Released: Decryptor for Cl0p ransomware’s Linux variant

helpnetsecurity.com/2023/02/07/cl0p-ransomware-decryptor-linux/

February 7, 2023

Flawed encryption logic used in Cl0p (Clop) ransomware’s Linux (ELF) variant has allowed SentinelOne researchers to create and release a free decryptor.

“The [Cl0p] Windows variant encrypts the generated RC4 key responsible for the file encryption using the asymmetric algorithm RSA and a public key. In the Linux variant, the generated RC4 key is encrypted with a RC4 [hardcoded] ‘master-key’,” the researchers explained.

The differences between Windows and Linux variants

The Linux Cl0p variant is relatively new, and was first spotted by the researchers in late December 2022.

“It appears to be in its initial development phases as some functionalities present in the Windows versions do not currently exist in this new Linux version,” they noted.

“A reason for this could be that the threat actor has not needed to dedicate time and resources to improve obfuscation or evasiveness due to the fact that it is currently undetected by all 64 security engines on VirusTotal.”

The differences between the Windows and Linux variant are many. For example, the former avoids encrypting specific folders, files and files with specific extenstions, and the latter does not. The former can be executed with different parameters to guide which drives will be targeted for encryption, while the latter is focused on encrypting just the specified hardcoded folders. The former carries an encrypted ransom note that gets encrypted, but the former stores the note as plain text.

But the most consequential difference – from the victims' perspective, that is – is the flaw that made possible the creation of the decryptor.

"Over the last twelve months or so we have continued to observe the increased targeting of multiple platforms by individual ransomware operators or variants," the researchers noted.

"While the Linux-flavored variation of Cl0p is, at this time, in its infancy, its development and the almost ubiquitous use of Linux in servers and cloud workloads suggests that defenders should expect to see more Linux-targeted ransomware campaigns going forward."

It is to be expected that Cl0p ransomware developers will fix the vulnerability soon. In the meantime, victims can use the decryption tool and look into better protecting their systems against ransomware attacks in general.