Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

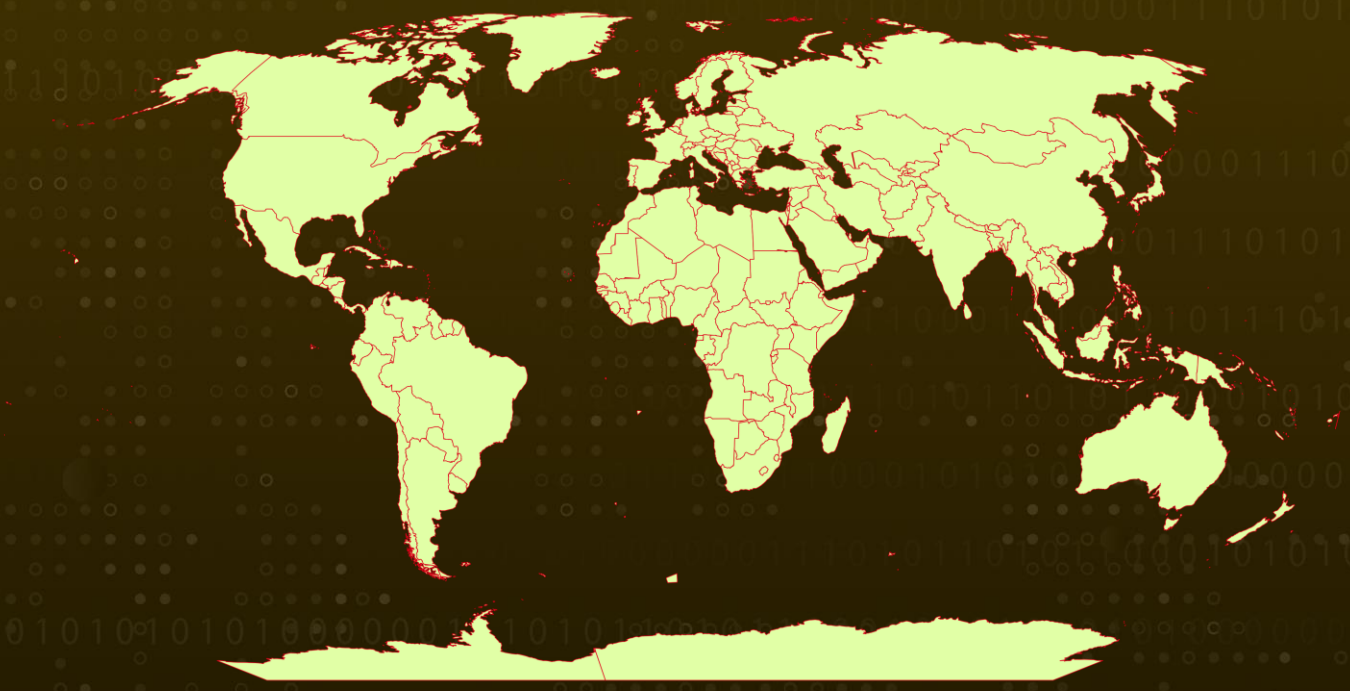
Typhon Stealer back with new variant named Typhon Reborn

Date of Publication	Admiralty Code	TA Number
November 16, 2022	A1	TA2022260

Summary

First Activity Observed: August 2022
Attack Region: Worldwide
Attack: Typhon stealer is a Malware-as-a-service offering crypto mining and many more capabilities.

Attack Regions



Attack Details

#1 Typhon Stealer, a malware who became widely known for its capabilities to steal crypto wallets, monitor keystrokes, and evade antivirus programs, became widely known in early August 2022. Soon after, they released an updated version known as Typhon Reborn. With this new version, anti-analysis techniques have been enhanced and the stealer and file grabber features have been enhanced.

#2 Multiple new features and configurable options are included in Typhon Reborn. There are also block-listed usernames and countries, new message clients, and a crypto-extension stealer for Google Chrome and Microsoft Edge.

#3 The Typhon Stealer provided threat actors with an easy-to-use and configurable builder. In order to evade security systems and exfiltrate data smoothly, they continually update their code.

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

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
T1566 Phishing	T1204 User Execution	T1497.001 System Checks	T1555 Credentials from Password Stores
T1539 Steal Web Session Cookie	T1552 Unsecured Credentials	T1528 Steal Application Access Token	T1113 Screen Capture
T1124 System Time Discovery	T1007 System Service Discovery	T1614 System Location Discovery	T1087 Account Discovery
T1518 Software Discovery	T1057 Process Discovery	T1095 Non-Application Layer Protocol	T1041 Exfiltration Over C2 Channel
T1567 Exfiltration Over Web Service			

Indicator of Compromise (IOC)

TYPE	VALUE
SHA256	A12933ab47993f5b6d09bec935163c7f077576a8b7b8362e397fe4f1ce4e791c, 48133d1aaf1a47f63ec73781f6a2b085b28174895b5865b8993487daec373e0a e04e65ddad749789f4f05bb88e2c8bde8df9263950eb120ad1191f217ca0c742 d68f00429a5f39c718cc704ee11e8e10d37c8ffc831630d753c922269bc01b86 524180810d0b9764e5ef3923a8eb34b2ed8ca1923244be37e94ca57d889ede9b

TYPE	VALUE
SHA1	8af9fc9aa7517ac327cc8692c2adf54537f39fe5 7c4ff5acfc57573279c9abc6779a8bc547b23d12 51aa7b94b3f3921d21e730b113faa20e0f6b6902 b4d71ad21f6f6cff7d297bbe1431a007b0d3e792
MD5	a1f146eb008f077be809ab4e61f46f4e 79dc4a4192469c3e697afd81409a52da 77f7d71475362232d13adbdb19e876ff ce4675c0ab630d8e1e89eb7c9d23188d
URLs	hxxp://lindesbergparkeringsanmarkning[.]netlify[.]app hxxps://formspree[.]io/f/xknylake

References

https://unit42.paloaltonetworks.com/typhon-reborn-stealer/

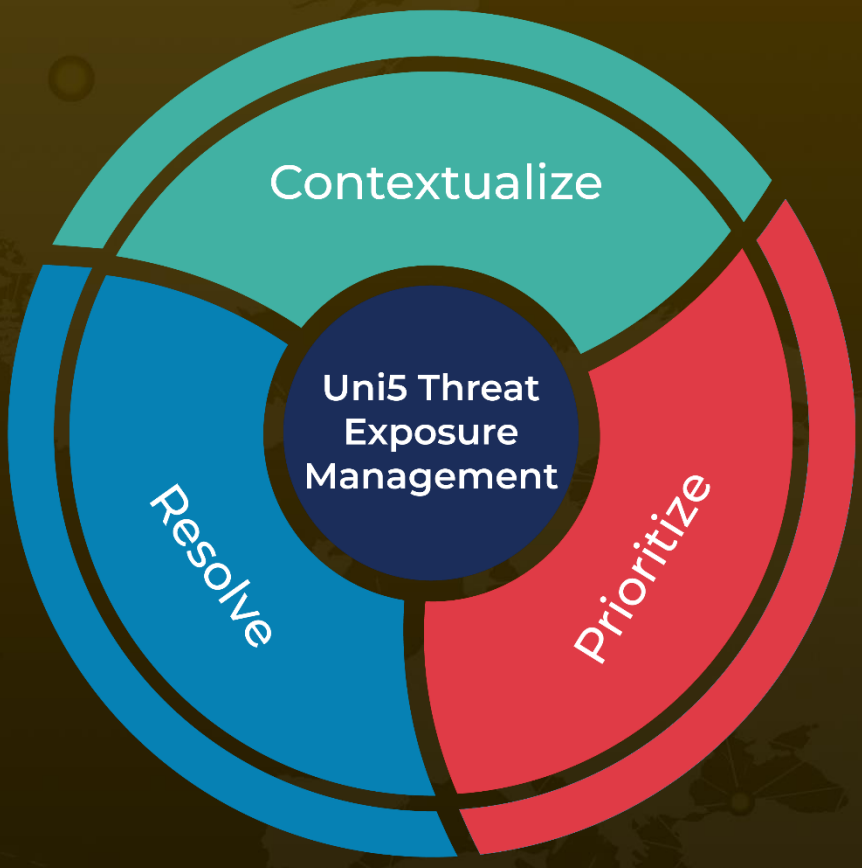
https://blog.cyble.com/2022/08/16/phishing-site-used-to-spread-typhon-stealer/

https://otx.alienvault.com/pulse/63733fcd9e604e13870b25b8/

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

November 16, 2022 . 6:00 AM

More at www.hivepro.com