New PwndLocker Ransomware Targeting U.S. Cities, Enterprises

bleepingcomputer.com/news/security/new-pwndlocker-ransomware-targeting-us-cities-enterprises/

Lawrence Abrams

By
Lawrence Abrams

- March 2, 2020
- 03:08 PM
- 0

Driven by the temptation of big ransom payments, a new ransomware called PwndLocker has started targeting the networks of businesses and local governments with ransom demands over $650,000.

This new ransomware began operating in late 2019 and has since encrypted a stream of victims ranging from local cities to organizations.

BleepingComputer has been told that the ransom amounts being demanded by PwndLocker range from $175,000 to over $660,000 depending on the size of the network.

It is not known if any of these victims have paid at this time.

PwndLocker says they encrypted Lasalle County's network

A source recently told BleepingComputer that the ransomware attack against Lasalle County in Illinois was conducted by the operators of the PwndLocker Ransomware.

When asked by BleepingComputer, the ransomware operators said they are behind the attack and are demanding a 50 bitcoin ransom ($442,000) for a decryptor.

The attackers have also told BleepingComputer that they have stolen data from the county before encrypting the network. From an image and a list of folders shared with BleepingComputer by the attackers, it does look like files were stolen from the county.

Local media reports that Lasalle County has no plans on paying the ransom.

BleepingComputer has contacted Lasalle County via email for confirmation but the emails were rejected. We have also left a voicemail but have not heard back at this time.

Update 3/3/2020 8:19 AM: PwndLocker has also encrypted the network for the City of Novi Sad in Serbia.
Update 3/3/2020 7:18 PM: PwndLocker shared an image and a list of folders that they say were stolen from Lasalle County.

The PwndLocker Ransomware

In a sample shared with BleepingComputer by MalwareHunterTeam, when executed PwndLocker will attempt to disable a variety of Windows services using the 'net stop' command so that their data can be encrypted.

Some of the applications whose services are targeted include Veeam, Microsoft SQL Server, MySQL, Exchange, Acronis, Zoolz, Backup Exec, Oracle, Internet Information Server (IIS), and security software such as Kaspersky, Malwarebytes, Sophos, and McAfee.

The ransomware will also target various processes and terminate them if detected. Some of the processes targeted include Firefox, Word, Excel, Access, and other processes related to security software, backup applications, and database servers.

PwndLocker will now clear the Shadow Volume Copies so that they cannot be used to recover files with the following commands:

```
vssadmin.exe delete shadows /all /quiet
vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=401MB
vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=unbounded
```

Once the system has been prepped for encryption, PwndLocker will begin to encrypt the computer.

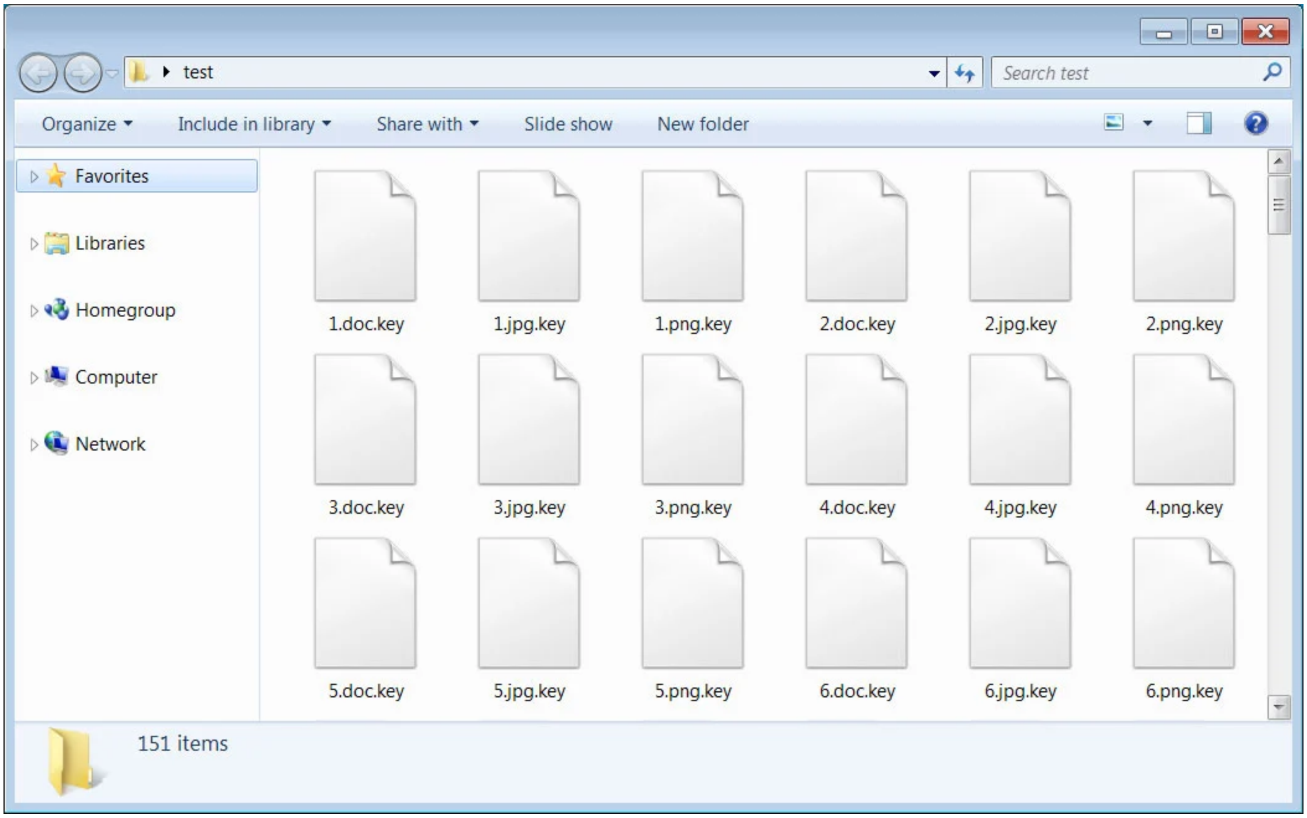
While encrypting files, it will skip any files that contain one of the following extensions.

```
.exe, .dll, .lnk, .ico, .ini, .msi, .chm, .sys, .hlf, .lng, .inf, .ttf, .cmd, .bat,
.vhd, .bac, .bak, .wbc, .bkf, .set, .win, .dsk
```

The ransomware will also skip all files located in the following folders:

```
$Recycle.Bin
Windows
System Volume Information
PerfLogs
Common Files
DVD Maker
Internet Explorer
Kaspersky Lab
Kaspersky Lab Setup Files
WindowsPowerShell
Microsoft
Microsoft.NET
Mozilla Firefox
MSBuild
Windows Defender
Windows Mail
Windows Media Player
Windows NT
Windows Photo Viewer
Windows Portable Devices
Windows Sidebar
WindowsApps
All Users
Uninstall Information
Microsoft
Adobe
Microsoft
Microsoft_Corporation
Packages
Temp
```

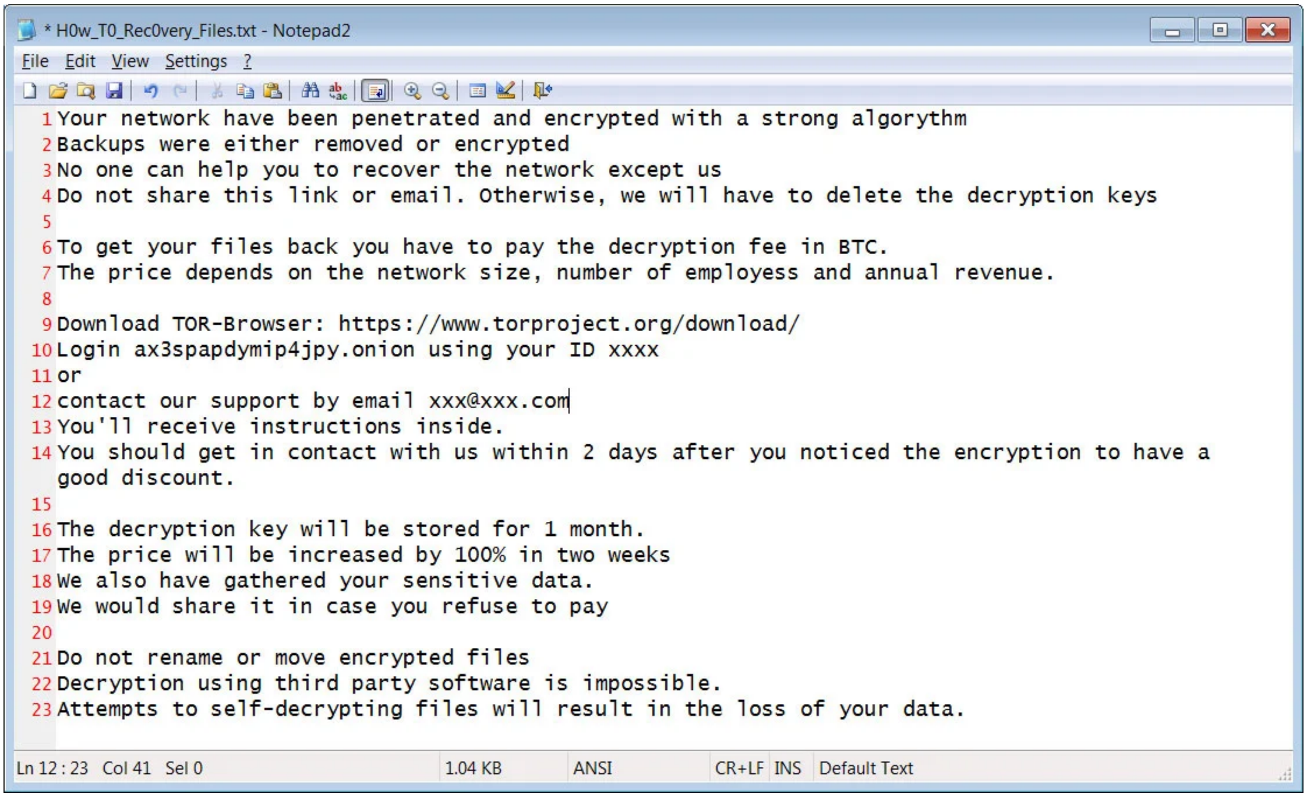
When encrypting files, MalwareHunterTeam has seen it using the **.key** and **.pwnd** extensions depending on the victim. The sample BleepingComputer analyzed uses the .key extension as shown below.



Files encrypted by PwndLocker

When done encrypting, ransom notes named **H0w_T0_Rec0very_Files.txt** will be located throughout the computer and on the Windows desktop.

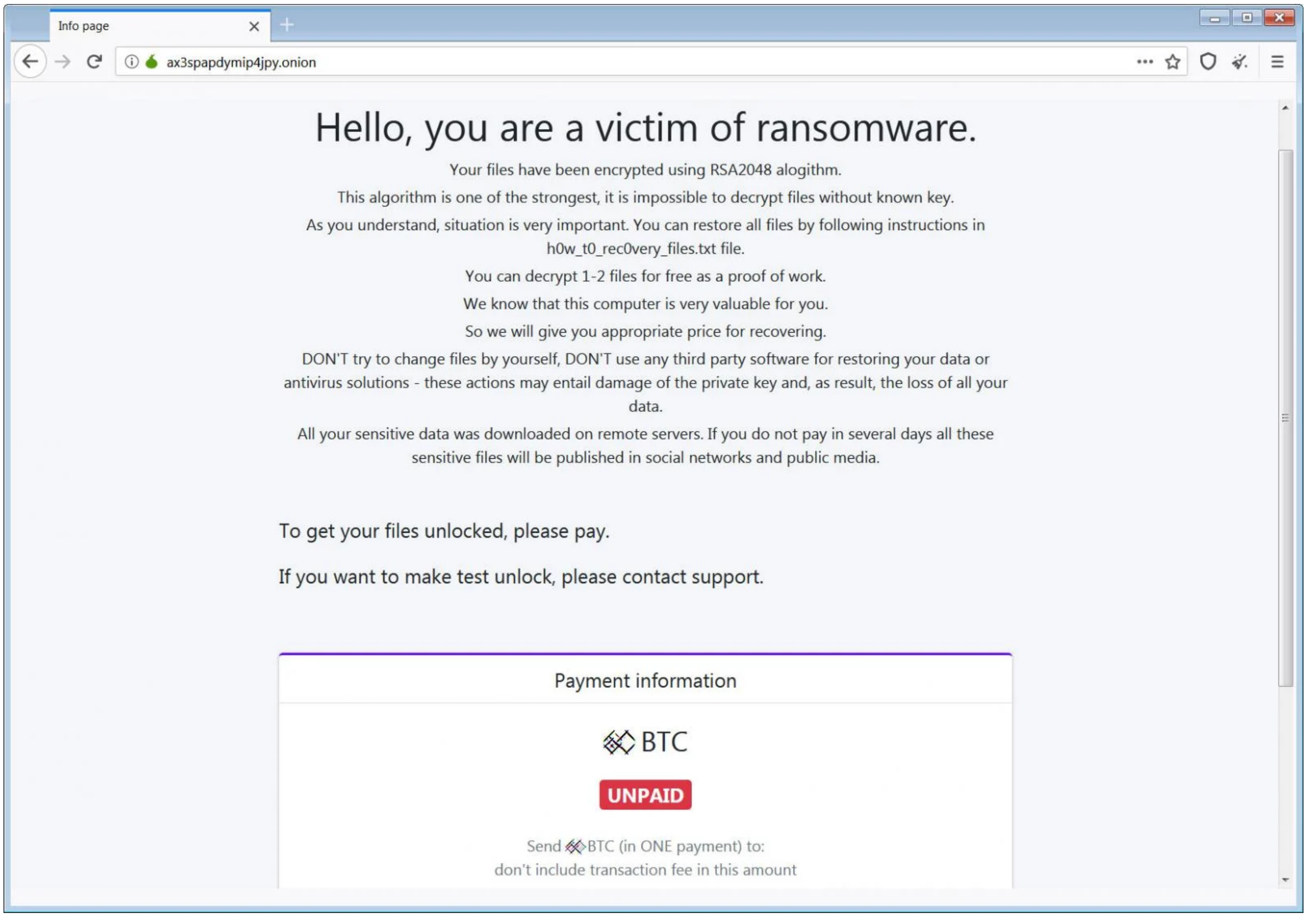
These ransom notes will contain an email address and Tor payment site that can be used to get payment instructions and the ransom amount.


* H0w_T0_Rec0very_Files.txt - Notepad2
File Edit View Settings ?
Ln 12 : 23 Col 41 Sel 0
1.04 KB
ANSI
CR+LF INS
Default Text

```
Your network have been penetrated and encrypted with a strong algorythm
Backups were either removed or encrypted
No one can help you to recover the network except us
Do not share this link or email. Otherwise, we will have to delete the decryption keys

To get your files back you have to pay the decryption fee in BTC.
The price depends on the network size, number of employess and annual revenue.

Download TOR-Browser: https://www.torproject.org/download/
Login ax3spapdymip4jpy.onion using your ID xxxx
or
contact our support by email xxx@xxx.com
You'll receive instructions inside.
You should get in contact with us within 2 days after you noticed the encryption to have a good discount.

The decryption key will be stored for 1 month.
The price will be increased by 100% in two weeks
We also have gathered your sensitive data.
We would share it in case you refuse to pay

Do not rename or move encrypted files
Decryption using third party software is impossible.
Attempts to self-decrypting files will result in the loss of your data.
```

PwndLocker Ransom Note

The PwndLocker Payment Site allows victims to decrypt two files for free, talk to the ransomware operators and contains the ransom amount in bitcoins.



Hello, you are a victim of ransomware.

Your files have been encrypted using RSA2048 alogithm.
This algorithm is one of the strongest, it is impossible to decrypt files without known key.
As you understand, situation is very important. You can restore all files by following instructions in h0w_t0_rec0very_files.txt file.
You can decrypt 1-2 files for free as a proof of work.
We know that this computer is very valuable for you.
So we will give you appropriate price for recovering.
DON'T try to change files by yourself, DON'T use any third party software for restoring your data or antivirus solutions - these actions may entail damage of the private key and, as result, the loss of all your data.
All your sensitive data was downloaded on remote servers. If you do not pay in several days all these sensitive files will be published in social networks and public media.

To get your files unlocked, please pay.

If you want to make test unlock, please contact support.

Payment information

BTC

UNPAID

Send BTC (in ONE payment) to:
don't include transaction fee in this amount

PwndLocker Tor Payment Site

It is not known at this time if there are any weaknesses in the encryption algorithm.

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

IOCs

Known Extensions:

```
.key
.pwnd
```

Associated Files:

```
H0w_T0_Rec0very_Files.txt
C:\Programdata\lock.xml
```

Ransom Note Text:

```
Your network have been penetrated and encrypted with a strong algorythm
Backups were either removed or encrypted
No one can help you to recover the network except us
Do not share this link or email. Otherwise, we will have to delete the decryption keys

To get your files back you have to pay the decryption fee in BTC.
The price depends on the network size, number of employess and annual revenue.

Download TOR-Browser: https://www.torproject.org/download/
Login ax3spapdymip4jpy.onion using your ID xxxx
or
contact our support by email xxx@xxx.com
You'll receive instructions inside.
You should get in contact with us within 2 days after you noticed the encryption to have a good discount.

The decryption key will be stored for 1 month.
The price will be increased by 100% in two weeks
We also have gathered your sensitive data.
We would share it in case you refuse to pay

Do not rename or move encrypted files
Decryption using third party software is impossible.
Attempts to self-decrypting files will result in the loss of your data.
```

- Enterprise
- Government
- PwndLocker
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: