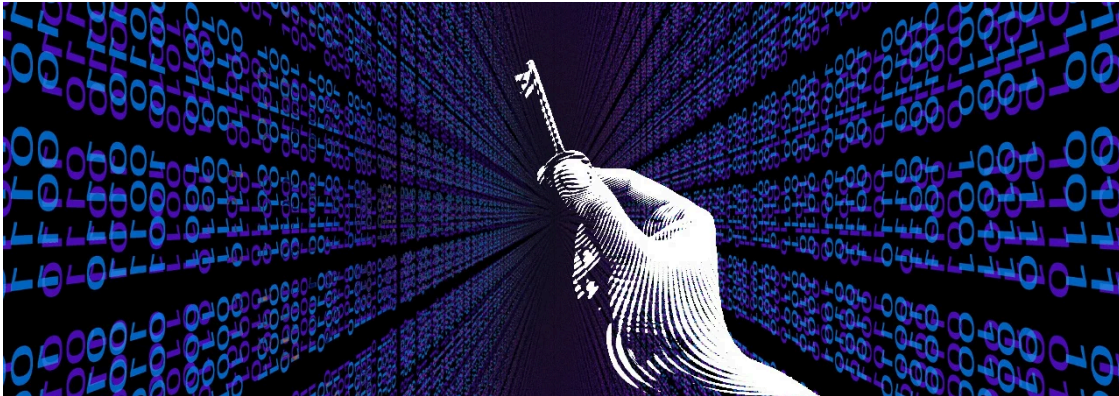


## PwndLocker Ransomware Gets Pwned: Decryption Now Available

By Lawrence Abrams

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



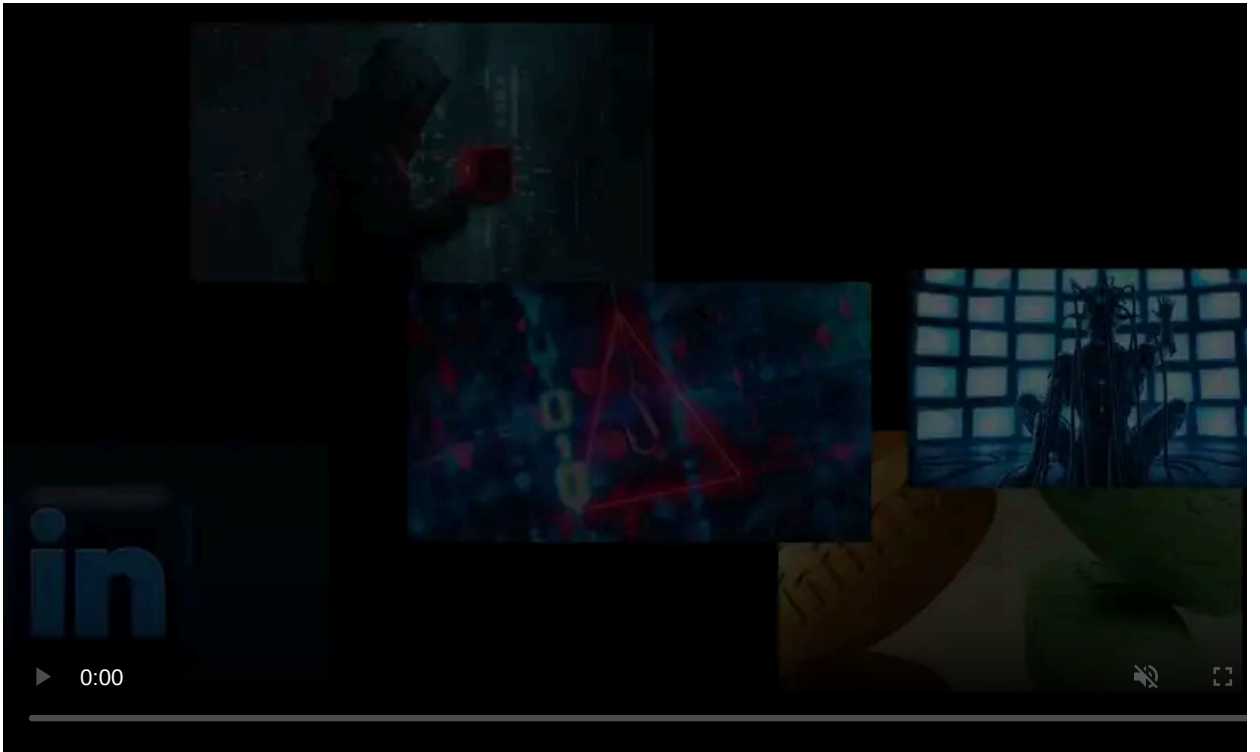
Emsisoft has discovered a way to decrypt files encrypted by the new PwndLocker Ransomware so that victims can recover their files without paying a ransom.

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.

```
H0w_T0_Rec0very_Files.txt - Notepad2
File Edit View Settings 2
1 Your network have been penetrated and encrypted with a strong algorithm
2 Backups were either removed or encrypted
3 No one can help you to recover the network except us
4 Do not share this link or email. Otherwise, we will have to delete the decryption keys
5
6 To get your files back you have to pay the decryption fee in BTC.
7 The price depends on the network size, number of employess and annual revenue.
8
9 Download TOR-Browser: https://www.torproject.org/download/
10 Login ax3spapdymp4jpy.onion using your ID xxxx
11 or
12 contact our support by email xxx@xxx.com
13 You'll receive instructions inside.
14 You should get in contact with us within 2 days after you noticed the encryption to have a
    good discount.
15
16 The decryption key will be stored for 1 month.
17 The price will be increased by 100% in two weeks
18 We also have gathered your sensitive data.
19 We would share it in case you refuse to pay
20
21 Do not rename or move encrypted files
22 Decryption using third party software is impossible.
23 Attempts to self-decrypting files will result in the loss of your data.
Ln 12 : 23 Col 41 Sel 0 1.04 KB ANSI CR+LF INS Default Text
```

### 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.



Visit Advertiser website [GO TO PAGE](#)

## Flaw found in ransomware

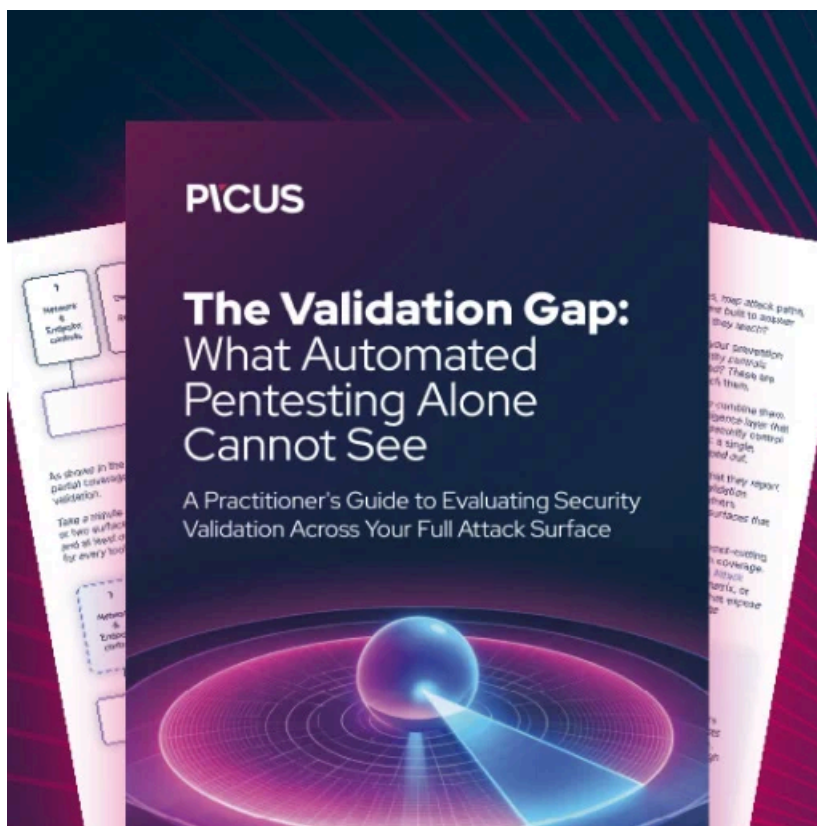
After analyzing the PwndLocker ransomware, Emsisoft's Fabian Wosar was able to spot a weakness in the malware that allows victims to recover their files without paying the ransom.

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.



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

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