New FuxSocy Ransomware Impersonates the Notorious Cerber

bleepingcomputer.com/news/security/new-fuxsocy-ransomware-impersonates-the-notorious-cerber/

Lawrence Abrams

By
Lawrence Abrams

- October 25, 2019
- 04:45 PM
- 2

A new ransomware has been discovered called FuxSocy that borrows much of its behavior from the notorious and now-defunct Cerber Ransomware.

Discovered by MalwareHunterTeam, this ransomware calls itself FuxSocy Encryptor, which is named after the FSociety hacking group in the Mr. Robot television series.

Like any other ransomware, FuxSocy will encrypt a victim's files and then demand a ransom in order to get a decryptor.

What is interesting about this ransomware, though, is that the developers decided to model it after the Cerber Ransomware by adopting its outward appearance as well as some of the internals.

Similarities to Cerber

When analyzed by reverse engineer Vitali Kremez, the researcher told BleepingComputer he noticed that some of the ransomware internals are similar to those used by Cerber.

For example, when encrypting files FuxSocy will skip files whose file path contain certain strings. Many of the strings are taken directly from Cerber, who used the same exception list, with FuxSocy adding some additional ones.

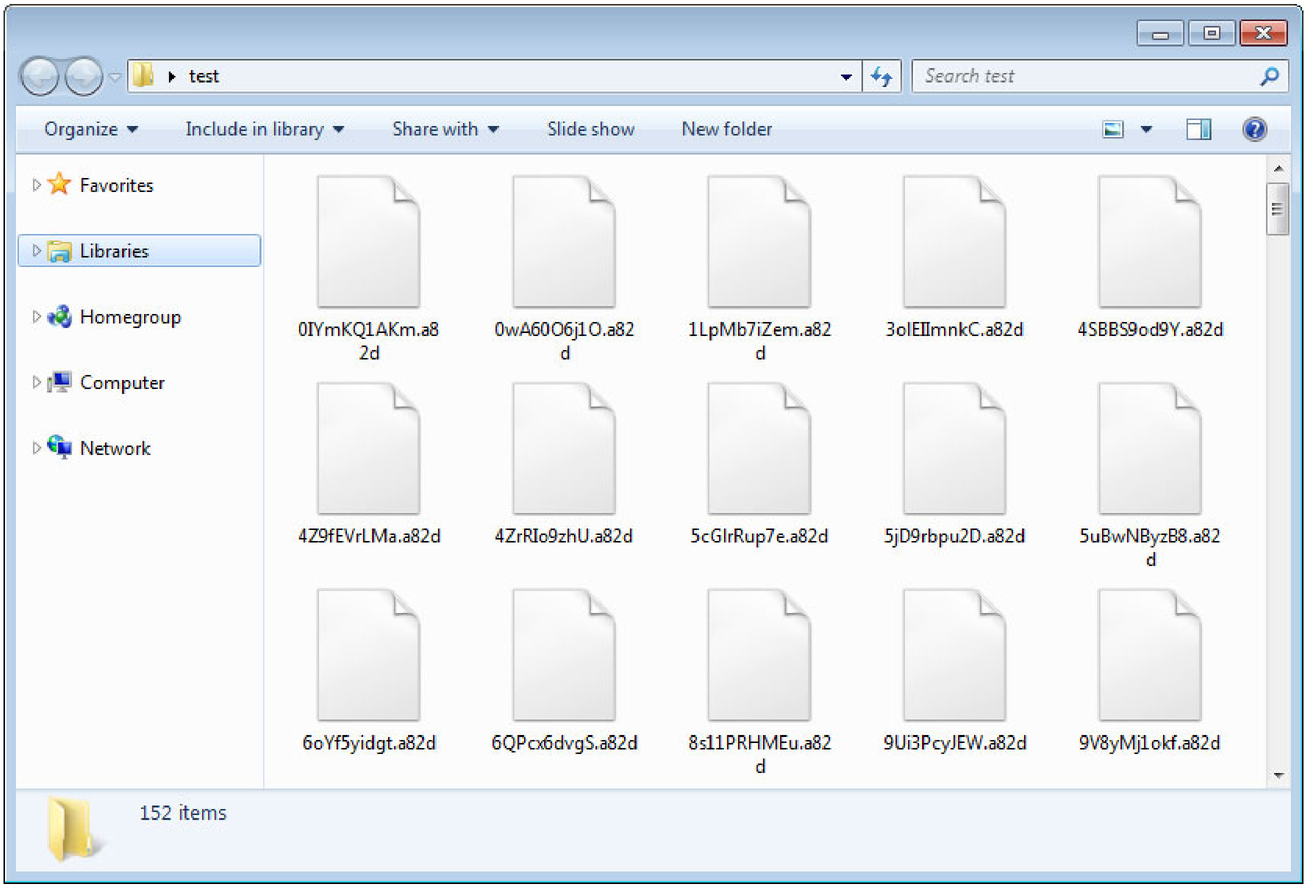
The full list of bypassed folders are below:

```
*:\$getcurrent\*
*:\$recycle.bin\*
*:\$windows.~bt\*
*:\$windows.~ws\*
*:\boot\*
*:\documents and settings\all users\*
*:\documents and settings\default user\*
*:\documents and settings\localservice\*
*:\documents and settings\networkservice\*
*:\intel\*
*:\msocache\*
*:\perflogs\*
*:\program files (x86)\*
*:\program files\*
*:\programdata\*
*:\recovery\*
*:\recycled\*
*:\recycler\*
*:\system volume information\*
*:\temp\*
*:\tmp\*
*:\windows.old\*
*:\windows10upgrade\*
*:\windows\*
*:\winnt\*
*:\.*\*
*\appdata\local\*
*\appdata\locallow\*
*\appdata\roaming\*
*\local settings\*
*\public\music\sample music\*
*\public\pictures\sample pictures\*
*\public\videos\sample videos\*
*\tor browser\*
.txt
.jpg
```

Like Cerber, FuxSocy will also prioritize certain folders to make sure they get encrypted. This list of priority folders are:

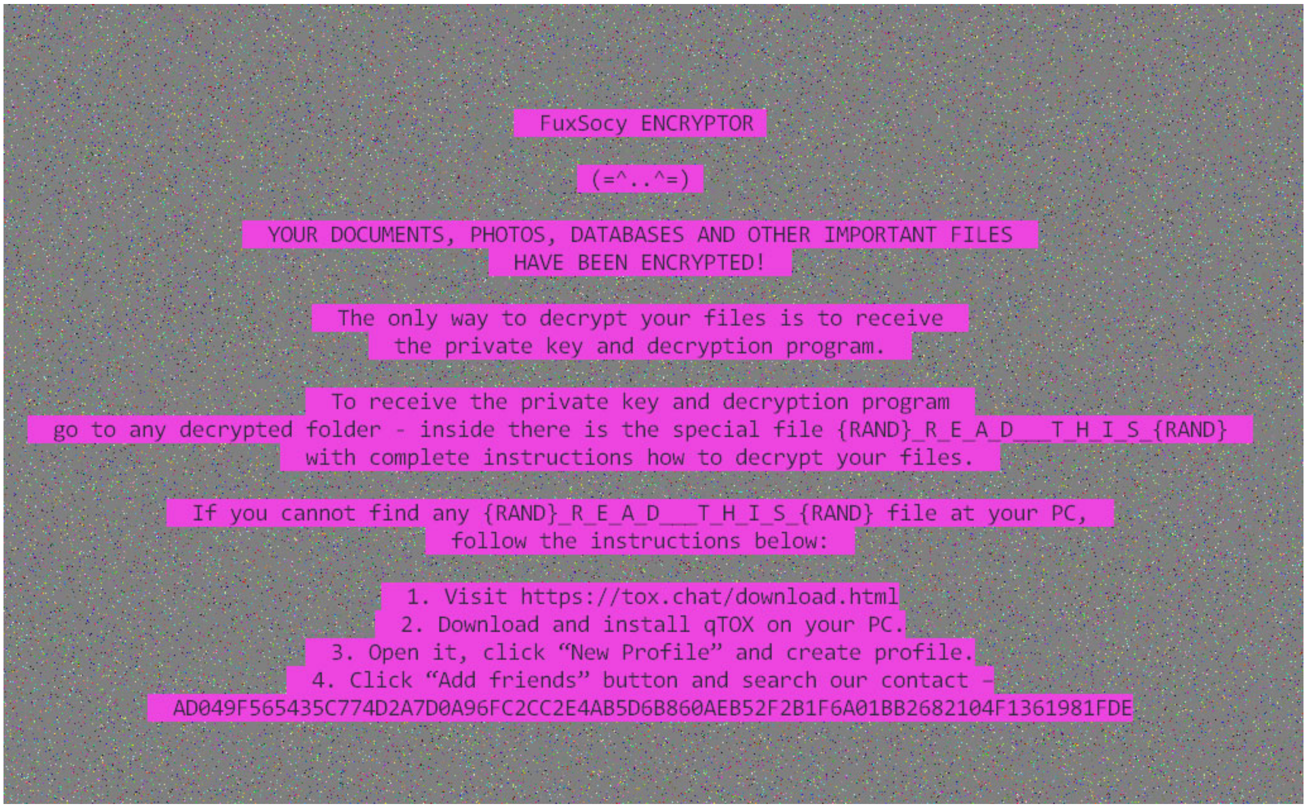
```
bitcoin
excel
microsoft sql server
microsoft\excel
microsoft\microsoft sql server
microsoft\office
microsoft\onenote
microsoft\outlook
microsoft\powerpoint
microsoft\word
office
onenote
outlook
powerpoint
steam
the bat!
thunderbird
word
autodesk
solidworks*
OpenSCAD
```

In addition, FuxSocy also scrambles the file name and extensions used by encrypted files in a similar manner as Cerber.



Encrypted FuxSocy Files

Finally, after encrypting a computer the Windows desktop background will be changed to an almost identical background that was originally used by Cerber.



FuxSocy ENCRYPTOR

(=^..^=)

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file {RAND}_R_E_A_D___T_H_I_S_{RAND}
with complete instructions how to decrypt your files.

If you cannot find any {RAND}_R_E_A_D___T_H_I_S_{RAND} file at your PC,
follow the instructions below:

1. Visit https://tox.chat/download.html
2. Download and install qTOX on your PC.
3. Open it, click “New Profile” and create profile.
4. Click “Add friends” button and search our contact -
AD049F565435C774D2A7D0A96FC2CC2E4AB5D6B860AEB52F2B1F6A01BB2682104F1361981FDE

FuxSocy Desktop Background

So what has changed?

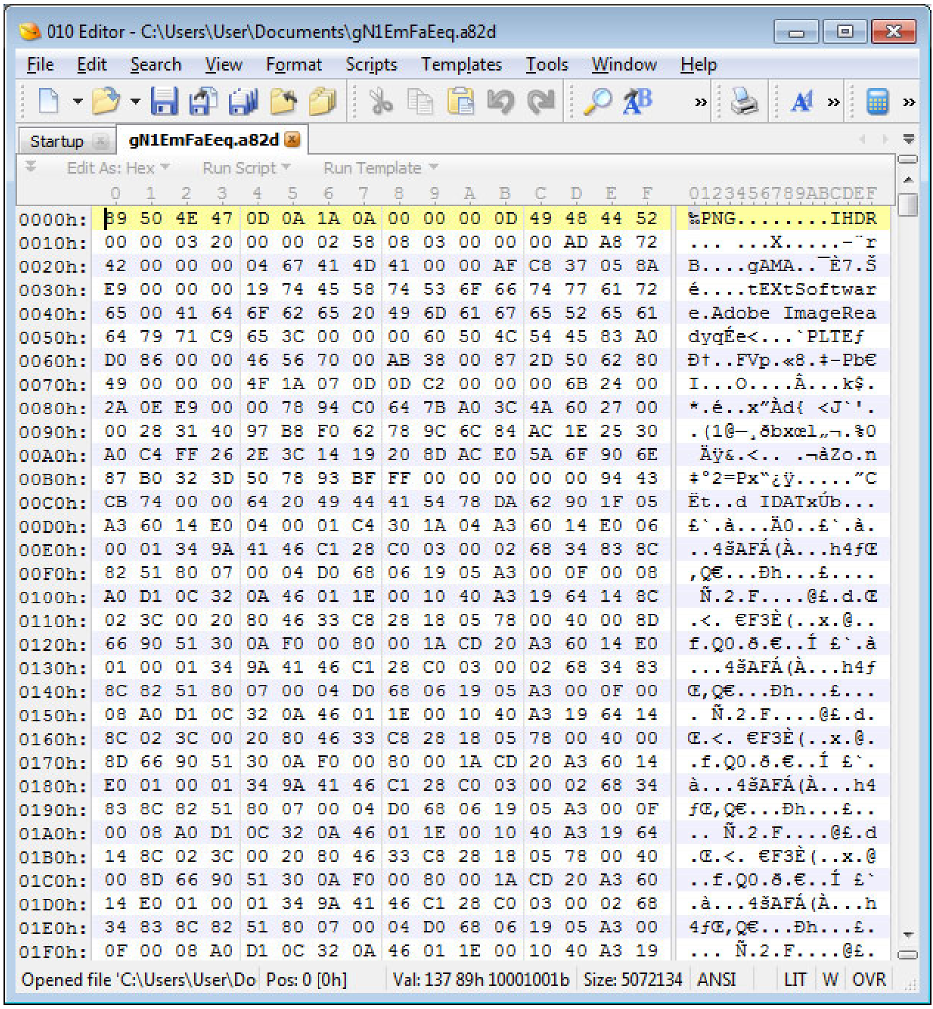
While outwardly FuxSocy looks very similar to Cerber, there are also quite a few differences.

For example, FuxSocy attempts to more extensively block users from running the ransomware on a virtual machine by looking for the following processes, files, and named pipes:

```
prl_cc.exe
prl_tools.exe
vboxservice.exe
vboxtray.exe
VMSrvc.exe
VMUSrvc.exe
vmtoolsd.exe
vmwaretray.exe
vmwareuser.exe
VGAuthService.exe
vmacthlp.exe
xenservice.exe
qemu-ga.exe
\\.\VBoxMiniRdrDN
\\.\VBoxGuest
\\.\pipe\VBoxMiniRdDN
\\.\VBoxTrayIPC
\\.\pipe\VBoxTrayIPC
\\.\HGFS
\\.\vmci
system32\drivers\VBoxMouse.sys
system32\drivers\VBoxGuest.sys
system32\drivers\VBoxSF.sys
system32\drivers\VBoxVideo.sys
system32\vboxdisp.dll
system32\vboxhook.dll
system32\vboxmrxnp.dll
system32\vboxogl.dll
system32\vboxoglarrayspu.dll
system32\vboxoglcrutil.dll
system32\vboxoglerrorspu.dll
system32\vboxoglfeedbackspu.dll
system32\vboxoglpackspu.dll
system32\vboxoglpassthroughspu.dll
system32\vboxservice.exe
system32\vboxtray.exe
system32\VBoxControl.exe
system32\drivers\vmmouse.sys
system32\drivers\vmhgfs.sys
system32\drivers\vm3dmp.sys
system32\drivers\vmci.sys
system32\drivers\vmmemctl.sys
system32\drivers\vmrawdsk.sys
system32\drivers\vmusbmouse.sys
```

Another strange feature is that the FuxSocy Encryptor does not encrypt the entire file.

According to Michael Gillespie, the ransomware will start encrypting files at 0x708 bytes, which for the most part will make documents unusable.



010 Editor - C:\Users\User\Documents\gN1EmFaEeq.a82d

gN1EmFaEeq.a82d

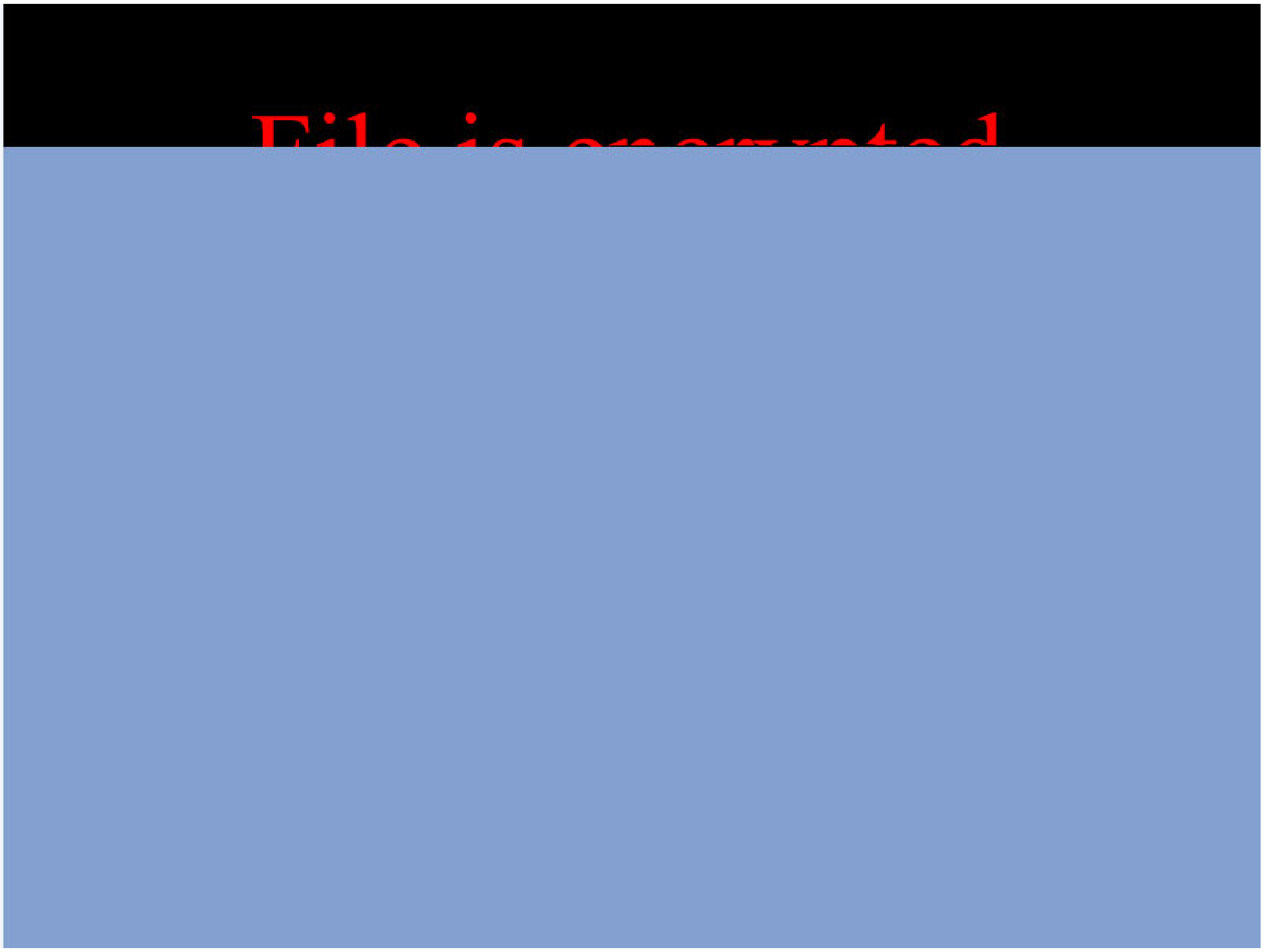
```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h:  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52   ‰PNG........IHDR
0010h:  00 00 03 20 00 00 02 58 08 03 00 00 00 AD A8 72   ... ...X.....-¨r
0020h:  42 00 00 00 04 67 41 4D 41 00 00 AF C8 37 05 8A   B....gAMA..¯È7.Š
0030h:  E9 00 00 00 19 74 45 58 74 53 6F 66 74 77 61 72   é....tEXtSoftwar
0040h:  65 00 41 64 6F 62 65 20 49 6D 61 67 65 52 65 61   e.Adobe ImageRea
0050h:  64 79 71 C9 65 3C 00 00 00 60 50 4C 54 45 83 A0   dyqÉe<...`PLTEƒ 
0060h:  D0 86 00 00 46 56 70 00 AB 38 00 87 2D 50 62 80   Ð†..FVp.«8.‡-Pb€
0070h:  49 00 00 00 4F 1A 07 0D 0D C2 00 00 00 6B 24 00   I...O....Â...k$.
0080h:  2A 0E E9 00 00 78 94 C0 64 7B A0 3C 4A 60 27 00   *.é..x”Àd{ <J`'.
0090h:  00 28 31 40 97 B8 F0 62 78 9C 6C 84 AC 1E 25 30   .(1@—¸ðbxœl„¬.%0
00A0h:  A0 C4 FF 26 2E 3C 14 19 20 8D AC E0 5A 6F 90 6E    Äÿ&.<.. .¬àZo.n
00B0h:  87 B0 32 3D 50 78 93 BF FF 00 00 00 00 00 94 43   ‡°2=Px“¿ÿ.....”C
00C0h:  CB 74 00 00 64 20 49 44 41 54 78 DA 62 90 1F 05   Ët..d IDATxÚb...
00D0h:  A3 60 14 E0 04 00 01 C4 30 1A 04 A3 60 14 E0 06   £`.à...Ä0..£`.à.
00E0h:  00 01 34 9A 41 46 C1 28 C0 03 00 02 68 34 83 8C   ..4šAFÁ(À...h4ƒŒ
00F0h:  82 51 80 07 00 04 D0 68 06 19 05 A3 00 0F 00 08   ‚Q€...Ðh...£....
0100h:  A0 D1 0C 32 0A 46 01 1E 00 10 40 A3 19 64 14 8C    Ñ.2.F....@£.d.Œ
0110h:  02 3C 00 20 80 46 33 C8 28 18 05 78 00 40 00 8D   .<. €F3È(..x.@..
0120h:  66 90 51 30 0A F0 00 80 00 1A CD 20 A3 60 14 E0   f.Q0.ð.€..Í £`.à
0130h:  01 00 01 34 9A 41 46 C1 28 C0 03 00 02 68 34 83   ...4šAFÁ(À...h4ƒ
0140h:  8C 82 51 80 07 00 04 D0 68 06 19 05 A3 00 0F 00   Œ‚Q€...Ðh...£...
0150h:  08 A0 D1 0C 32 0A 46 01 1E 00 10 40 A3 19 64 14   . Ñ.2.F....@£.d.
0160h:  8C 02 3C 00 20 80 46 33 C8 28 18 05 78 00 40 00   Œ.<. €F3È(..x.@.
0170h:  8D 66 90 51 30 0A F0 00 80 00 1A CD 20 A3 60 14   .f.Q0.ð.€..Í £`.
0180h:  E0 01 00 01 34 9A 41 46 C1 28 C0 03 00 02 68 34   à...4šAFÁ(À...h4
0190h:  83 8C 82 51 80 07 00 04 D0 68 06 19 05 A3 00 0F   ƒŒ‚Q€...Ðh...£..
01A0h:  00 08 A0 D1 0C 32 0A 46 01 1E 00 10 40 A3 19 64   .. Ñ.2.F....@£.d
01B0h:  14 8C 02 3C 00 20 80 46 33 C8 28 18 05 78 00 40   .Œ.<. €F3È(..x.@
01C0h:  00 8D 66 90 51 30 0A F0 00 80 00 1A CD 20 A3 60   ..f.Q0.ð.€..Í £`
01D0h:  14 E0 01 00 01 34 9A 41 46 C1 28 C0 03 00 02 68   .à...4šAFÁ(À...h
01E0h:  34 83 8C 82 51 80 07 00 04 D0 68 06 19 05 A3 00   4ƒŒ‚Q€...Ðh...£.
01F0h:  0F 00 08 A0 D1 0C 32 0A 46 01 1E 00 10 40 A3 19   ... Ñ.2.F....@£.
```

Opened file 'C:\Users\User\Do | Pos: 0 [0h] | Val: 137 89h 10001001b | Size: 5072134 | ANSI | LIT | W | OVR

Partially Encrypted

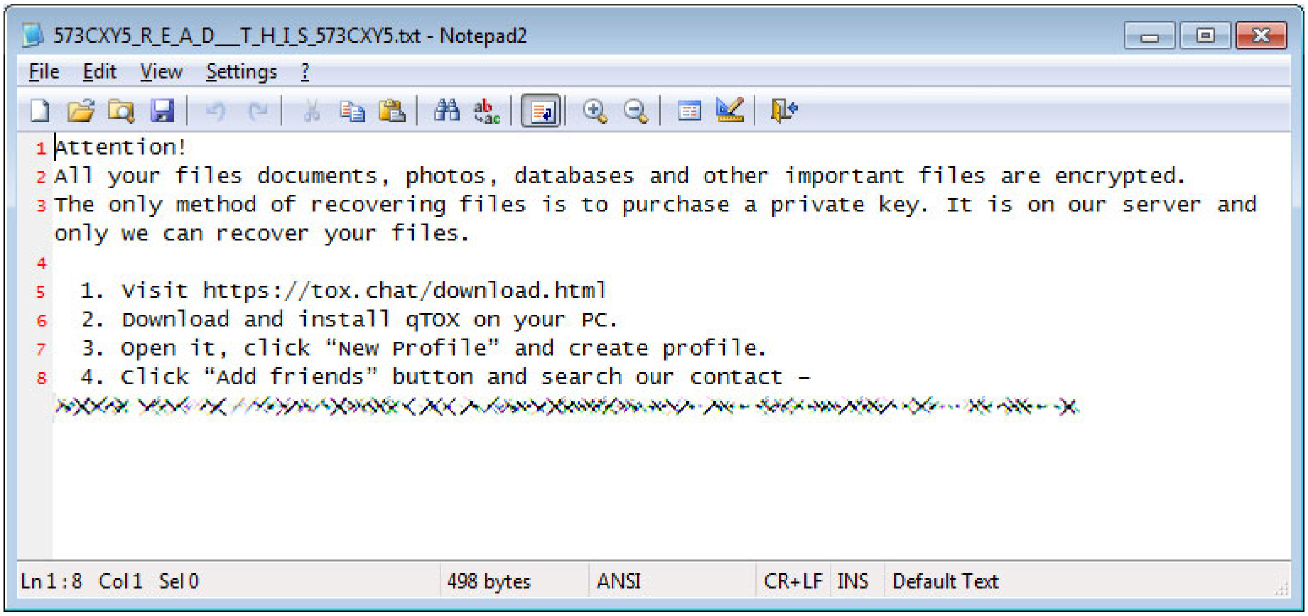
Image

Some image files, though, will have their unencryption regions viewable as shown below, with the rest being corrupted.



Corrupted Image File

Finally the ransom notes are different, with Cerber using a Tor payment site, while FuxSocy asks you to contact them via the ToxChat messaging app.


573CXY5_R_E_A_D___T_H_I_S_573CXY5.txt - Notepad2
File Edit View Settings ?
Ln 1 : 8 Col 1 Sel 0
498 bytes
ANSI
CR+LF
INS
Default Text

```
Attention!
All your files documents, photos, databases and other important files are encrypted.
The only method of recovering files is to purchase a private key. It is on our server and
only we can recover your files.

  1. Visit https://tox.chat/download.html
  2. Download and install qTOX on your PC.
  3. Open it, click "New Profile" and create profile.
  4. Click "Add friends" button and search our contact -
[redacted]
```

FuxSociety Ransom Note

While the similarities and differences are interesting, ultimately both ransomware infections do the same thing. They encrypt your data and make you pay a ransom to get your files back.

Unfortunately, at this time preliminary research of this ransomware indicates that the ransomware cannot be decrypted for free. It is advised that any victims restore their files backup rather than paying the ransom.

Update 10/28/19: Made a correction that some of the folders we stated were bypassed are actualy given prioritized encryption.

Related Articles:

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

US Senate: Govt’s ransomware fight hindered by limited reporting

- Cerber
- FuxSociety
- FuxSocy Encryptor
- 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

Comments

-

  Morality - 2 years ago

  -
  -

  Ain't the Corrupted Image File a image from DirtyDecrypt?

-

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: