Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

FatalRAT's Calculated Cryptocurrency Carnage

Date of Publication	Admiralty Code	TA Number
April 18, 2024	A1	TA2024154

Summary

First Seen: August 2021
Malware: FatalRAT
Attack Region: Worldwide
Targeted Industry: Cryptocurrency
Attack: FatalRAT, a Remote Access Trojan, initiated a targeted phishing campaign primarily targeting cryptocurrency enthusiasts, especially those utilizing the Exodus platform. This campaign strategically deploys FatalRAT alongside additional malware such as Clipper and Keylogger, specifically focusing on Chinese-speaking individuals and organizations.

Attack Regions

Attack Details

#1 FatalRAT, a Remote Access Trojan boasting diverse capabilities, facilitates remote exploitation by malicious actors. Initially uncovered in August 2021, it has recently embarked on a targeted phishing campaign aimed at cryptocurrency enthusiasts.

#2 This campaign deploys FatalRAT alongside supplementary malware such as Clipper and Keylogger, specifically focusing on Chinese-speaking individuals and entities. The threat actors have created a deceptive website meticulously designed to mimic legitimate cryptocurrency applications.

#3 Unsuspecting users are lured into downloading software disguised as authentic Exodus installers from this phishing site. Subsequently, the threat actors employ the DLL side-loading technique to inject and execute FatalRAT, Clipper, and Keylogger modules.

#4 The Clipper functionality operates discreetly in the background, continuously monitoring clipboard activity. Before activating the keylogger feature, the malware conducts reconnaissance to identify virtual environments by scrutinizing VMware-related processes, file paths, and other indicators.

#5 The Trojanized Exodus crypto-wallet installer grants attackers unauthorized access and control, enabling them to steal sensitive data from web browsers, capture keystrokes, manipulate data especially wallet addresses in the clipboard, and execute other malicious activities, all while remaining concealed from unsuspecting users.

Recommendations

Exercise Vigilance with URLs: Before accessing or downloading from any site, meticulously verify the URLs to ensure legitimacy and avoid falling victim to phishing attempts.

Verify Wallet Addresses: Crypto users should meticulously check their wallet addresses before executing any transactions, ensuring there are no alterations when copying and pasting addresses.

Enable Application Whitelisting: Utilize application whitelisting to restrict the execution of unauthorized applications, preventing the launch of malicious payloads like FatalRAT.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0009 Collection
TA0010 Exfiltration	TA0040 Impact	T1566 Phishing	T1204 User Execution
T1036.008 Masquerade File Type	T1036 Masquerading	T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow
T1562.001 Disable or Modify Tools	T1562 Impair Defenses	T1115 Clipboard Data	T1041 Exfiltration Over C2 Channel
T1657 Financial Theft			

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxps[://]exodue[.]com
IPv4	38[.]181[.]70[.]178

TYPE	VALUE
Domain	1-27[.]qq-weixin[.]org, 1-31.qq-weixin[.]org, 1-8.qq-weixin[.]org
SHA256	f80f8a725028bcc09639f7b1ff9439436d974f0bf92871048092eaec5d7458f0, d56471adbfd095d1be1d4b8288d14283efbf6414912064a97423751a69c1427f, 715138e6cb30bd18cc6afad6322e35f6f1a3d40ac135a1a9bc76cb884508c686, 8b0fde6e42ba17b0b475bb8dd54b8554cc6682d81b9e632f8890daa9ceefd48d, a5ca7b8af70d6e483007c6c9c60b0a2002e150b0f479744989fdd58ad2fc62d3, 03e8610b95753eee43179b1ccc3fb72c8595a7d76e9b0290ea765f8e6372d4f9, 0555ba582ffdb07a3e93a4d936d2d0d2bd506040f12e5b55e042e82d4bc169ad, fba1b353b063a068bd8a191ce699d335158028a6c94282a27f86b784cd4e94e5, b3c47e48facfb1d6e4f93b1e9b91c1a931f5e491c5ab4aa0fc5c10ed077674b4, 149271557eec7f5b17cd046d1f9936dca1654be1edd7835f005fbba145d65b8c, 1b6ab4d69332a041109c9a8b7bc1d12dd28566a0614363f7887d9044e4345a2e, e1368e893c44b29acfe7e9e190bbe448deda18d1847ed697b01c17a373207053, efc27a42e520918f83b041f81975e8dbca9916d159dfc41380112c20b43bcd39, c03a524b4e0561141012a6dc17f09bc8d0bf772cf2c94731971a50d67dccb2f4, 47835bbb98d4660ffa225000797e22c3cfd48ae43af8ccf0999a760b8c3a92ba

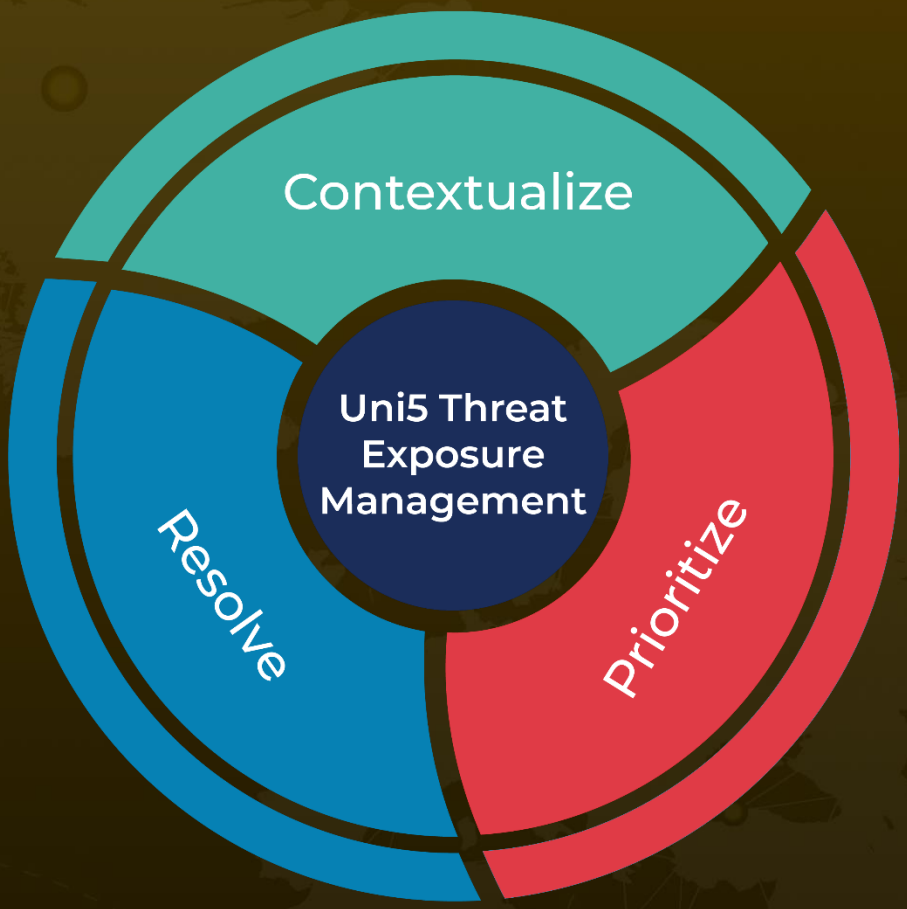
References

https://cyble.com/blog/fatalrats-new-prey-cryptocurrency-users-in-the-crosshairs/

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

April 18, 2024 • 9:30 PM

More at www.hivepro.com