AL2022_38 Symbiote Linux Malware targeting Latin America Financial Sector (10th June 2022)

Description

Symbiote, a recently found Linux malware, infects all running processes on infected computers, harvests account credentials, and provides backdoor access to its operators.

Summary

Symbiote's creators are thought to have started working on the virus in November 2021, with the threat actor primarily targeting the Latin American financial sector, including banks like Banco do Brasil and Caixa, based on the domain names used.

The malware functions as a system-wide parasite after injecting itself into all operating processes, leaving no visible evidence of infection even during painstaking in-depth inspections.

How it works

Instead of being an executable, Symbiote is a shared object (SO) library that is loaded into running processes using the LD PRELOAD command to take precedence over other SOs. Symbiote can hook the "libc" and "libpcap" routines and conduct different activities to hide its presence, such as hiding parasitic processes, hiding malware files, and so on, because it is the first to be loaded.

The malware can choose which results it presents when it injects itself into processes. Symbiote will insert itself into the inspection software's process and utilize BPF hooking to filter out results that will show its activity if an administrator launches a packet capture on the infected machine to analyze some suspicious network traffic. Symbiote scrapes connection entries it wants to hide, performs packet filtering using BPF, and eliminates UDP traffic to domain names in its list to disguise its malicious network activities on the compromised machine.

By hooking the "libc read" function, this stealthy new virus is primarily used for automatic credential harvesting from infected Linux computers. When targeting Linux servers in high-value networks, this is a critical task because acquiring admin account credentials allows for unrestricted lateral movement and full access to the entire system. Symbiote also provides its operators with remote SSH access

to the computer via the PAM service, as well as a mechanism for the threat actor to get root privileges.

Remediation

Since the malware operates as a user-land level rootkit, detecting an infection may be difficult. Anomaly DNS requests can be detected using network telemetry, and security products like antivirus and intrusion detection systems should be statically linked to avoid being 'infected' by userland rootkits.

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

References

- Toulas, Bill. (9th June 2022). New Symbiote malware infects all running processes on Linux systems. Retrieved from Bleeping computer. https://www.bleepingcomputer.com/news/security/new-symbiote-malware-infects-all-running-processes-on-linux-systems/

- Lakshmanan, Ravie. (9th June 2022). Symbiote: A Stealthy Linux Malware Targeting Latin American Financial Sector. Retrieved from The Hacker News. https://thehackernews.com/2022/06/symbiote-stealthy-linux-malware.html