Orbit

Threat: **Backdoor**

Author: **Jeffrey Farnan** Date Originally Published: **July 29th, 2022**

1. SUMMARY

- A recently identified Linux malware is being used to secretly access backdoor Linux computers, steal information, and infect all running processes. To remain persistent on the infected systems, the malware employs cutting-edge evasion strategies and hooks crucial functions. OrBit collects passwords, logs TTY commands, and enables operators to gain remote access capabilities via SSH.

2. MALWARE FAMILY

- **Type** = Backdoor.
- **Sub-type** = Spyware.

- **Backdoor:** A backdoor is a vulnerability in a Linux machine or software that allows otherwise unauthorized users to gain access to the system.
- **Spyware:** Spyware is a form of malware that hides on your Linux machine, monitors your activity, and steals sensitive information such as bank details and passwords.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Unknown.
- **First seen date/period** = June / July 2022.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** =July 20th, 2022.

4. MALWARE HISTORY

- Linux is a popular operating system for servers and cloud infrastructure, which makes it a tempting target for cyber criminals. Nowadays, malware that is designed to infect Linux computers has been steadily expanding and becoming more sophisticated.

- OrBit is a new malware that surfaced recently but uses new capabilities that make it almost impossible to detect. Dubbed OrBit by the security researchers who first spotted it. The malware's name comes from the filenames it uses to temporarily store the output of executed commands ("/tmp/.orbit").
- OrBit is the fourth Linux malware to have come to light in a short span of three months, having similar capabilities and functions with other recently discovered Linux malware. Symbiote malware which is also designed to infect all of the running processes on the compromised machines. A Linux backdoor called BPfDoor also uses hooking functionality to monitor and manipulate network traffic hiding their communication channels.

5. MALWARE DESCRIPTION

- OrBit is a new and growing trend of malware attack geared towards the Linux operating system. It can be either installed with persistence capabilities or as a volatile implant. This malware has many capabilities and functions:
    - This malware implements advanced evasion techniques.
    - Gains persistence on the machine by hooking key functions.
    - Provides the threat actors with remote access capabilities over SSH (Secure Socket Shell).
    - Harvest credentials and logs TTY (teletypewriter) commands.
    - It infects running processes on the machine, including new ones.
- **Goal:** The ultimate goal of this malware is to steal information. It does this by hooking read and write functions to capture data that's' being written by the executed processes on the machine.
- **Installation:** OrBit is known to have different ways to gain access to the targeted system. It receives command line arguments and based on them it extracts the payload to one of the locations. Using these command line arguments the installation path can be swapped and the content of the payload can be updated or entirely uninstalled. Orbit gets installed via an ELF dropper which installs the payload but also prepares the environment for the malware's execution.
- **Execution:** Once the malware is installed it will infect all of the running processes, including new processes running on the machine. Other threats hijack shared libraries by modifying the environment variable _ LD_PRELOAD, this malware uses 2 different ways to load the malicious library. The first way is by adding the shared object to the configuration file that is used by the loader. The second way is by patching the binary of the loader itself so it will load the malicious shared object.
- **Stealth:** Orbit uses XOR encrypted strings and steals passwords. The malware stores the stolen data on the device itself, which means that security tools don't detect the leakage to the hacker's server. Stores the stolen information in specific files on the machine.
- **Persistence**: OrBit relies on a barrage of methods which allow it to function without alerting its presence and establish persistence. It can hook different libraries to avoid detection, maintain persistence by infection new processes, control process behaviour and mask network activity. This makes it difficult to remove from infected machines. After gaining persistence, the malware provides the attackers with an SSH backdoor to the system, allowing them to gain remote access, steal credentials, and log TTY commands. Since Linux is the most commonly used OS for servers, the malware poses a significant risk to enterprises.

6. POTENTIAL CUSTOMER DEFENSE

- Security tools are failing to keep up with this evolving threat targeting Linux machines. OrBit's dropper and payload are completely undetected by antivirus engines when the malware was first spotted, some anti-malware vendors have since updated their products to warn customers of its presence.
- Some remediation actions can be taken:
    - Regularly update your security software.
    - Backup and protect important data.
    - Restrict user access.
    - Have a policy for securing passwords.
    - Examine event logs frequently to spot odd behavior.
    - Conduct penetration tests and vulnerability assessments.
    - Inform your employees of the dangers and risks posed by this type of malware.

Research Sources:

- https://cybersrcc.com/2022/07/15/orbit-undetected-linux-malware/
- https://thehackernews.com/2022/07/researchers-warn-of-new-orbit-linux.html
- https://securityaffairs.co/wordpress/132966/hacking/orbit-linux-malware.html
- https://threatpost.com/sneaky-malware-backdoors-linux/180158/
- https://cyware.com/news/orbit-a-new-highly-evasive-linux-malware-a4ec6237/?web_view=true
- https://cybersecuritynews.com/orbit-undetected-linux-malware/
- https://www.bleepingcomputer.com/news/linux/new-stealthy-orbit-malware-steals-data-from-linux-devices/

Disclaimer: All opinions expressed in this article are the opinions solely of the author.