FBI issues second alert about ProLock ransomware stealing data

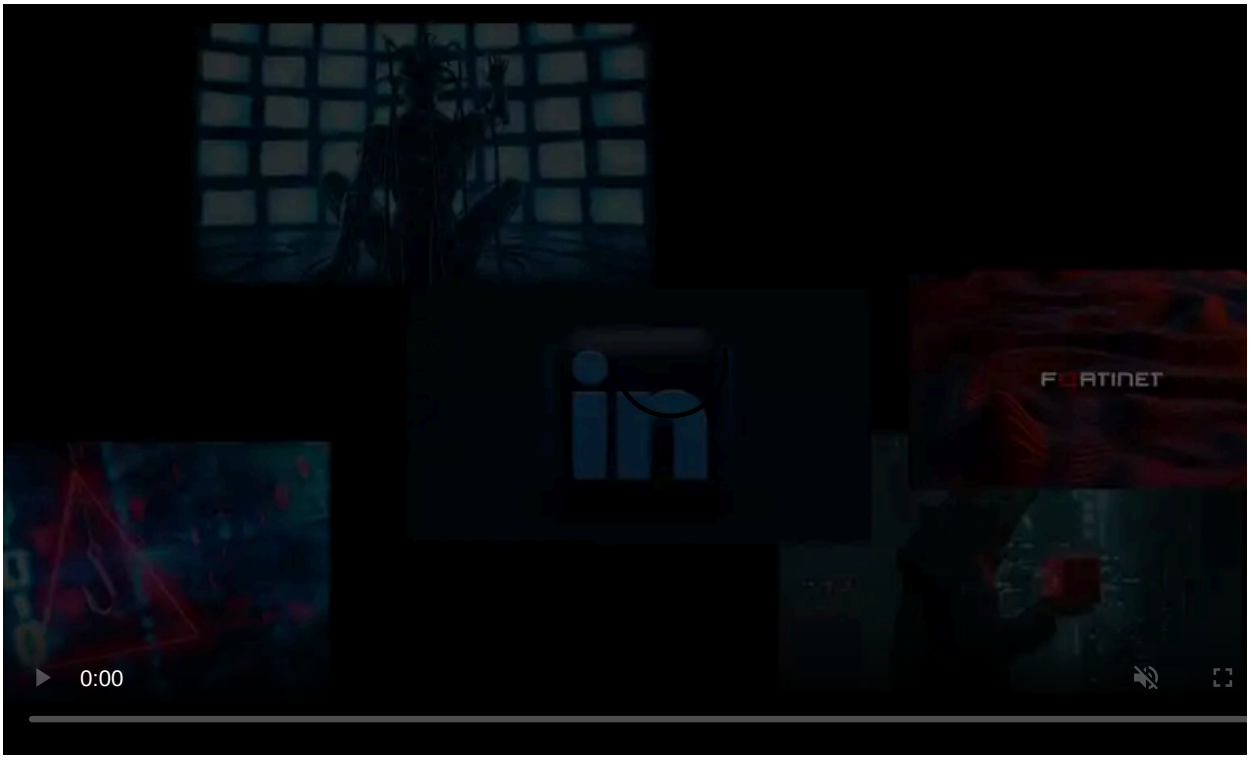
By Sergiu Gatlan

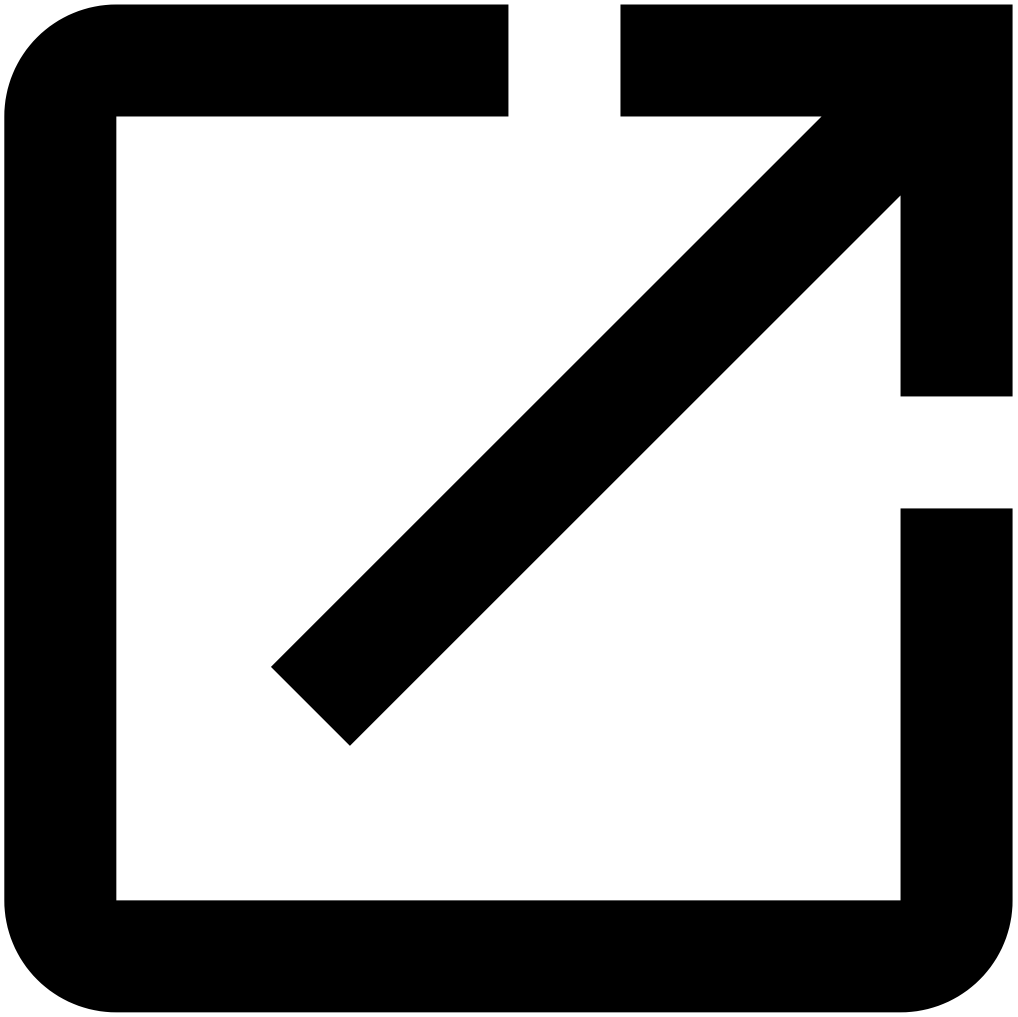
Published: 2020-09-04 · Archived: 2026-04-05 20:21:57 UTC

Image: Kushagra Kevat

The FBI issued a second warning this week to alert US companies of ProLock ransomware operators stealing data from compromised networks before encrypting their victims' systems.

The 20200901-001 Private Industry Notification seen by BleepingComputer on September 1st comes after the MI-000125-MW Flash Alert on the same subject issued by the FBI four months ago, on May 4th, 2020.


0:00

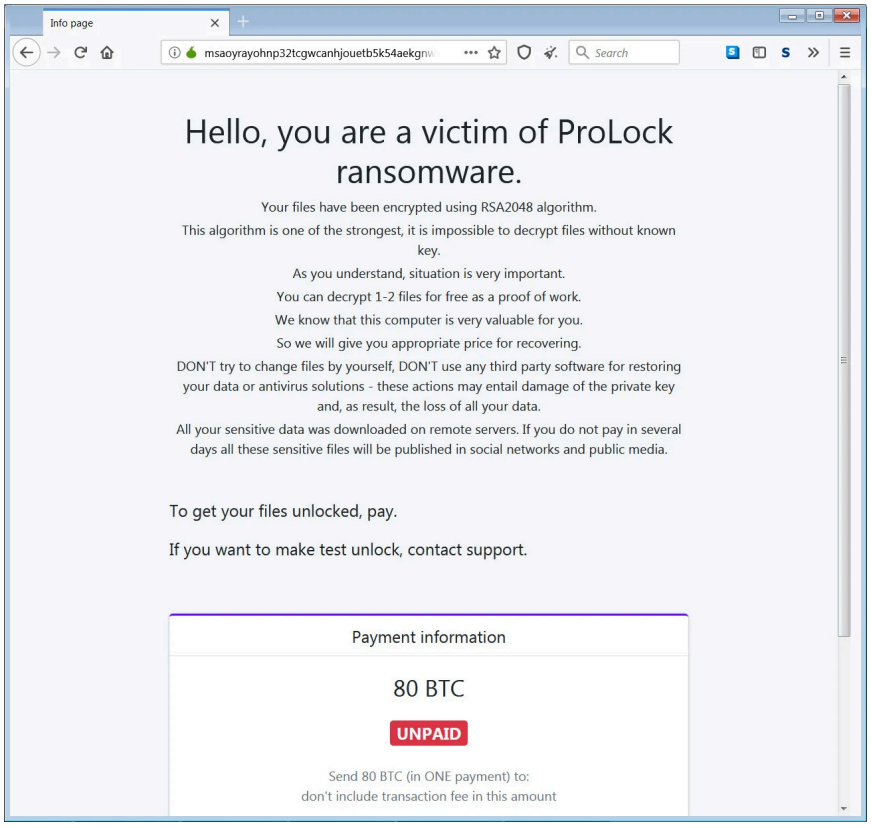


FBI's previous alert also warned private industry partners that ProLock's decryptor is not working properly and that data will be lost since files over 64MB might be corrupted as part of the decryption process.

ProLock ransomware started as PwndLocker during late 2019, slowly making a reputation for itself while targeting both US businesses and local governments.

PwndLocker rebranded itself as ProLocker in March after fixing a bug that allowed free decryption of locked files, and its activity started to escalate as it started targeting corporate networks again.

The boost in activity was most likely caused by partnering with the QakBot banking trojan gang which made it a lot easier to gain access to new victims' networks.



ProLock Tor payment site

ProLock ransoms can reach almost $700K

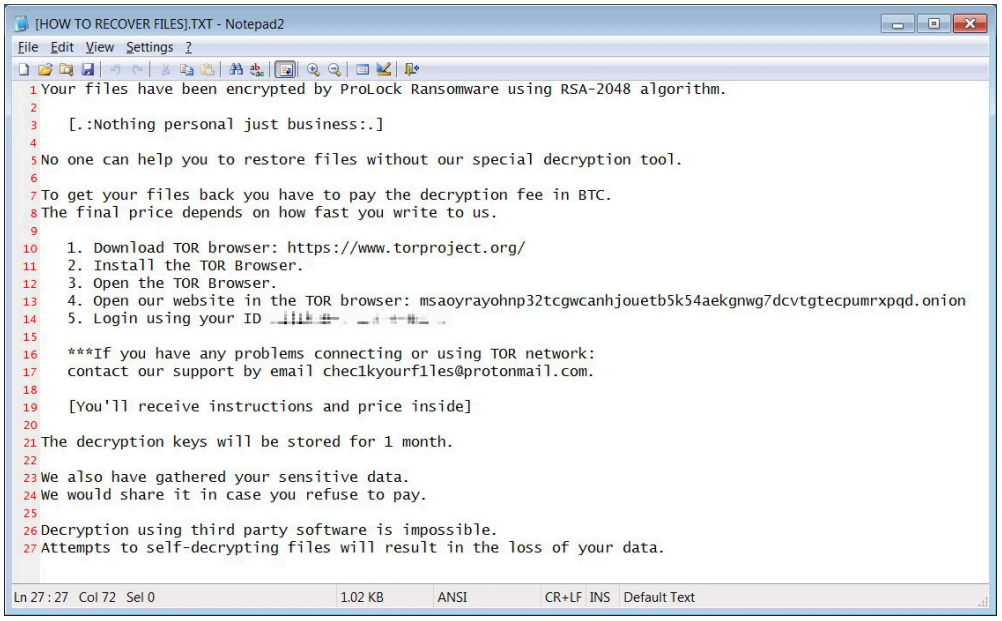
The operators behind the human-operated ProLock ransomware have been harvesting and exfiltrating information from their victims' devices before deploying their payloads since March 2020 according to the FBI.

The stolen data is later used by the threat actors as leverage in persuading the victim organizations into paying ransoms ranging between $175,000 to more than $660,000 depending on the size of the compromised network as BleepingComputer found.

So far, ProLock has successfully encrypted the networks of organizations around the world from multiple industry sectors including healthcare, construction, finance, and legal, including US government agencies and industrial entities.

ProLock's operators have used several attack vectors to breach their victims' systems including phishing emails with QakBot malicious attachments, using stolen credentials, and exploiting system configuration flaws.

The threat actors were observed archiving the stolen data and uploading to cloud storage platforms including OneDrive, Google Drive, and Mega with the help of the Rclone cloud storage sync command-line tool.



ProLock ransom note

Victims encouraged not to pay the ransoms

The FBI encourages private industry partners affected by ProLock ransomware attacks not to give in to the threat actors' demands and pay the ransoms.

Doing so would only embolden them to target other victims and will also directly fund their future illicit operations as the FBI explained.

However, the FBI recognizes the damages companies could face following such attacks and urges victims to report the attacks as soon as possible after having their systems infected with ProLock ransomware regardless of their decision to pay for a decryptor or not.

Reporting the attack to the local FBI field office to provide attack-related information such as phishing emails, recovered ransomware samples, ransom notes, and network traffic logs could help counter other attacks, as well as to identify and hold the attackers accountable for their activity.

The FBI recommends US orgs to periodically back up their data to an off-line/off-site backup location and to always keep their software up to date to patch any newly discovered security flaws the ProLock operators could exploit.

They are also recommended to make use of two-factor authentication (2FA) wherever possible, to disable unused Remote Desktop Protocol (RDP) instances, and to disable automatic attachment downloads in email clients.

Source: https://www.bleepingcomputer.com/news/security/fbi-issues-second-alert-about-prolock-ransomware-stealing-data/