## Crypto Malware – How to live with it & what to do

Ever since the late eighties when PC's emerged, PC users have been trying to avoid virus & malware
Issues: https://en.wikipedia.org/wiki/Stoned_(computer_virus)

Nowadays we have high speed modems and the number of PC's, users and programs has continued to grow exponentially, as have the threats. Variations of Cryptolocker Malware is the latest problem that not only can cause an entire companies computer system to go down but can also make the authors money. (When a user pays the Ransom)

The only way to try and stop or at least not support such Malware is to Not Pay the Criminals.
I've been a member of Tech Republic since mid 1990's, I visited their site when I was formulating this article and even they mention paying ransom.

Ransomware-as-a-service is exploding: Be ready to pay:
http://www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/

They recommend:
http://www.techrepublic.com/article/10-tips-to-avoid-ransomware-attacks/
To prevent a ransomware attack, experts say IT and information security leaders should do the following:-

1. Keep clear inventories of all of your digital assets and their locations, so cyber criminals do not attack a system you are unaware of.
2. Keep all software up to date, including operating systems and applications.
3. Back up all information every day, including information on employee devices, so you can restore encrypted data if attacked.
4. Back up all information to a secure, offsite location.
5. Segment your network: Don't place all data on one file share accessed by everyone in the company.
6. Train staff on cyber security practices, emphasizing not opening attachments or links from unknown sources.
7. Develop a communication strategy to inform employees if a virus reaches the company network.
8. Before an attack happens, work with your board to determine if your company will plan to pay a ransom or launch an investigation.

9. Perform a threat analysis in communication with vendors to go over the cyber security throughout the lifecycle of a particular device or application.
10. Instruct information security teams to perform penetration testing to find any vulnerabilities.

Really items 3 & 4 are the most important and can easily be practised by the average MelbPC user today. Microsoft Backup became usable When Windows 7 came out however I personally still prefer using a single 3rd party backup application.

The Free total backup solution for any Windows platform I recommend is Macrium Reflect: http://www.macrium.com/reflectfree.aspx
(I won't go into any more detail about this now but if you want more info, contact the iHelp Team or locate the iHelp article on this subject.)

Manual Disinfection of a PC that has such software running is certainly possible, however recovering data that has already been encrypted is not. You could choose to pay the authors of the Malware but even then, there is no guarantee. The solution to this threat is always to have at least two backups and at least one if not both should not remain connected to your PC or the Network.

Here is a list of instructional videos on removing some of the various strains of this type of Malware.
Britec Ransomware removal page
https://www.youtube.com/playlist?list=PL302CE7037FD86F7B

If you are interested to see Cryptolocker in action, lease view the following short clip made by Sophos, in order help sell their software.
Sophos Watch CryptoLocker in action
https://www.youtube.com/watch?v=Gz2kmmsMpMI

CryptoLocker Ransomware What You Need To Know
https://www.youtube.com/watch?v=FoNTXTyly-s&feature=youtu.be

In the above video Brian of Britec Computers in the UK references two bits of software in particular.
The very good and free Crypto Prevent tool made by FoolishIT in the U.S. and ShadowExplorer.

Crypto Prevent tool
https://www.foolishit.com/cryptoprevent-malware-prevention/

I purchased and run the Crypto Prevent software on my main PC. I purchased it because I like buying good software that works (as you saw in Brian's video), so as to encourage the writing of more software and so I am entitled to receive updates to the software. This type of Malware is changing and evolving all the time and it pays to at least try to keep up. I found it did not detrimentally affect the speed of using my PC at all.

Shadow Explorer
www.shadowexplorer.com
Since the Volume Shadow Copy Service is included, and turned on by default, in all editions of Windows Vista / 7 / 8, why not take advantage of it? All it takes is an additional tool like ShadowExplorer, that can access the shadow storage and make the point-in-time copies accessible to the user.

Using the above tool(s) along with maintaining a sensible backup regime will prevent you from falling victim to this new and currently evolving menace on the Web.

DS Aug 2016