Mar 19 2024

NETMANAGEIT

Intelligence Report

From Delivery To Execution: An Evasive Azorult Campaign Smuggled Through Google Sites

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Netskope Threat Labs uncovered an evasive Azorult malware campaign that uses multiple techniques to avoid detection, including HTML smuggling, reflective loading, and AMSI bypass. The campaign tricks users by hosting malicious payloads on fake Google Sites pages and stealing sensitive data including crypto wallet info, credentials, documents, and screenshots from victims.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name
52a0ca6fec42896245bb3b6a7caa876a44779c98102c5e28781cca46bfaf2ed9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '52a0ca6fec42896245bb3b6a7caa876a44779c98102c5e28781cca46bfaf2ed9']
Name
55e283ee275e0367328013dc835cc63338defdcf5b6fe6cd74d6ce2c46af1981
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '55e283ee275e0367328013dc835cc63338defdcf5b6fe6cd74d6ce2c46af1981']
Name

350dae93066ddd84327e87f2bb784dfc0b70178629afd1fae298ee1376d42450

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '350dae93066ddd84327e87f2bb784dfc0b70178629afd1fae298ee1376d42450']

Name

380f9784f4b3db7a711f48baaa2864161ad88b66eec79521011ab8e5871c387a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '380f9784f4b3db7a711f48baaa2864161ad88b66eec79521011ab8e5871c387a']

Name

030b3d76a054d5a48cbb595d49e7e1cbc6dfdddbccd676f9642640f0429bd8c4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '030b3d76a054d5a48cbb595d49e7e1cbc6dfdddbccd676f9642640f0429bd8c4']

Name

e644d5ef63786fd6b732e8837bd7ff974b6c76b06ad9629ff6bf4fccef7ee6cb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e644d5ef63786fd6b732e8837bd7ff974b6c76b06ad9629ff6bf4fccef7ee6cb']

Name

http://mayanboats.com

Description

- **Unsafe:** True - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '11 months ago', 'timestamp': 1682017625, 'iso': '2023-04-20T15:07:05-04:00'} - **IPQS: Domain:** mayanboats.com - **IPQS: IP Address:** 185.132.179.211

Pattern Type

stix

Pattern

[url:value = 'http://mayanboats.com']

Name

http://195.123.220.40/index.php\nhttp://mayanboats.com\n

Pattern Type

stix

Pattern

[url:value = 'http://195.123.220.40/index.php\\nhttp://mayanboats.com\\n']

Name

97c9caaaf7d3861e30d9ff647e952e880b670c5c3dca4537c515b38438ee18ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '97c9caaaf7d3861e30d9ff647e952e880b670c5c3dca4537c515b38438ee18ee']

Name

18a72a5f52e9da32098cb60b38a3b07e311428bb379f1f6d438031337f855d95

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '18a72a5f52e9da32098cb60b38a3b07e311428bb379f1f6d438031337f855d95']

Name

195.123.220.40

Description

- **Zip Code:** N/A - **ISP:** ITL - **ASN:** 21100 - **Organization:** ITL - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** 195.123.220.40 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** Drenthe - **City:** Meppel - **Latitude:** 52.69589996 - **Longitude:** 6.18470001

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.123.220.40']

Name

http://sqjeans.com

Description

- **Unsafe:** False - **Server:** Apache - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** ECommerce - **Domain Age:** {'human': '13 years ago', 'timestamp': 1311412121, 'iso': '2011-07-23T05:08:41-04:00'} - **IPQS: Domain:** sqjeans.com - **IPQS: IP Address:** 72.167.68.119

Pattern Type
stix
Pattern
[url:value = 'http://sqjeans.com']

Malware

Name
Azorult - S0344
Name
infostealer
Name
azorult
Description
[Azorult](https://attack.mitre.org/software/S0344) is a commercial Trojan that is used to steal information from compromised hosts. [Azorult](https://attack.mitre.org/software/S0344) has been observed in the wild as early as 2016. In July 2018, [Azorult](https://attack.mitre.org/software/S0344) was seen used in a spearphishing campaign against targets in North America. [Azorult](https://attack.mitre.org/software/S0344) has been seen used for cryptocurrency theft. (Citation: Unit42 Azorult Nov 2018)(Citation: Proofpoint Azorult July 2018)

Attack-Pattern

Name
T1081
ID
T1081
Name
T1056
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name

T1027

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

T1566

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1497

ID

T1497

Description

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during

automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. (Citation: Unit 42 Pirpi July 2015)

Name

T1112

ID

T1112

Description

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

Name

T1560

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Name

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1140

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

T1003

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools

mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

StixFile

Value
52a0ca6fec42896245bb3b6a7caa876a44779c98102c5e28781cca46bfaf2ed9
55e283ee275e0367328013dc835cc63338defdcf5b6fe6cd74d6ce2c46af1981
350dae93066ddd84327e87f2bb784dfc0b70178629afd1fae298ee1376d42450
380f9784f4b3db7a711f48baaa2864161ad88b66eec79521011ab8e5871c387a
030b3d76a054d5a48cbb595d49e7e1cbc6dfdddbccd676f9642640f0429bd8c4
e644d5ef63786fd6b732e8837bd7ff974b6c76b06ad9629ff6bf4fccef7ee6cb
97c9caaaf7d3861e30d9ff647e952e880b670c5c3dca4537c515b38438ee18ee
18a72a5f52e9da32098cb60b38a3b07e311428bb379f1f6d438031337f855d95

Url

Value
http://mayanboats.com
http://195.123.220.40/index.php\nhttp://mayanboats.com\n
http://sqjeans.com

IPv4-Addr

Value
195.123.220.40

External References

- https://github.com/netskopeoss/NetskopeThreatLabsIOCs/tree/main/Malware/Azorult/IOCs
- https://www.netskope.com/blog/from-delivery-to-execution-an-evasive-azorult-campaign-smuggled-through-google-sites
- https://otx.alienvault.com/pulse/65f8128f333d80e67df7261a