Sep 18 2023

NETMANAGEIT

Intelligence Report

New MidgeDropper Variant

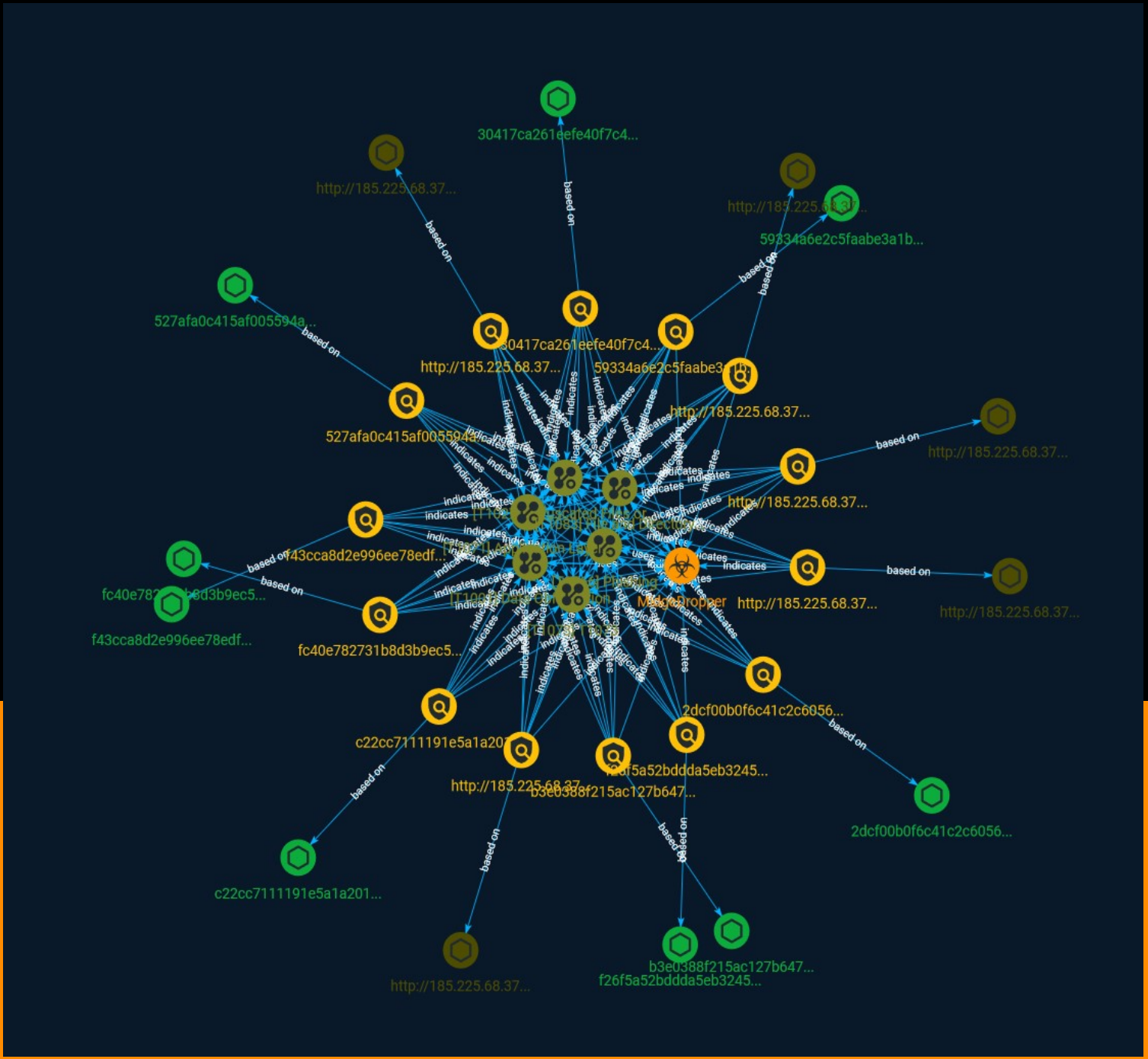

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The previously unseen dropper variant recently found, named MidgeDropper, has a complex infection chain that includes code obfuscation and sideloading, making it an interesting use case.

Confidence

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

15 / 100

Attack-Pattern

Name
Phishing
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

Data Obfuscation

ID

T1001

Description

Adversaries may obfuscate command and control traffic to make it more difficult to detect. Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

Name

Obfuscated Files or Information

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

T1073

ID

T1073

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

File and Directory Discovery

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Indicator

Name

30417ca261eefe40f7c44ff956f9940b766ae9a0c574cd1c06a4b545e46f692e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '30417ca261eefe40f7c44ff956f9940b766ae9a0c574cd1c06a4b545e46f692e']

Name

2dcf00b0f6c41c2c60561ca92893a0a9bf060e1d46af426de022d0c5d23d8704

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2dcf00b0f6c41c2c60561ca92893a0a9bf060e1d46af426de022d0c5d23d8704']

Name

fc40e782731b8d3b9ec5e5cf8a9d8b8126dc05028ca58ec52db155b3dadc5fc6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fc40e782731b8d3b9ec5e5cf8a9d8b8126dc05028ca58ec52db155b3dadc5fc6']

Name

http://185.225.68.37/jay/nl/VCRUNTIME140_1.dll

Pattern Type

stix

Pattern

[url:value = 'http://185.225.68.37/jay/nl/VCRUNTIME140_1.dll']

Name

b3e0388f215ac127b647cd7d3f186f2f666dc0535d66797b6e1adb74f828254e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b3e0388f215ac127b647cd7d3f186f2f666dc0535d66797b6e1adb74f828254e']

Name
527afa0c415af005594acaac1093a1ea79e3639fa5563602497eabbae7438130
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '527afa0c415af005594acaac1093a1ea79e3639fa5563602497eabbae7438130']
Name
http://185.225.68.37/jay/nl/35g3498734gkb.xn--dat-9o0a
Pattern Type
stix
Pattern
[url:value = 'http://185.225.68.37/jay/nl/35g3498734gkb.xn--dat-9o0a']
Name
c22cc7111191e5a1a2010f4bc3127058bff41ecba8d753378feabee37d5b43bb
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'c22cc7111191e5a1a2010f4bc3127058bff41ecba8d753378feabee37d5b43bb']

Name

59334a6e2c5faabe3a1baf5347ba01f2419d731fcbb7ab1b021185c059c8fa6f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '59334a6e2c5faabe3a1baf5347ba01f2419d731fcbb7ab1b021185c059c8fa6f']

Name

f26f5a52bddda5eb3245161b784b58635ffa2381818816e50b8bae9680ff88eb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f26f5a52bddda5eb3245161b784b58635ffa2381818816e50b8bae9680ff88eb']

Name

f43cca8d2e996ee78edf8d9e64e05f35e94a730fbe51e9feecc5e364280d8534

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f43cca8d2e996ee78edf8d9e64e05f35e94a730fbe51e9feecc5e364280d8534']

Name

http://185.225.68.37/jay/nl/seAgnt.exe

Pattern Type

stix

Pattern

[url:value = 'http://185.225.68.37/jay/nl/seAgnt.exe']

Name

http://185.225.68.37/jay/nl/

Pattern Type

stix

Pattern

[url:value = 'http://185.225.68.37/jay/nl/']

Name

http://185.225.68.37/jay/nl/35g3498734gkb.dat

Pattern Type
stix

Pattern
[url:value = 'http://185.225.68.37/jay/nl/35g3498734gkb.dat']

Malware

Name
MidgeDropper

StixFile

Value
527afa0c415af005594acaac1093a1ea79e3639fa5563602497eabbae7438130
fc40e782731b8d3b9ec5e5cf8a9d8b8126dc05028ca58ec52db155b3dadc5fc6
c22cc7111191e5a1a2010f4bc3127058bff41ecba8d753378feabee37d5b43bb
f26f5a52bddda5eb3245161b784b58635ffa2381818816e50b8bae9680ff88eb
b3e0388f215ac127b647cd7d3f186f2f666dc0535d66797b6e1adb74f828254e
f43cca8d2e996ee78edf8d9e64e05f35e94a730fbe51e9feecc5e364280d8534
2dcf00b0f6c41c2c60561ca92893a0a9bf060e1d46af426de022d0c5d23d8704
59334a6e2c5faabe3a1baf5347ba01f2419d731fcbb7ab1b021185c059c8fa6f
30417ca261eefe40f7c44ff956f9940b766ae9a0c574cd1c06a4b545e46f692e

Url

Value
http://185.225.68.37/jay/nl/35g3498734gkb.dat
http://185.225.68.37/jay/nl/VCRUNTIME140_1.dll
http://185.225.68.37/jay/nl/seAgnt.exe
http://185.225.68.37/jay/nl/35g3498734gkb.xn--dat-9o0a
http://185.225.68.37/jay/nl/

External References

- https://otx.alienvault.com/pulse/650815eae6309eba75a1d6a2
- https://www.fortinet.com/blog/threat-research/new-midgedropper-variant