Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

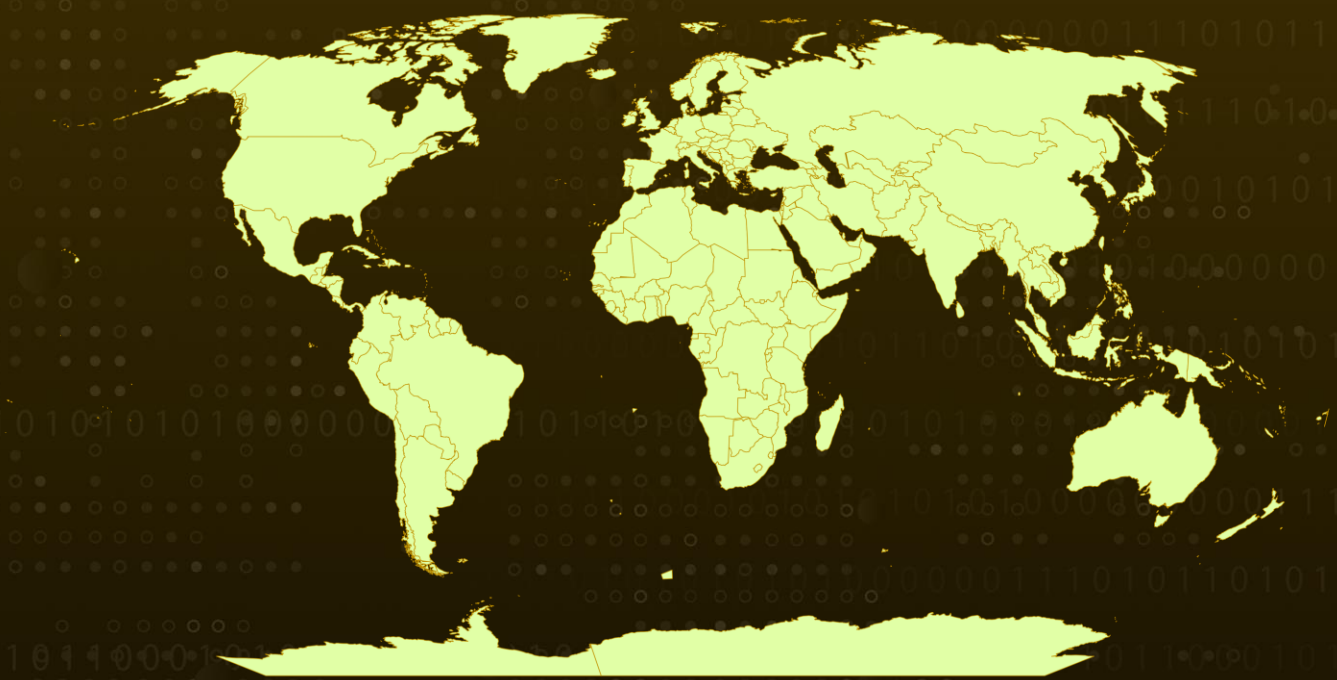
Kematian: The Versatile Information-Stealing Malware

Date of Publication	Admiralty Code	TA Number
July 11, 2024	A1	TA2024269

Summary

Malware: Kematian Stealer
Affected Product: Windows
Attack Region: Worldwide
Attack: Kematian is an open-source, PowerShell-based malware available on GitHub under the "Somali-Devs" account, featuring significant contributions from user KDot227. This highly effective malicious software is designed to discreetly collect a broad spectrum of sensitive information, including cryptocurrency wallet data.

Attack Regions



Attack Details

#1 Kematian is an open-source tool freely available on GitHub under the "Somali-Devs" account, with substantial contributions from the user KDot227.

#2 This malicious software is designed to discreetly collect sensitive information and cryptocurrency wallet data from victims, making it highly favored for its effectiveness and accessibility.

#3 The Kematian stealer covertly extracts a broad spectrum of sensitive information from victims' computers. This PowerShell-based tool is used for stealthy access and data transfer from Windows systems.

#4 It collects sensitive data such as seed phrases, session files, passwords, application data, and Discord tokens. This information is securely transmitted over TCP to a dedicated command-and-control (C2) server for decryption and further exploitation.

#5 Kematian malware exhibits alarming capabilities in evading detection, gathering sensitive data, and maintaining persistence on compromised systems. With continuous updates and a versatile builder tool offering various customization options, threat actors can tailor and deploy the malware for their malicious purposes. The Kematian stealer poses a significant risk to both organizations and individuals.

Recommendations

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Implement Network Segmentation: Segment your network to isolate critical systems and sensitive data from general user access and potential malware spread. Use intrusion detection and prevention systems (IDPS) to monitor and analyze network traffic for abnormal behavior.

User Education and Awareness: Educate users about the dangers of opening suspicious documents or files received via email or other channels. Encourage them to be cautious and vigilant when interacting with unknown or unexpected content.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats by proactively blocking access to harmful content and preventing the execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
TA0040 Impact	T1566 Phishing	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter
T1027 Obfuscated Files or Information	T1053 Scheduled Task/Job	T1564.001 Hidden Files and Directories	T1204 User Execution
T1564 Hide Artifacts	T1087 Account Discovery	T1083 File and Directory Discovery	T1005 Data from Local System
T1105 Ingress Tool Transfer	T1082 System Information Discovery	T1113 Screen Capture	T1204.002 Malicious File
T1041 Exfiltration Over C2 Channel	T1048 Exfiltration Over Alternative Protocol	T1485 Data Destruction	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	736376a77af0a4eb7108ba02d989c137, 02f3b7596cff59b0a04fd2b0676bc395, d2ea85153d712cce3ea2abd1a593a028, a3619b0a3ee7b7138cefb9f7e896f168, 18b5977b1a59c585f00ed7dca0fa81c9, 80cf2d7ae1f3acc750f2cf454b4832c6
URL	hxxps[:]//ptb[.]discord[.]com/api/webhooks/1247594902611562546/VpMh55OYaqHByOG1Q8vjiiF_seZ3lgXeGdLWhpxfr2UlP261GpZWDiu4lqiTNyAvsrs-, hxxps[:]//discord[.]gg/vk3rBhcj2y, hxxps[:]//github[.]com/KDot227/Powershell-Token-Grabber/releases/download/Fixed_version/main[.]exe, hxxps[:]//github[.]com/Somali-Devs/Kematian-Stealer/releases/download/Fixed_version/main[.]exe, hxxps[:]//github[.]com/Somali-Devs/Kematian-Stealer/, hxxps[:]//github[.]com/KDot227/Powershell-Token-Grabber/, hxxps[:]//github[.]com/Somali-Devs/Kematian-Stealer/releases/download/AutoBuild/main[.]exe, hxxps[:]//github[.]com/Somali-Devs/Kematian-Stealer/blob/main/frontend-src/main[.]ps1, hxxps[:]//raw[.]githubusercontent[.]com/Somali-Devs/Kematian-Stealer/main/frontend-src/blockhosts[.]ps1, hxxps[:]//github[.]com/Somali-Devs/Kematian-Stealer/raw/main/frontend-src/antivm[.]ps1, hxxps[:]//raw[.]githubusercontent[.]com/Somali-Devs/Kematian-Stealer/main/frontend-src/kematian_shellcode[.]ps1, hxxps[:]//github[.]com/Somali-Devs/Kematian-Stealer/releases/download/KematianBuild/kematian[.]bin

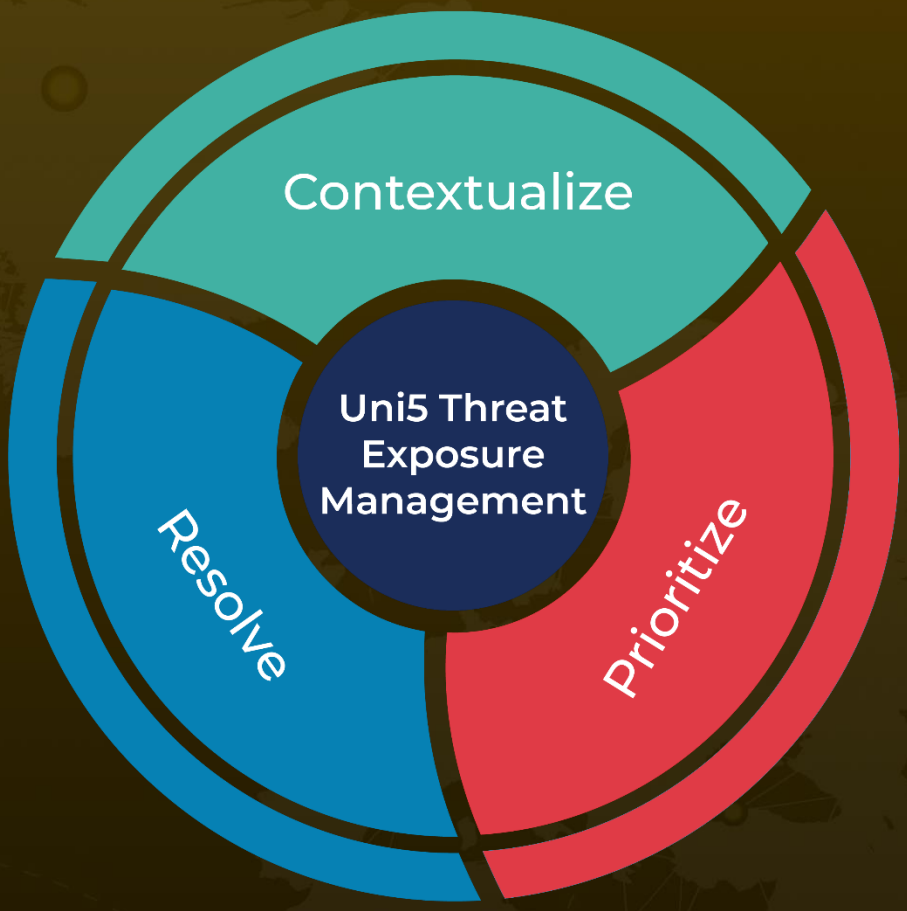
References

https://www.cyfirma.com/research/kematian-stealer-a-deep-dive-into-a-new-information-stealer/

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

July 11, 2024 • 6:30 AM

More at www.hivepro.com