Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

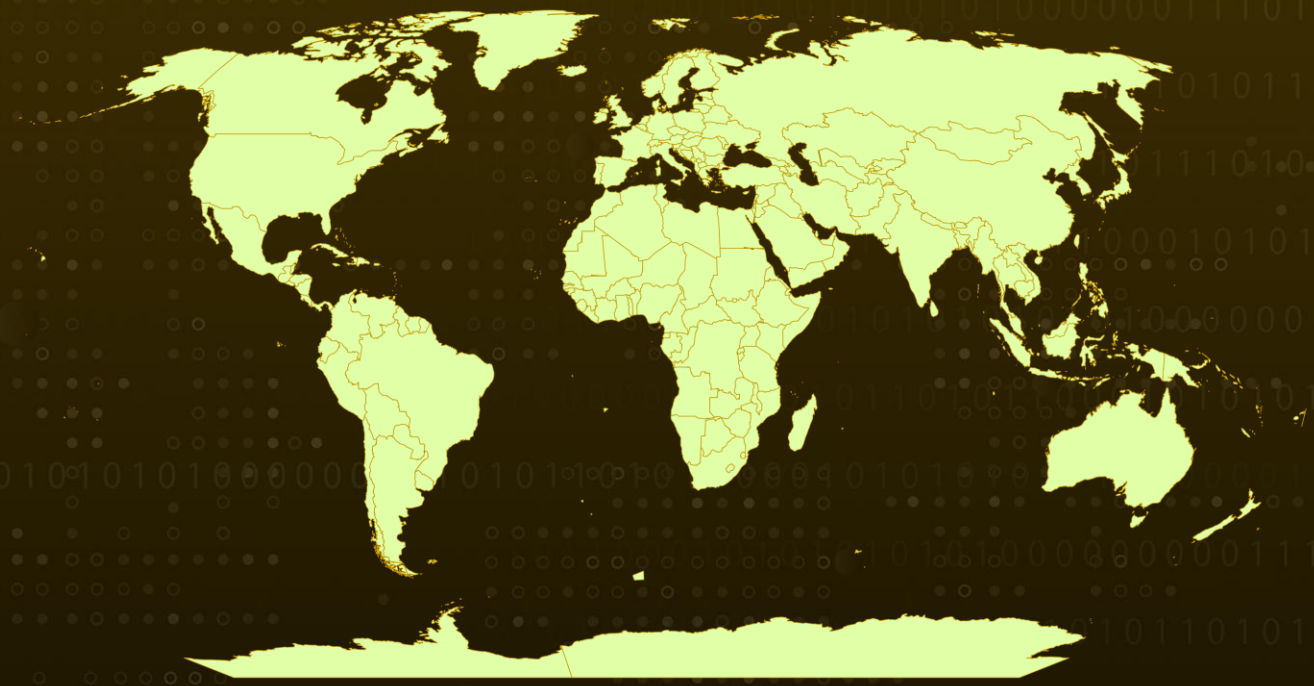
Deceptive Crypto Sites: A Breeding Ground for XPhase Clipper

Date of Publication	Admiralty Code	TA Number
February 8, 2024	A1	TA2024048

Summary

Malware: XPhase Clipper
Targeted Industries: Cryptocurrency
Attack Region: Worldwide
Impersonated Vendors: Metamask, Wazirx, Lunoapp, and Cryptonotify
Attack: A global malware campaign is actively targeting cryptocurrency enthusiasts, employing deceptive websites that masquerade as authentic cryptocurrency applications and ultimately leading to the execution of the XPhase Clipper payload.

Attack Regions



Attack Details

#1 A malware campaign is actively targeting cryptocurrency enthusiasts through deceptive websites that masquerade as legitimate cryptocurrency applications, including Metamask, Wazirx, Lunoapp, and Cryptonotify. The malevolent actors orchestrating this extensive campaign primarily focus on global cryptocurrency users, with select phishing sites specifically tailored to exploit individuals in the Indian and Russian crypto communities.

#2 Additionally, the threat actor has cloned YouTube videos and shorts related to cryptocurrency topics to potentially lure users into their nefarious schemes. The malware infection unfolds through a multi-stage process. Upon downloading the file from these phishing sites, it appears as a zip file containing a malicious executable that functions as a dropper.

#3 This dropper then deploys a VB Script and a Batch script file onto the system, subsequently initiating the execution of the XPhase Clipper payload. The core objective of the XPhase Clipper malware is to replace cryptocurrency wallet addresses copied by users with addresses under the control of the attacker.

#4 Typically, users copy and paste wallet addresses when transferring cryptocurrency funds between applications. The Clipper malware intervenes in this process, enabling attackers to reroute funds to their wallets instead of the intended recipients.

Recommendations

Enhance Email Security Protocols: Strengthen email security measures to filter out phishing emails. Educate employees on recognizing and reporting suspicious emails, especially those with compressed attachments.

Implement Multi-Signature Wallets: Consider using multi-signature wallets for cryptocurrency transactions. This requires multiple private keys to authorize a transaction, enhancing security by reducing the risk of a single point of failure.

Heighten Awareness: Familiarize yourself with common phishing tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0009 Collection	TA0040 Impact	T1585 Establish Accounts
T1566 Phishing	T1204 User Execution	T1059.005 Visual Basic	T1059.003 Windows Command Shell
T1547.001 Registry Run Keys / Startup Folder	T1036.008 Masquerade File Type	T1115 Clipboard Data	T1657 Financial Theft

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps://metamaskapp[.]space, hxxps://cryptonotify[.]ru, hxxps://wazirxapp[.]space/, hxxps://lunoapp[.]space/, hxxps://coinsbot[.]space/
SHA256	c69045a04115dabc6fe35ce6429f46f867eba680f3c863ff920daa9d1480e7a1, e116fa2900a6e0f1aa448be9dacd06ffa84f2adb48f03ad5c5b02fb1fb29f0b3, 1a4e8c51f4673c52677707f42437a181572715719763ebd5e841e07bd78b6003, ef28d77d1719b65fffa8849b36e7f96ba239021b0a5eebf441af21cc7dabaa25, 8ba85e0f0b7edddb4c2facadfde7b25162481c24944fced9901f8a86c0df8d72, 3bd57de116ae8a4f7dc69ac6fa73358e2063ea2b9c90fcb5886c3ccd35f5c524, 6c8dc2c77bd5a4776348f7c63b81b3c9c1a521eda3099d19c3014db7a246bdde, e6be2e040d1c7e3c745e3c53d85aa141b936a8269ca165daeb85dc49c06c07a

TYPE	VALUE
IPv4	31[.]31[.]198[.]206
Email	acc[@]metamaskapp[.]space

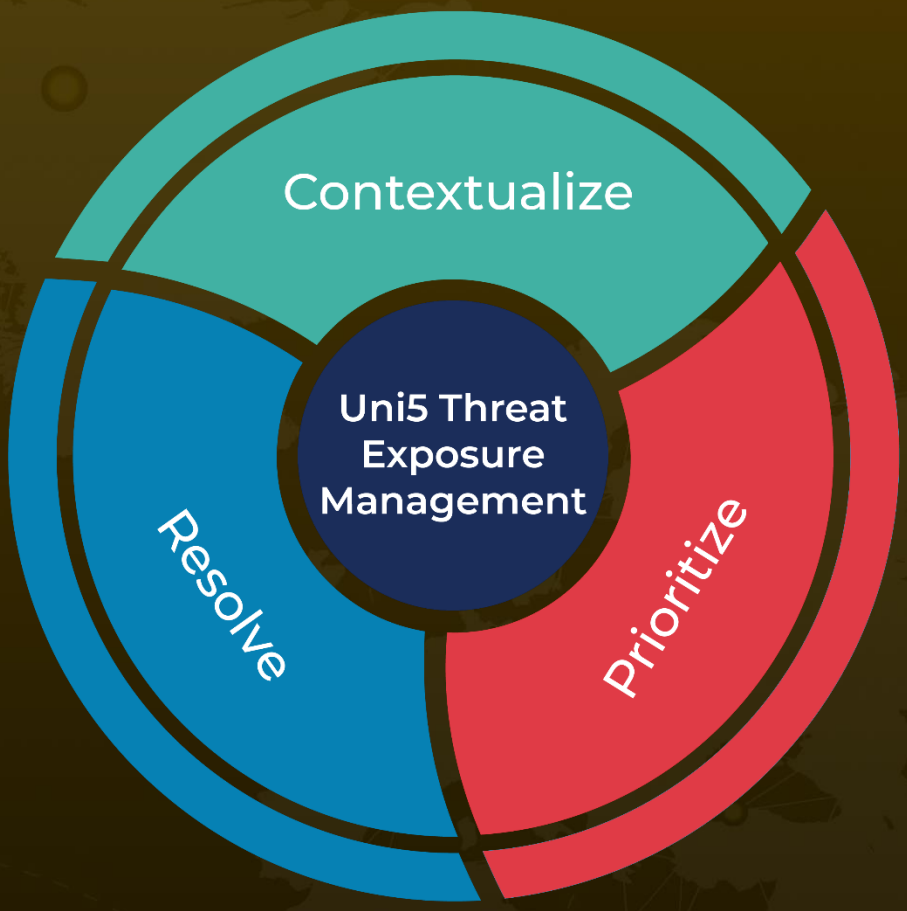
References

https://cyble.com/blog/doppelganger-dilemma-new-xphase-clippers-proliferation-via-deceptive-crypto-sites-and-cloned-youtube-videos/

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

February 8, 2024 • 3:30 AM

More at www.hivepro.com