Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Creal Stealer Preys on Cryptocurrency Users

Date of Publication	Admiralty Code	TA Number
March 30, 2023	A1	TA2023166

Summary

First appeared: 2023
Malware: Creal Stealer
Attack Region: Worldwide
Attack: A phishing site that is impersonating a cryptocurrency mining platform is disseminating the New Creal Stealer.

Attack Regions

Attack Details

#1

The new stealer binary, dubbed Creal, is spread via a fake cryptocurrency mining website. The stealer binary is compiled with PyInstaller, indicating that it was written in Python. There are 50 samples in the wild, demonstrating that threat actors were actively using the open-source code to infect unwitting victims. During the initial execution, the stealer determines whether it is being run in a controlled environment.

#2

The stealer then checks to see if the victim's public IP address is on a blacklist known as "sblacklist." The stealer achieves persistence by creating many threads in Python using the threading module and launching the data-stealing code concurrently. Chromium-based browsers, chat and gaming apps, cold crypto wallets, and browser extensions are all targets. Creal Stealer may exfiltrate data using Discord Webhooks and many file-hosting and sharing platforms, such as Anonfiles and Gofiles.

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

TA0002 Execution	TA0003 Persistence	TA0006 Credential Access	TA0007 Discovery
TA0010 Exfiltration	TA0011 Command and Control	T1204 User Execution	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1555 Credentials from Password Stores	T1539 Steal Web Session Cookie	T1528 Steal Application Access Token
T1087 Account Discovery	T1518 Software Discovery	T1057 Process Discovery	T1124 System Time Discovery
T1007 System Service Discovery	T1614 System Location Discovery	T1071 Application Layer Protocol	T1102 Web Service
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxps[:]//www.dropbox[.]com/s/dl/x4vgcaac6hcdgla/kryptex-setup-4.25.7[.]zip
Domain	kryptex[.]software
SHA256	4ee417cbefa1673d088a32df48b8182bdad244541e8dc02faf540b9aa483fdcb f3197e998822bc45cb9f42c8b153c59573aad409da01ac139b7edd8877600511
MD5	bb2ca78ffff72d58599d66bf9b2f0ae6 929e6f2c8896059c72368915abcaefa2
SHA1	20dcb84660e5f79a98c190d3d455fce368d96f35 7122f0b88607061806fd62282e8b175ae28b7e29

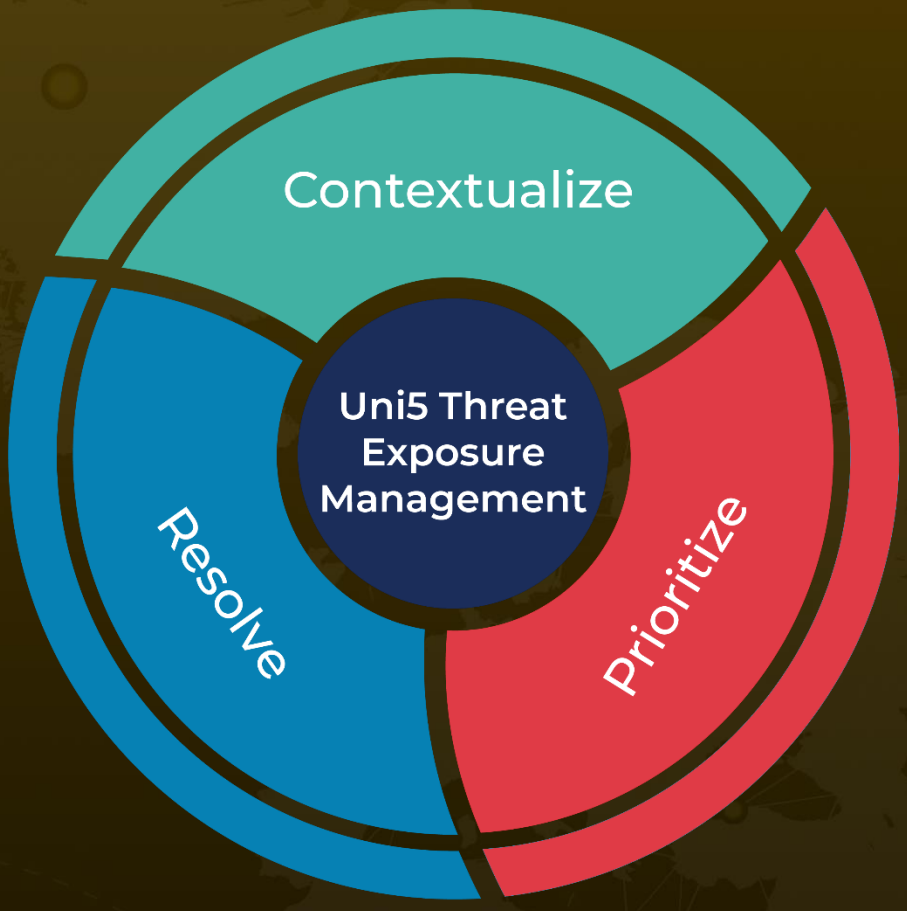
References

https://blog.cyble.com/2023/03/29/creal-new-stealer-targeting-cryptocurrency-users-via-phishing-sites/

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

March 30, 2023 • 6:44 AM

More at www.hivepro.com