COMPUTER SECURITY BULLETIN

Risk/Impact Rating: SERIOUS

< VirLocker Ransomware >

CSB17-007

Description:

VirLocker was the first example of a mainstream polymorphic ransomware and it left no expense of misery to its victims. It is also a perfect example of data-blocking Ransomware. Its main activities after it has infected your machine include:

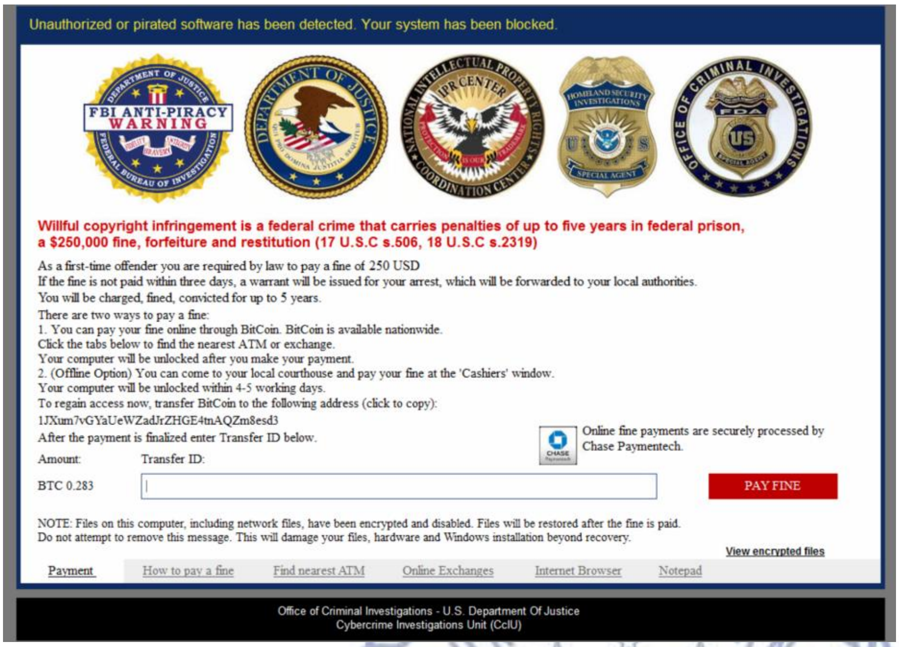
- Completely scanning your hard disks and drives;
- Compiling a list with all the files that have currently been in use;
- Locking up every single file from the aforementioned list with a very difficult to crack encryption key;
- After all the data has been encoded – generating an extremely disturbing ransom alert; and
- Normally, such a ransom-demanding message will include threats to further motivate you to pay the demanded ransom; some payment details and a deadline.

Every file that VirLocker touches becomes VirLocker itself. When getting infected by VirLocker, you can no longer trust a single file that is on the affected machine.

VirLocker will attempt to infect the new file before it is even opened if VirLocker is running on the machine.

VirLocker can add “Fake Code” to itself in certain sections to cause the file to be different, it can use different API’s in the main loader of the malware to avoid section fingerprinting, it can use different XOR and ROL seeds to make the encrypted content of the exe entirely different, and more.

If you find yourself infected with VirLocker and want your files back, DON’T REMOVE IT RIGHT AWAY. We need to trick the infection. If you have removed the infection, clicking on any of the “encypted/infected” files will bring up the screen again that VirLocker uses.



Unauthorized or pirated software has been detected. Your system has been blocked.

FBI ANTI-PIRACY WARNING
DEPARTMENT OF JUSTICE
NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER
HOMELAND SECURITY INVESTIGATIONS
SPECIAL AGENT
OFFICE OF CRIMINAL INVESTIGATIONS
FDA
US

Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C s.506, 18 U.S.C s.2319)

As a first-time offender you are required by law to pay a fine of 250 USD
If the fine is not paid within three days, a warrant will be issued for your arrest, which will be forwarded to your local authorities.
You will be charged, fined, convicted for up to 5 years.
There are two ways to pay a fine:
1. You can pay your fine online through BitCoin. BitCoin is available nationwide.
Click the tabs below to find the nearest ATM or exchange.
Your computer will be unlocked after you make your payment.
2. (Offline Option) You can come to your local courthouse and pay your fine at the 'Cashiers' window.
Your computer will be unlocked within 4-5 working days.
To regain access now, transfer BitCoin to the following address (click to copy):
1JXum7vGYaUeWZadJrZHGE4tnAQZm8esd3
After the payment is finalized enter Transfer ID below.

Online fine payments are securely processed by Chase Paymentech.

Amount: BTC 0.283
Transfer ID:

PAY FINE

NOTE: Files on this computer, including network files, have been encrypted and disabled. Files will be restored after the fine is paid.
Do not attempt to remove this message. This will damage your files, hardware and Windows installation beyond recovery.

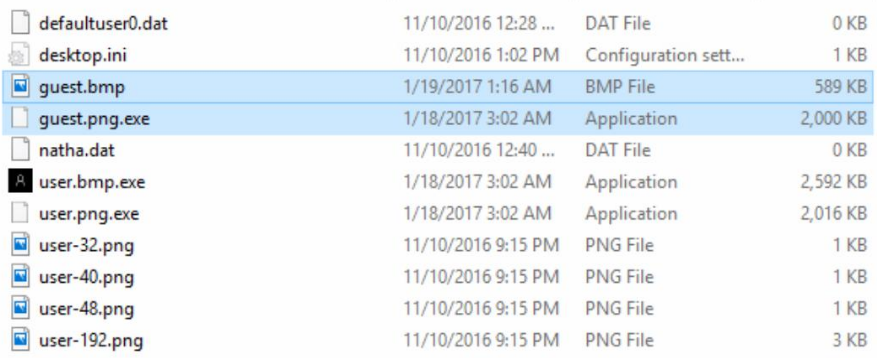
Office of Criminal Investigations - U.S. Department Of Justice
Cybercrime Investigations Unit (CcIU)

VirLocker has screens that look like in the left. They seem to always impersonate some type of legal authority. This one claims to be the Office of Criminal Investigation, where past versions called themselves "Operation Global 3" with different legal emblems.

The important part is the "Transfer ID:" text-box. Researchers found that any 64-length string will be accepted here as a real payment on this latest version of VirLocker. So, on your infected machine type the following into the Textbox:

0000000000000000000000000000000000000000000000000000000000000000
(That is 64 Zero's)

Then, hit "Pay Fine". This will cause the Ransom Lock Screen to disappear. VirLocker now thinks you have paid the ransom. So, any of your infected files, upon double clicking them to open them, will no longer start the ransomware, but instead extract the original file inside of it.



defaultuser0.dat	11/10/2016 12:28 ...	DAT File	0 KB
desktop.ini	11/10/2016 1:02 PM	Configuration sett...	1 KB
guest.bmp	1/19/2017 1:16 AM	BMP File	589 KB
guest.png.exe	1/18/2017 3:02 AM	Application	2,000 KB
natha.dat	11/10/2016 12:40 ...	DAT File	0 KB
user.bmp.exe	1/18/2017 3:02 AM	Application	2,592 KB
user.png.exe	1/18/2017 3:02 AM	Application	2,016 KB
user-32.png	11/10/2016 9:15 PM	PNG File	1 KB
user-40.png	11/10/2016 9:15 PM	PNG File	1 KB
user-48.png	11/10/2016 9:15 PM	PNG File	1 KB
user-192.png	11/10/2016 9:15 PM	PNG File	3 KB

In this image, clicking on the infected file "guest.bmp.exe" extracted the "guest.bmp" file, which is the original good version of the file. You may now use a non-important USB drive to back up all the files that are important and that you need recovered from this nasty infection.

Recommendations / Solutions / How To's:

NEVER put any .EXE files onto your backup drive, this can cause the infection to spread. Only backup the extracted original files. And perform this action ONLY on the machine you entered the "0's" on the lockscreen. Opening the EXE files on any other machine will infect them.

To avoid this type of infection in the future, use anti-ransomware solution that has anti-ransomware functionalities built into it. Also:

- Avoid all the emails you have received and you are unable to recognize. Be especially careful with the ones with strange titles or bad writing style;
- Do not download any email attachments – even images and text documents may be infected with data-locking up malware;
- Avoid clicking on a link on a website or in a chat message if you aren't absolutely sure the sender is trustworthy;
- Stay away from all the pop-ups that you come across on the web; and
- Sometimes you may receive a desktop notification stating that you need to update a component of your system – avoid such messages. Manually check for updates as sometimes these may be malware-containing pop-ups.

References:

https://blog.malwarebytes.com/threat-analysis/2017/01/virlockers-comeback-including-recovery-instructions/

https://howtoremove.guide/virlocker-ransomware-removal/

https://securityintelligence.com/news/new-virlocker-ransomware-is-easily-fooled/

https://www.scmagazine.com/virlocker-ransomware-resurges-but-a-solution-is-offered/article/633964/

*For dissemination to All PNP Personnel