Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

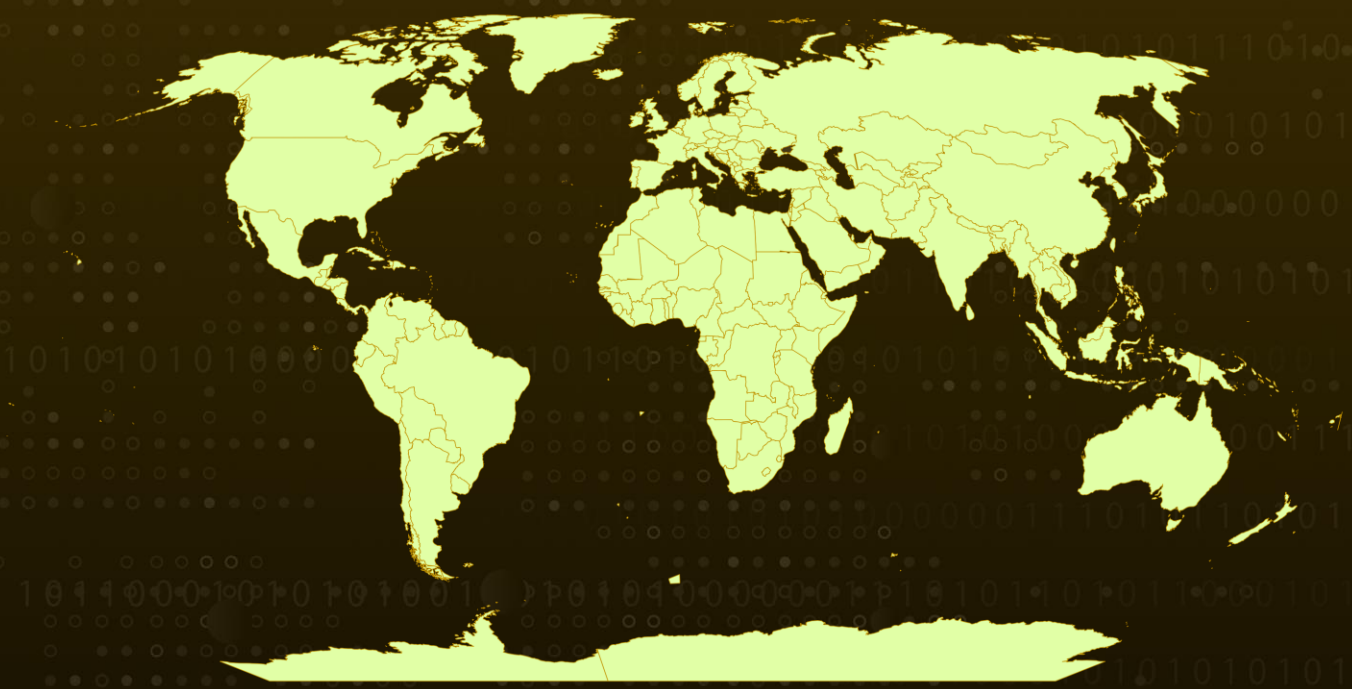
Agniane Stealer's Cryptocurrency Quest

Date of Publication	Admiralty Code	TA Number
August 29, 2023	A1	TA2023348

Summary

Attack Began: August 2023
Malware: Agniane Stealer
Attack Region: Worldwide
Targeted Industry: Cryptocurrency
Attack: The Agniane Stealer, coded in C#, operates as an information pilferer. It primarily focuses on extracting stored credentials from a wide array of sources, with a specific emphasis on targeting cryptocurrency extensions and wallets. This malware functions as a purchasable service on the dark web, representing a substantial and commanding expansion of its capabilities.

Attack Regions



Attack Details

#1 The Agniane Stealer, programmed in C#, operates as an information pilferer. It focuses on extracting stored credentials from diverse sources, encompassing web browsers, Telegram and Discord sessions, Steam, WinSCP, and Filezilla activities. Moreover, it proficiently captures screenshots of users' desktops, rapidly compiling OpenVPN profiles alongside comprehensive system particulars.

#2 Once it acquires this crucial information, Agniane Stealer securely transmits the unlawfully obtained data to designated command-and-control (C2) servers. This sophisticated malicious software maintains its association within the Malware-as-a-Service (MaaS) domain recognized as the Cinoshi Project.

#3 Cinoshi was introduced in the initial months of 2023, this platform significantly mirrors a substantial portion of its code infrastructure from the aforementioned project. Operating as a purchasable service on the concealed corners of the internet the darkweb, Stealer emerges as a powerful augmentation to the continually expanding arsenal of malevolent tools within the Cinoshi Project.

#4 Upon execution, Agniane Stealer initiates the creation of a randomized 32-bit alphanumeric sequence. This uniquely generated string serves as the name for a sub-folder, meticulously created within the %TEMP% directory, specifically designed for containing the unlawfully acquired data. Additionally, the program conducts an examination of the system's memory, searching for potential analysis tools.

#5 Agniane Stealer employs the resourceful mechanism of WMI (Windows Management Instrumentation) queries to determine whether its operation is occurring within the confines of a virtual environment, and Agniane Stealer terminates execution if True. Moreover, Agniane Stealer encompasses an added layer of functionality by harnessing its clipper attributes, allowing for the covert extraction of cryptocurrency-related data.

Recommendations

Application Whitelisting: Utilize application whitelisting to permit only authorized and trusted applications to run. This can help prevent the execution of malicious software like Agniane Stealer.

Anomaly Detection and Centralized Logging: Implement a robust anomaly detection system coupled with centralized logging to swiftly identify unusual activities and behaviors across your network and endpoints. Regular analysis of these logs aids in detecting potential Agniane Stealer activities, unauthorized access, or data exfiltration.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0040 Impact	**T1113** Screen Capture	**T1562.001** Disable or Modify Tools	**T1003** OS Credential Dumping
T1497 Virtualization/Sandbox Evasion	**T1027** Obfuscated Files or Information	**T1071** Application Layer Protocol	**T1047** Windows Management Instrumentation
T1106 Native API	**T1129** Shared Modules	**T1112** Modify Registry	**T1027.002** Software Packing
T1036 Masquerading	**T1070.006** Timestomp	**T1105** Ingress Tool Transfer	**T1222** File and Directory Permissions Modification
T1552.002 Credentials in Registry	**T1010** Application Window Discovery	**T1082** System Information Discovery	**T1573** Encrypted Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	f82093aa3c483dca6ace0f5c8dec104800b8d494, cdab34eea2dfd5e96412e34c0b3eb090a9661377, 3830039ada6bb8d3050dc7748d77bcb7b0cc003f

TYPE	VALUE
Domain	central-cee-doja[.]ru
SHA256	b5f11e9a19a7972bb65d5c46664a7f7594a946b3bdd9760697fd39f6d607b557, 560017cc0ca317e8c6437ed46a417e782f02a860f917d6fa682bca26158d1cf0, 24bd790bc9427021121ec0e318db93369c2d893e40309f7083f178d3a5819161
MD5	d811a57bc0e8b86b449277f9ffb50cc9, b62ef0920a545f547d6cd3cd2abd60d2, a2b20120a92c3de445b0b384a494ed39

References

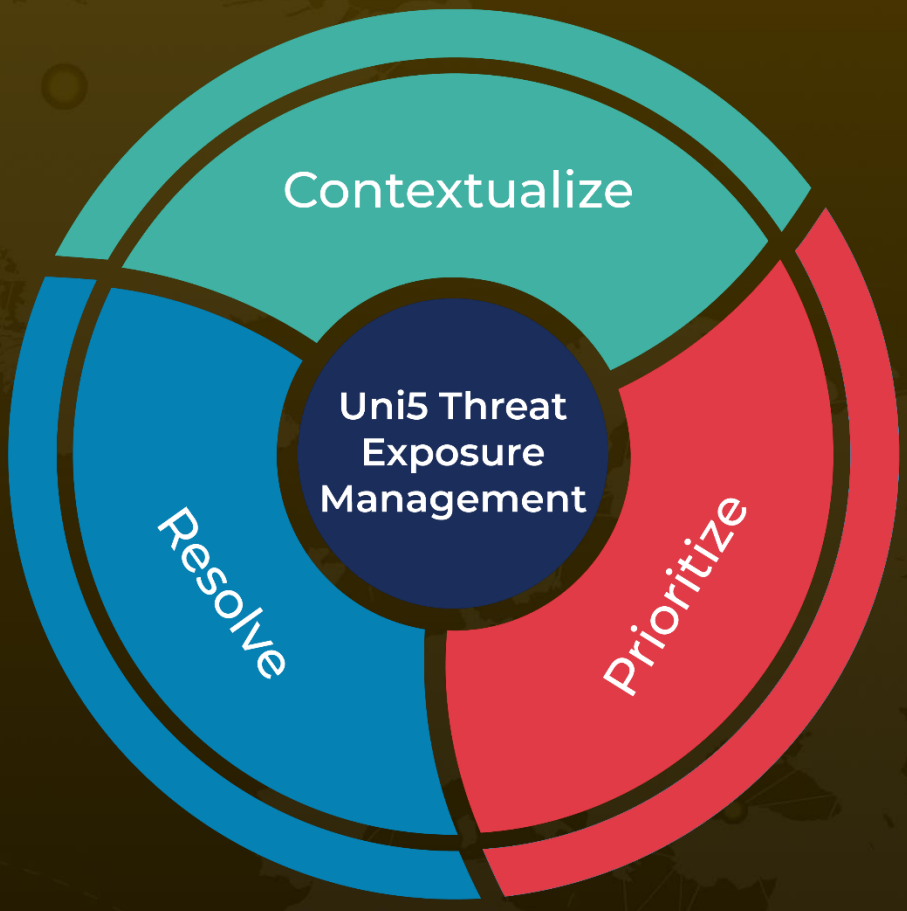
https://www.zscaler.com/blogs/security-research/agniane-stealer-dark-webs-crypto-threat

https://www.hivepro.com/cinoshi-a-novel-malware-as-a-service-platform/

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

August 29, 2023 • 5:30 AM

More at www.hivepro.com