Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Emerging MortalKombat Ransomware and Laplas Clipper Malware Targeting Cryptocurrency

Date of Publication

February 15, 2023

Admiralty Code

A1

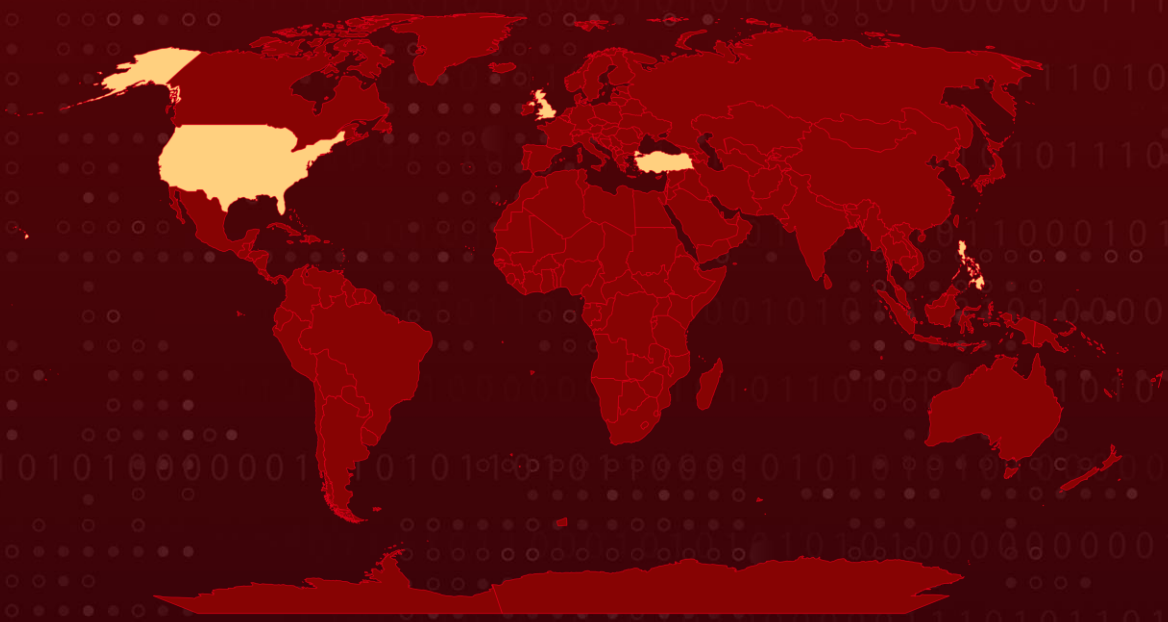
TA Number

TA2023080

Summary

First Seen: December 2022
Affected Industry: Cryptocurrency
Attack Regions: The United States, United Kingdom, Turkey, and Philippines
Impact: The theft of cryptocurrency from victims was carried out by an actor whose identity remains unknown, using both the MortalKombat ransomware and a GO variant of the Laplas Clipper malware.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 An unidentified actor using the MortalKombat ransomware and a GO variant of the Laplas Clipper malware to steal cryptocurrency from victims. This campaign aims to steal or demand ransom payments in cryptocurrency, which offers anonymity, decentralization, and a lack of regulation.

#2 The initial infection vector is a phishing email purporting to be from CoinPayments, which includes a malicious BAT loader script that downloads and executes either Laplas Clipper malware or MortalKombat ransomware. MortalKombat encrypts various files on the victim machine's file system, leaving the machine inoperable, but does not delete the volume shadow copies.

#3 The attacker uses qTOX, an instant messaging application, to communicate with the victim. Laplas Clipper targets users by employing regular expressions to monitor the victim machine's clipboard for their cryptocurrency wallet address. Once it finds the victim's wallet address, it sends it to the attacker-controlled Clipper bot, which generates a lookalike wallet address and overwrites it on the victim's machine's clipboard.

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	TA0001 Initial Access	TA0002 Execution	TA0007 Discovery
TA0003 Persistence	TA0042 Resource Development	TA0040 Impact	T1509 Command and Scripting Interpreter
T1490 Inhibit System Recovery	T1012 Query Registry	T1021 Remote Services	T1048 Exfiltration Over Alternative Protocol
T1496 Resource Hijacking	T1060 Registry Run Keys / Startup Folder	T1064 Scripting	T1070 Indicator Removal on Host
T1082 System Information Discovery	T1106 Native API	T1566 Phishing	T1486 Data Encrypted for Impact
T1120 Peripheral Device Discovery	T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol	T1083 File and Directory Discovery	T1197 BITS Jobs

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	9a5a5d50dea40645697fabc8168cc32faf8e71ca77a2ea3f5f73d1b9a57fc7b0 26d870d277e2eca955e51a8ea77d942ebafbbf3cbf29371a04a43cfe1546db17 1bf30c5c51a3533b4f0d7d3d560df691657d62374441d772f563376b55a60818 f02512e7e2950bdf5fa0cd6fa6b097f806e1b0f6a25538d3314c793998484220 63ec10e267a71885089fe6de698d2730c5c7bc6541f40370680b86ab4581a47d E5f60df786e9da9850b7f01480ebffced3be396618c230fa94b5cbc846723553

TYPE	VALUE
URLs	http://193.169.255.78/fw-apgksdtpx4hoaujjmbvdnxpohz.pdf.zip http://193.169.255.78/fw-cpgk2xfpx4hoaujjmbvdnxpohz.pdf.zip
IPV4	193.169.255.78 144.76.136.153

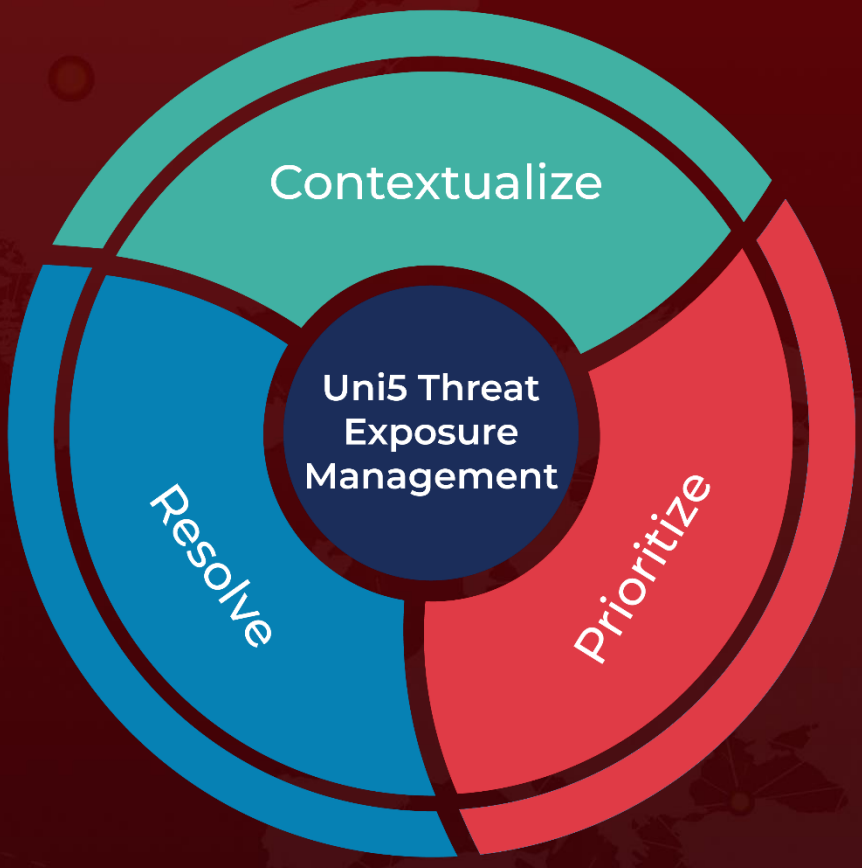
References

https://blog.talosintelligence.com/new-mortalkombat-ransomware-and-laplas-clipper-malware-threats/

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 15, 2023 . 1:00 PM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com