Oct 29 2023

NETMANAGEIT

Intelligence Report

Organizations under attack from cryptominer-keylogger-backdoor combo

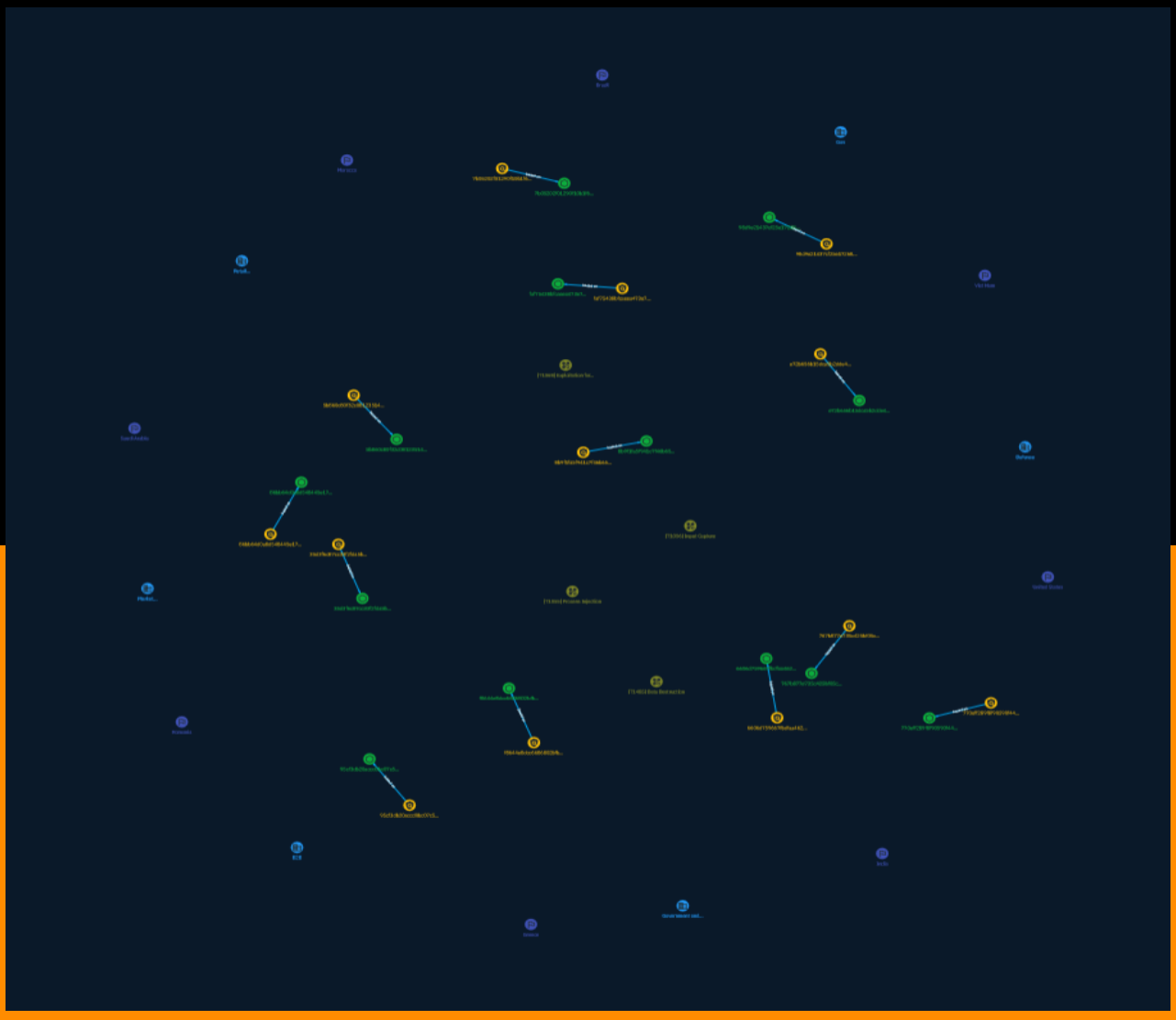

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Sector 10
- Indicator 12
- Country 19

Observables

- StixFile 21

External References

- External References 22

Overview

Description

In April of this year, the FBI published an advisory on attacks targeting government, law enforcement, and non-profit organizations. Attackers download scripts onto victims' devices, delivering several types of malware all at once. The main aim is to utilize company resources for mining, steal data using keyloggers, and gain backdoor access to systems.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Input Capture
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
Process Injection
ID
T1055
Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is

sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Data Destruction

ID

T1485

Description

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018)(Citation: Talos Olympic Destroyer 2018) Common operating system file deletion commands such as `del` and `rm` often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from [Disk Content Wipe](https://attack.mitre.org/techniques/T1561/001) and [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) because individual files are destroyed rather than sections of a storage disk or the disk's logical structure. Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable.(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) In some cases politically oriented image files have been used to overwrite data.(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017) To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Talos Olympic Destroyer 2018). In cloud environments, adversaries may leverage access to delete cloud storage, cloud storage accounts, machine

images, and other infrastructure crucial to operations to damage an organization or their customers.(Citation: Data Destruction - Threat Post)(Citation: DOJ - Cisco Insider)

Sector

Name
Market infrastructures
Description
Encompasses all the systems necessary for the smooth process of market financing operations. Are included payment systems, clearing houses, central securities depositories, securities settlement systems and trade repositories.
Name
Gas
Description
Public or private entities involved in exploration, extraction, refining, transporting and marketing of natural gas products.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Name
Retail (distribution)
Description
Distribution and sale of goods directly to the consumer.
Name
Defense
Description
Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.
Name
B2B

Indicator

Name

8b9f1fa5f941c7f46b65bf8929ca80d132435151e1dcb3a5de7693b70b254467

Description

stack_string SHA256 of a7cde18f991e97037a7899b7669e2548

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b9f1fa5f941c7f46b65bf8929ca80d132435151e1dcb3a5de7693b70b254467']

Name

faf75438bfcaeea473e72aeb5463b4e0f5c41c2afbebf8d94f1373eb7f7ec122

Description

!#LowFiWriteMZInUnusualExtensions SHA256 of 474f517eb23bdfa4c320c091c3eb2dba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'faf75438bfcaeea473e72aeb5463b4e0f5c41c2afbebf8d94f1373eb7f7ec122']

Name

f8644e8dcc6686802bfb8907b772f186aef24090d50c5a370b7919d302e6955a

Description

!#LowFiWriteMZInUnusualExtensions SHA256 of 752940da17469330c38ab98d04f3d6b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f8644e8dcc6686802bfb8907b772f186aef24090d50c5a370b7919d302e6955a']

Name

5b860c80f32c08123514e2cee7fc75b680a3a51c8ac8598a3585b3a16252354d

Description

SHA256 of ddab66730a84583b98d3415f9181d092

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5b860c80f32c08123514e2cee7fc75b680a3a51c8ac8598a3585b3a16252354d']

Name

767b877e735c425bf05c34683356abfde4070b092f17a4741ea5ac490611f3de

Description

SHA256 of ddd12566b99343b96609afa2524ecec3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '767b877e735c425bf05c34683356abfde4070b092f17a4741ea5ac490611f3de']

Name

86bb64d0a8d548445e17d4edef0a0e5f97d019f3af524fc9cd625294916c973d

Description

SHA256 of 3c47d45f09948b8e6fdb5f96523bc60b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '86bb64d0a8d548445e17d4edef0a0e5f97d019f3af524fc9cd625294916c973d']

Name

e72b656b15dca5b2dde4784bb113ca7c9768eeb731264fe10d057fc7909ef9c4

Description

SHA256 of 1da8e7c92c86fc8dbab5287bdca91ca1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e72b656b15dca5b2dde4784bb113ca7c9768eeb731264fe10d057fc7909ef9c4']

Name

6606d759667fbdfaa46241db7ffb4839d2c47b88a20120446f41e916cad77d0b

Description

autoit SHA256 of 0a50081a6cd37aea0945c91de91c5d97

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6606d759667fbdfaa46241db7ffb4839d2c47b88a20120446f41e916cad77d0b']

Name

35d3f6c87cc33f2fda5b594a6990d8d14e085e313564127a9c0606cedb398f93

Description

SHA256 of ac27de51896a5ba2fd0dda9b7955a201

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35d3f6c87cc33f2fda5b594a6990d8d14e085e313564127a9c0606cedb398f93']

Name

98d9e21437cf25e1726848d09de61ef32ff56e0114052b3d05cef84f6f4859f9

Description

!#LowFiWriteMZInUnusualExtensions SHA256 of a38dece5bcb9f6d1c027d86e0318a60e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '98d9e21437cf25e1726848d09de61ef32ff56e0114052b3d05cef84f6f4859f9']

Name

95cf3db20accd0bc07c521284bd3031732c3f10da536e88268852032d789b974

Description

stack_string SHA256 of 227fa5d690a943114ff3ccfe7977192a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '95cf3db20accd0bc07c521284bd3031732c3f10da536e88268852032d789b974']

Name

7b05202f01290f10b1f6bbac4f1e2cbb71c63f56200e574020aae833b0388973

Description

!#LowFiWriteMZInUnusualExtensions SHA256 of 7d0f67343f128d29a50ccd3639b72884

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7b05202f01290f10b1f6bbac4f1e2cbb71c63f56200e574020aae833b0388973']

Name

770eff289f8f90590f44e1c8a05a00079717ded32aff660f127dfdabe79a5c6b

Description

!#LowFiWriteMZInUnusualExtensions SHA256 of 830debd1f6d39c726c2d3208e3314f44

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '770eff289f8f90590f44e1c8a05a00079717ded32aff660f127dfdabe79a5c6b']

Country

Name
Brazil
Name
India
Name
Saudi Arabia
Name
Viet Nam
Name
Greece
Name
Morocco
Name
United States

Name
Romania

StixFile

Value
f8644e8dcc6686802bfb8907b772f186aef24090d50c5a370b7919d302e6955a
6606d759667fbdfaa46241db7ffb4839d2c47b88a20120446f41e916cad77d0b
35d3f6c87cc33f2fda5b594a6990d8d14e085e313564127a9c0606cedb398f93
86bb64d0a8d548445e17d4edef0a0e5f97d019f3af524fc9cd625294916c973d
e72b656b15dca5b2dde4784bb113ca7c9768eeb731264fe10d057fc7909ef9c4
95cf3db20accd0bc07c521284bd3031732c3f10da536e88268852032d789b974
7b05202f01290f10b1f6bbac4f1e2cbb71c63f56200e574020aae833b0388973
767b877e735c425bf05c34683356abfde4070b092f17a4741ea5ac490611f3de
faf75438bfcaeea473e72aeb5463b4e0f5c41c2afbebf8d94f1373eb7f7ec122
8b9f1fa5f941c7f46b65bf8929ca80d132435151e1dcb3a5de7693b70b254467
5b860c80f32c08123514e2cee7fc75b680a3a51c8ac8598a3585b3a16252354d
98d9e21437cf25e1726848d09de61ef32ff56e0114052b3d05cef84f6f4859f9
770eff289f8f90590f44e1c8a05a00079717ded32aff660f127dfdabe79a5c6b

External References

- https://otx.alienvault.com/pulse/65330195bd87e4d1ebf51211
- https://securelist.com/miner-keylogger-backdoor-attack-b2b/110761/