SECURITY ADVISORY

CYBER STASH

January, 2025

NonEuclid RAT

Context

First identified in late 2024, NonEuclid is an advanced Remote Access Trojan (RAT) specifically designed to target Windows systems. Actively promoted on underground channels such as Discord and YouTube, it is distributed through spear-phishing campaigns and the exploitation of software vulnerabilities, making it a versatile and highly effective tool for cybercriminals.

What sets NonEuclid apart is its ability to evade robust security measures, including the Anti-Malware Scan Interface (AMSI) and User Account Control (UAC). This capability enables it to execute a range of malicious activities, including data exfiltration, keylogging, and facilitating ransomware attacks. The sophisticated nature of this malware poses a significant threat to both individuals and organisations, underscoring the critical need for proactive and layered cybersecurity defences. By leveraging advanced evasion techniques, NonEuclid poses a critical risk to organisations relying solely on Microsoft Defender for endpoint security.

While Microsoft Defender provides baseline protection, its effectiveness can be undermined by NonEuclid's ability to bypass key defences, such as the Anti-Malware Scan Interface (AMSI) and User Account Control (UAC). This leaves endpoints vulnerable to data exfiltration, keylogging, and ransomware attacks, potentially leading to significant financial and reputational damage.

To mitigate these risks, organisations must adopt a multi-layered security approach that combines robust endpoint detection and response (EDR) solutions with proactive threat hunting, behavioural analysis, and continuous monitoring to stay ahead of sophisticated threats like NonEuclid.

Mitigation

Defending against NonEuclid RAT requires proactive measures, including:

Independent Breach Detection: Regular forensic assessments and independent detection tools identify breaches missed by traditional "advanced" Endpoint Detection and Response (EDR) defences.

Evasion Behaviour Detection: Monitor for AMSI and UAC bypass attempts to catch evasive threats early.

Block High-Risk Traffic: Restrict traffic to high-risk infrastructure to reduce attack surface.

Technical Details

Malware Delivery
NonEuclid RAT is disseminated through spear-phishing emails with malicious attachments or links, exploitation of unpatched software vulnerabilities, and drive-by downloads from compromised websites. Its widespread availability is further amplified by tutorials and discussions shared on underground platforms such as Discord and YouTube, enabling cybercriminals to easily adopt and distribute the malware.

Malware Analysis
Upon execution, *NonEuclid RAT* initiates a series of actions to secure control over the infected system and evade detection:

- **Initialization**: Introduces a startup delay and configures application settings.
- **Privilege and Security Checks**: Assesses process handling, performs anti-defender scans, and validates administrative privileges for advanced functionality.
- **Installation and Mutex Handling**: Installs itself and ensures no conflicting instances are active using mutex control.
- **Anti-Detection and Logging**: Detects sandboxed environments and activates anti-process blocking and sleep prevention mechanisms while logging activity asynchronously.
- **Socket Communication**: Establishes a client socket connection to the C2 server, with reconnection capabilities to maintain persistence.

Backdoor Command Functions
NonEuclid RAT includes several malicious backdoor commands, including:

- **Keylogging**: Monitors and captures keystrokes for credential theft.
- **Data Exfiltration**: Identifies and exfiltrates sensitive files based on predefined criteria.
- **Process Termination**: Disables security software and forensic utilities to hinder detection.
- **Dynamic DLL Loading**: Evades static analysis by loading code dynamically.
- **Ransomware Encryption**: Encrypts files with AES encryption and appends the ".NonEuclid" extension, locking the user out of critical data.

This sophisticated, evolving campaign leverages a mix of social engineering, obfuscation, and persistence strategies to continually target and exploit users across multiple sectors.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to NonEuclid RAT:

Tactic	Technique	Description
Initial Access	Phishing (T1566)	Spear-phishing emails deliver malicious payloads.
	Exploit Public-Facing Application (T1190)	Exploits vulnerabilities in public-facing applications.
Execution	Command and Scripting Interpreter (T1059)	Uses scripting languages.
	Native API (T1106)	Directly interacts with Windows API for privileged actions.
Persistence	Boot/Logon Auto-Start (T1547)	Configures malware to start on boot/logon.
	Registry Run Keys (T1547.001)	Adds entries to registry/startup for persistence.
Privilege Escalation	Bypass UAC (T1548.002)	Bypasses User Account Control to escalate privileges.
Defence Evasion	Obfuscated Files (T1027)	Hides malicious code through obfuscation.
	Impair Defences (T1562)	Disables security measures to evade detection.
	Virtualization/ Sandbox Evasion (T1497)	Evades virtual environments and sandboxes.
Discovery	Account Discovery (T1087)	Identifies user accounts and privileges.
	System Information (T1082)	Gathers system info for tailoring the attack.
C2	Application Layer Protocol (T1071)	Uses HTTP/other protocols for C2 and exfiltration.
Exfiltration	C2 Exfiltration (T1041)	Exfiltrates data through encrypted C2 channels.
Impact	Ransomware (T1486)	Encrypts files with ransomware to disrupt operations.

References

IOCs:

File Hashes (SHA-256)

- d32585b207fd3e2ce87dc2ea33890a445d68a4001ea923daa750d32b5de52bf0
- E1f19a2bc3ce5153e8dfe2f630cc43d6695fac73f5aaa59cd96dc214ca81c2b0

Yara Rule

```
rule Detect_Suspicious_Filenames_and_Paths
{
    meta:
        author = "CyberStash"
        description = "Detects suspicious file names and paths for Discord Update and Commonuadate.exe"
        date = "2025-01-20"

    strings:
        // Paths and filenames to detect
        $path1 = "C:\\Users\\\\AppData\\Roaming\\obs-studio\\updates.exe"
        $path2 = "C:\\Users\\\\AppData\\Roaming\\Microsoft\\Windows\\Templates Intel\\Games\\Common\\Commonuadate.exe"
        $filename1 = "Discord Update"
        $filename2 = /update-[0-9]+-[0-9]+-[0-9]+-[0-9]+-[0-9]+-[0-9]+-[0-9]+/

    condition:
        ($path1 and $filename1) or
        ($path2 and $filename2)
}
```

Public Intelligence:

- https://www.cyfirma.com/research/noneuclid-rat/
- https://cybersecsentinel.com/advanced-evasion-techniques-used-by-noneuclid-rat/
- https://thehackernews.com/2025/01/researchers-expose-noneuclid-rat-using.html
- https://thesecmaster.com/blog/researchers-expose-noneuclid-rat-with-advanced-evasion-and-ransomware-capabilitie
- https://hivepro.com/wp-content/uploads/2025/01/TA2025002.pdf?utm_sr=(direct)&utm_cmd=(none)&utm_ccn=(not%20set)