Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

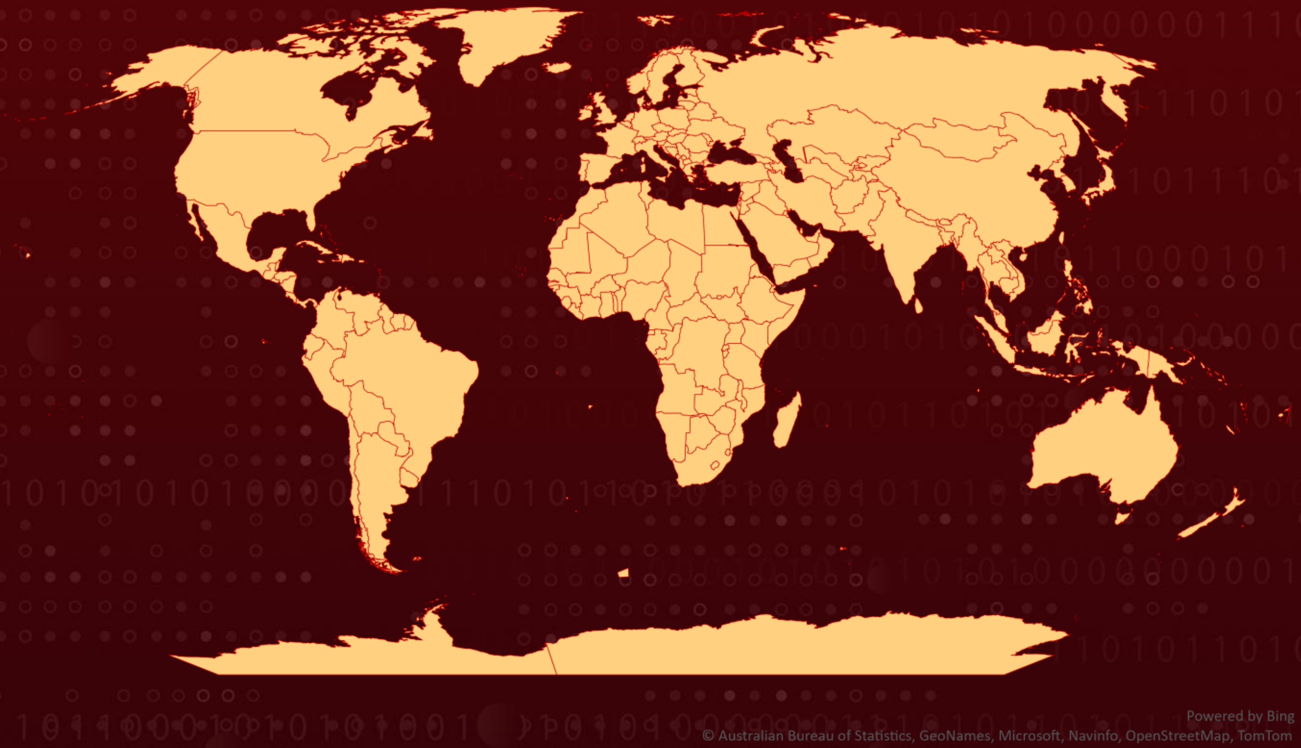
ParallaxRAT targets cryptocurrency organizations through phishing emails

Date of Publication	Admiralty Code	TA Number
March 01, 2023	A1	TA2023111

Summary

First Appearance: December 2019
Target Countries: Worldwide
Malware: ParallaxRAT
Target Sector: Cryptocurrency
Attack: ParallaxRAT targets cryptocurrency organizations through phishing emails and performs malicious activities such as keylogging and remote control of compromised machines.

Attack Regions


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

Attack Details

#1

ParallaxRAT is a remote access Trojan (RAT) that has been distributed through phishing emails since December 2019. Recently, ParallaxRAT has been targeting cryptocurrency organizations. The malware uses injection techniques to hide within legitimate processes, making it difficult to detect. Once it successfully infects a victim's machine, the attacker can interact with them through Notepad and instruct them to connect to a Telegram channel.

#2

ParallaxRAT performs various malicious activities such as accessing files, keylogging, remote desktop control, and remote control of compromised machines. It can gather sensitive information from victimized machines, including system information, keystrokes, and data stored in the clipboard. The malware also has the ability to read and record its victim's keystrokes, which are then encrypted and stored in the appdata directory.

#3

The threat actor behind ParallaxRAT uses a commercially available RAT tool and grabs private email addresses of cryptocurrency companies from the website dnsdumpster.com. The malware is disseminated via phishing emails, and sensitive data is obtained.

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

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
T1566 Phishing	T1056 Input Capture	T1056.001 Keylogging	T1027 Obfuscated Files or Information
T1055 Process Injection	T1006 Direct Volume Access	T1021 Remote Services	T1021.001 Remote Desktop Protocol
T1586 Compromise Accounts	T1055.012 Process Hollowing	T1140 Deobfuscate/Decode Files or Information	T1529 System Shutdown/Reboot
T1083 File and Directory Discovery	T1623 Command and Scripting Interpreter	T1082 System Information Discovery	T1057 Process Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	40256ea622aa1d0678f5bde48b9aa0fb 698463fffdf10c619ce6aebcb790e46a 3c98cee428375b531a5c98f101b1e063 40256ea622aa1d0678f5bde48b9aa0fb

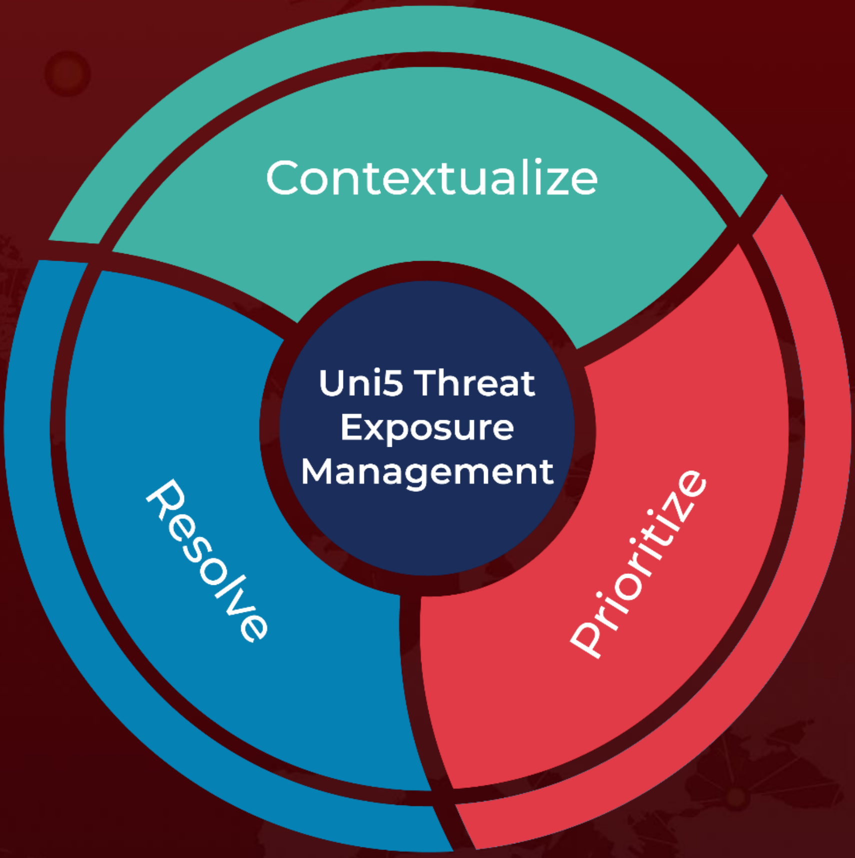
References

https://www.uptycs.com/blog/cryptocurrency-entities-at-risk-threat-actor-uses-parallax-rat-for-infiltration

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 01, 2023 • 6:30 AM

More at www.hivepro.com