Open-Source Xeno RAT Trojan Emerges as a Potent Threat on GitHub

Date: 14th April 2024 | Severity: High

Summary

An “intricately designed” remote access trojan (RAT) called Xeno RAT has been made available on GitHub, making it easily accessible to other actors at no extra cost.

Nood RAT is a backdoor malware that can receive commands from the C&C server to perform malicious activities such as downloading malicious files, stealing systems’ internal files, and executing commands. Although simple in form, it is equipped with the encryption feature to avoid network packet detection and can receive commands from threat actors to carry out multiple malicious activities.

The development comes as the AhnLab Security Intelligence Center (ASEC) revealed the use of a Gh0st RAT variant called Nood RAT that’s used in attacks targeting Linux systems, allowing adversaries to harvest sensitive information.

Attack Vectors

- Xeno RAT, an open-source RAT written in C#, is designed for remote system management and compatible with Windows 10 and Windows 11 operating systems.
- It includes a SOCKS5 reverse proxy, real-time audio recording, and a hidden virtual network computing module like DarkVNC.
- The RAT also has a builder that allows for the creation of bespoke variants of the malware. The malware uses a multi-stage sequence, disguised as a WhatsApp screenshot, to launch a malicious DLL and establish persistence.
- This comes as the AhnLab Security Intelligence Center (ASEC) revealed the use of a Gh0st RAT variant called Nood RAT, which is used in attacks targeting Linux systems. Nood RAT is equipped with encryption to avoid network packet detection and can execute multiple malicious activities.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 035f83018cf96f5e1f6817ccd39fc0b6 • b4910e998cf58da452f8151b71c868cb • 4f3afdcfff8f7994b7d3d3fbaa6858b4 • a15ebd19cac42b0297858018da62b1be • c440bd814be37fac669567131c4ba996 • 75838e5d481da40db2e235a6d5a222ef • 905c2158fadfe31850766f010e149a0f • 8457f71c6a5fe83bb513d1dfba99271a • 35743db3dc333245ef5b69100721ced9 • 7d631e5b0c78805dd5d440cce788d25b • 0a35e06f53c17ab1c8e18e7e0c0821d8 • 97db3f7676380f0baa3840ed5d5c1767 • d9f00f71efabdfcca7c63d4b0805673c
IPs	• 43.156.118.72:443 • 42.51.40.184:56 • 13.214.222.35:443 • 43.140.251.218:8080 • 101.42.139.110:8443 • 101.42.139.110:53 • 81.68.143.132:1234 • 81.68.143.132:8080 • 194.36.191.75:443 • 1.117.165.141:53 • 23.100.88.61:53
Domains	• Bo[.]appleupcheck[.]com • Cloud[.]awsxtd[.]com • Update[.]kworker[.]net • Check[.]snapupdate.org • b.niupilao[.]vip

Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Regularly back up the data and store it in a secure location.
- Ensure that all software, operating systems, and security applications are up to date with the latest patches and updates.
- Monitor the network for suspicious activity.
- Change the passwords regularly and use strong passwords with multi-factor authentication (MFA).
- Educate employees about the risks of ransomware/malware, how to identify phishing attempts, and safe online behavior.

Reference Links

- https://www.adgm.com/documents/financial-crime-prevention-unit/cybercrime-prevention/20240226-cyber-security-council-alert-27.pdf
- https://asec.ahnlab.com/en/62144/
- Open-Source Xeno RAT Trojan Emerges as a Potent Threat on GitHub (thehackernews.com)