AL2023_64 New SprySOCKS malware targets Linux devices in recent Cyber Espionage attacks (September 21, 2023)

Description

A new Linux backdoor called 'SprySOCKS' has raised significant concerns. This sophisticated malware is believed to be the work of a Chinese espionage-focused hacker group known as Earth Lusca. With its origins traced to the Trochilus open-source Windows malware, SprySOCKS showcases an alarming fusion of functionalities from different malware strains. Notably, it targets government agencies in multiple countries, posing a substantial risk to national security and sensitive data.

Details

SprySOCKS exhibits characteristics of multiple malware strains. Its command-and-control server (C2) communication protocol resembles that of RedLeaves, a Windows-based backdoor. The implementation of its interactive shell component appears to be derived from Derusbi, a Linux malware.

The SprySOCKS loader is a variant of the Linux ELF injector named mandibule. The attackers adapted mandibule for their purposes, but traces of debugging messages and symbols were left behind. It arrives on targeted systems in the form of a file named ‘libmonitor.so.2’.

To evade detection, the SprySOCKS loader runs under the process name ‘kworker/0:22’, mimicking the Linux kernel worker thread process. It decrypts the second-stage payload (SprySOCKS) and establishes persistence on the compromised computer. Once inside a compromised network, Earth Lusca deploys Cobalt Strike beacons, providing the attackers with remote access. The attackers use these beacons to spread laterally within the network, exfiltrate files, steal account credentials, and introduce additional payloads, including ShadowPad.

SprySOCKS generates a unique client ID (victim number) using the MAC address of the first listed network interface and some CPU features. This ID is then converted into a 28-byte hexadecimal string.

Some of SprySOCKS capabilities and key functionalities are listed below:

- SprySOCKS employs a high-performance networking framework called ‘HP-Socket’ for its operations.

- Its TCP communications with the C2 server are encrypted using AES-ECB encryption.
- SprySOCKS collects system information, such as OS details, memory, IP address, group name, language, and CPU.
- The malware utilizes an interactive shell that uses the PTY subsystem. (A pseudoterminal (abbreviated "pty") is a pair of virtual character devices that provide a bidirectional communication channel, where one end of the channel is called the master, and the other end is called the slave.)
- SprySOCKS can detect and list network connections.
- It manages SOCKS proxy configurations.
- SprySOCKS can perform basic file operations, including uploading, downloading, listing, deleting, renaming, and creating directories.

Indicators of Compromise

Please see the link for a list of IOCs including domains, IP addresses and email addresses associated with this malicious campaign: https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/i/earth-lusca-employs-new-linux-backdoor/ioc-earth-lusca-employs-new-linux-backdoor.txt

Remediation

To protect yourself against SprySOCKS, it is recommended to practice proper cyber security hygiene when navigating the internet. Here are some tips to consider:

1. **Apply Security Updates**: The top priority should be to apply security updates promptly, especially for public-facing server products. This can prevent initial compromises, for known vulnerabilities.
2. **Enhance Network Securit**y: Implement robust network security measures, including intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect and block malicious activities.
3. **Endpoint Protection:** Employ advanced endpoint protection solutions to detect and mitigate SprySOCKS and other malware threats at the device level.
4. **User Training:** Educate employees and users about phishing threats and the importance of not clicking on suspicious links or downloading unknown attachments.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (2023, September 19). *Earth Lusca's new SprySOCKS Linux backdoor targets government entities*. https://thehackernews.com/2023/09/earth-luscas-new-sprysocks-linux.html
- Toulas, B. (2023, September 18). New SprySOCKS Linux malware used in cyber espionage attacks. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/new-sprysocks-linux-malware-used-in-cyber-espionage-attacks/