The Scourge of Law Firms: Ransomware That Encrypts Your Data

by Sharon D. Nelson and John W. Simek

Remember the good old days of ransomware? You would get an e-mail saying that you owed the IRS money and could pay it via a helpfully included link. Lots of people did this because it was only a couple of hundred dollars. And who wants to duke it out with the IRS? The same dull-witted people fell for the e-mail claiming that someone at your home had downloaded music or movies illegally (much more likely true than the first scenario) and you needed to pay a fine so no one would come after you (or your spouse/child) for a much greater sum. Again, the price was relatively small and many people paid.

The likelihood that a lawyer would fall for these primitive versions of ransomware was small. Fast forward to the days of Cryptolocker which began in 2013. This ransomware Trojan attacked computers running Microsoft Windows, propagating itself by getting a user to click on an attachment or a link contained in an e-mail. Click on the link or attachment and "Winner, Winner, Chicken Dinner" the malware invisibly downloaded and began to encrypt your files. The malware encrypted files stored locally on the computer system as well as on any mapped network drives, such as those files on your server, connected flash drives and other external USB drives.

You then got a message on your screen indicating that you would be given the decryption key to unlock your data for a reasonable sum of $300-$500 – no checks or credit cards though – the payment of choice was and still is usually bitcoins. Curiously enough, there has been considerable honor amongst this brand of criminal who normally provide the decryption key once the ransom is paid. Not 100% but most victims report that they did get the decryption key, though it took them as much as a week to decrypt all their data.

Before we understood Cryptolocker well, many backups (especially in solo and small firms) were engineered in such a way that they too were easily infected and encrypted. This immediately caused IT folks to re-engineer backups so that they were not vulnerable to attack by ransomware meaning that you could restore the encrypted files from your backup and not pay the ransom. But we still regularly see backups that have not been re-engineered endangering all of the law firm's files. The simple solution for most solo/small firm lawyers? Unplug the external USB

hard disk after the backup job completes. Another solution is to use agent-based backup implementations. This is our customary solution.

After some period of time, standard enterprise level security suites began to get a handle on Cryptolocker (and its variants) and were able to detect and stop the malware from infecting machines. We began to see a lot less of Cryptolocker.

But along came Cryptolocker's evil cousin, Cryptowall, and the fight to defeat Cryptowall – (and all its variants) has proven to be much harder. Frankly, it has had many IT consultants tearing their hair out. Criminals have gotten smarter too, often spoofing sender e-mail addresses that make the recipient think they are receiving the e-mail from a court or a reputable law firm. And the English and grammar are much better too!

The Symantec 2015 Internet Security Threat Report has a lot of meat to digest, including the stat that ransomware (the general kind) increased by 113% in 2014. That's bad enough but what made us reel was the finding that ransomware that encrypts your data and demands money to provide the decryption key rose by 4000% in 2014. That's one heck of a percentage!

This is consistent with the deluge of calls we received in 2014 (and 2015) about data encrypted by ransomware. It is a scourge which shows no sign of abating. Standard enterprise security suites have been unable to slow the tsunami of variants, especially the Cryptowall variants.

Herewith, some guidance on how to fight ransomware, particularly for solo and small firms who cannot afford the wallet-busting protections that large firm utilize.

As we say all the time, **THERE IS NO SILVER BULLET THAT PROTECTS AGAINST ALL RANSOMWARE**. Sadly, new variants are released every day.

Besides making sure that your backup is properly engineered as described above, you need a high quality enterprise security suite installed. We like Trend Micro and Kaspersky, but there are many good suites to choose from - talk to your IT consultant.

Another way to protect your data is to attach to the network resources using UNC (Universal Naming Convention) pathing instead of drive letters. For those less familiar with UNC, it is accessing files using a \\server\share\file_path convention instead of a drive letter. Ransomware isn't attacking data via UNC at the present time, but it wouldn't surprise us if the next generation of attacks will.

Let's suppose, in spite of all you do, that you do get hit by ransomware. Do you have a plan for proceeding? Do you have cybersecurity experts to call in? Do you know what your insurance will and will not cover? And remember that no plan survives first contact with the enemy, so be prepared to revise the plan on the fly.

You might check out CryptoPrevent, software which offers the ability to prevent (in large measure) Windows computer systems from infection by ransomware. This software is relatively inexpensive, costing $15 or less per computer depending on the number of licenses needed. The configuration of this software has to be customized for each client, depending on the applications that will need to be allowed to run on your systems - this requires input from you. It will take some amount of time and money as each computer is manually configured.

Another "no software cost" alternative is to configure Windows policies to achieve the same operational restrictions that CryptoPrevent provides. CryptoPrevent is automatically updated, whereas the "no software cost" solution is static. You see the trade-off.

At ABA TECHSHOW, we asked our very knowledgeable faculty colleague, IT consultant Ben Schorr, about CryptoPrevent and he noted that clients (understandably) don't like the manual intervention required by CryptoPrevent to whitelist applications. He had especially run into problems where automated software updates were not permitted by CryptoPrevent, requiring more manual work. Ben shook his head and commiserated with us on the difficulty of advising solo and small firms on how best to defend themselves against this kind of ransomware while keeping costs down.

We became aware recently of four law firms that were successfully attacked by a Cryptowall variant in one month in Northern Virginia. Given that, we have begun recommending the installation of CryptoPrevent – or at least making clients aware that it exists so they can make the money/aggravation vs. risk decision. We warned firms that you may get "pushback" from employees who are accustomed to installing any software they want. CryptoPrevent has proven to be quite effective by **disallowing** the installation and execution of software unless it has been whitelisted. You must determine for yourself if the risk of infection is high enough that you believe this kind of precaution is warranted, even as we tell you that no solution has been 100% effective.

The most common way that law firms get ransomware? Employees click on an attachment or a malicious link in an e-mail. This brings us to another important

point: One of the most often-overlooked aspects of an organization's security readiness is end-user training. It is just as important that your employees know what not to click on as it is to have security software installed to help prevent these types of malware outbreaks. Your best bet is to train your employees - every year - what NOT to click on and to educate them about the indicators that they might see which should cause them to question whether the e-mail is suspect. And this is something law firms steadfastly refuse to do. Some firms cite the training cost (pretty minimal compared to the risk in our judgment) and others cite the loss of billable time. We have a slide in one of our PowerPoints that says simply, "Training, training, training – oh, have we mentioned training?" You can see where we come down on that issue.

We live in a world where half of the people think "the cloud" is impacted by weather and where National Park Service rangers report that one of the questions they are asked most frequently is "Why were so many Civil War battles fought in National Parks?" Very basic security education can go a long way toward defeating ransomware and other security demons.

To conclude - check out the possibility of installing CryptoPrevent along making it a part of your overall business information security protection, which also should include your firewall, IDS/IPS device, physical security, securely-engineered backup, security awareness training, etc.

Don't think you can wish this problem away. The new breed of ransomware is a devilish adversary!

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com