user interfaces that look like official apps to steal passwords. CherryBlos can utilize OCR to extract text from images stored on the device. This poses a risk when people store cryptocurrency wallet recovery codes as photos on their devices, as the malware can potentially access and misuse these codes to gain unauthorized access to crypto wallets. 'com.example.walljsdemo' is the package name of the malware sample. The MD5 hash of this CherryBlos sample is e355f01472bc880619bf9fe930cd5743.</p>

<b>Name</b>	<b>Description</b>
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_915b0fb	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 915b0fb556fe6f8a48c3f5da0cb28ec.
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.

<b>Name</b>	<b>Description</b>
Strike donot_13f3862b	<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. Constant strings in the code of the malware have been encrypted. The MD5 hash of this malware sample is 13f3862bce2b20b7e2a8aa39b18eab3d.</p>
Strike donot_14302b21	<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 malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 14302b218060aacc3e9ee23d09feffb.</p>
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>

<b>Name</b>	<b>Description</b>
Strike donot_22043936	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 22043936d5b59339d628aaf54d42c996.
Strike eXoticVisit_15f2f960	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.
Strike eXoticVisit_1910399f	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.
Strike eXoticVisit_1f82b889	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.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.

<b>Name</b>	<b>Description</b>
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>
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>

<b>Name</b>	<b>Description</b>
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. 'com.egoosoft.siminfo' is the package name of the malware sample. Constant strings in the code has 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>
Strike hiddenad_2199cc1d	<p>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.</p>
Strike hiddenad_baa63680	<p>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.</p>

<b>Name</b>	<b>Description</b>
Strike hiddenad_df520950	<p>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.</p>
Strike napchat_23955a9a	<p>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.</p>
Strike napchat_26850d7b	<p>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.</p>
Strike napchat_737a07be	<p>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.</p>

<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_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.
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.

<b>Name</b>	<b>Description</b>
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 e3dc900cce448b432e1b1662b3fd36d.
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 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.
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.

Name	Description
Strike spynote_026fae1c	<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 026fae1c816399a5c18da7b70567b70e.</p>
Strike spynote_3f59e1ea	<p>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.</p>
Strike spynote_92df3770	<p>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.</p>
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>

<b>Name</b>	<b>Description</b>
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_6d98034e	<p>This strike sends a malware sample known as triada. It's an android malware which poses as the telegram app. 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. 'org.telegram.messenger' is the package name of the malware sample. The MD5 hash of this triada sample is 6d98034ee48ee1e055f3f50fd2a5b31a.</p>
Strike triada_c5822691	<p>This strike sends a malware sample known as triada. It's an android malware which poses as the telegram app. 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. 'org.telegram.messenger' is the package name of the malware sample. The MD5 hash of this triada sample is 6d98034ee48ee1e055f3f50fd2a5b31a. The malware has been rebuilt without any modifications.</p>
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.lhmrsg.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>

<b>Name</b>	<b>Description</b>
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_015f01ca	<p>This strike sends a 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.provide.badge' is the package name of the malware sample. The MD5 hash of this wyrmspy sample is 015f01cacca56bb4c8b1978a29194491.</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.provide.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>

Name	Description
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_9c1bed66	<p>This strike sends a 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 MD5 hash of this wyrmspy sample is 9c1bed665f214e8fc77fc388baedc2a1.</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>

<b>Name</b>	<b>Description</b>
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>
Strike zanubis_248b2b76	<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 248b2b76b5fb6e35c2d0a8657e080759.</p>
Strike zanubis_5f1f70d4	<p>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.</p>
Strike zanubis_a487e70a	<p>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.</p>

Name	Description
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

<b>Name</b>	<b>Description</b>
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.
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.

Name	Description
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.