CRITICALSTART®

Situation Update – LockBit Announces New Variant

Summary

Russian-based ransomware group LockBit continues to expand its arsenal with the addition of a new variant, LockBit Green. The acquisition of Green comes less than a year after the deployment of LockBit Black. Threat researchers at SentinelOne indicated a large portion of this variant overlaps with the Conti ransomware version whose source code was leaked last year. LockBit is expected to continue to dominate the ransomware arena as the operators make strides to increase its capabilities and versatility.

Details

LockBit ransomware group operates under a Ransomware-as-a-Service (RaaS) model leveraging double, and sometimes triple, extortion techniques. Historically, they have targeted organizations opportunistically, working with initial access brokers to save time and allow for a larger profit potential. It's estimated LockBit had nearly 1100 victims in 2022 alone. Unlike other ransomware groups that prioritize highly impactful, high-profile, or critical national infrastructure (CNI) targets, Lockbit routinely focuses on small and medium-sized businesses.

Originally observed in September 2019 as LockBit (a.k.a. ABCD Ransomware), operators continue to push limits in developing new and novel variants, boasting at least three different color options in addition to a Linux/ESXi alternative as of early 2023. Notably version 2.0, 3.0, and Green have emerged in less than a two-year span of time. It's assessed that the adaptation and use of leaked source code from reputable competitors have increased the speed of the development lifecycle, allowing for this increased pace of improvement and implementation.

LockBit currently advertises the following to their affiliates:

- LockBit **Red:** a.k.a. LockBit 2.0; released June 2021
- LockBit **Black:** a.k.a. LockBit 3.0; released May 2022 with code heavily borrowed from BlackMatter
- LockBit **Green:** announced February 2023 with majority of code taken from leaked Conti source code
- Linux/ESXi: released October 2021; uses a combination of AES and ECC (Curve25519) for encryption
- StealBit: information stealer developed to support affiliates, acts as a file grabber and dumps/uploads victim data to the LockBit victim-shaming site

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the evolution of LockBit variants 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 updates via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

https://securityaffairs.com/141666/cyber-crime/lockbit-green-ransomware-variant.html
https://unit42.paloaltonetworks.com/lockbit-2-ransomware/
http://gbhackers.com/new-lockbit-linux-esxi-locker-ransomware/
https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/