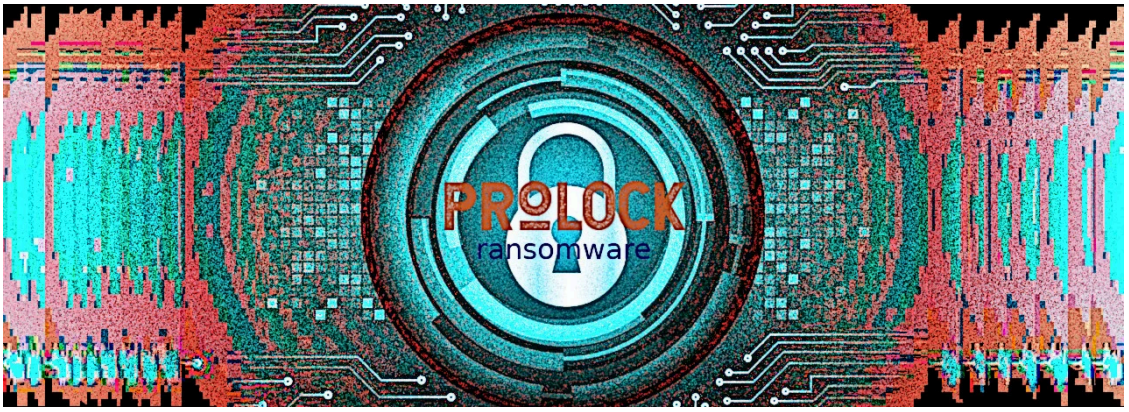
FBI warns of ProLock ransomware decryptor not working properly

By Ionut Ilascu

Published: 2020-05-18 · Archived: 2026-04-05 14:25:19 UTC



Multiple actors in the ransomware business saw the new coronavirus pandemic as the perfect opportunity to focus on an already overburdened healthcare sector. ProLock is yet another threat to the list.

The FBI issued a flash alert at the beginning of the month to alert organizations of the new threat actor, saying that its targets in the US include entities in the following sectors: healthcare, government, financial, and retail.

Decryptor malfunction

The FBI does not encourage giving in to the demands of any ransomware actor. Doing so would only increase their confidence to continue such attacks.


DIE LINKE.
0:00

With ProLock, the decryptor is not working properly and data will be lost. Files larger than 64MB may become corrupted during the decryption process.

Integrity loss of 1 byte per 1KB is possible with files over 100MB and additional work may be needed to make the decryptor work properly. This issue will increase the downtime of an organization even they agree to the actor's demands.

The malware started as PwndLocker in late 2019 but made a reputation by targeting businesses and local governments, adjusting its ransom demands to the size of the compromised network.

After fixing a bug that allowed free decryption, PwndLocker emerged as ProLocker in March and its activity started to escalate.

Getting in the network

As cybersecurity company Group-IB points out in a recent report, ProLock has partnered with QakBot banking trojan to obtain access to victims' networks; this likely contributed to this ransomware's ascension.

The trojan does not install this ransomware family but runs a set of scripts to let its operators on the victim network so they can map it and move laterally. The payload is extracted from a BMP or JPG file named WinMgr, and is loaded into memory.

Like other ransomware operators, ProLock's spend some time on the victim network looking for high-value systems and important data to steal. The information is siphoned out using the Rclone a command-line tool for syncing with various cloud storage services.

The ransom demand following the encryption comes with the threat that victim data would be released on public websites and social media unless payment for decryption is not received.

Other methods include misconfigured remote desktop protocol (RDP). For networks with single-factor authentication, the actor uses stolen logins.

Once inside, ProLock operators make sure that they leave no option for recovering the files without paying. If backups and volume shadow copies are found, they are either deleted or encrypted.

With ransom demands between $175,000 to over $660,000, ProLock is as serious a threat as other, more infamous ransomware families like Maze, Sodinokibi, Ryuk, or LockerGoga, which are considered top earners in the ransomware business.
