Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

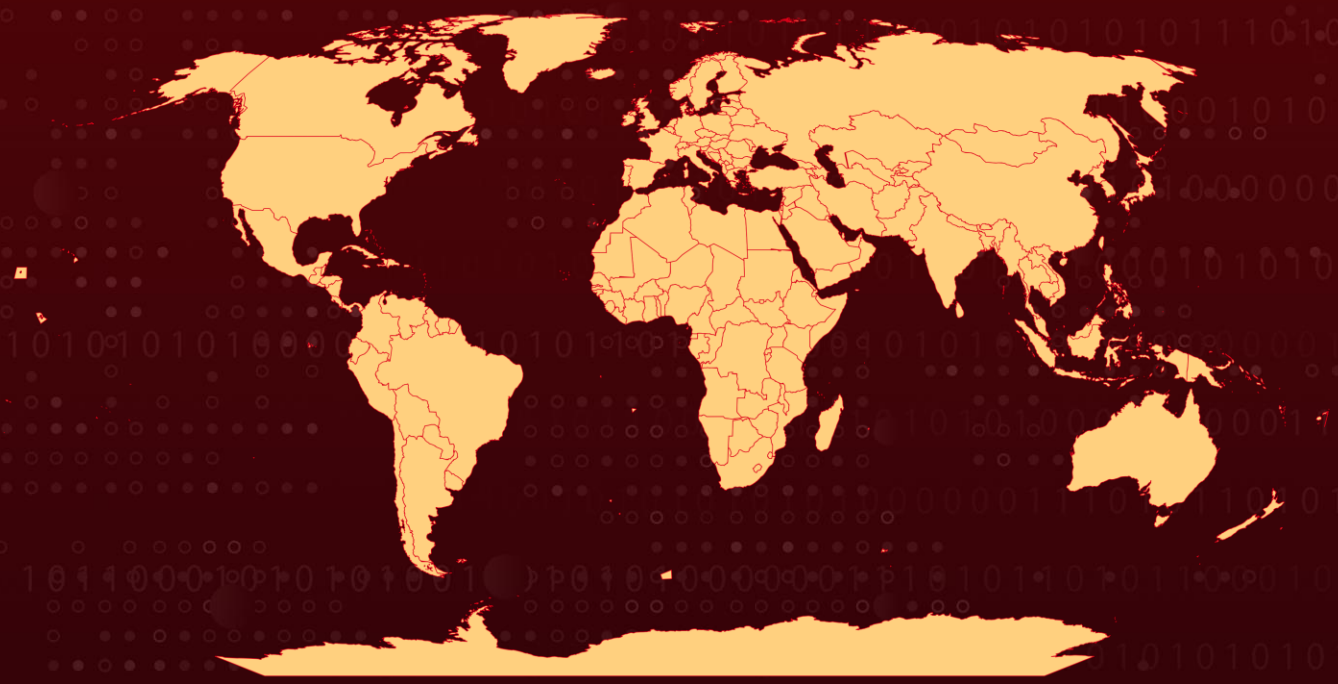
Kasseika Ransomware Employs BYOVD Tactic to Impair Defenses

Date of Publication	Admiralty Code	TA Number
January 24, 2024	A1	TA2024031

Summary

Attack Discovered: December 2023
Attack Region: Worldwide
Malware: Kasseika ransomware
Attack: The ransomware operation 'Kasseika' has recently been identified using the Bring Your Own Vulnerable Driver (BYOVD) tactic. This involves exploiting vulnerabilities in a loaded driver to disable antivirus software before initiating the file encryption process. Through this strategy, the malware gains privileges to terminate 991 processes, including those related to antivirus products, security tools, analysis tools, and system utilities.

Attack Regions



Attack Details

#1 In 2023, there has been a rise in bring-your-own-vulnerable-driver (BYOVD) attacks by ransomware groups. Kasseika ransomware is one of the latest to adopt this trend, utilizing a tactic that enables threat actors to terminate antivirus processes and services before deploying ransomware. Kasseika ransomware was found leveraging the Martini driver to terminate antivirus-related processes on the victim's machine.

#2 The Kasseika ransomware attack chain exhibits several similarities with BlackMatter. Upon closer examination, a substantial portion of the source code from BlackMatter was found to be used in the Kasseika attack. Given that the BlackMatter source code is not widely available, its utilization in the Kasseika ransomware attack implies the involvement of groups that acquired or purchased its code.

#3 The Kasseika group gains initial access through phishing, acquiring credentials and unauthorized entry into the corporate network. The operators utilize tools such as the Windows PsExec tool to move laterally and execute malicious .bat files to load malicious components. It checks for any running instance of "Martini.exe", driver process, and terminates it.

#4 A new instance of Martini.exe is executed, which checks for the presence of the vulnerable 'Martini.sys' driver. If Martini.sys is not found, it terminates and discontinues its intended routine. Upon verifying the presence of the system file, Kasseika proceeds to create a service and activates it. After loading Martini.sys, It continuously scans all active processes in the system. Upon detecting a listed process, it communicates this information to the driver through the DeviceIoControl function.

#5 The malware employs BYOVD attacks to terminate 991 processes, which include antivirus products, security tools, and analysis tools. It initiates Martini.exe to terminate antivirus processes and then executes the primary ransomware binary. The ransomware utilizes ChaCha20 and RSA encryption algorithms to encrypt the targeted files, appending a pseudo-random string to filenames, a pattern reminiscent of BlackMatter.

#6 After encrypting files, Kasseika ransomware places a ransom note in the encrypted directories and alters the computer's wallpaper to display an attack message. It also utilizes commands such as 'wevutil.exe' to clear system event logs, including Application, Security, and System logs, making it more difficult for security tools to detect and respond to malicious activities, enhancing the malware's ability to evade detection.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious content

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Limit Privileges: Limiting administrative rights and access to employees only when necessary is a crucial security measure to reduce the risk of unauthorized system modifications, installations, and potential security breaches.

Regular Backup: Implement regular backup procedures and store the backups offline or on a separate network to safeguard your data against potential ransomware attacks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	TA0040 Impact
T1566 Phishing	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1070 Indicator Removal

T1070.001 Clear Windows Event Logs	T1486 Data Encrypted for Impact	T1543 Create or Modify System Process	T1543.003 Windows Service
T1021 Remote Services	T1021.002 SMB/Windows Admin Shares	T1570 Lateral Tool Transfer	T1057 Process Discovery
T1518 Software Discovery	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1203 Exploitation for Client Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	22f8fa1b42e487f6f6d6c6a62bba65267e2d292f80989031f8529558c86a9119, ae635a4dd36a2bf7047b6a63605a9d20aae4bcc313d93068e5e0b6676a32a39f, 8a0cd4fb3542458849e20c547a684578dd7fdd4317021dacf5517f607f8ceea7, 63c336d18884369c4c721363b88f7a23fe05bc7fc7db84c8b248703b94ca8196, 3d52113286b6229ea6ee5ab0be773d4dff8d56d3f54691ad849910e7153979aa, 07eb1ef3ed7af7cd0c735d20315b66dec3a7d0fc7b1bc604d442f76ce07f2739, d2fcf0e66ba6a81931159c7a76f497f283751e50435dda56d4c912d9034b84a8, cfac38a276ea508da50703915692cb8bd9d734ce74dc051239beb68cf89b2b37, c33acab1ddbee95302f0d54feb1c49c40dec807cec251fb6d30d056f571155e0

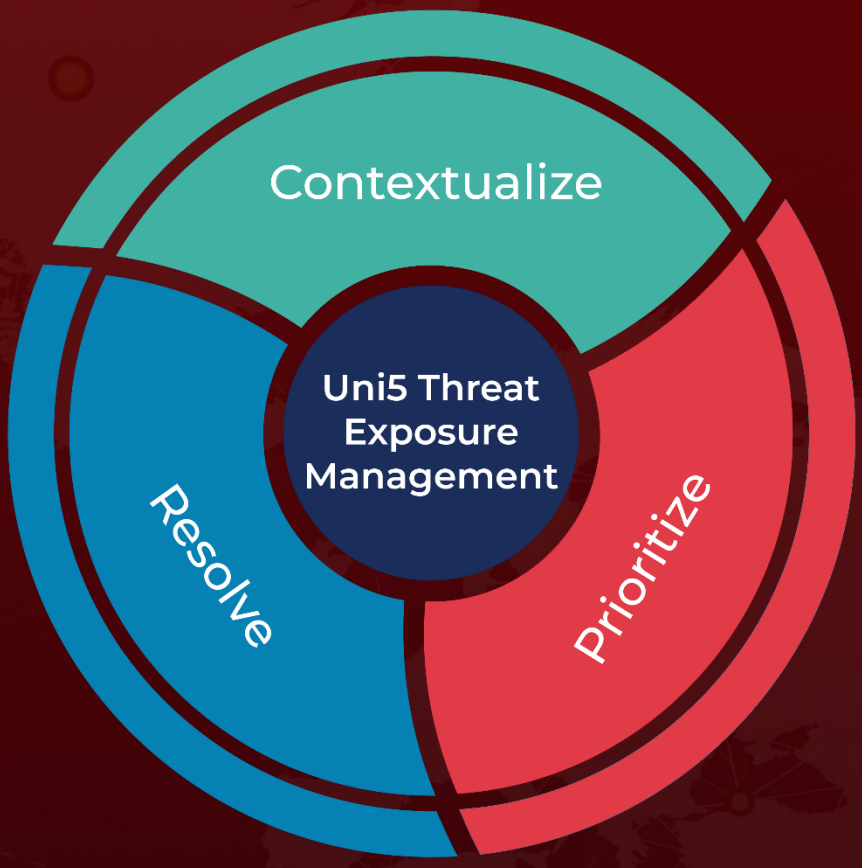
References

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 24, 2024 . 5:45 AM

More at www.hivepro.com