New NONEUCLID RAT Malware Infected Multiple Devices Worldwide

By AnuPriya

Published: 2024-12-09 · Archived: 2026-04-05 22:44:51 UTC

A new Remote Access Trojan (RAT) named **NONEUCLID** has emerged in the cyber threat landscape, infecting devices worldwide.

Developed under the alias **SheetRAT** (also known as LiberiumRAT or ShadowRoot), this malware has gained attention for its advanced capabilities, making it a potent tool for cybercriminals.

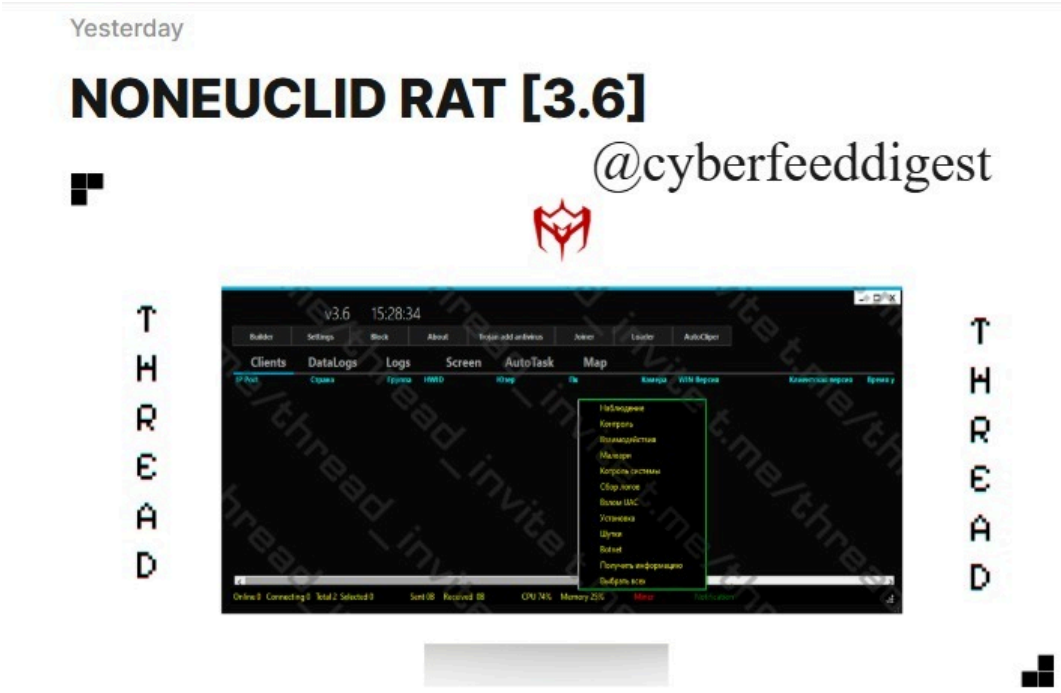
According to cybersecurity experts, NONEUCLID RAT is equipped with features such as a rootkit, autoload functionality, and a User Account Control (UAC) bypass. These functionalities allow the malware to maintain persistence on infected systems and evade detection.

Additionally, NONEUCLID employs obfuscation techniques and anti-debugging mechanisms to make reverse engineering and analysis by security researchers more challenging.

The malware also integrates a botnet framework and utilizes Discord webhooks for command-and-control communication, enabling attackers to remotely control compromised machines.

Global Impact and Potential Threats

According to the post from cyberundergroundfeed, the spread of NONEUCLID RAT has been reported globally, with victims ranging from individual users to organizations.



Ratnik is aimed at PC users with a large number of tools for everything that could be thought of. METRO visual interface. Ratnik by developer SheetRAT aka LiberiumRAT aka ShadowRoot .

Peculiarities:

- Autoload
- Rootkit
- Masking (icon, assembly)
- Joiner
- Bypass UAC
- Obfuscation
- Anti-Debug

Its ability to bypass security measures and remain undetected for extended periods poses a significant threat to data privacy and system integrity.

Cybersecurity analysts warn that the malware's botnet capabilities could be exploited for large-scale attacks, including Distributed Denial-of-Service (DDoS) operations or data exfiltration campaigns.

What sets NONEUCLID apart from other RATs is its inclusion of unusual features such as "jokes," suggesting that its creators may be experimenting with unconventional functionalities or attempting to mock their victims.

Despite this seemingly playful element, the malware's overall design underscores its dangerous potential in the hands of skilled attackers.

Call for Vigilance and Mitigation

Cybersecurity professionals are urging users and organizations to remain vigilant against this emerging threat.

To mitigate the risk of infection, it is recommended to implement robust endpoint protection solutions, regularly update software, and avoid downloading files or clicking on links from untrusted sources.

Security teams should also monitor network traffic for suspicious activity associated with Discord webhooks or botnet communications.

The rise of NONEUCLID RAT highlights the evolving sophistication of cyber threats in 2024.

As attackers continue to develop more advanced tools, collaboration between cybersecurity firms, governments, and individuals will be essential to combat these threats effectively.

Also Read:

AnuPriya

Any Priya is a cybersecurity reporter at Cyber Press, specializing in cyber attacks, dark web monitoring, data breaches, vulnerabilities, and malware. She delivers in-depth analysis on emerging threats and digital security trends.

Source: https://cyberpress.org/noneuclid-rat-malware/