

New FuxSocy Ransomware Impersonates the Notorious Cerber

By Lawrence Abrams

Published: 2019-10-25 · Archived: 2026-04-06 00:33:38 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

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:

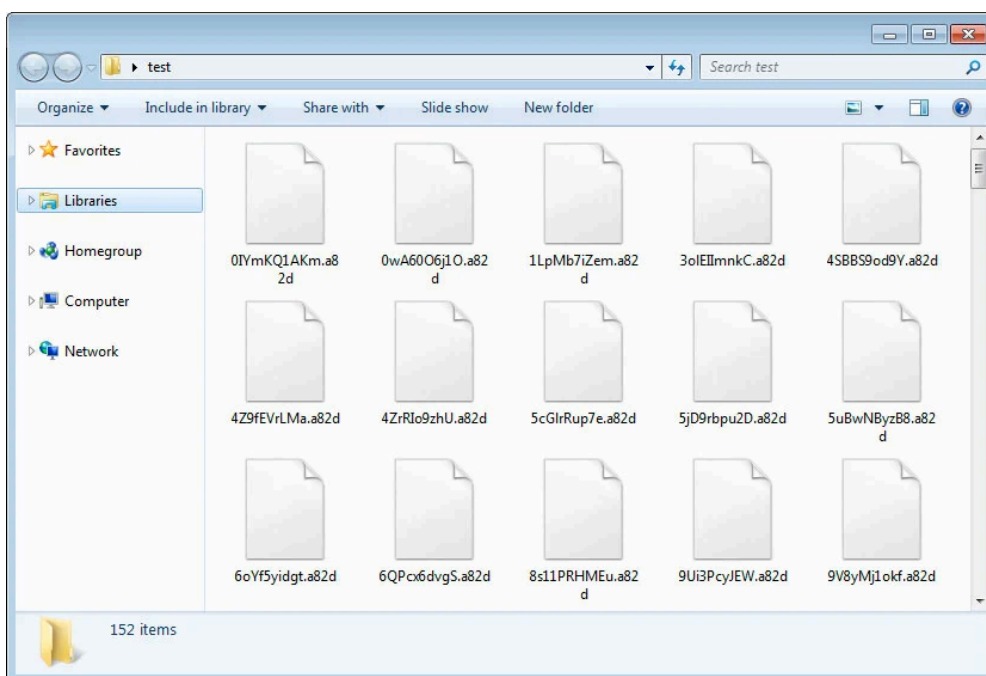
```
*:\$getcurrent\*
*:\$recycle.bin\*
*:\$windows.~bt\*
*:\$windows.~ws\*
*:\boot\*
*:\documents and settings\all users\*
*:\documents and settings\default user\*
*:\documents and settings\localservice\*
*:\documents and settings\networkservice\*
*:\intel\*
*:\msocache\*
*:\perflogs\*
*:\program files (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
```

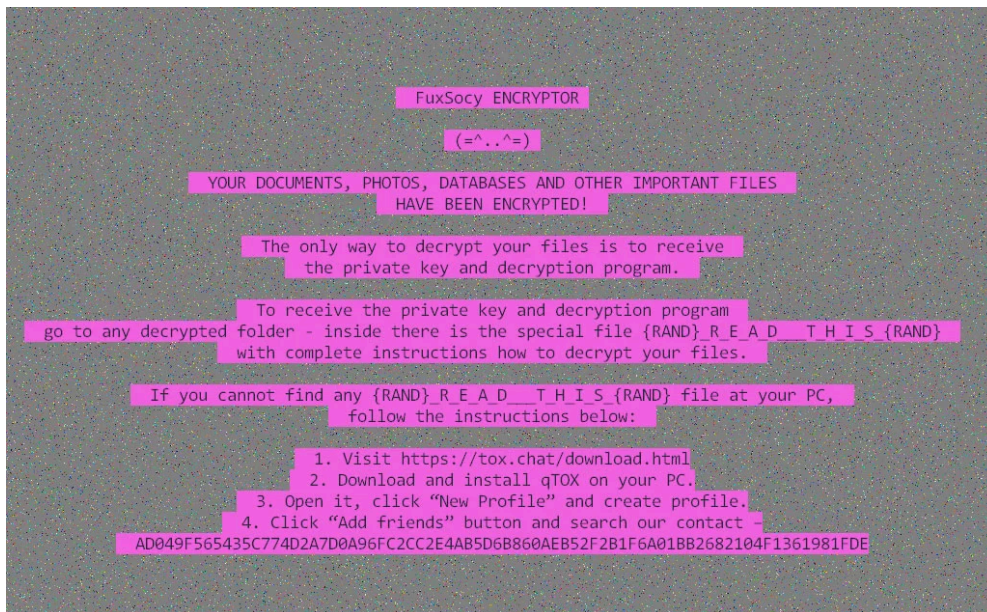
```
microsoft\microsoft sql server
microsoft\office
microsoft\onenote
microsoft\outlook
microsoft\powerpoint
microsoft\word
office
onenote
outlook
powerpoint
steam
the bat!
thunderbird
word
autodesk
solidworks*
OpenSCAD
```

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 Desktop Background

So what has changed?

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

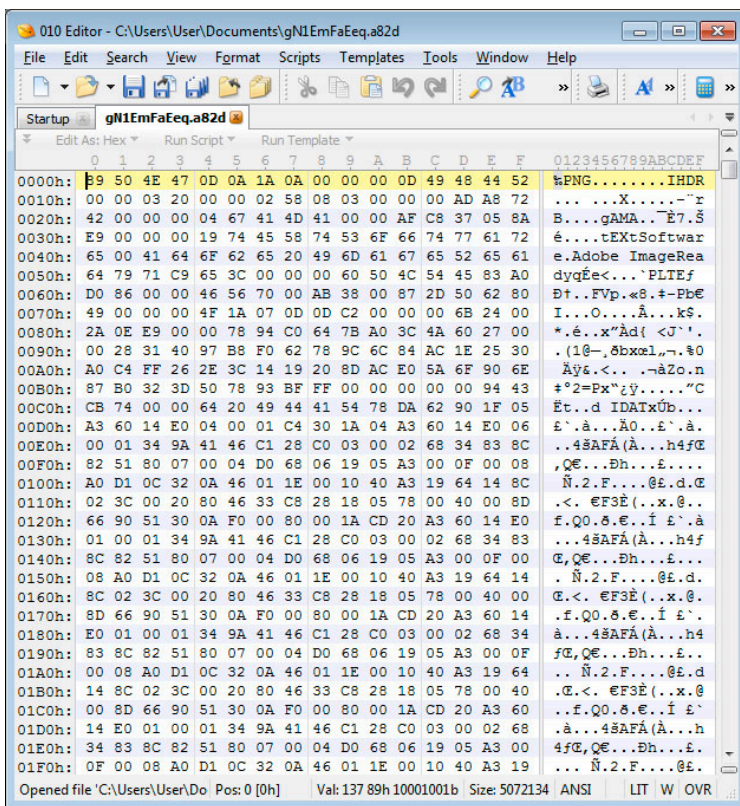
For example, FuxSocy attempts to more extensively block users from running the ransomware on a virtual machine by looking for the following processes, files, and named pipes:

```
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\vbboxglerrorspu.dll
system32\vbboxglfeedbackspu.dll
system32\vbboxglpackspu.dll
system32\vbboxglpassthroughspu.dll
system32\vbboxservice.exe
system32\vbboxtray.exe
system32\VBBoxControl.exe
system32\drivers\vmmouse.sys
system32\drivers\vmhgfs.sys
system32\drivers\vm3dmp.sys
system32\drivers\vmci.sys
system32\drivers\vmemctl.sys
system32\drivers\vmrawdsk.sys
system32\drivers\vmusbmouse.sys
```

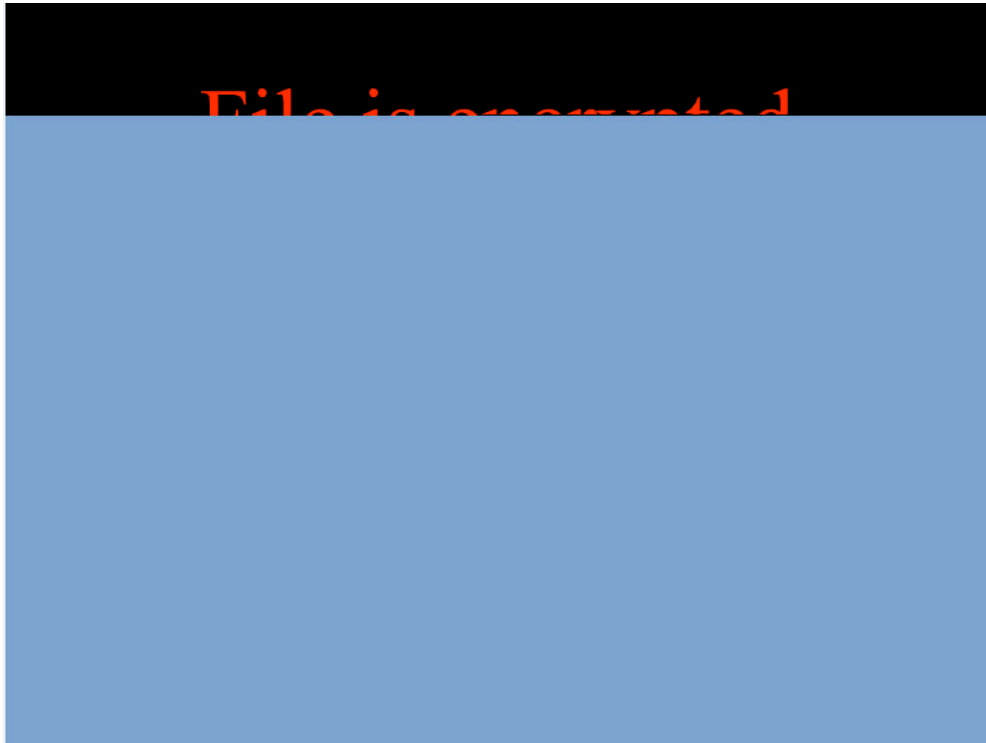
Another strange feature is that the FuxSocy Encryptor does not encrypt the entire file.

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



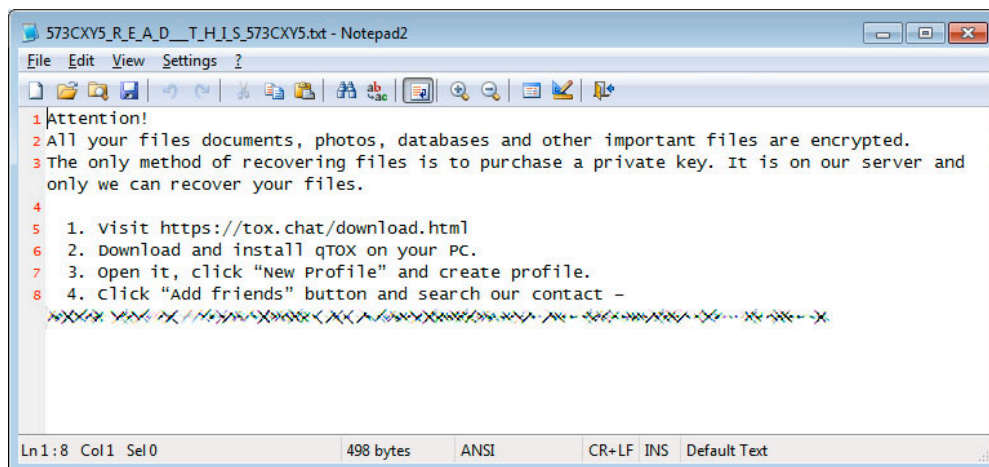
Partially Encrypted Image

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.

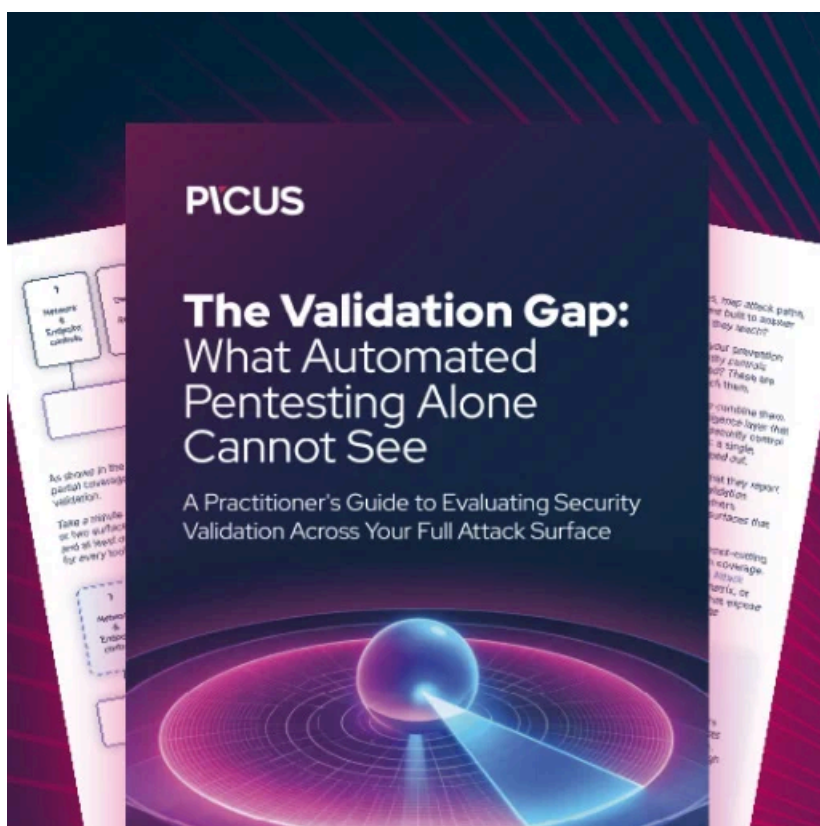


FuxSociety Ransom Note

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 actually given prioritized encryption.



[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/new-fuxsocy-ransomware-impersonates-the-notorious-cerber/>