CryptoLocker and CryptoWall: The Threat of Ransomware

by Brian Mauch, President of BMC Networks

Imagine trying to open an important document on your network, only to find that the document has been encrypted by a malicious virus or other type of malware. You receive a prompt that your file will only be unencrypted if you pay a fee to an untraceable account. How did this happen? What can you do to get your file back? Most importantly, what could you have done to help prevent this from happening in the first place?

This scenario is playing itself out in many businesses, including local law firms. The original malware of this sort was called CryptoLocker, which first appeared in September 2013. Since then, different variants of this attack, such as CryptoWall, have been developed and released by malicious programmers on an unsuspecting public.

In December 2014, the Law Society of British Columbia released a Notice to the Profession that warned law firms about this type of fraud, suggested methods to protect their computer systems, and reminded lawyers of their obligations to keep a client's information confidential.

HOW DID THIS HAPPEN?

CryptoLocker and its variants are usually transmitted via infected email attachments or links in malicious emails, which are sent by multiple infected computers called botnets. The emails often pretend to be about customer support related issues from financial institutions, government agencies, or courier companies. The attachments are often executable ZIP files disguised as PDF files. If an infected email attachment is opened and antivirus software is either not present or ineffective against that variant, the computer is infected. Computers can also become infected if the user visits websites that are serving malicious ads which deliver the ransomware when clicked on.

Once infected, a computer begins encrypting files on the local hard drive and mapped network drives. It encrypts one folder at a time, and can take hours to encrypt large collections of files.

WHAT CAN YOU DO TO GET YOUR FILE BACK?

Once a CryptoLocker variant is identified, the first thing to be done is to identify which computer(s) are infected, and disconnect them from the network so they stop encrypting files. These computers should have the malware completely removed before they are connected back to the network. Sometimes antivirus software can remove the infection, but if you're unsure whether removal was successful, the safest course of action is to backup any data, reformat the computer's hard drive, and reinstall the operating systems and applications.

The next step is to identify which folders have been encrypted, which can be a time-consuming process. Encrypted files should then be restored from a recent backup. If backups are not available, paying the ransom

...continued on page 15

Ransomware... continued from page 14
often results in the files actually being unencrypted. According to a report from Dell, the original version of the CryptoLocker collected an estimated $30 million in paid ransom for its creators.

WHAT COULD YOU HAVE DONE TO HELP PREVENT THIS?

Unfortunately, there isn't one "silver bullet" that will protect your firms against computer malware. No antivirus software is 100% effective – the very best are usually no higher than 98% effective. The reason for this is that new malware and variants are being created every day. Antivirus developers do their best to identify new threats and update their protection, but there will always be a time lag between the creation of malware and the time when a given computer receives an antivirus update. Moreover, even the best antivirus applications have difficulty detecting CryptoLocker/Wall variants.

Since there isn't one effective shield, a five-fold approach to prevention works best:

1. Educate users to not open suspicious attachments, and confirm with (even normally reliable) senders before opening an clicking a link in an unexpected email;
2. Have a reputable antivirus application installed on all computers, and keep the antivirus application updated;
3. Protect your network connection with a gateway firewall that has antivirus capabilities, and keep the firewall updated;
4. Utilize an external firewall service such as OpenDNS Umbrella, which blocks outgoing requests to known malicious IP addresses; and
5. Above all, ensure your files are backed up regularly and reliably.

Some industry experts think that ransomware like CryptoLocker will be the future of cybercrime, in that the infection offers the end user a means with which to remove the threat and recover their files in exchange for paying a ransom. Therefore, it is vitally important to take every reasonable measure to protect your firm's network, and to educate your users about the possible dangers.

Brian Mauch, LL.B., is the President of BMC Networks, an outsourced IT provider of cloud and on-premises solutions for law firms. For more information, email Brian at bmauch@bmcnetworks.ca

SAVE THE DATE

BCLMA Annual Summer Social Reception
Thursday, June 4, 2015 from 5:15 pm - 7:30 pm
Bridges Restaurant, Granville Island

For more information, visit www.bclma.org

Stay tuned: more Information coming soon
BCLMA Biennial 2016 Conference
March 2nd – Wednesday evening - *Kick-off event*
March 3rd – Thursday – *one full day with speakers, workshops, trade show and wind-up dinner*