

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
  - [Cloud Security](#)
  - [Identity & Access](#)
  - [Data Protection](#)
  - [Network Security](#)
  - [Application Security](#)
- ▼ [Security Strategy](#)
  - [Risk Management](#)
  - [Security Architecture](#)
  - [Disaster Recovery](#)
  - [Training & Certification](#)
  - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Virus & Threats](#)



## Highly-Evasive Linux Malware 'Symbiote' Infects All Running Processes

By [Ionut Arghire](#) on June 10, 2022

Share

Tweet

推荐 0



Security researchers with BlackBerry and Intezer have shared details on a new Linux malware that “parasitically” infects all running processes on a target machine.

Once it has infected all running processes, the malware, which the researchers have named [Symbiote](#), provides attackers with rootkit capabilities, as well as with remote backdoor access and the ability to harvest credentials.

The malware, BlackBerry and Intezer discovered, can execute commands with the highest privileges possible on an infected machine.

“What makes Symbiote different from other Linux malware that we usually come across, is that it needs to infect other running processes to inflict damage on infected machines. Instead of being a standalone executable file that is run to infect a machine, it is a shared object (SO) library that is loaded into all running processes using LD\_PRELOAD, and parasitically infects the machine,” the researchers explain.

Initially observed in November 2021, targeting the financial sector in Latin America, Symbiote is highly evasive, being capable of hiding itself and other malware employed by its operators, thus making infections very hard to detect, the researchers say.

“Performing live forensics on an infected machine may not turn anything up since all the file, processes, and network artifacts are hidden by the malware,” they claim.

BlackBerry and Intezer also note that, because of Symbiote’s highly evasive nature, they were not able to determine whether the malware is being used in broad or targeted attacks.

The researchers discovered that Symbiote employs the Berkeley Packet Filter (BPF) hooking functionality to hide malicious network traffic - other malware too has used BPF for covert communication, including an advanced backdoor attributed to the Equation Group.

“When an administrator starts any packet capture tool on the infected machine, BPF bytecode is injected into the kernel that defines which packets should be captured. In this process, Symbiote adds its bytecode first so it can filter out network traffic that it doesn’t want the packet-capturing software to see,” the researchers explain.

The malware is loaded by the linker via the LD\_PRELOAD directive, before any other shared objects, which allows it to hijack the imports from other libraries that are being loaded. Thus, it hooks libc and libpcap functions to hide its presence.

Symbiote also monitors hooked functions being called and, based on whether the calling application is trying to access a file or folder under /proc, it scrubs the output from process/file names that are on an RC4 encrypted file list within its binary.

The malware uses three different methods to hide network activity, such as hooking specific functions so that it can exclude results from being delivered when an application tries to open /proc/net/tcp, hijacking injected packet filtering bytecode if an application attempts to use extended Berkeley Packet Filter (eBPF) - which is employed by the Linux kernel for packet filtering -, and hooking libpcap functions to filter out UDP traffic to domains on a specific list.

Symbiote appears created mainly to harvest credentials from the infected machines, an operation performed by hooking the libc read function. The malware stores the harvested credentials locally, but also exfiltrates them to a domain controlled by the threat actor.

To provide attackers with remote access to an infected system, the malware hooks a few Linux Pluggable Authentication Module (PAM) functions. It monitors authentication attempts to see if the provided password matches a hardcoded one, which returns a success response, thus allowing the attackers to authenticate to the machine via a service that uses PAM, including SSH. If the password is not a match, it saves and exfiltrates it.

Symbiote provides authenticated attackers with root privileges by checking the HTTP\_SETTHIS environment variable and changing the user and group ID to the root user if the variable is set with content. It “then clears the variable before executing the content via the system command,” the researchers explain.

The malware’s operators use domain names that impersonate major Brazilian banks, which suggests that either the banks or their customers are being targeted. Following these domain names, the security researchers were able to identify several Symbiote samples that the attackers uploaded to VirusTotal to test antivirus detection before using them in attacks.

Symbiote is not the first Linux malware to be designed for remote access and credential theft, but BlackBerry and Intezer did not find code similarities with previously observed threats (such as [Ebury/Windigo](#), an OpenSSH backdoor discovered in 2014).

**Related:** [How Linux Became the New Bullseye for Bad Guys](#)

**Related:** [Chinese Researchers Detail Linux Backdoor of NSA-Linked Equation Group](#)

**Related:** [Schneider Electric Warns Customers of Drovorub Linux Malware](#)