Urgent Warning: Cypto Virus

Crypto Virus | Tech Tips Podcast by PcCG

Subscribe via Itunes [1] | Subscribe via RSS [1]

Download Crpyto-Preventer Program [2]

Sadly, a new virus has been spreading around the internet in the past few months and has come to a climax recently. It is known as the **"crypto virus,"** another style of "ransomware".

If you have been infected with this, you should disconnect your computer from the internet immediately in an attempt to minimize damage, though it may already be too late.

The crypto virus is spread primarily via Email, usually as fake UPS or Fedex notifications with tracking numbers. Once you click on the tracking numbers, you can download and infect your system.

Once the system is infected, the virus encrypts files on your computer. These encrypted files are locked from you, and you are given time (usually 100 or 72 hours) to pay the ransom to get your files back. The ransom is typically $100 or $300.

Reports from infected parties do say they typically did regain access to their files after paying the ransom.

There is, of course, a moral component that one must consider on an individual level. By paying the ransom, you may be funding activities and organizations such Al-Queda, Semolian pirating or other nefarious groups. We do not know where this has come from; nor do we know where the money is going. This is something to consider.

A list of encrypted files can be found by using this community generated program: ListCrilock.exe [3]

Some have been able to recover files without paying the random via a program written by Fabian Wosar. You can download that file here: decrypt_mdlblock.exe [4]. Further instructions can be found by Fabian's post found on bleepingcomputer.com [5]

Others claim it is impossible to recover files without paying the ransom. This likely indicates different variants, or "look-alike" viruses.

Another alternative solution is to recover files from a backup or from Windows Shadow Copy. Windows has a feature built in to many versions that allow the computer to automatically make copies of a file when it's modified for a backup - should you want to revert to an older version. This however is not always available. You can try Shadow Explorer [6] for an easy way to view any shadow files that can be used to replace the corrupted files.

Some of the look-alike viruses don't actually encrypt your files, they only pretend to have encrypted files. In these situations, it's possible to clean the infection like any other virus.

To remove the virus, it has been reported that Norton Power Eraser [7] will do the job. Note however it is possible that Power Eraser can cause problems with the computer and should be used with caution. Essentially, it's a chance you take; most of the time yielding positive results. However it's important to understand removing the virus WILL NOT decrypt or unlock your files. Files should be decrypted (if possible by paying the ransom or the using the program listed above) before removing the infection.

Prevention is always preferred.
Simply use a GOOD Antivirus (we recommend Norton Internet Security), keep your system up to date (specifically Windows, Java and Adobe) and back up your computer to recover from such disasters.

We have a detailed, albeit lengthy video that demonstrates how to avoid fake emails [8] such as the Crypto Virus email. If you have not already watched this video, now may be the time to consider watching it. I will say it is not the most entertaining video, but very worth it in terms of security.

Tech Tips [9]
Tech Tips Articles [10]
Tech Tips Podcasts [11]

Links
[1] http://pccomputerguy.com/podcast/feed.xml [2]
https://www.pccomputerguy.com/downloads/CryptoPreventerSetup.exe [3]

https://www.pccomputerguy.com/images/crypto/ListCrilock.exe [4]
https://www.pccomputerguy.com/images/crypto/decrypt_mblblock.exe [5]
http://www.bleepingcomputer.com/forums/t/494759/decrypt-protect-ransomware/page-3 [6]
http://www.shadowexplorer.com/ [7] https://security.symantec.com/nbrt/npe.aspx [8]
http://www.pccomputerguy.com/Tech-Tips-Video-Spot-Fake-Emails-Phishing-Viruses [9]
https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips [10]
https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Articles [11]
https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Podcasts