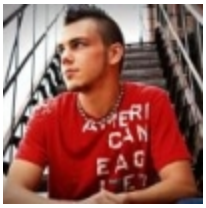
TorrentLocker Ransomware Cracked and Decrypter has been made

bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/

DecrypterFixer

- 
- Security Colleague
- 1,617 posts
- OFFLINE

- Gender:Male
- Location:Florida
- Local time:07:15 PM

Update 12/4/14: Dedicated guide with all known information can be found here:

Added new information guide and FAQ:

TorrentLocker (fake CryptoLocker) Ransomware Information Guide and FAQ

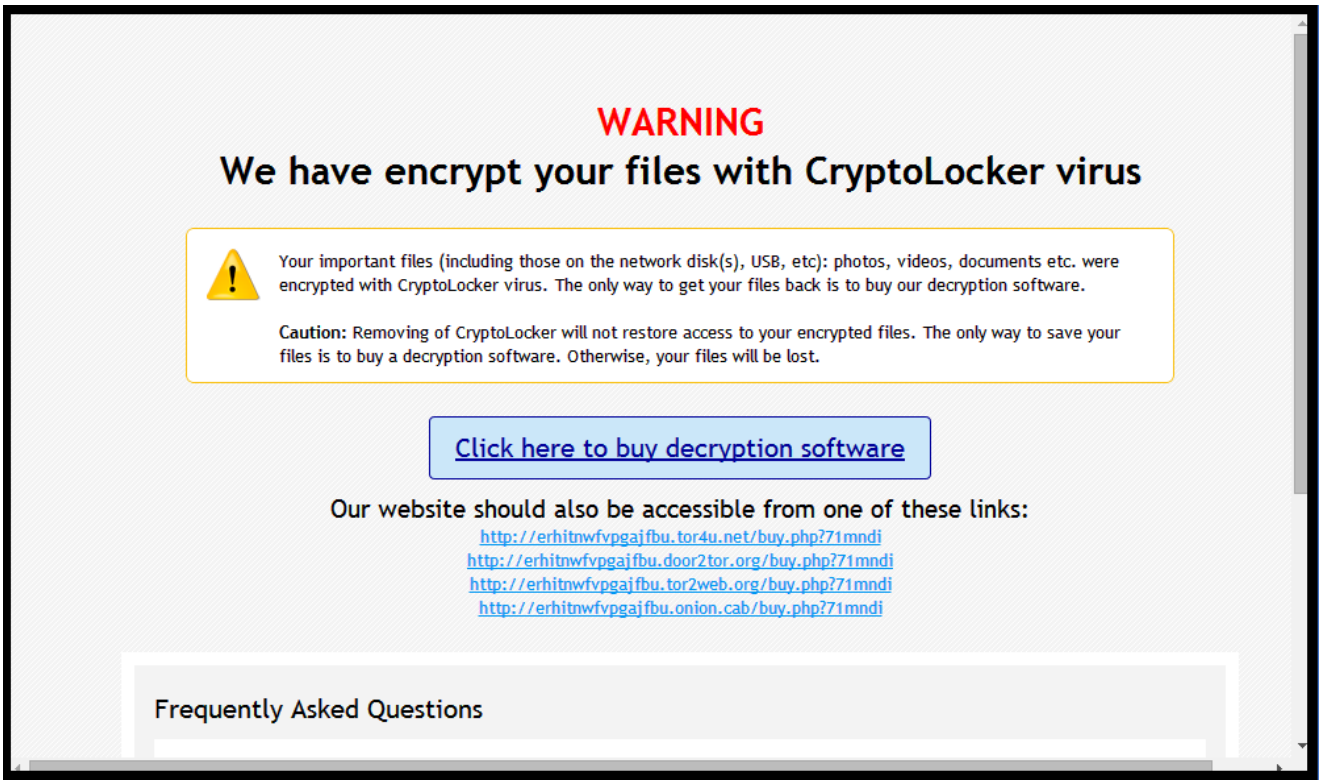
Also contains country specific information. If you are from a country listed, or not listed, and have further info please feel free to shoot me a PM.

http://www.bleepingcomputer.com/virus-removal/torrentlocker-cryptolocker-ransomware-information#regions

The easy decryption method in TorrentLocker has been fixed by the developer. We have no way of decrypting your files anymore.

--
The Bleeping Computer Staff

** Visitors looking for just the Decrypter and not the TorrentLocker Analysis can Download and read about it at the bottom of the page or download it from **Here** **



Main Startup Window and Ransom Note

TorrentLocker Decrypted

On Aug. 12th 2014, a new sample was sent to me with the victim claiming it to be **CryptoLocker**. Upon running and quickly analyzing the exe, I found that it was a new Encrypting Ransomware (Whats new?). This infection claimed to be **Cryptolocker**, but also used the Ransom File Format of **Cryptowall**. I would guess the reason behind this was to gain fear in the victim when infected as those 2 Ransomware's are uncrackable. After running through my normal checks when first getting a Encryption infection sample, I started my not so normal ones. I made it a unwritten rule to myself that before trying to figure out hard encryption schemes the infection may use, to always try the easy ones quickly first. This means testing a encrypted file for **MD5**, **SHA-1**, **RC2**, **RC4**, **XOR, Bit Shift** and other lower encryption schemes first. (I started doing this because of **Cryptorbits** simple encryption that I spent far to long on.)

After going through the list, my jaw about dropped to the floor when I hit XOR. The virus creator of this infection used a simple (and I mean nothing else) XOR algorithm. I found this by taking a encrypted file and XOR'ing its bytes with the good files bytes. This produced a file with a 2MB key buffered with zero's at the bottom. The zeros happen because the infection only encrypts the first 2MB of files. When taking the 2MB key and XOR'ing it with a different encrypted file, it was successfully decrypted.

Xor Key Sample File (2MB)

After finding this out, seeing as how it is such a simple mistake, I knew I had to keep it quite and just build a public application for victims to use without disclosing how it works, as the virus creator would simply fix the issue. So for the last few weeks I have been spending time making the decryption application for the victims, but it seems that a few bloggers didn't feel the same way (Again, Whats new?)

2 days ago **Digital-forensics Blog** decided that after also finding out this information, to post it publicly that there was a "*mistake on the malware author's part*", and continued to describe in detail what those mistakes were, and also gave the virus creator some pointers! One thing they did not do though is post a way for any victims to decrypt their files after now alerting the virus creator that he made a mistake.

Since then the story has circled around and has been posted on multiple blogs, making almost certain that if the virus creator didn't know, he does by now.

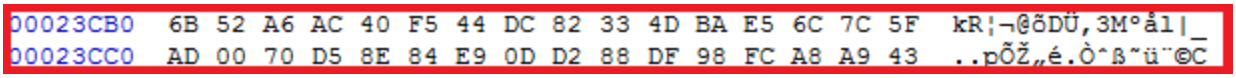
TorrentLocker Details

To go into a little more detail about this infection, When ran it Inject itself into a new instance of Explorer, Query all Logical Drives, and loop through each drive encrypting each file it finds that has the below extension and adding .Encrypted to the end.

TorrentLocker Effected Extensions:

```
*.wb2,*.psd,*.p7c,*.p7b,*.p12,*.pfx,*.pem,*.crt,*.cer,*.der,*.pl,*.py,*.lua,*.css,*.js
journal,*.db,*.cls,*.bdb,*.al,*.adb,*.backupdb,*.bik,*.backup,*.bak,*.bkp,*.moneywell,
```

The viruses Import table consists of: NTDLL.DLL, SHLWAPI.DLL, WININET.DLL, CRYPT32.DLL, MAPI32.DLL, KERNEL32.DLL, USER32.DLL, ADVAPI32.DLL, SHELL32.DLL, OLE32.DLL, and OLEAUT32.DLL. The virus actually uses an open source Lib to assist in the encryption which is named **LibTom**. Alot of these bloggers seem to think that the virus creator used AES or another advance encryption to generate the XOR key, and simply forgot/ignored to used the key with a advanced encryption before using XOR. Yet, the code proves otherwise. The author simply uses a 32 byte seed to generate the 2MB key stream, and its used to XOR the file. Simple as that.



Example of 32 Byte Seed

File List:

C:\Windows\<Random>.exe - Duplicate infection EXE

***\DECRYPT_INSTRUCTIONS.HTML - Ransomnote (Dropped in any encrypted folder)**

%ProgramData%\<Random>\<Random> - Temp file for the infection (No Extension)

Registry List:

HKCU\Software\<Random>\01000000 - Hex of infection

HKCU\Software\<Random>\02000000 - Path to infection exe

HKCU\Software\<Random>\03000000 - UID for infection

HKCU\Software\<Random>\04000000 - HTML Document in hex

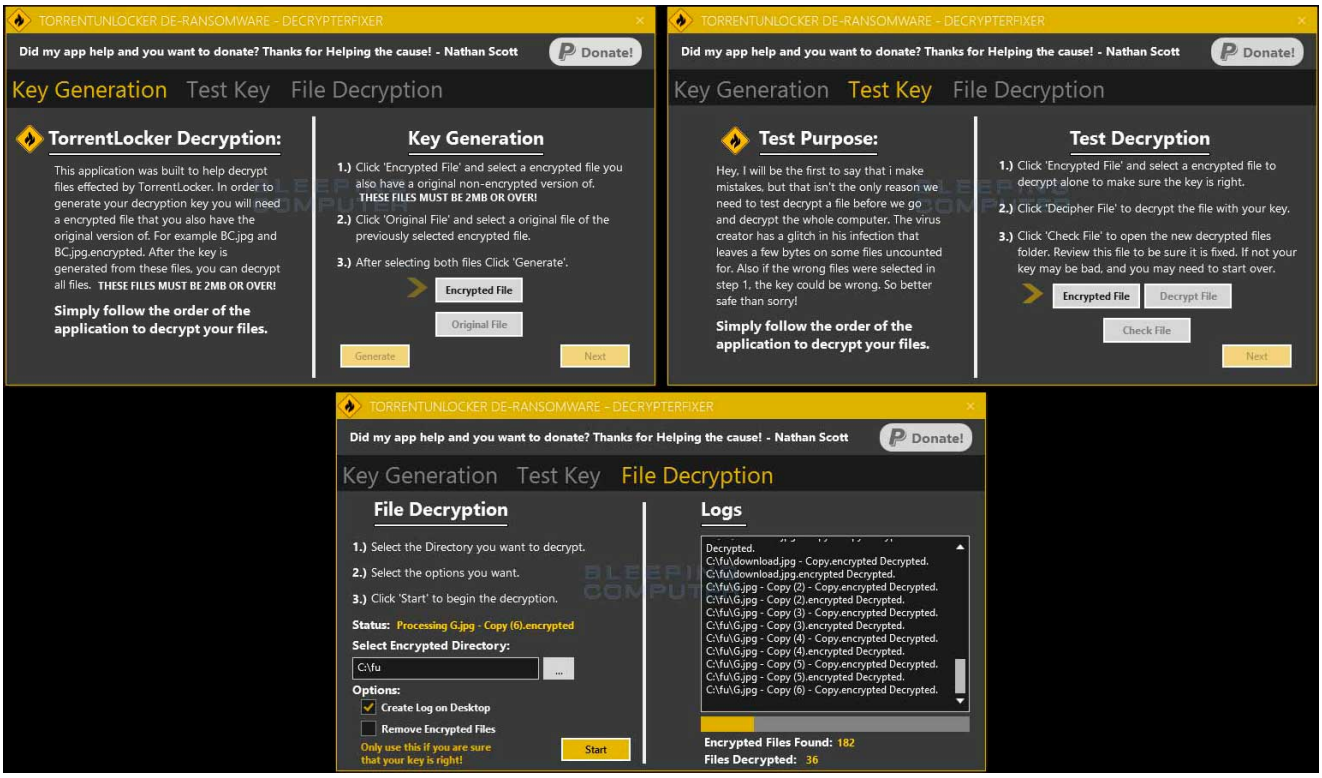
HKCU\Software\<Random>\05000000 - Number of infected files

C&C List:

Https://server38.info/gate.php

Note: It is also important to mention that this infection will not infect a computer without contacting its C&C server.

TorrentLocker Decrypter



To download TorrentUnlocker, Please use the following link:

TorrentLocker De-Ransomware V1.0.5.0

Once the file has been downloaded, run the **TorrentUnlocker.exe** program. This will open the main window seen above, then simply follow the instructions.

If you need any help with TorrentUnlocker please message me, Nathan (DecrypterFixer)

This is V 1.0.5.0 of TorrentUnlocker De-Ransomware. This software will help you decrypt files that were effected by TorrentLocker. There is a catch though! In order to use this Decrypter, you must have a Original version of a encrypted file that is at least 2MB. Lets say I have a image on my DropBox that is untouched by the infection named "**Family.jpg**" that is over **2MB**, and that I had a copy of it on my local computer when the infection hit. To use this app, all I would need is that "**Family.jpg**" and the "**Family.jpg.encrypted**" on my local computer.

This application requires .NET 4.0, but has it packaged inside. So if you do not have .Net 4.0, it will install it for you. Even more important is, this application relies on you to give it the correct files to make the TorrentLocker key. That means if you mess up, it messes up. So it is ALWAYS recommended to run this application on a folder with copies of your encrypted files first! Once everything is confirmed to be okay, then you may select your whole drive.

** This application also has step by step guide arrows to help you glide through decrypting your files with ease. If you ever find yourself confused on what the next step is, Simply look for the blinking arrow to continue.*

A newer version will be coming soon with the following features to help victims more:

- **Resize ability**
- **Support for files over 4GB**
- **Auto Correct Key detection**

Thanks for reading!
Edited by Grinler, 10 December 2014 - 06:02 PM.

- Back to top

Community Forum Software by IP.Board