# New Symbiote malware is capable of infecting all processes running on Linux computers

Symbiote has the ability to infect all processes running on the compromised system to steal account credentials and other data.

A newly discovered Linux malware called Symbiote is posing a great threat to the user community. The reason is because Symbiote has the ability to infect all processes running on the compromised system to steal account credentials and other data and then send it back to its owner.

After infecting running processes, Symbiote acts as a system-wide parasite, leaving no sign that the computer is infected. Even the most in-depth, meticulous inspection can't detect it.

Symbiote uses BPF (Berkeley Packet Filter) connectivity to monitor network packets and hide its own communication channels from security tools.

Security researchers from BlackBerry and Intezer Labs discovered the existence of Symbiote. They worked closely together to explore all aspects of this malicious code then published in a detailed technical report. According to them, Symbiote has been actively developing since last year.


## System-wide infection through shared objects

Often malicious code is spread through executable files. However, Symbiote is a shared object library (SO) that is loaded into running processes using the LD_PRELOAD directive to gain priority over other SOs.

As it is loaded first, Symbiote can connect to the functions "libc" and "libpcap" and perform various actions to mask its presence such as hiding parasitic processes, hiding files deployed with malware.

> *"As it infects itself with processes, the malicious code can choose which results it displays ,"* the researchers said. *"If the administrator starts collecting packets on the infected machine to investigate anomalous network traffic, Symbiote will feed itself into the test software's process and use BPF hooking to filter out the results." may reveal its activity" .*

To hide its malicious network activities, Symbiote deletes connection entries it wants to hide, performs packet filtering via BPF, and discards UDP traffic to domains on its list.

## Backdoor and data theft

Symbiote is mainly used to steal credentials from hacked Linux machines surreptitiously. When targeting the right Linux servers in large organizations, Symbiote will cause serious problems. If the administrator's password is stolen, the path of peer-to-peer infection will not be hindered and the hacker also has unlimited access to the entire system.

In addition, Symbiote provides the attacker with remote SHH access to the machine via the PAM service and provides a method for the attacker to gain root privileges on the system.

Symbiote targets financial entities in Latin America, impersonating banks and the Brazilian federal police.

Due to the sophisticated mode of infection, Symbiotes are difficult to detect. Therefore, administrators should pay more attention to network traffic. Network telemetry can be used to detect unusual DNS requests, and security tools such as anti-virus software and Endpoint Detection and Response (EDR) need to be statically linked to ensure they are not infected with malicious code.

Experts predict that in the near future, the number of malicious attacks with the ability to evade as well as Symbiote will increase significantly. Therefore, administrators and security engineers should prepare prevention and response plans.