Malware Targeting Linux Systems

The Critical Start Cyber Threat Intelligence Team is aware of and monitoring a trend in malware being developed to specifically target Linux systems. Targeting of Linux systems has been relatively scarce and primitive in comparison to other proprietary operating systems. Organizations currently use Linux operating systems and servers for critical areas including cloud services such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms within businesses. Threat actors targeting Linux systems pose a significant risk as roughly 78% of websites are powered by Linux.

New malware observed in the wild includes Mélofée malware and Cylance ransomware. Mélofée is a new malware family recently discovered being used by the Chinese state-sponsored hacking groups Winnti APT, and Earth Berberoka, targeting Linux servers. There are three different samples of the malware being circulated. All three versions of the malware share a common code base that uses shell commands to download the rootkit and the main implant from an attacker-controlled server. However, their communication protocols and encryption methods are still in development. The malware enables threat actors to establish a connection to a remote server, receive commands to carry out different operations, launch a shell, create sockets, and execute arbitrary commands.

Cylance, a new ransomware, has been updated with a Power-Packed CommandLine Options that targets both Windows and Linux Operating System Users. The ransomware can accept different command line parameters and can adjust to customized encryption tactics. The Linux variant is executed manually by the threat actor calling out targeted folders in the command lines. Once the folder and subfolders are encrypted, a ransom note is placed within the folder. Additionally, Cylance ransomware provides the threat actor with escalated privileges enabling debugging processes, modifying system security settings, and restoring files and directories.

Threat actors will continue to modify or develop new malware to specifically target Linux systems as they are viewed as a prime target due to being used for critical areas of business. Organizations should be aware of this shift in targeting Linux systems and establish or update security best practices. Additionally, companies should educate their IT departments on the increased risk of Linux systems being targeted to heighten vigilance and mitigate potential threats.

For more information, please refer to TLP WHITE // [CS-TR-23-0305] Malware Targeting Linux Operating Systems.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://blog.cyble.com/2023/04/07/new-cylance-ransomware-with-power-packed-commandline-options/