Practice Resource

The Law Society of British Columbia

Cryptolocker Ransomware Alert

Firms cautioned after two BC law firms hit with Cryptolocker ransomware

Cryptolocker Ransomware is malware that is typically installed by clicking on an attachment to an email, by watching an infected video on the internet or by using an infected USB flash drive. Emails will appear to be legitimate and purport to be from government departments, banks, delivery companies such as FedEx, major corporations or even friends. The attachments may appear to be PDFs, but if you look carefully they may have "PDF.exe" extensions at the end of the file name, which indicates that they may actually be dangerous executable files. (An executable file is generally used for installing software, but is also capable of causing a computer to perform tasks.) The executable file installs the malware without your knowledge or consent.

Once it has infected your system, the malware starts encrypting important files on your computer and network. It can spread to every computer on the network and, in some cases, to backups, external hard drives and USB flash drives if the devices are connected. Once fully infected it locks up most, if not all, of your important files and computers. It may also scan your system for passwords and credit card numbers and pass that information back to the malware developers (but this doesn't seem to be typical behaviour of this particular malware).

Cryptolocker uses a dual key (public/private) encryption method, which means that unencrypting the files is impossible without the private key. This is where the ransom part comes into play: after infection the malware displays an announcement demanding a ransom within a set time (typically about $300 to $2,000 within 72 hours). Sometimes payment is required to be in Bitcoin, which is an untraceable electronic monetary system. If you fail to pay the ransom, the malware will disappear from your system leaving your important files still encrypted – and unusable. The ransom notice may appear to come from the government or the police, but this is not the case. Do not be mistaken – this is malicious software. Paying the ransom may – or may not – remove the malware and there is no guarantee it will not re-infect your system in the future.

In the cases of the two firms that were hit, one paid the ransom (and recovered their files) and the other did not. The firm that did not pay was fortunate to recover its accounting data, which had been stored in a zip file that escaped infection.

There are websites and anti-virus software on the internet that purport to be able to remove the malware (such as the free tool available from Sophos at www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx), but unless you have the private encryption key, your data will still be fully encrypted and useless to you. This can include all your Microsoft files (Word, Excel, PowerPoint), PDFs, and all trust and general accounting data. Graham Cluey (grahamcluley.com/2013/11/cryptolocker-protect/) reports that the malware can encrypt the following types of files:

> *.jpe, *.jpg, *.3fr, *.accdb, *.ai, *.arw, *.bay, *.cdr, *.cer, *.cr2, *.crt, *.crw, *.dbf, *.dcr, *.der, *.dng, *.doc, *.docm, *.docx, *.dwg, *.dxf, *.dxg, *.eps, *.erf, *.indd, *.kdc, *.mdb, *.mdf, *.mef, *.mrw, *.nef, *.nrw, *.odb, *.odc, *.odm, *.odp, *.ods, *.odt, *.orf, *.p7b, *.p7c, *.p12, *.pdd, *.pef, *.pem, *.pfx, *.ppt, *.pptm, *.pptx, *.psd, *.pst, *.ptx, *.r3d, *.raf, *.raw, *.rtf, *.rw2, *.rwl, *.sr2, *.srf, *.srw, *.wb2, *.wpd, *.wps, *.x3f, *.xlk, *.xls, *.xlsb, *.xlsm, *.xlsx, img_*.jpg

How can you best protect yourself? Here are ten steps that you can take:

1. Only open attachments that you trust. If you are at all suspicious, contact the sender directly (do not use the telephone number in the suspect email) to verify the bona fides of the message and the attachment.

2. When you backup your system, disconnect the device from your network after the backup is complete. This isolates the backup and it *may* allow you rebuild your system by using the data backup (once your system has been cleansed of the malware) without paying the ransom.

3. Maintain effective anti-virus software that includes anti-malware protection, and keep it up to date. You can run a deep scan using a reputable internet anti-virus system at any time to see if you have malware (or other threats) on your system. Websense (www.websense.com/content/websense-technologies.aspx) is one company that claims its product can stop the Cryptolocker malware.

4. Restrict the ability of users to install software. This may prevent the malware from being installed in the first place.

5. Use software that stores a complete backup in the cloud. If you are hit with the malware, you *may* be able to go back and restore from the cloud backup if it has not been infected.

   The Winter 2014 *Benchers' Bulletin* article entitled "Time for Robust Backups" lists a number of Canadian cloud-based backup storage companies.

   The Law Society has also published the following resources:

   - Cloud computing due diligence guidelines
   - Cloud computing checklist

6. Consider using tools that are specifically designed to minimize the threat from CryptoLocker malware. Krebs on Security, an internet and security expert (krebsonsecurity.com/2013/11/how-to-avoid-cryptolocker-ransomware/#more-22877), reports:

    > A team of coders and administrators from enterprise consulting firm thirdtier.net have released the CryptoLocker Prevention Kit – a comprehensive set of group policies that can be used to block CryptoLocker infections across a domain. The set of instructions that accompanies this free toolkit is comprehensive and well documented, and the group policies appear to be quite effective.

7. Upgrade your computers from Microsoft XP. Some experts feel that this older operating system (which will be unsupported by Microsoft after April 8, 2014 anyway) may be more vulnerable to malware attacks than Windows 7 or 8.

8. Have an IT professional conduct a security audit to determine if your system meets current protection and backup best standards. Remember that Cryptolocker is just one of many types of malware; others track every keystroke and collect bank logins, passwords and other information that can lead to identity theft. And if you are hit with any malware, immediately turn off all computers to prevent it from spreading any further, then call a professional to help you deal with the infection.

9. Use strong and different passwords for each site that requires them. Gibson Research Corporation has a strong password generator that will create a completely random 63-character password for you each time you enter (www.grc.com/passwords.htm). LastPass or similar service providers keep all those strong and unique passwords organized for you (lastpass.com/index.php?fromwebsite=1).

10. Consider buying insurance to protect you and your firm from these risks. Talk to a broker about cyber-insurance policies available from commercial underwriters.