New LockBit Ransomware Encryptor Targets macOS

Russian-based ransomware group LockBit continues to expand its arsenal with the addition of a new variant specifically targeting macOS. Cybersecurity researcher MalwareHunterTeam discovered a ZIP (.zip file) archive on VirusTotal containing various available LockBit encryptors. Besides previously known variants targeting Windows, Linux, and VMware ESXI servers, there were several encryptors discovered for macOS, ARM, FreeBSD, MIPS, and SPARC CPUs. Samples collected indicate these new encryptors have been around since at least November 2022. Currently, the new macOS ransomware variant is not signed with a trusted certificate preventing it from being run. The base code was taken from the other variants and has yet to be updated for the mac environment with multiple references to VMware ESXi and extensions and filenames that are distinctly Windows related. The coding issues coupled with a lack of a trusted signature suggest that these variants are not yet fully operational.

For more information on the variants of LockBit ransomware please reference [CS-SU-23-0202] Situation Update – LockBit Announces New Variant

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://twitter.com/malwrhunterteam/status/1647384505550876675
2. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-encryptors-found-targeting-mac-devices/