Ransomware: How Many Bitcoins are in Your Wallet?

by Sharon D. Nelson, Esq. and John W. Simek

Ransomware is growing by leaps and bounds. There are reports that ransomware attacks have increased by 748% over the last year. A major international study found that almost forty percent of businesses were hit by ransomware last year. Those are some staggering numbers. Law firms are not immune to ransomware attacks either. Any business is at risk, including the solo attorney. What can we do about ransomware attacks?

In order to understand how to deal with a ransomware attack, we need to understand what ransomware is, how it is contracted, and what impact there may be on your law practice.

What is ransomware?

Let's start with a quick lesson. Basically, ransomware is malware that encrypts your data with a key that you don't have. You can't access the data since it's encrypted and won't be usable until it is decrypted. Effectively, your data is held hostage until you pay the ransom to get the decryption key from the criminals that distributed the ransomware. Normally, there is a countdown timer indicating how long you have to pay the ransom. After the timer expires, the ransom may increase (doubling is not uncommon) or the ability to obtain a decryption key expires forever. There is big money in ransomware. Cybercriminals pocketed more than $1 billion in 2016 alone.

The ransom is requested to be paid in cryptocurrency. Bitcoin is the most requested method of payment. Currently, the average payment is from $650 to $2000. A couple of years ago, you could get by with a $300 payment, but not anymore. At a CLE we were presenting in rural Virginia, a solo attorney told us that he paid $2500 to get the decryption key. Don't worry if you don't know anything about cryptocurrencies. The writers of the ransomware code have very good help files to assist you in creating an electronic wallet and telling you where to go to convert your actual money into bitcoin or whatever other type of virtual currency is acceptable. You probably don't want to pay the ransom these days as you'll only get the decryption key about 50 percent of the time. So much for honor among thieves . . .

You don't even have to be a proficient programmer to take part in the ransomware movement. Some criminal groups are offering ransomware-as-a-service. Instead of charging a fee for the code, they take a portion of the ransoms paid. Typically, they ask for fifty percent of the collected fees.

How do you contract ransomware?

Generally, ransomware is contracted via a malicious attachment or link delivered in a phishing e-mail. It is just amazing how many people will open an attachment from an unknown sender. Some ransomware requires that a second step be taken in order to launch the attack.

One example would be the Locky ransomware. A common way for Locky to be delivered is as a Word document attachment. Once you open the document, the text is unreadable except for a message instructing you to enable macros "if the data encoding is incorrect." Seriously? You shouldn't have opened the attachment to begin with and you certainly shouldn’t enable macros, which would launch Locky and start the encryption of your data.

Several ransomware campaigns have been very successful over the years. Locky and Cryptowall have found success for a long time. Their success is due to the regular updates to the code that allow avoidance of detection. Locky has even been updated to support 30 different languages meaning it can target specific countries and the ransom demand will be understood.

Ransomware has morphed

As previously mentioned, ransomware is normally invoked by opening a malicious attachment or link. That thinking changed in May of 2017 when the WannaCry ransomware attack spread like wildfire across the globe. WannaCry "was easily the worst ransomware attack in history," says Avast's Penn. "On May 12th, the ransomware started taking hold in Europe. Just four days later, Avast had detected more than 250,000 detections in 116 countries."

The really scary part about WannaCry is that it is the first ransomware attack that spreads across devices on the network WITHOUT any user interaction. No clicking. No opening of attachments. To be technically correct, WannaCry is classified as a worm because of the self-propagation. WannaCry exploited a vulnerability in Microsoft’s implementation of the SMB (Server Message Block) protocol. Microsoft had already issued a patch for the vulnerability, but many people hadn’t installed it yet. Lesson one…patch your software as soon as possible.

Another reason WannaCry spread so quickly is that many companies were allowing port 445 (the port used by the SMB protocol) through their firewalls, thereby exposing themselves to the Internet. Lesson two…don’t configure your firewall to allow traffic that isn’t needed.

According to Kaspersky Lab’s APT Trends report for Q2 2017, the next big threat facing the enterprise is destructive malware **disguised** as a simple ransomware attack. That threat is already here. We first saw it with the WannaCry attack and then again in June with the NotPetya (also known as ExPetr) attack. It is alleged that both attacks were nation-state backed. Even though the attacks were originally thought to be typical ransomware campaigns looking for money, further research determined that the real goal was to destroy data. Specifically for NotPetya, analysis of the encryption routine would not allow decryption of the victim’s data even if payment was made for the key.

Business impact

To bring things closer to home for the legal profession, it is believed that a NotPetya attack is what brought DLA Piper to its knees and virtually shut down the law firm for days. Some of the shutdown was done as a precaution, but DLA Piper’s e-mail was “offline” for several days. As most of us know, e-mail communications is critical to a law firm.

Further, cybersecurity company Malwarebytes found that as many as one third of small to medium businesses were hit with ransomware last year. In addition, one in five had to shut down operations immediately. Not a very pleasant experience if you are the unlucky one to get hit.

Prevention

Obviously, the best thing is not to be the recipient of a ransomware attack at all. We believe that is the ostrich in the sand approach. Employees are human beings and somebody is going to do something they shouldn't do at some point. Ransomware is constantly evolving and taking advantage of vulnerabilities we don't even know exist. Our belief is that we need to be prepared for the inevitable attack and position ourselves in the best way to recover.

One of the first steps would be training. Since a very large portion of the ransomware attacks happen as a result of a phishing e-mail, training employees to recognize those e-mails is a good thing. Some are fairly obvious with misspelled words and poor grammar, but don't count on that to be the only sign. We've seen some very good phishing e-mails that have no errors and appear to come from someone we know. There are several free services that can test employees with phishing e-mails. Take a look at the free phishing services available at OpenDNS, Duo Security or SonicWall.

As previously mentioned, another step is to install all updates and patches as soon as possible. Of course your computer operating systems and software should be updated, but don't forget about the network components as well. Router and firewall manufacturers also distribute updates for their products. Make sure you install them too.

You should also have some sort of security suite installed. The modern day security suites include features such as anti-virus, anti-malware, firewall, anti-phishing, etc. There are other technologies you can utilize to reduce your chance of a ransomware attack. One very simple step is to practice the concept of least privilege mode. Users should have the least amount of permissions required for them to do their job. Unfortunately, we see far too many firms configuring user IDs with administrator access. Avoid this temptation and only logon as an administrator when absolutely necessary. You should also consider restricting user IDs to prevent installation of applications. We guarantee that move will not be very popular, but it will significantly reduce your chance of any ransomware attack being successful.

Recovery

No matter how much training you do or how much technology you implement, there is no solution which will stop a ransomware attack 100% of the time. That means we must operate on the assumption that some data will get encrypted or be destroyed at some point. It's not a question of preventing the attack, but being able to recover from it. You could always pay the ransom (assuming you have requisite bitcoins available within the time period), but that does not ensure you'll even get the decryption key. Paying the ransom also encourages the cybercriminals to continue ransomware attacks.

However, some companies may elect to pay the ransom - as did the Hollywood Presbyterian Medical Center in Los Angeles following systems getting infected with the Locky ransomware. Allen Stefanek, CEO of the hospital said, “The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key.”

Backups are your friend. Having a backup of your data unconnected from the network allows you to recover from a ransomware attack. If your data does get encrypted, you can just restore from your backup. However, the important part is to make sure your backup solution is engineered properly. We'll run through a few of the choices here.

Many solo and small firm attorneys use external USB drives for their backup. That is a perfectly good solution, but disconnect the drive once the backup is completed. Also, you should have at least two backup drives in case one of them is connected at the same time your computer experiences a ransomware infection. Using a cloud-based backup solution will also allow you to restore data following a ransomware attack. Just like the external USB drives, make sure you have at least two backup sets in the cloud.

Another solution is to use a backup appliance that is agent-based. This means that you install a software agent on the computer to be backed up and data is transferred over the network to the appliance by using the agent. Typically, the backup appliance solution is used to backup local servers. The software is configured to periodically take snapshots of the server and stores the backup data on the appliance. In addition, consider sending an encrypted version of the backup data to the cloud. Some appliances have the ability to virtualize the server should the actual server suffer a hardware or software failure. As an example, the backup appliances that we implement can take snapshots every 15 minutes and virtualize a server within a few hours.

Last words

Ransomware really is an epidemic today. The "bad guys" are constantly updating code and discovering new vulnerabilities to exploit. We hope you never have to experience a ransomware event. But if you do, make sure you have properly engineered your backup so you can get back in business with minimal effort and pain.

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