Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

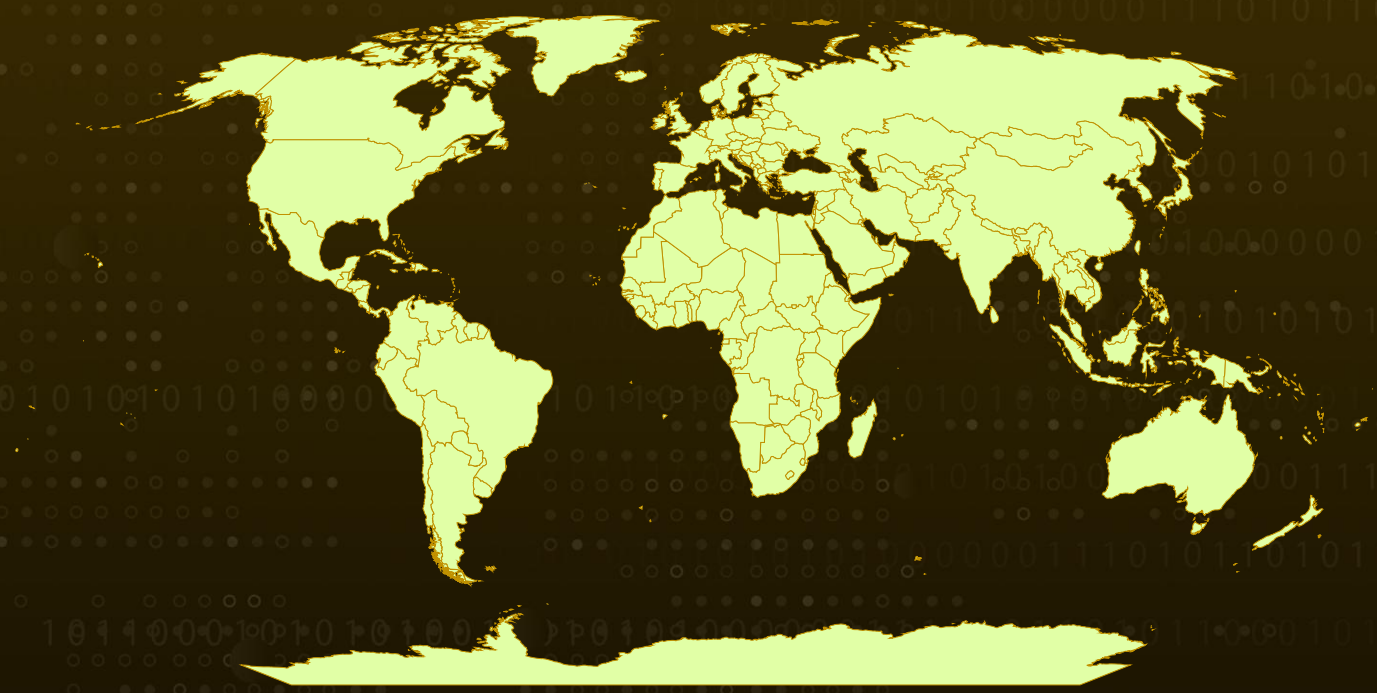
Ransomware Meets RAT NonEuclid's Destructive Capabilities Revealed

Date of Publication	Admiralty Code	TA Number
January 3, 2025	A1	TA2025002

Summary

Malware: NonEuclid
Targeted Region: Worldwide
Attack: The NonEuclid Remote Access Trojan (RAT) is a powerful C# malware designed to grant unauthorized control over victim computers while evading detection. Promoted on underground forums and platforms like Discord, this stealthy RAT employs advanced tactics, including antivirus bypass, privilege escalation, AES encryption, and anti-virtual machine checks, to ensure persistence and resilience.

Attack Regions



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

Attack Details

#1 The NonEuclid Remote Access Trojan (RAT) is a sophisticated piece of malware engineered to grant unauthorized remote access and control over a victim's computer. Written in C# for the .NET Framework 4.8, it incorporates advanced evasion techniques and destructive functionalities, making it a serious threat in the realm of cybersecurity.

#2 Designed to bypass safeguards such as antivirus programs and user account controls, it ensures persistence while reducing the likelihood of detection. This malware has garnered significant attention among cybercriminals, largely due to its promotion on underground forums and platforms like Discord and YouTube.

#3 Its wide appeal stems from an impressive array of features, including antivirus evasion, privilege escalation, ransomware encryption, and anti-detection mechanisms. It also uses dynamic DLL loading, anti-virtual machine (anti-VM) checks, and AES encryption to enhance its stealth and durability.

#4 The NonEuclid RAT initiates its attack by setting delays, verifying administrative privileges, and executing anti-detection checks. Additionally, it can terminate system monitoring applications like Task Manager and Process Explorer to hinder user intervention.

#5 One of its standout evasion strategies is its ability to recognize virtualized or sandboxed environments. If such conditions are detected, the RAT shuts itself down to evade analysis. Beyond these evasive techniques, the NonEuclid RAT exhibits destructive capabilities by encrypting critical files.

#6 Using AES encryption, it targets file types such as .csv, .txt, and .php, appending the .NonEuclid extension and demanding a ransom for decryption. The NonEuclid RAT highlights the growing sophistication of modern malware, combining stealthy behavior with destructive potential.

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.

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.

Zero Trust Architecture: Implement a Zero Trust security model, where all users and devices are continuously authenticated and verified, regardless of their location within the network.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**TA0040** Impact
T1059 Command and Scripting Interpreter	**T1106** Native API	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder
T1505 Server Software Component	**T1548.002** Bypass User Account Control	**T1548.001** Setuid and Setgid	**T1027** Obfuscated Files or Information
T1027.004 Compile After Delivery	**T1070** Indicator Removal	**T1070.006** Timestomp	**T1112** Modify Registry
T1140 Deobfuscate/Decode Files or Information	**T1222** File and Directory Permissions Modification	**T1497** Virtualization/Sandbox Evasion	**T1497.001** System Checks
T1562 Impair Defenses	**T1562.001** Disable or Modify Tools	**T1620** Reflective Code Loading	**T1012** Query Registry
T1033 System Owner/User Discovery	**T1057** Process Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery

T1087 Account Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery	T1614 System Location Discovery
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1041 Exfiltration Over C2 Channel	T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d32585b207fd3e2ce87dc2ea33890a445d68a4001ea923daa750d32b5de52bf0, e1f19a2bc3ce5153e8dfe2f630cc43d6695fac73f5aaa59cd96dc214ca81c2b0

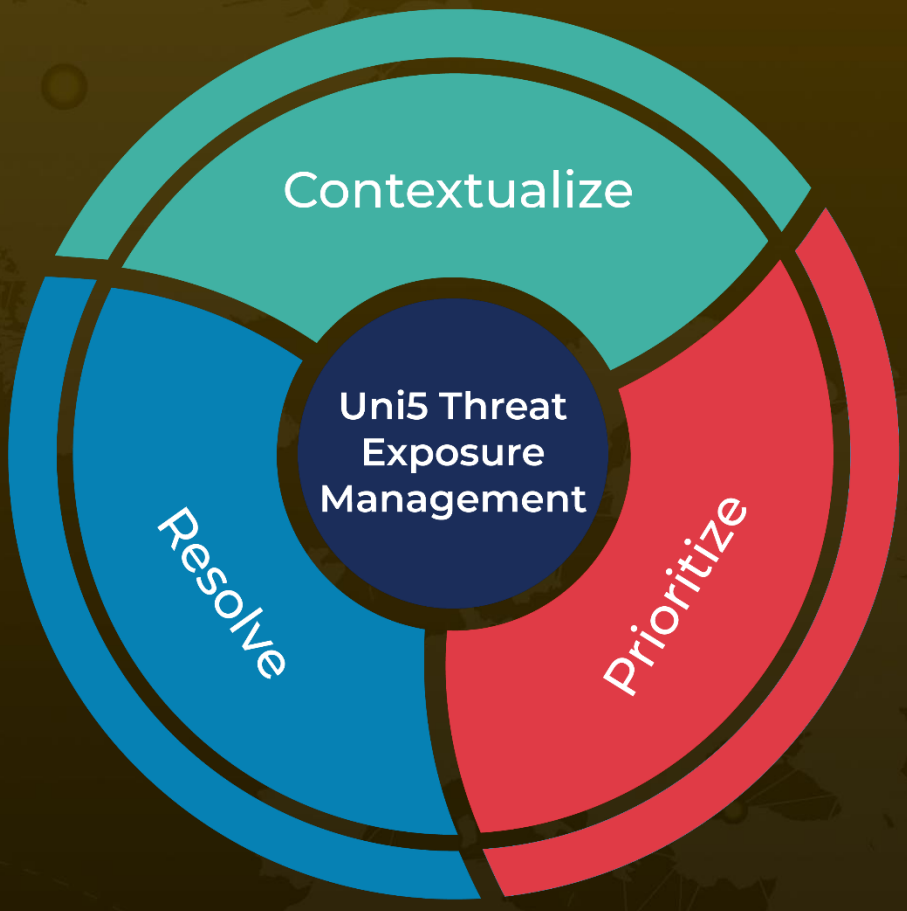
References

https://www.cyfirma.com/research/noneclid-rat/

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

January 3, 2025 • 4:00 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com