NiceRAT Malware Targets South Korean Users via Cracked Software

Date: 18th June 2024 | Severity: Medium

Summary

Threat actors have been observed deploying a malware called NiceRAT to co-opt infected devices into a botnet. The attacks, which target South Korean users, are designed to propagate the malware under the guise of cracked software, such as Microsoft Windows, or tools that purport to offer license verification for Microsoft Office.

Attack Vectors

- NiceRAT is an actively developed open-source RAT and stealer malware written in Python that uses a Discord Webhook for command-and-control (C2), allowing the threat actors to siphon sensitive information from the compromised host.
- Due to the nature of crack programs, information sharing amongst ordinary users contributes to the malware's distribution independently from the initial distributor," the AhnLab Security Intelligence Center (ASEC) said.
- "Because threat actors typically explain ways to remove anti-malware programs during the distribution phase, it is difficult to detect the distributed malware."
- Alternate distribution vectors involve the use of a botnet comprising zombie computers that are infiltrated by a remote access trojan (RAT) known as NanoCore RAT, mirroring prior activity that leveraged the Nitol DDoS malware for propagating another malware dubbed Amadey Bot.
- First released on April 17, 2024, the current version of the program is 1.1.0. It's also available as a premium version, according to its developer, suggesting that it's advertised under the malware-as-a-service (MaaS) model.
- The development comes amid the return of a cryptocurrency mining botnet referred to as Bondnet, which has been detected using the high-performance miner bots as C2 servers since 2023 by configuring a reverse proxy using a modified version of a legitimate tool called Fast Reverse Proxy (FRP).

Indicator of compromise

INDICATOR TYPE	INDICATORS
C&Cs	• Hxxps[:]//discord[.]com/api/webhooks/1242723656166146119/stYCi_haHIy8MpHXGkrMX0f_bp4-yAEIlnWaINtua0M_sgvcXVRXo77MzCFOIPUe8xT7 • gandigod.ddns[.]net:8080
Filehash	• 16014adaf287779265e33c698287046a • 4b44c4b3ab34a7946987fe7a601de5d6 • 8cf502f9a053a7f65dc83651c21ea9de • 06e5bcc514f78794ba83779ea4c30841 • 00287b8dfdc58c4b413a29042e32d86b • 99df897a57e5d7dc8ecd11b73ee24726 • ba34c7a913b0fa18e434d6a96d612a2c • 6fcdf8ef4c409addf1ebf785440f32ee • 691f894f028994a2553b2438ea011c34 • fb5b169d0844dd9b6228599f313cf983 • 76e232928e26a1929efe0302cce1cc88 • cfb73473df35a1fd6c3cd70d09ec8be3 • 0ff5ecbe655b0b5781700195d2e8475e • df9ef2b14a8d4e5ddf8ac1e03909e0a4 • 2800ebfde7f0a94f00494fc72a3f8149 • 28f08aa165f19b2efb9254f223512dee • c5e49e44495d09a523173e9656a496fc • d94d7d20f2c88aaf8f84f6e771878fa7 • 061ea0f42ce0a6840c692f6ee36578af • a62bfe438f822cf369e434528325ed74 • 58678eb1df7e8bf574e67573a2beddaa • 7b4fe1a72a25163098827e9def8f497e • fc1333bdce23896e343f0fe6e9a30db8 • 20e2e1c6900aacb6ba529d148545c283

Recommendation

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Avoid Cracked Software: Refrain from downloading or using cracked software, especially if it claims to activate Microsoft Windows or Office. These programs are often used as a disguise to propagate NiceRAT.
- Use Legitimate Software Sources: Obtain software only from official sources or authorized distributors. Avoid third-party websites or torrents that offer cracked versions.
- Install Security Software: Use reputable antivirus and anti-malware software. Regularly update and scan your system to detect and remove any malicious programs.
- Keep Software Updated: Ensure that your operating system, applications, and security software are up to date. Patches and updates often address vulnerabilities exploited by malware.
- Monitor Network Traffic: Monitor network traffic for unusual or suspicious activity. Look for communication with Discord webhooks, which NiceRAT uses for command and control (C2) purposes.
- Implement Network Segmentation: Segment your network to limit lateral movement in case of an infection. Isolate critical systems from less critical ones.

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://thehackernews.com/2024/06/nicerat-malware-targets-south-korean.html
- https://cybersecuritynews.com/nicerat-malware-botnet-attack/
- https://asec.ahnlab.com/en/66790/