PRACTICE TIPS, by Dave Bilinsky, Practice Management Advisor

Dealing with Cryptowall ransomware

> ♫ *Tired, frustrated …*
> *I think I'm hitting the wall … ♫*
>
> Music and lyrics by Adrenaline Mob

THE LAW SOCIETY issued a Fraud Alert on December 31, 2014 concerning the Cryptowall virus ransomware. This article expands on the information in that notice.

WHAT IS IT?

According to Wikipedia:

> **Ransomware** is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive (cryptoviral extortion, a threat originally envisioned by Adam Young and Moti Yung), while some may simply lock the system and display messages intended to coax the user into paying.
>
> While initially popular in Russia, the use of ransomware scams has grown internationally; in June 2013, security software vendor McAfee released data showing that it had collected over 250,000 unique samples of ransomware in the first quarter of 2013 – more than double the number it had obtained in the first quarter of 2012. CryptoLocker, a ransomware worm that surfaced in late-2013, had procured an estimated US$3 million before it was taken down by authorities.

There are at least three different types of ransomware. The first is software that appears to have detected something nasty on your computer and demands that you buy a clean-up tool to "remove" it. This is really bogus ransomware and typically can be removed from a computer without too much effort.

The second type of ransomware displays what appears to be a notice from the police or other authorities and demands payment of a fine since you have "illegal" content on your computer (typically copyrighted materials or porn). Again, this type of ransomware should not be too difficult to remove by someone with an IT background.

The third type of ransomware, most commonly known as Cryptowall or Cryptolocker, is much more dangerous and malicious, and is the focus of this article. It has infected at least seven BC lawyers' systems over the last while.

WHAT IS CRYPTOWALL?

According to Techrepublic:

> CryptoWall is classified as a Trojan horse, which is known for masking its viral payload through the guise of a seemingly non-threatening application or file. Its payload involves encrypting the files of infected computers in an effort to extract money for the decryption key.

A Trojan horse is, as the name suggests, a malicious application wrapped up in sheep's clothing. It works by tricking you into clicking on what you think is an innocent attachment from a trusted source. The exact opposite is true.

WHERE DOES IT COME FROM AND HOW IS IT SPREAD?

Techrepublic continues:

> Geographically speaking, that is unknown as of this writing. What is known regarding origins of infection is that CryptoWall is most typically spread through email as an attachment and from infected websites that pass on the virus – also known as a drive-by download.
>
> Additionally, CryptoWall has been linked to some ad sites that serve up advertising for many common websites users visit on a daily basis, further spreading its distribution.

HOW PREVALENT IS IT?

According to Secureworks.com, the top 10 countries infected with CryptoWall are:

Country	Infected systems
United States	253,521
Vietnam	66,590
United Kingdom	40,258
Canada	32,579
India	22,582
Australia	19,562
Thailand	13,718
France	13,005
Germany	12,826
Turkey	9,488

As you can see, it is not a trivial threat.

WHAT DOES IT DO?

Once it is on a computer, it searches for and encrypts files located within shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives (there are reports of Dropbox files being encrypted by the malware).

The malware uses a very strong public/private encryption key and uploads the private encryption key to a "command and control" server, placing the private key required to unencrypt the files out of the victim's reach.

It starts out demanding a ransom (typically around $500 USD or 1 Bitcoin) and may increase the amount as the deadline for payment nears. It may also offer de-encryption after the deadline for yet a higher ransom.

HOW DO YOU PREVENT IT?

The important things to realize about this malware are:

- Once it encrypts your files, there is no way to "unencrypt" them without paying the ransom and receiving the private key. The length of the encryption key (reported to be a 2048-bit RSA key pair) is such that a "brute force" attack will not succeed to break the encryption in the time allotted to pay the ransom.
- While it is reasonably easy to remove the malware from your system using known tools, this does not affect the encrypted files. Removal of the malware still leaves your files encrypted and unavailable to you.
- In talking with the firms that have been hit, even the best internet security and anti-virus software suites have not stopped this malware from infecting their computers and systems. In spite of what these security suites may state on their websites, the malware has succeeded in attacking systems that were protected by Kaspersky, Microsoft Security Essentials, McAfee and others. Many security suites claim that they can remove the malware and, doubtless, many of them do. However, what they do not say is that removal of the malware does not de-encrypt the infected files.
- After having done an exhaustive search of the internet, I could not find anyone who reported a reputable tool to break the encryption on the infected files. You are left with a Hobson's choice: either pay the ransom (which may or may not result in your encrypted files being unencrypted), or not. If you do not pay the ransom, you will be left to recover or recreate the files that are now lost to you.
- The best way to deal with this malware is by taking preventive measures. Once your system is hit, it is really a matter of damage control.
- Keep your operating system current and fully up to date. One firm that was infected was still using Microsoft XP well after April 8, 2014, which was the date that Microsoft stopped supporting this operating system. As Microsoft states:

  > If you continue to use Windows XP now that support has ended, your computer will still work but it might become more vulnerable to security risks and viruses. Internet Explorer 8 is also no longer supported, so if your Windows XP PC is connected to the internet and you use Internet Explorer 8 to surf the web, you might be exposing your PC to additional threats.

- Do not allow peer-to-peer file sharing applications on your network.
- Disable autorun on your Windows computers on network drives and USB ports. This will prevent malware from being introduced using this function.
- Be very careful about opening attachments to emails or other messages (including instant messaging). In some of these cases, the malware appears to have been an executable file masquerading as a PDF attachment to an email. Once opened, the executable file installed the ransomware on the firm's system.

  If you have what appears to be a questionable email, do not click on it. Forward it to your IT support and ask that they open it in a "sandboxed" computer, which has special protection that can allow the email and attachment to be safely examined without infecting your system.

  Note that email addresses can be "spoofed," and an email may appear to be from someone you trust. If the email appears to be at all questionable, or not in keeping with what you would expect receive from that address, treat it as suspicious and send it to your IT department without opening any attachments.

It starts out demanding a ransom (typically around $500 USD or 1 Bitcoin) and may increase the amount as the deadline for payment nears.

- Educate the people you work with about the risks of:
  - attachments to email and other messages;
  - downloading applications from the web that have not been approved by IT;
  - visiting websites of questionable content, as they may contain malware.
- Maintain up-to-date browsers and set security settings high to help prevent phishing and other malware attacks.
- Have an internet and authorized use policy in place in the office (a precedent can be found on the Law Society website), and educate your staff and lawyers on the risks outlined in that policy.

- Consider restricting software and installing blocking applications. Techrepublic states: "Lastly, consider enabling software restriction policies if you're a system administrator on an enterprise network or using a freely available application such as CryptoPrevent to block many of the avenues to which Cryptowall uses to gain a foothold on your computer." Note that blocking applications may or may not work against future versions of Cryptowall or similar viruses as they evolve.

IS IT POSSIBLE TO RECOVER ENCRYPTED FILES IF YOU DO NOT PAY THE RANSOM?

The short answer is, there is no known way to unencrypt affected files without paying the ransom. However, several different approaches have allowed lawyers to restore some or all of their lost files from earlier versions and/or backups that were not themselves encrypted by the virus.

Here is a selection of ways that *may* work if you have been hit by the virus:

- If you have enabled a cloud backup that maintains versions of documents, you may be able to go back to a version that has not been encrypted. Microsoft OneDrive states that you may be able to restore files from earlier versions in OneDrive.

  However, this virus is known to disable the versioning aspect of Windows. Again, according to Techrepublic:

  > Finally, once the encryption process has completed, Cryptowall will execute some commands locally to stop the Volume Shadow Copy Service (VSS) that runs on all modern versions of Windows. VSS is the service that controls the backup and restoration of data on a host computer. It also controls file versioning, a feature introduced in Windows 7 that keeps histories of changes made to files. The file may be rolled back or restored to a previous version in the event of an unintended change or catastrophic event that causes the integrity of the file to have been modified. The command run by the virus stops the service altogether and also adds the command argument to clear/delete the existing cache, making it even more difficult to recover files through versioning or system restore.

- You may be able to retrieve your files if you use SpiderOak or similar zero knowledge systems. These online backup services encrypt files uploaded to their cloud storage via a key that is only known to you. The cloud provider has no way of knowing either your password or your de-encryption key. (Of course, you are well advised to store that key in a very safe place, as it is the only way to access your files.) The files are potentially unreachable and therefore safe from the ransomware.

  SpiderOak's website states:

  > Ransomware attacks are on the rise these days. In order to ensure protection against attacks like Cryptowall, it is extremely important to back up your files and folders in a trusted cloud storage system. SpiderOak is one of the few cloud storage systems that uses "zero knowledge" privacy and uses strong security controls to protect customer data. SpiderOak encrypts the files in your computer before uploading them to the server. As a result, only you, have access to your unencrypted data. Even SpiderOak cannot read your data because the keys used for encryption only belong to you. SpiderOak offers amazing products like SpiderOak Hive and SpiderOak Blue to secure consumer and enterprise data. SpiderOak Blue provides enterprises with a fully private cloud service featuring all of the benefits of cloud storage along with total data privacy.

- Have a backup of your files that is disconnected from the network and thereby isolated from the propagation of the virus. This will work only if the virus does not have the opportunity to find this backup and encrypt it or disable the versioning.

- If you are fortunate enough to have an uninfected backup, do not attempt to restore your data until you are absolutely certain that your network has been fully sanitized of the malware. You wouldn't want to find that your only backup has now become infected courtesy of a vestige of the malware left on the system.

Here is what has not worked for firms that have been hit:

- At least one firm was unable to restore its files in Dropbox. The virus also found the firm's Dropbox files and encrypted them as well – notwithstanding that Dropbox maintains versions of files.

  It is an open question as to whether files that are themselves placed within an encrypted volume in Dropbox using a third-party encryption application (such as Boxcrypt or Viivo) might survive an attack.

- Restoring files stored on an USB drive or NAS (networked attached storage) device, unless the USB or NAS was disconnected from the network when it was infected. If the USB drive or NAS was connected to the network at the time of the infestation, the virus can find and encrypt these devices.

CONCLUSION

Everyone should see ransomware as a serious threat and take steps to minimize their risk. According to Secureworks.com:

> In mid-March 2014, Cryptowall emerged as the leading file-encrypting ransomware threat. The threat actors behind this malware have several years of successful cybercrime experience and have demonstrated a diversity of distribution methods. As a result, CTU researchers expect this threat will continue to grow.

This is clearly one case where a gram of prevention is worth a kilogram of cure. Lawyers are urged to harden their systems, to take action to prevent viruses from infecting their systems, to maintain backups that are out of reach of ransomware and to educate their users on the role that they play in preventing infections.

After all, once you are infected the effort to try to recover and restore encrypted files can cause you to be tired, frustrated and eventually, hit the wall.❖

Conduct reviews

THE PUBLICATION OF conduct review summaries is intended to assist lawyers by providing information about ethical and conduct standards.

A conduct review is a confidential meeting between a lawyer against whom a complaint has been made and a conduct review subcommittee, which may also be attended by the complainant at the discretion of the subcommittee. The Discipline Committee may order a conduct review pursuant to Rule 4-4, rather than issue a citation to hold a hearing regarding the lawyer's conduct, if it considers that a conduct review is a more effective disposition and is in the public interest. The committee takes into account a number of factors, including:

- the lawyer's professional conduct record;
- the need for specific or general deterrence;
- the lawyer's acknowledgement of misconduct and any steps taken to remedy any loss or damage caused by his or her conduct; and
- the likelihood that a conduct review will provide an effective rehabilitation or remedial result.

RESTRICTIONS ON CONTINGENT FEE AGREEMENTS

A lawyer breached section 67(2) of the *Legal Profession Act* when he billed clients on a contingent fee agreement that purported to permit him to take a percentage of the settlement proceeds and a percentage of the taxable costs recovered. The lawyer knew or ought to have known that he was not entitled to a portion of the amount recovered for costs. He used an out-of-date precedent agreement and was unaware of the *Act* provisions at the time of billing. The lawyer promptly repaid the excess fees billed to the clients. A conduct review subcommittee stated that the lawyer's conduct was inappropriate and that ignorance of the law was no excuse. He was clearly in violation of the *Act*, which was designed to protect clients from potential abuse. The lawyer has changed his precedent agreement and incorporated the proper wording, which prohibits taking of a percentage of costs. The lawyer has no professional conduct record, and the subcommittee accepted that his conduct was the result of oversight and not any dishonest intent. (CR 2014-21)

OBLIGATIONS TO CLIENTS AND UNREPRESENTED PERSONS IN LOAN TRANSACTION

A lawyer breached a number of professional obligations owed to a client and unrepresented party in a loan transaction. She failed to advise the lender, who was self-represented, that she was acting for the borrower in a loan transaction and not protecting the lender's interest, contrary to Chapter 4, Rule 1 of the *Professional Conduct Handbook* then in force. The lawyer also failed to ensure the accuracy of the lending documents prepared by her staff, and subsequently disclosed to the lender confidential information regarding her instructions from the borrower, contrary to Chapter 5, Rules 1 and 4 of the *Handbook*. A conduct review subcommittee recommended various strategies to ensure that the lawyer does not find herself in this position again, including (1) confirming in writing who she is acting for and who she is not acting for; (2) making clear notes about who attends a meeting; (3) providing clear instructions to her paralegal, preferably in writing, so that documents are not drafted incorrectly; (4) taking continuing legal education courses in conveyancing, secured transactions and real estate; and (5) reviewing a file and obtaining instructions from her client before responding to inquiries about the file or transaction. The lawyer acknowledged her misconduct and has taken steps to prevent reoccurrence. (CR 2014-22)

DISHONOURABLE CONDUCT

A lawyer failed to faithfully discharge the ethical obligations of his employment, contrary to Rule 2.2-1 of the *Code of Professional Conduct for British Columbia.* Due to a deteriorating relationship between the lawyer and his law firm, he gave notice that he would be resigning from the firm. He set up a personal law corporation, with its own bank and trust accounts, then diverted fees he earned on a client file that were due to the law firm. He stated that leaving the firm was emotional and it was always his intention to pay the firm the portion of the fee owing to it. A conduct review subcommittee advised the lawyer that his actions were inappropriate and, but for the lack of a professional conduct record, may have resulted in a citation. One way to characterize his conduct was misappropriation of funds, and that, seen from this perspective, fell far below acceptable standards. The lawyer acknowledged his misconduct and expressed remorse. He now practises in an office-sharing arrangement with other lawyers whom he can rely upon for counsel. (CR 2015-01)

BREACH OF UNDERTAKING OR TRUST CONDITIONS

A lawyer breached an undertaking in a real estate transaction by failing to concurrently register a release of a Certificate of Pending Litigation (CPL) with his client's new mortgage and by subsequently failing to make an application to the Land Title Office to withdraw the release of the CPL, contrary to Rule 7.2-11 of the *Code of Professional Conduct for British Columbia.* The release of CPL and first mortgage were registered, but there were two outstanding conditions that had not been met by the client with respect to the second mortgage. As the lawyer did not have sufficient funds to pay out the amount owing to the credit union, the transaction did not complete on time. The lawyer ignored demands from the credit union's counsel to withdraw the release of the CPL, in breach of his written undertakings. The second mortgage was later registered, and the lawyer forwarded the required

continued on page 27