Jan 25 2024

NETMANAGEIT

Intelligence Report

Kasseika Ransomware Deploys BYOVD Attacks, Abuses PsExec and Exploits Martini Driver

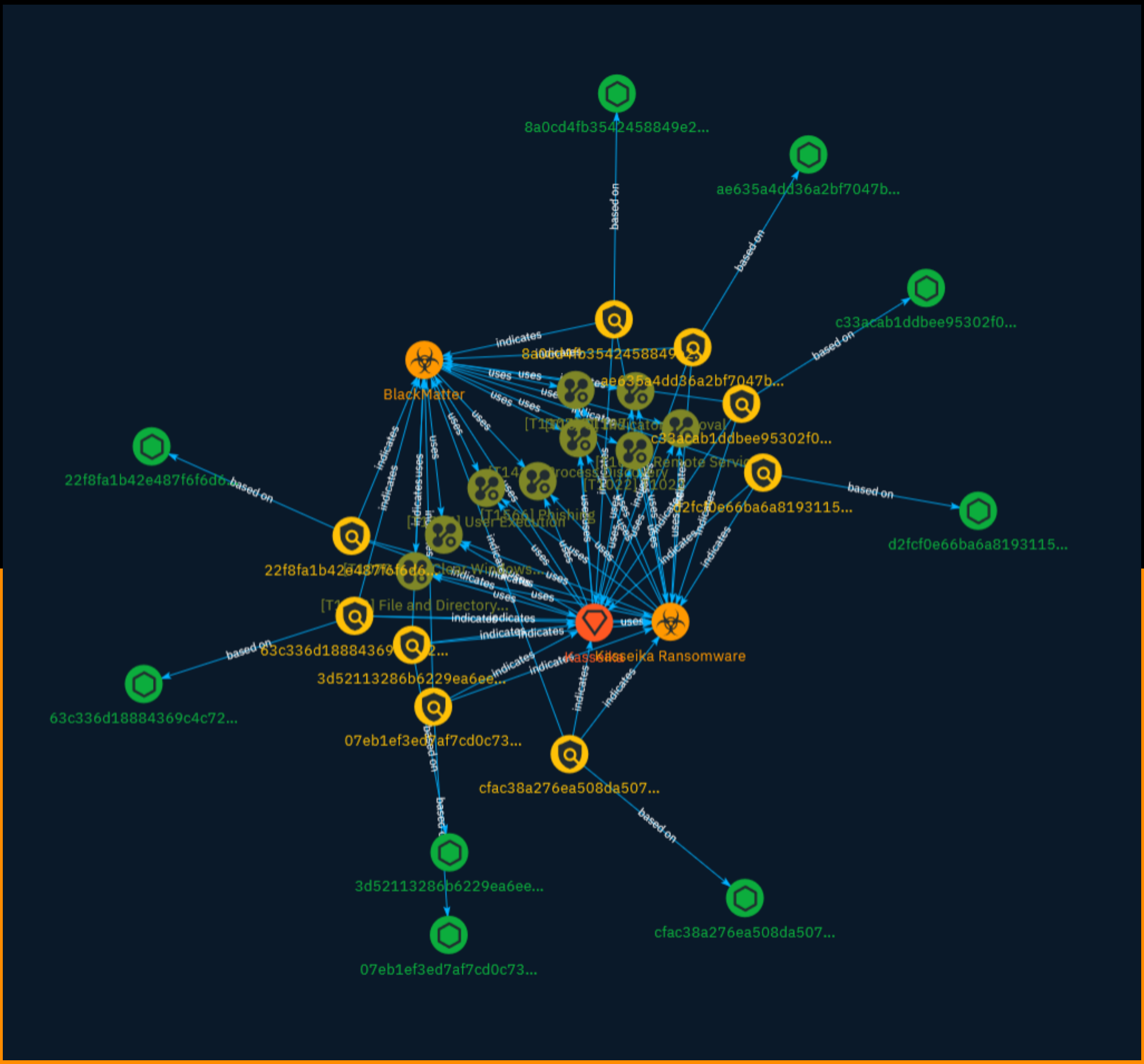

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Following an increase in bring-your-own-vulnerable-driver (BYOVD) attacks launched by ransomware groups in 2023, the Kasseika ransomware is among the latest groups to take part in the trend. Kasseika joins Akira, BlackByte, and AvosLocker in using the tactic that allows threat actors to terminate antivirus processes and services for the deployment of ransomware. In this case we investigated, the Kasseika ransomware abused Martini driver to terminate the victim machine's antivirus-related processes.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Process Discovery

ID

T1424

Description

Adversaries may attempt to get information about running processes on a device. Information obtained could be used to gain an understanding of common software/applications running on devices within a network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1424) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Recent Android security enhancements have made it more difficult to obtain a list of running processes. On Android 7 and later, there is no way for an application to obtain the process list without abusing elevated privileges. This is due to the Android kernel utilizing the `hidepid` mount feature. Prior to Android 7, applications could utilize the `ps` command or examine the `/proc` directory on the device.(Citation: Android-SELinuxChanges) In iOS, applications have previously been able to use the `sysctl` command to obtain a list of running processes. This functionality has been removed in later iOS versions.

Name

T1107

ID

T1107

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

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

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction.

Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer.(Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Name

Clear Windows Event Logs

ID

T1070.001

Description

Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alerts and notifications. There are three system-defined sources of events: System, Application, and Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit. The event logs can be cleared with the following utility commands: * `wevtutil cl system` * `wevtutil cl application` * `wevtutil cl security` These logs may also be cleared through other mechanisms, such as the event viewer GUI or [PowerShell](https://attack.mitre.org/techniques/T1059/001). For example, adversaries may use the PowerShell command `Remove-EventLog -LogName Security` to delete the Security EventLog and after reboot, disable future logging. Note: events may still be generated and logged in the .evtx file between the time the command is run and the reboot.(Citation: disable_win_evt_logging)

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)

Name
T1022

ID
T1022

Indicator

Name
ae635a4dd36a2bf7047b6a63605a9d20aae4bcc313d93068e5e0b6676a32a39f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ae635a4dd36a2bf7047b6a63605a9d20aae4bcc313d93068e5e0b6676a32a39f']
Name
07eb1ef3ed7af7cd0c735d20315b66dec3a7d0fc7b1bc604d442f76ce07f2739
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '07eb1ef3ed7af7cd0c735d20315b66dec3a7d0fc7b1bc604d442f76ce07f2739']
Name

63c336d18884369c4c721363b88f7a23fe05bc7fc7db84c8b248703b94ca8196

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '63c336d18884369c4c721363b88f7a23fe05bc7fc7db84c8b248703b94ca8196']

Name

c33acab1ddbee95302f0d54feb1c49c40dec807cec251fb6d30d056f571155e0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c33acab1ddbee95302f0d54feb1c49c40dec807cec251fb6d30d056f571155e0']

Name

3d52113286b6229ea6ee5ab0be773d4dff8d56d3f54691ad849910e7153979aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d52113286b6229ea6ee5ab0be773d4dff8d56d3f54691ad849910e7153979aa']

Name

8a0cd4fb3542458849e20c547a684578dd7fdd4317021dacf5517f607f8ceea7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8a0cd4fb3542458849e20c547a684578dd7fdd4317021dacf5517f607f8ceea7']

Name

cfac38a276ea508da50703915692cb8bd9d734ce74dc051239beb68cf89b2b37

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cfac38a276ea508da50703915692cb8bd9d734ce74dc051239beb68cf89b2b37']

Name

22f8fa1b42e487f6f6d6c6a62bba65267e2d292f80989031f8529558c86a9119

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '22f8fa1b42e487f6f6d6c6a62bba65267e2d292f80989031f8529558c86a9119']

Name

d2fcf0e66ba6a81931159c7a76f497f283751e50435dda56d4c912d9034b84a8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd2fcf0e66ba6a81931159c7a76f497f283751e50435dda56d4c912d9034b84a8']

Intrusion-Set

Name
Kasseika

Malware

Name
BlackMatter

Name
Kasseika Ransomware

StixFile

Value
d2fcf0e66ba6a81931159c7a76f497f283751e50435dda56d4c912d9034b84a8
ae635a4dd36a2bf7047b6a63605a9d20aae4bcc313d93068e5e0b6676a32a39f
63c336d18884369c4c721363b88f7a23fe05bc7fc7db84c8b248703b94ca8196
c33acab1ddbee95302f0d54feb1c49c40dec807cec251fb6d30d056f571155e0
3d52113286b6229ea6ee5ab0be773d4dff8d56d3f54691ad849910e7153979aa
07eb1ef3ed7af7cd0c735d20315b66dec3a7d0fc7b1bc604d442f76ce07f2739
22f8fa1b42e487f6f6d6c6a62bba65267e2d292f80989031f8529558c86a9119
cfac38a276ea508da50703915692cb8bd9d734ce74dc051239beb68cf89b2b37
8a0cd4fb3542458849e20c547a684578dd7fdd4317021dacf5517f607f8ceea7

External References

- https://otx.alienvault.com/pulse/65b14dad54060636a7291eb0
- https://www.trendmicro.com/en_us/research/24/a/kasseika-ransomware-deploys-byovd-attacks-abuses-psexec-and-expl.html