AL2022_46 OrBit malware steals information from Linux devices. (20th July 2022)

Description

A newly discovered Linux malware is being used to steal information from backdoored Linux systems and has the potential of infecting all running processes.

Summary

This malware, named OrBit, hijacks shared libraries to intercept function calls by modifying the LD_PRELOAD environment variable on compromised devices.

How it Works

When the malicious software is installed, it immediately begins infecting all processes running on the device, including any new processes that are launched. The malware employs advanced evasion techniques and gains persistence on the machines by hooking key functions. It also grants threat actors remote access via SSH (Secure Socket Shell), harvests credentials, and logs TTY (teletypewriter) commands. The malware loads the dangerous library in one of two ways.

The first method is to include the shared object in the loader's configuration file.

The second method entails modifying the loader's binary file so that when it is invoked, it loads the malicious shared object.

Remediation

Anti-malware vendors have updated their products to detect this malware. A list of these vendors along with the malware detection names can be found at the following URL: https://www.virustotal.com/gui/file/f1612924814ac73339f777b48b0de28b716d606e142d4d3f4308ec648e3f56c8

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

References

- Brown, E. (2022, July 8). *New Malware Called OrBit Has Been Infecting, Stealing Data From Linux Devices*. Retrieved from iTech Post.

https://www.itechpost.com/articles/111931/20220708/new-malware-called-orbit-infecting-stealing-data-linux-devices.htm

- Gatlan, S. (2022, July 7). *New stealthy OrBit malware steals data from Linux devices*. Retrieved from BleepingComputer https://www.bleepingcomputer.com/news/linux/new-stealthy-orbit-malware-steals-data-from-linux-devices/

- Lakshmanan, R. (2022, July 7). *Researchers Warn of New OrBit Linux Malware That Hijacks Execution Flow*. Retrieved from The Hacker News. https://thehackernews.com/2022/07/researchers-warn-of-new-orbit-linux.html