Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

New Variant of BlackGuard Stealer Malware Steals Sensitive Information and Crypto Wallets

Date of Publication

March 24, 2023

Admiralty Code

A1

TA Number

TA2023157

Summary

First appeared: 2021
Attack Region: Worldwide
Targeted Industries: Crypto wallets, Technology
Malware: BlackGuard stealer
Attack: A new variant of the BlackGuard stealer malware that propagates through removable media and hijacks crypto wallets. It can steal sensitive information from various applications and supports stealing popular crypto assets.

Attack Regions

Attack Details

#1

A new variant of BlackGuard stealer, a malware sold in underground forums and Telegram since 2021, steals sensitive information from various applications and browsers. The new variant has evolved since its previous version and now arrives with new capabilities. It propagates through removable media and shared devices and can hijack crypto wallets copied to the clipboard, replacing the victim's address with the threat actor's address.

#2

Additionally, the malware downloads and executes additional malware with process injection and duplicates itself to every folder in the C:\ drive recursively with a random name. The malware steals cryptocurrency wallets, login data, and other sensitive information from messaging, gaming, email, FTP, VPN, and other applications.

#3

It also collects information about the machine, such as the antivirus software installed, external IP address, localization, file system information, and operating system, among others. The malware supports stealing popular crypto assets and uses different handlers for messaging applications like Telegram, Discord, and Pidgin.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	**TA0001** Initial Access	**TA0003** Persistence	**TA0009** Collection
TA0005 Defense Evasion	**TA0010** Exfiltration	**TA0002** Execution	**TA0006** Credential Access
TA0008 Lateral Movement	**TA0011** Command and Control	**T1020** Automated Exfiltration	**T1027** Obfuscated Files or Information
T1566 Phishing	**T1106** Native API	**T1047** Windows Management Instrumentation	**T1547.001** Registry Run Keys / Startup Folder
T1112 Modify Registry	**T1012** Query Registry	**T1083** File and Directory Discovery	**T1003** OS Credential Dumping
T1539 Steal Web Session Cookie	**T1528** Steal Application Access Token	**T1552** Unsecured Credentials	**T1552.002** Credentials in Registry
T1522.001 Credentials in Files	**T1010** Application Window Discovery	**T1622** Debugger Evasion	**T1057** Process Discovery
T1082 System Information Discovery	**T1497** Virtualization/Sandbox Evasion	**T1091** Replication Through Removable Media	**T1115** Clipboard Data
T1213 Data from Information Repositories	**T1005** Data from Local System	**T1071** Application Layer Protocol	**T1105** Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	23.83.114[.]131
SHA256	88e9780ce5cac572013aebdd99d154fa0b61db12faffeff6f29f9d2800c915b3
SHA1	88e9780ce5cac572013aebdd99d154fa0b61db12
MD5	3235ebcead914e4a210dc9dbe5c36c2f

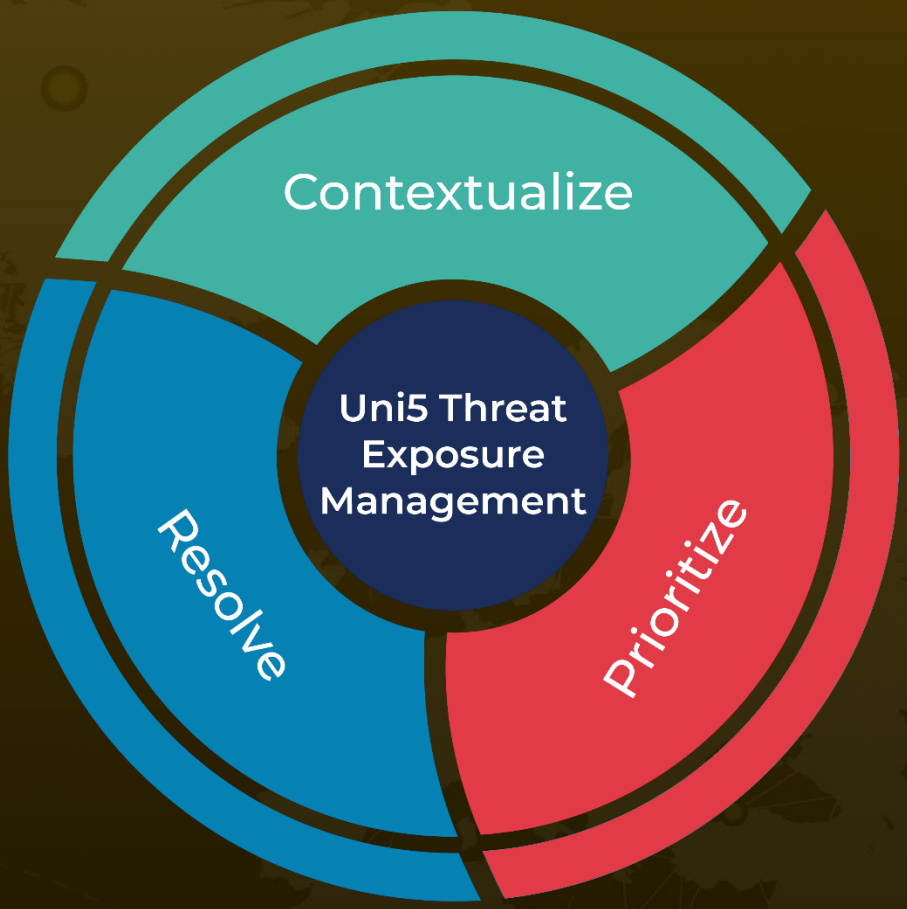
References

https://cybersecurity.att.com/blogs/labs-research/blackguard-stealer-extends-its-capabilities-in-new-variant

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

March 24, 2023 • 1:30 AM

More at www.hivepro.com