Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

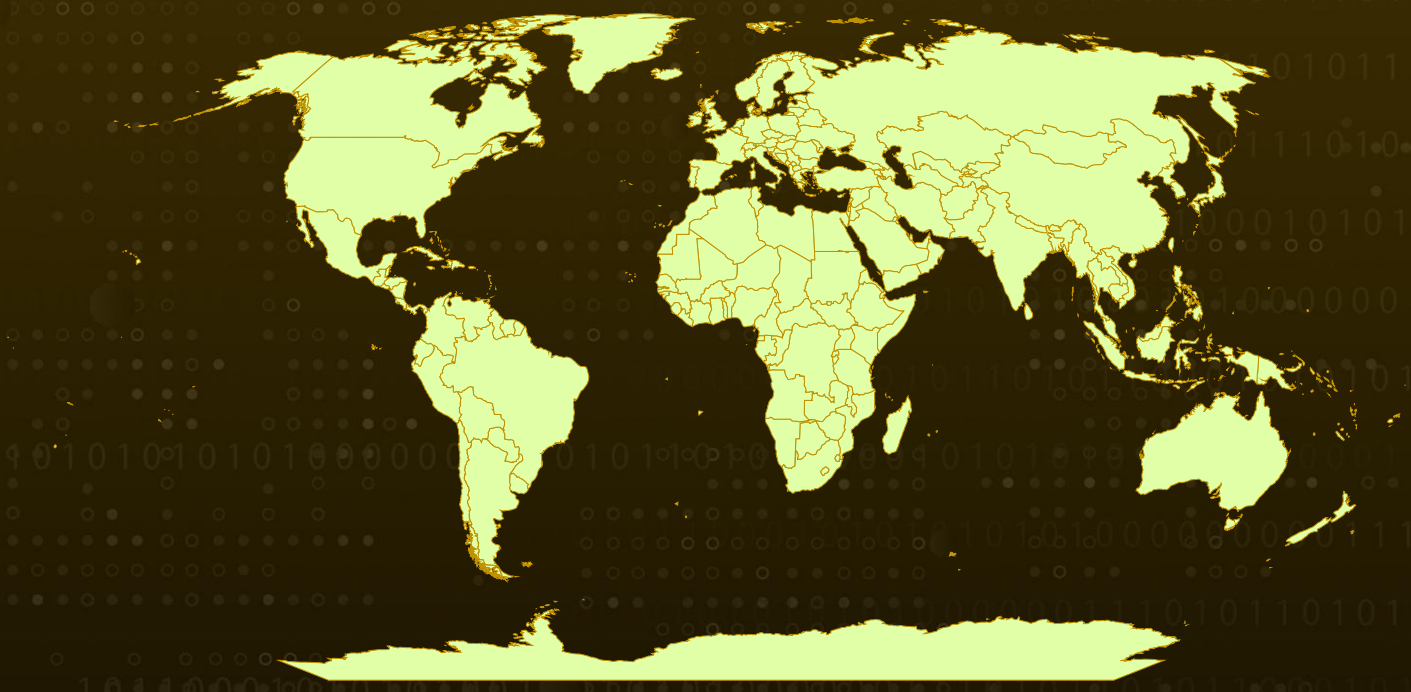
Neptune RAT's Triple Threat: To Steal, Spy, and Encrypt

Date of Publication	Admiralty Code	TA Number
April 11, 2025	A1	TA2025111

Summary

First Seen: January 2025
Malware: Neptune RAT
Affected Platform: Windows
Targeted Regions: Worldwide
Attack: Neptune RAT is a deceptive and dangerous malware posing as a remote access tool, spreading through platforms like GitHub and Telegram. Beneath the surface, it functions as a versatile tool for cybercriminals capable of stealing credentials, intercepting cryptocurrency transactions, monitoring user activity, and severely compromising system integrity.

Attack Regions



Attack Details

#1 Neptune RAT is a sophisticated piece of malware written in Visual Basic .NET, explicitly designed to take control of Windows systems. It's been spreading rapidly through platforms like GitHub, Telegram, and YouTube. It typically begins its infection with a simple PowerShell command that silently downloads a malicious script from sites like catbox.moe.

#2 Once executed, the malware embeds itself deep within the system usually in the AppData folder, and establishes a connection back to the attacker's server, granting full remote control over the compromised machine. What makes Neptune RAT particularly threatening is its wide array of destructive features.

#3 It includes a crypto clipper that silently swaps copied wallet addresses to steal cryptocurrency, a password stealer capable of exfiltrating credentials from over 270 applications, ransomware functions that encrypt user data, and the ability to monitor the desktop in real-time. In some cases, it can even overwrite the Master Boot Record, rendering the system unusable.

#4 To avoid detection, Neptune RAT employs heavy obfuscation, inserting Arabic characters and emojis into its code and automated security tools. It checks for virtual environments and halts execution if it suspects it's being analyzed. Persistence is achieved by modifying system registries and creating scheduled tasks to ensure it continues running after reboots.

#5 It also leverages legitimate tools, such as Email Password Recovery Pro, to extract email credentials without raising alarms. The so-called "free version" is riddled with deliberate bugs such as trying to execute a .bat file as if it were a .exe presumably to frustrate users into purchasing a paid version with full functionality. Neptune RAT poses a serious threat due to its stealth, resilience, and versatility. It's engineered not only to steal sensitive data but to cause lasting damage, often beyond easy recovery.

Recommendations

Deploy Endpoint Detection and Response (EDR) Solutions: Implement EDR tools to detect suspicious activities, such as unauthorized registry changes, process injections, and the creation of persistent tasks. Ensure rapid response and containment capabilities to neutralize threats as they occur.

Network Segmentation & Zero Trust Implementation: Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.

Implement Strict Privilege Management: Enforce least-privilege access policies to limit user permissions and minimize attack surfaces. Monitor and log all administrative actions to detect and prevent privilege escalation attempts by malware.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0011 Command and Control	**TA0010** Exfiltration	**TA0040** Impact	**T1566** Phishing
T1059.001 PowerShell	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1548** Abuse Elevation Control Mechanism
T1548.002 Bypass User Account Control	**T1027** Obfuscated Files or Information	**T1027.002** Software Packing	**T1027.009** Embedded Payloads
T1606.001 Web Cookies	**T1555.003** Credentials from Web Browsers	**T1056** Input Capture	**T1056.001** Keylogging

T1087 Account Discovery	**T1217** Browser Bookmark Discovery	**T1083** File and Directory Discovery	**T1082** System Information Discovery
T1123 Audio Capture	**T1185** Browser Session Hijacking	**T1115** Clipboard Data	**T1005** Data from Local System
T1113 Screen Capture	**T1125** Video Capture	**T1572** Protocol Tunneling	**T1041** Exfiltration Over C2 Channel
T1485 Data Destruction	**T1140** Deobfuscate/Decode Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8df1065d03a97cc214e2d78cf9264a73e00012b972f4b35a85c090855d71c3a5, 9fe8a026b5f41a4d434bb808273b83a364a1994a60e2ab7e232a31bf2b76a33f, e03f6f8d0ce9abdda3e3fff801babcd4448a567f330c4cac498fec39652f3c77, 21c832f9d76b8ae74320b8fac811a761f09f871ee32c9ab1c8fb1492b95a7d04, e8c8f74ae15e7d809d9013bdfa2a10dd54e00d4ea5ff4ed6cd4a163b80d2d318, 14e196e089014313c9fa8c86ce8cffb1c7adacd7d1df7373d97b30d31b965df9, add3e9a1c6654d1ec9b7fd0ffea6bdcd0eb7b3e4afa70c6776835cc238e8f179, da27b3619e958d58f0a8867d765421328632b834b3a18955508609a3028a96df, dec534ab858a71575a3836b96d0f96df89eb8ba50f9bc69350faa0f7bcccfd25, 88cc579613730f847f72e28b4e880bd8104edf6d6ab37ffa0d18f273889d1a40, e310a1b264912ae886cd956abc42dee846455a99f67c3ea8336a202240bd7dfa,

TYPE	VALUE
SHA256	2b4aa36247da1af1de0091e7444fbf8f829d133743bb3b931618c66bbd10d10b, 9a35113e1d9412701d85b5af01b4ad2b1e584c6e0963e439053808b29b4da90a, 684d2d50dd42e7ba4e9bd595e9b6f77eb850185556c71db4eda6f78478a5e6fb, 9ca70da0ea94b3bea68c9a3259ec60192c5be1ae7630a08924053168bbf41335, d0c6f5d916933a1f8d852ca42163ff50bfe07132fcacac03db7d20f573284208, 1bbd4262c8821a0290fe40a8e374c6e5fa2084331670ede42e995d3d5902efcd, a19ef7ace3118ff9e5be24b388aff3e56a5bac0d4069bf8480721e3f4508706a, 20c31ac326b5c6076f9b1497f98b14a0acd36ff562dfa2076589a47a41d0e078, 6d02eb3349046034cf05e25e28ef173c01d9e0ea1f4d96530defe9e2a3d5e8a0, 62fdc4b159ad1b4225098276e6f2dcf29d49d9545ac9575d4ff1f6b4f00cdb65, 70554db8312c03c8cce38925db900cdbe8e57e88da29b0bf2f61ed1bbcaa03bd, cd2b320433843d4d694ae8185c7ef07a90d7dce6d05a38ac4481ad2eab9bcfe5, 630b1879c2e09b2f49dd703a951fb3786ede36b79c5f00b813e6cb99462bf07c
File Name	NeptuneRAT.exe, MasonClient.exe, Ping.exe, px5r4x.bat, AntiFormat.dll, BlockerAntiVirus.dll, bomber.dll, Bookmarks.dll, BSOD.dll, Chromium.dll, Clipper.dll, Cmstp-Bypass.dll, WebCam.dll, DeletePoints.dll, Destry.dll, DisableWD.dll, WDExclusion.dll, UACBypass.dll, Info.dll, KillCPU.dll,

TYPE	VALUE
File Name	Microphone.dll, Ransomware.dll, ScreenRotation.dll, Encoder.dll

References

https://www.cyfirma.com/research/neptune-rat-an-advanced-windows-rat-with-system-destruction-capabilities-and-password-exfiltration-from-270-applications/

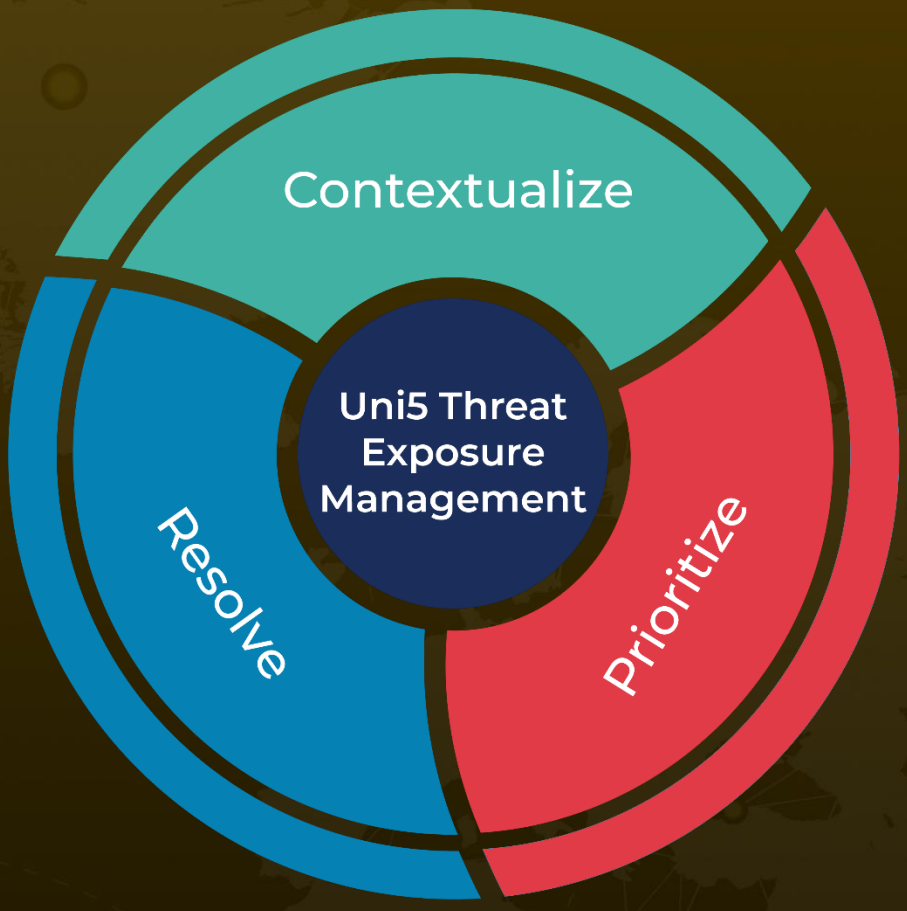
https://github.com/MasonGroup/NeptuneRatV1

https://hivepro.com/threat-advisory/ransomware-meets-rat-noneuclids-destructive-capabilities-revealed/

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

April 11, 2025 • 4:00 AM

More at www.hivepro.com