AL2024_40 GhostSpider Malware Analysis (29th November 2024)

Description

GhostSpider is a sophisticated backdoor malware employed by the Salt Typhoon hacking group, also known as Earth Estries or UNC2286. This group has been linked to cyber-espionage campaigns targeting critical infrastructure, telecommunications, and government organizations worldwide. GhostSpider operates as a modular backdoor designed for stealthy, long-term espionage.

Attack Details

GhostSpider gains access to target systems through exploits of known vulnerabilities in public-facing software like VPNs, firewalls, and mail servers. The malware employs DLL hijacking and is loaded as a service via legitimate tools such as *regsvr32.exe*. It uses encrypted communication over HTTPS to connect with its command-and-control (C2) servers, blending malicious traffic with legitimate activity.

The malware supports a variety of commands, including:

- **Upload**: Load and execute malicious modules.
- **Normal**: Perform core functions such as data exfiltration or system monitoring.
- **Close**: Remove active modules from memory.
- **Update**: Modify communication behaviors to evade detection.
- **Heartbeat**: Maintain communication with C2 servers.

GhostSpider's architecture allows attackers to adapt their tactics depending on the victim's defenses and network configurations.

Remediation

- **Patch Management:** Apply all security updates for VPNs, firewalls, and email servers promptly to mitigate exploitation of known vulnerabilities.
- **Endpoint Protection:** Deploy robust endpoint detection and response (EDR) tools to monitor and detect abnormal behaviors such as DLL hijacking and unauthorized memory access.
- **Network Monitoring:** Implement deep packet inspection (DPI) and traffic analysis to detect encrypted C2 communications.

- **Threat Intelligence:** Stay updated with IOCs and threat intelligence reports to adapt defenses proactively.
- **Incident Response:** Prepare for immediate containment by isolating affected systems and conducting memory forensics to identify and neutralize active modules.

GhostSpider represents a significant threat, underscoring the importance of proactive defenses and collaborative threat intelligence sharing to counter advanced persistent threats (APTs).

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

References

- Lakshmanan, R. (2024, November 24). Chinese Hackers Use GHOSTSPIDER Malware to Hack Telecoms Across 12+ Countries. Retrieved from The Hacker's News. https://thehackernews.com/2024/11/chinese-hackers-use-ghostspider-malware.html
- Toulas, B. (2024, November 25). Salt Typhoon hackers backdoor telcos with new GhostSpider malware. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/salt-typhoon-hackers-backdoor-telcos-with-new-ghostspider-malware/