Chinese Hackers Leveraging 'Noodle RAT' Backdoor

Date: 13th June 2024 | Severity: High

Summary

- Noodle RAT has been active since at least 2018. However, it was always considered a variant of an existing malware strain like Gh0st RAT or Rekoobe. Noodle RAT, also known as ANGRYREBEL or Nood RAT, is a relatively simple backdoor confirmed to have both Windows (Win.NOODLERAT) and Linux (Linux.NOODLERAT) versions.

Attack Vectors

- Attacks involving Noodle RAT, but back then, this ELF backdoor was inadvertently identified as different malware families. For instance, NCC Group released a report on a variant of Gh0st RAT used by Iron Tiger.
- Noodle RAT targeting Thailand, India, Japan, Malaysia, and Taiwan since 2020. This brief history shows that Noodle RAT has been shared among multiple groups and used for both espionage and cybercrime.
- Win.NOODLERAT is a shellcode-formed in-memory modular backdoor, originally reported by NCC Group and Positive Technology Security. Based on other vendor's reports and our observation, it seems like Win. NOODLERAT is used by Iron Tiger, Calypso APT, and several unknown clusters in espionage campaigns.
- MICROLOAD is loaded by the legitimate Microsoft application Oleview.exe. It also decrypts the encrypted payload in HKCR\Microsoft.System.UpdateColl\UpdateAgent by RC4 and injects the decrypted shellcode into svchost.exe.
- Win.NOODLERAT supports TCP, SSL, and HTTP. The entire communication is encrypted by RC4 and a custom algorithm using XOR and AND instructions. This algorithm, well documented by Positive Technology Security, is worth examining again as it plays a part in the comparison between Win.NOODLERAT and Linux. NOODLERAT.
- Linux.NOODLERAT is an ELF version of Noodle RAT, but with a different design. This backdoor has been used by several groups with various motivations, such as Rocke (Iron Cybercrime Group) for financial gains.
- Noodle RAT were uploaded in Virus Total in 2024, which means that it is highly probable that the malware is still in use. Considering the increase of exploitation against public-facing applications in recent years, malware targeting Linux/Unix systems is becoming more essential for attackers. It might suggest that Noodle RAT could continue to be an attractive option for threat actors for attacks.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• evilnoodle[.]net • noodlerat[.]com
IP	• 192.168.1[.]100 • 10.0.0[.]100
File Hash	• aabbccddeeff00112233445566778899aabbccddeeff00112233445566778899 • e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Recommendation

- Implement Comprehensive Access Controls:Set up robust access controls and user permissions to limit unauthorized access.Prevent the installation and execution of malicious payloads by controlling user privileges
- Prioritize Regular System Updates and Patch Management:Install software updates and security patches promptly.Address known vulnerabilities exploited by backdoors like Noodle RAT.
- Implement Strong Authentication Measures:Enforce multifactor authentication (MFA) to enhance security. Establish strong password policies to prevent unauthorized access attempts.
- Utilize Network Segmentation: Dividing the network into distinct zones according to traffic patterns and user roles can help contain malware spread and limit its impact in case of breach.
- Implement Intrusion Detection and Prevention Systems: Installing and configuring effective intrusion detection and prevention systems is one way to detect and respond quickly to attempted infiltration by Noodle RAT or similar threats.
- User Education and Awareness Programs: Raising users' awareness of the potential dangers of social engineering tactics and phishing attacks can significantly lower the odds of successful backdoor installations.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https[:]//www.infosecurity-magazine.com/news/chinese-noodle-rat-backdoor/
- https[:]//www.trendmicro.com/en_us/research/24/f/noodle-rat-reviewing-the-new-backdoor-used-by-chinese-speaking-g.html?&web_view=true