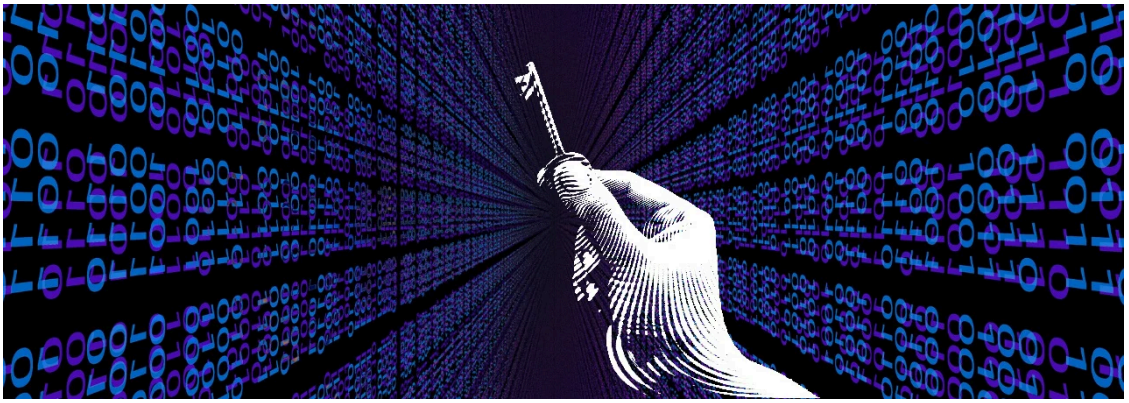
PwndLocker Ransomware Gets Pwned: Decryption Now Available

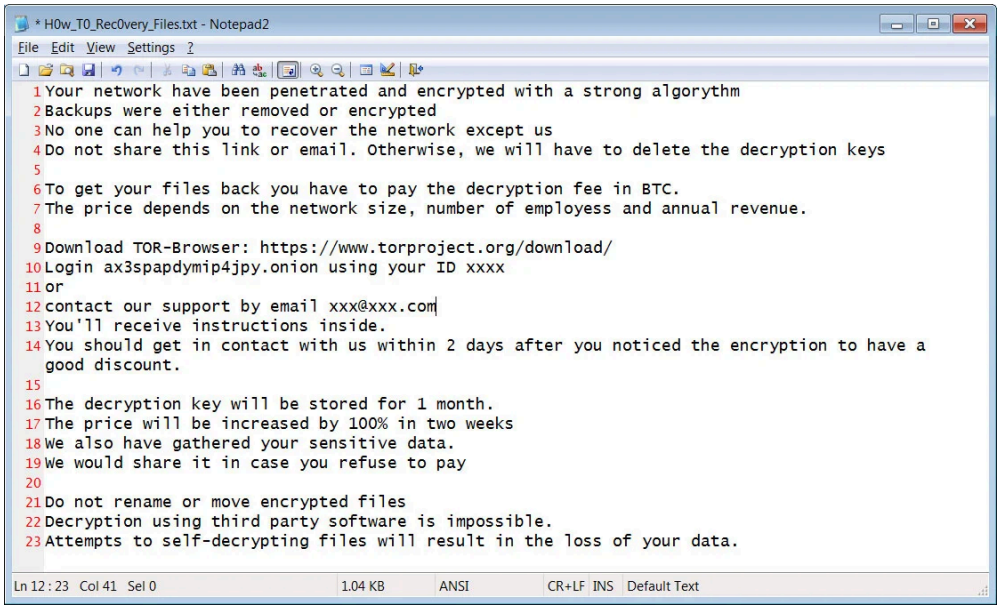
By Lawrence Abrams

Published: 2020-03-05 · Archived: 2026-04-05 16:11:24 UTC



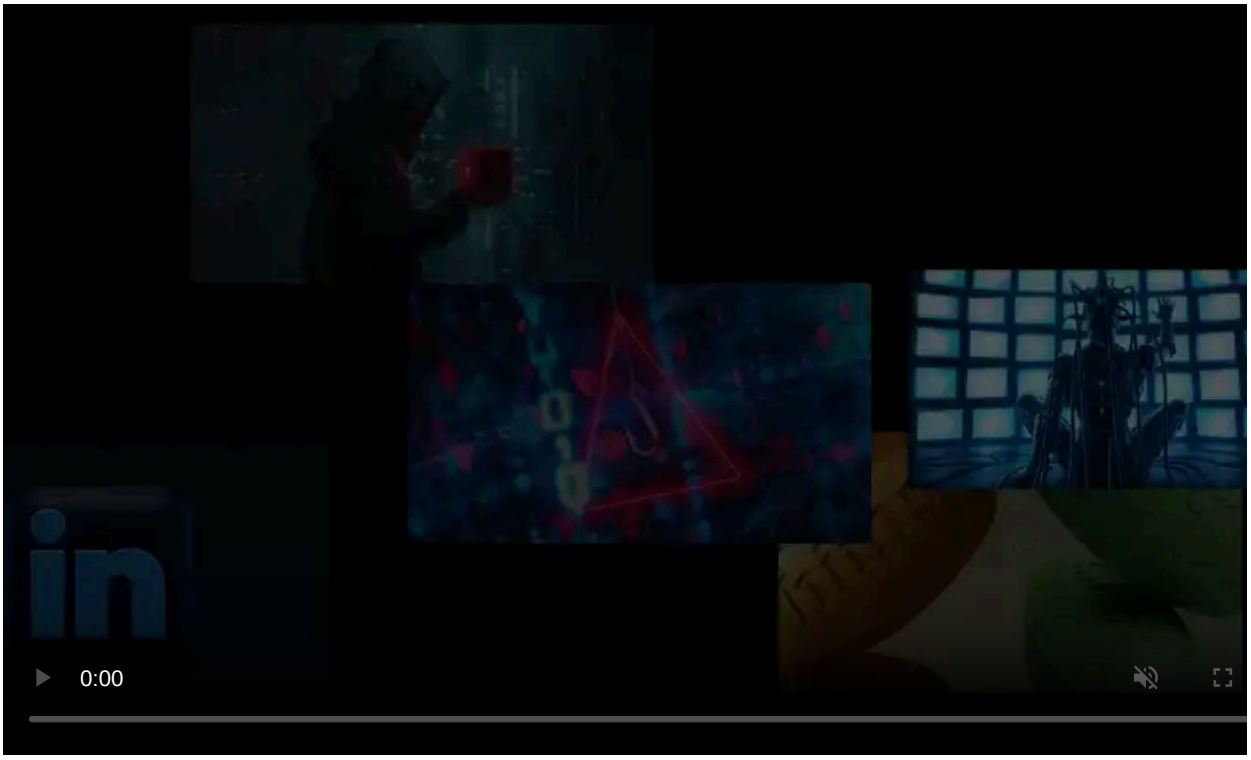
Emsisoft has discovered a way to decrypt files encrypted by the new PwndLocker Ransomware so that victims can recover their files without paying a ransom.

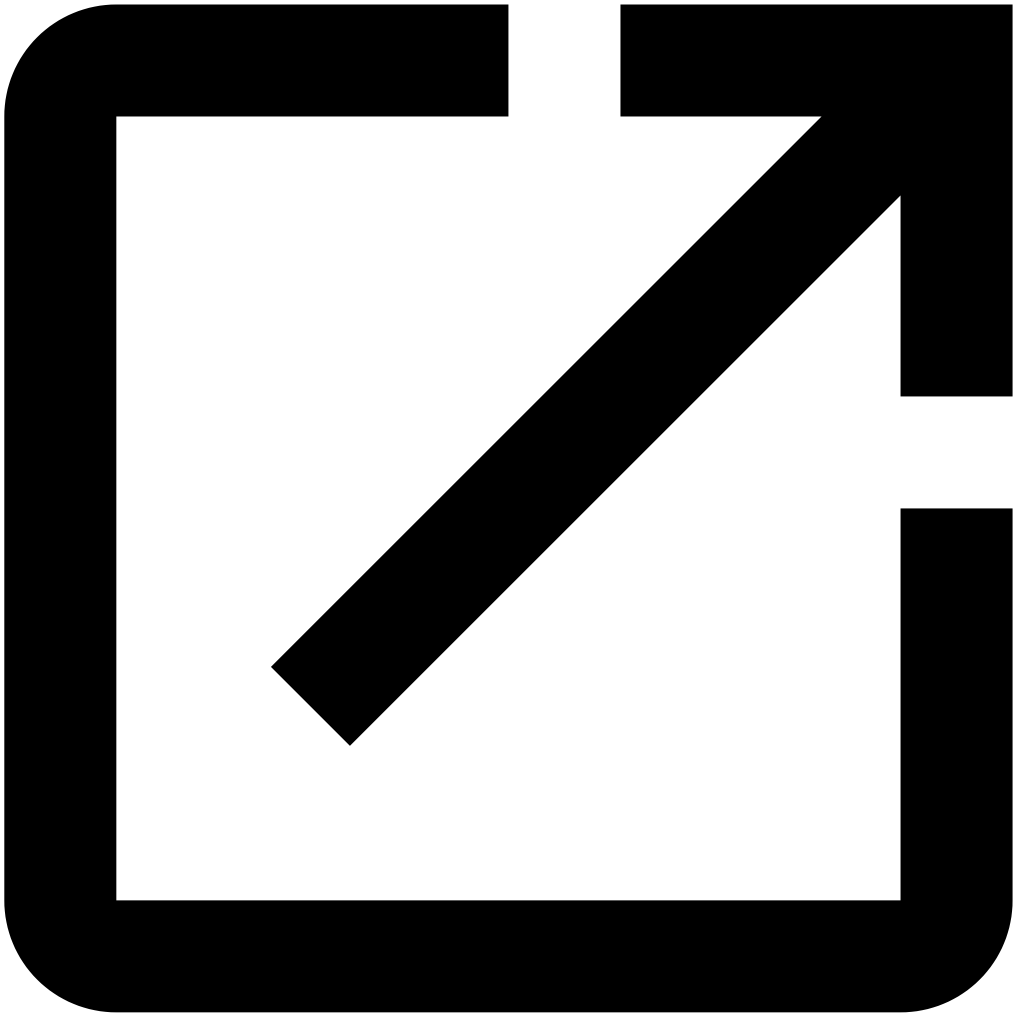
We were the first to report about a relatively new ransomware called PwndLocker that was encrypting organizations and cities around the world and then demanding ransoms ranging from $175,000 to over $660,000 depending on the size of the network.



PwndLocker Ransom Note

Among these victims is Lasalle County, Illinois who was hit with a 50 bitcoin ransom ($442,000) and the City of Novi Sad, Serbia who had over 50TB of data encrypted.


0:00



Flaw found in ransomware

After analyzing the PwndLocker ransomware, Emsisoft's Fabian Wosar was able to spot a weakness in the malware that allows victims to recover their files without paying the ransom.

To receive help with the ransomware, Wosar told BleepingComputer that victims need to send him a copy of the ransomware executable that was used in the attack.

Unfortunately, after deploying the ransomware the attackers are deleting this executable.

Victims may be able to recover the executable using Shadow Explorer or file recovery tools. When searching for the executable, victims should look in the %Temp%, C:\User folders, and %Appdata% folders.

Once an executable is found, victims can contact Emsisoft to receive help.

Source: https://www.bleepingcomputer.com/news/security/pwndlocker-ransomware-gets-pwned-decryption-now-available/