مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Malware Campaign- Nood RAT (Gh0st RAT) targeting Linux distributions

Tracking #:432315651

Date:26-02-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that the Nood RAT (Gh0st RAT's Variant) Targeting Linux Systems.

TECHNICAL DETAILS:

A new variant of Gh0st RAT, known as Nood RAT, has been observed targeting Linux systems alongside its traditional focus on Windows platforms. This variant exhibits similar functionality to other RATs, allowing attackers to execute commands remotely, upload and download files, and establish proxies. It was first identified in 2018 and the malware leverages the open-source code of Gh0st RAT for malicious purposes. In the past, the discovery of Nood RAT was linked to exploit attempts against WebLogic servers (CVE-2017-10271) and its utilization by the Rocke group to deploy CoinMiners. Furthermore, it played a role in the Cloud Snooper APT campaign, highlighting its utility in complex attack scenarios.

Nood RAT is created using a builder program called "NoodMaker.exe." This program facilitates the creation of executables compatible with different system architectures, such as x86 or x64. This versatility ensures compatibility with a wide range of targeted systems.

Nood RAT builder (A Linux version of Gh0st RAT)

A key feature of Nood RAT is its ability to disguise itself as legitimate processes. It achieves this by using the RC4 algorithm to encrypt both process names and configuration data, employing unique strings as keys. Upon initialization, the malware relocates to a temporary directory to further conceal its presence. Encrypted configuration data includes command and control (C2) server addresses, activation schedules, and communication intervals – measures designed to evade detection. Initial communication with the C2 server transmits encrypted system information, using time-based keys to bypass packet inspection.

Nood RAT supports various functionalities like remote shell access, file management, proxying, and port forwarding. These capabilities enable comprehensive system control, data exfiltration, and facilitating lateral movement within compromised networks.

INDICATORS OF COMPROMISE(IoCs):

- Attached in Excel File

RECOMMENDATIONS:

- 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 behaviour.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings (e.g. IOCs, TTPs...etc).

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://asec.ahnlab.com/en/62144/