Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

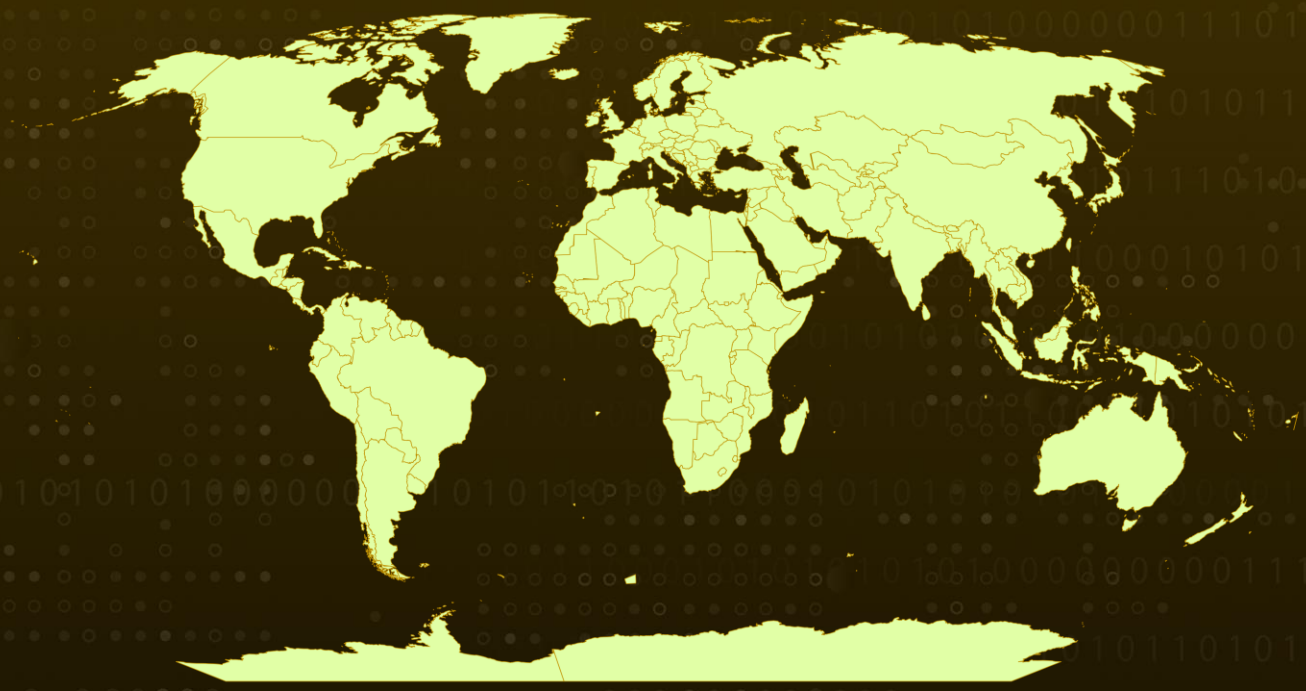
CRYPTBOT: Information-Stealing Malware Targeting Your Browser and Crypto-Wallet

Date of Publication	Admiralty Code	TA Number
January 27, 2023	A1	TA2023048

Summary

First appeared: 2019
Attack Region: Worldwide
Targeted Industry: Finance, Energy, Airline, Technology
Attack: CRYPTBOT is malware that steals personal information by gathering browser credentials, cookies, cryptocurrency wallets, and system information. It then compresses the collected data into a zip file and sends it to a command-and-control server through an HTTP POST request.

Attack Regions



Attack Details

#1

CryptBot is a data stealer that targets Windows operating systems and was discovered in the wild in 2019. It is designed to steal sensitive information such as browser credentials, cryptocurrency wallets, browser cookies, credit card information, and system screenshots from infected devices. It spreads through phishing emails and cracked software.

#2

The malware scans the system for installed software by traversing the 'Uninstall' registry tree. It accesses specific registry keys to identify the collection of system configuration information, which it then saves in temporary files of various formats in the %TEMP% directory.

#3

These C2s are often short domain names in the .top TLD. The malware begins by producing a zip of the exfil directory in the %temp% directory with a random filename. After creating the zip, the malware then runs the code to exfiltrate to the C2. The malware removes itself from the disc.

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

TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1518 Software Discovery
T1082 System Information Discovery	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1074 Data Staged
T1074.001 Local Data Staging	T1070 Indicator Removal	T1070.004 File Deletion	T1027 Obfuscated Files or Information
T1027.002 Software Packing			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	12d20a973f8cd9c6373929ae14efe123
SHA1	7f277f5f8f9c2831d40a2dc415566a089a820151
SHA256	183f842ce161e8f0cce88d6451b59fb681ac86bd3221ab35bfd675cb42f056ac
URLs	hxxp[:]//sginiv12[.]top/gate[.]php hxxp[:]//bytcox01[.]top/gesell[.]dat

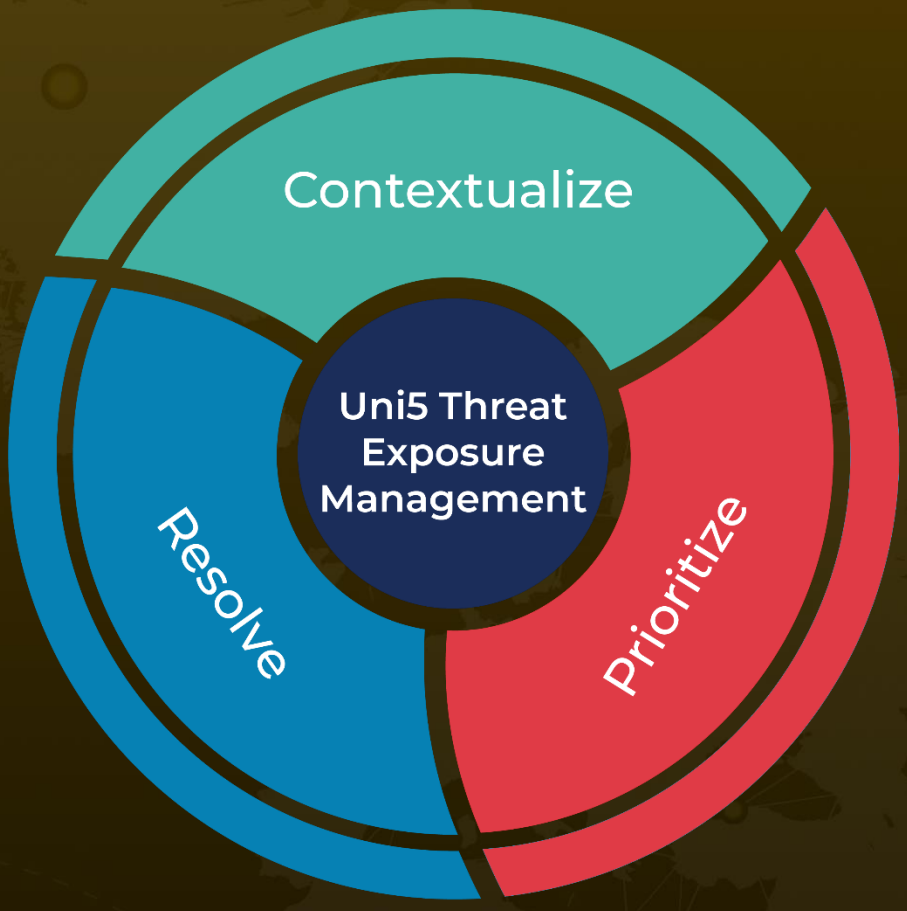
References

https://any.run/cybersecurity-blog/cryptbot-infostealer-malware-analysis/

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

January 27, 2023 . 1:55 AM

More at www.hivepro.com