SECURITY ADVISORY

CYBER STASH

May, 2023

Multiple CVEs

Snake Implant Malware

Context

The Snake implant is considered the most sophisticated cyber espionage tool designed and used by Center 16 of Russia's Federal Security Service (FSB) for long-term intelligence collection on sensitive targets. Globally, the FSB has used Snake to collect sensitive intelligence from high priority targets, such as government networks, research facilities, and journalists.

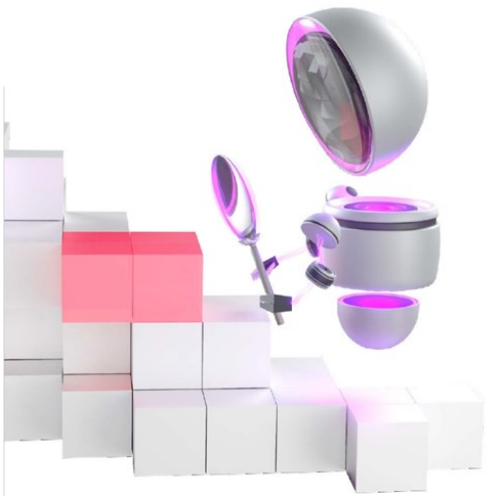
As one example, FSB actors used Snake to access and exfiltrate sensitive international relations documents, as well as other diplomatic communications, from a victim in a NATO country. Within the United States, the FSB has victimized industries including education, small businesses, and media organizations, as well as critical infrastructure sectors including government facilities, financial services, critical manufacturing, and communications.

Mitigation

Patch software: To prevent BellaCiao malware, regularly update your software and systems with the latest security patches. Give special attention to vulnerable apps that are exposed to the Internet.

Implement application controls: Establish strict controls for how each application interacts with its environment and the internet. Limit access and permissions to prevent unauthorized actions or communications that may compromise the software's security.

Block communication: Implement restrictions on communication with high-risk countries, Autonomous System Numbers (ASNs), Top-Level Domains (TLDs), and Threat Intelligence Data.



Conduct threat hunting using memory analysis: Capturing and analyzing the system's memory is an effective approach for detecting Snake malware. By bypassing many of Snake's hiding techniques, memory analysis provides a clearer view of its presence.

Technical Details

Tactics, Techniques and Procedures

The notable TTPs related to the Snake Implant Malware:

TA0005 - Advanced Evasion Techniques:

Snake Malware employs advanced evasion techniques to bypass traditional security measures. This includes the use of polymorphic code, rootkit functionality, and encryption to obfuscate its presence and avoid detection.

TA0043 - Network Reconnaissance:

Snake Malware actively scans the infected network to conduct network reconnaissance. It gathers information about the network architecture, system configurations, and user credentials to identify potential targets and facilitate lateral movement.

T1219 - Remote Access and Control:

Once infiltrated, Snake Malware establishes remote access capabilities, enabling attackers to gain unauthorized control over compromised systems. This TTP allows for unauthorized data access, system manipulation, or further propagation within the network.

TA0010 - Data Exfiltration:

Snake Malware possesses the ability to exfiltrate sensitive data from compromised systems. This includes the theft of login credentials, intellectual property, or financial information. The exfiltrated data is typically transferred to external servers controlled by the attackers, potentially leading to data breaches and financial loss.

Threat Intelligence

Operations involving Snake have been conducted from FSB facilities located in Ryazan, Russia. It has been observed that Snake activity tends to increase during FSB working hours in Ryazan, which are typically from approximately 7:00 AM to 8:00 PM, Moscow Standard Time (GMT+3). The development of Snake has primarily been carried out by FSB officers based in Ryazan, who are identifiable by the monikers included in the code of certain Snake versions. Although Snake's development and re-tooling have historically been handled by Ryazan-based FSB officers, there have also been instances where Snake operations were initiated from a building occupied by FSB Center 16 in Moscow. Investigations have revealed that while some FSB operators demonstrate a thorough understanding and utilization of Snake's advanced capabilities, others appear to be less familiar with them. These findings highlight the challenges associated with effectively deploying such a sophisticated toolset across geographically dispersed teams within FSB Center 16.

References

YARA Detection Rule

https://gist.github.com/msuiche/8c8fd278430dda0292b4cfdfc549ca2d

Public Intelligence

https://www.cyber.gov.au/about-us/advisories/hunting-russian-intelligence-snake-malware

https://socprime.com/blog/snake-malware-detection-cyber-espionage-implant-leveraged-by-russia-affiliated-turla-apt-in-a-long-lasting-campaign-against-nato-countries/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3389044/us-agencies-and-allies-partner-to-identify-russian-snake-malware-infrastructure/

https://atos.net/en/lp/snake-malware

https://www.hivepro.com/wp-content/uploads/2023/05/Snake-a-Stealthy-Cyber-Espionage-Malware_TA2023221.pdf