PLF *in*BRIEF

ISSUE 133 | JANUARY 2018

Malpractice Prevention Education for Oregon Lawyers

Anatomy of a Ransomware Attack: One Firm's Story

By Hong Dao

Imagine you post an ad on Craigslist to hire a legal assistant. Someone immediately responds by email and attaches a zip file. Believing the file contains the applicant's resume and cover letter, you click on the attachment and download it to your server. Soon afterward, you can't access any files on your computer.

You have just been infected by ransomware.

The above scenario is not fictional. A small law firm in central Oregon was the victim of this ransomware attack. One of the partners, whom I will call Sam, has graciously allowed us to share his firm's story to help educate lawyers on this type of cyberattack. I will describe the anatomy of this ransomware attack and discuss a few lessons we can learn from it.

The Bait

Before the attorney in Sam's firm clicked on the bait containing the ransomware, he had already opened other applicants' emails. None had a malicious zip file attached. It only took one.

The Infection

Within a short period of downloading the zip file onto the firm's server, tens of thousands of documents – essentially all of the firm's files – were encrypted. No one in the firm could access any files, including email programs and contact lists. Sam told everyone in the office to stop working on his or her computer, and he unplugged the server.

The Ransom Note

After the encryption was completed, a note appeared on the downloading attorney's computer. It said, "Congratulations. Your documents have been protected." The note then demanded that the firm pay $750 in bitcoins to decrypt the files. It contained instructions on how and where to send the bitcoins within four days.

Sam then contacted a private legal ethics counsel and the FBI. Legal ethics counsel advised the firm on its ethical obligation to notify clients. That obligation depends in part on determining whether the attacker had viewed or accessed client data. The firm made this determination by running a packet sniffer. It is a software designed to search the computer system to assess whether the attacker had installed a proxy server to access the firm's files. The firm's IT specialist who ran a packet sniffer confirmed that no third party had accessed the firm's files.

The Payment

The next thing the firm's partners did was to pay the ransom to decrypt the data. They encountered two problems in trying to buy bitcoins. First, no place in central Oregon sells bitcoins, so they drove to Portland to make the purchase. Bitcoins can also be purchased online, but it was difficult for Sam's firm to open an account, so they completed the transaction in person. To be safe, they decided to pay for the bitcoins with anonymous prepaid credit cards. They bought those credit cards at Safeway in an amount sufficient to cover the ransom payment plus a bit more. While they were driving to a bitcoin kiosk to buy the bitcoins with their Safeway credit cards, their IT specialist called to say he was able to open a bitcoin account online to make the purchase.

The second problem was that the value of bitcoins fluctuated a large amount each day. After transferring the bitcoins to the attacker, the firm got an email saying the bitcoins were insufficient. The $750 bitcoins the firm purchased just one or two days ago were not enough because of the fluctuation. The attacker gave the firm a few more days to send more bitcoins or not get the decryption key. This key consisted of approximately 200 random characters. The attacker gave the firm half of the key (approximately 100 characters). The attacker promised to give the firm the other half when the rest of the payment was received. The firm bought additional bitcoins online. Once the partners transferred the rest of the bitcoins, the attacker provided the other half of the decryption key.

Prior to this point, the infected server was already disconnected and isolated from all computers. Sam connected the infected server back to the Internet and waited for the attacker to download the decryption key onto the server to decrypt the files. Sam then permanently discontinued using the server after the download was done. It took almost two days for the files to be decrypted.

The Recovery

About 99 percent of the firm's data was decrypted, but emails and contact lists were not decrypted. The firm had to recover the other one percent from its backup. However, the backup was also infected because the external hard drive was plugged into the server when the ransomware attack occurred. Fortunately, the firm was able to rely on a second uninfected backup drive that Sam kept at his home; unfortunately, that backup was not fully up-to-date and did not contain all emails. In the end, the firm lost about two months' worth of the latest data from 11 people in the firm.

The Aftermath

After being down for five business days plus one weekend, the firm slowly reopened. Sam estimated that the ransomware attack cost the firm about $14,000 in IT support, a new server, other hardware, new software, bitcoins, and attorney fees.

The firm now does many things differently, including:

- **Cloud backup** – The firm now continuously and automatically backs up files to the cloud. Sam admitted that he was originally opposed to using the cloud due to security concerns. The cyberattack helped change his mind.
- **Written policy** – The firm has a written policy on data security, including instructions never to accept and open zip files sent via email regardless of who the sender is. New staff have to sign this written policy.
- **Ongoing meeting and training** – Sam regularly meets with staff to go over the policy and remind staff one-on-one not to open unsolicited emails or click on unexpected attachments.
- **Limited telephone calls and contacts** – Any phone calls asking staff if something could be emailed to them are sent directly to Sam to handle. All suspicious emails are also forwarded to Sam.
- **Thumb drives for large files** – The firm asks clients and others to send large files via thumb drives or CDs that can be scanned by the antivirus program.
- **Updated computer security** – Before the attack, each computer in the firm was running a different antivirus program. The computer of the attorney who downloaded the malicious zip file was running on an older operating system that Microsoft no longer supported. As a result, important security updates and antivirus protection could not be installed on that computer. Now everyone's computer runs on an updated operating system with the same antivirus protection. The password to each computer is changed every six months.
- **Responsive IT support** – The firm now works with an independent contractor IT specialist who is immediately available when needed.
- **Shut down Computer** – Everyone at the firm completely shuts down his or her computer at night.
- **Indeed for job posting** – The firm uses Indeed.com for job postings. It has a more secure job application process.

The firm has been doing and continues to do the following to limit the possession of client personal data:

- **No credit card numbers on file** – The firm does not keep clients' credit card numbers on file and has clients use a secured portal to make payments. Credit card numbers obtained on the phone are immediately shredded once the transaction is approved.
- **No full Social Security numbers on file** – Clients' Social Security numbers are not kept on the firm's server, except the last four digits when absolutely necessary in certain cases.

The Lessons

It's easy to dismiss the cyberattack on Sam's firm as a rare incident. It's not. According to Citigroup's Cyber Intelligence Center, law firms are at a high risk for data breaches because lawyers are warehouses of valuable data belonging to clients and third parties. Cyberattacks on law firms are usually not reported in the media. This underreporting can lead lawyers to miscalculate their data security risk.

Lawyers can learn two lessons from the cyberattack on Sam's firm.

First, be proactive. Think about how you might avoid an attack like this. You can use the steps that Sam's firm has taken as a guide. Educate and train yourself and your staff on the warning signs of cyberattacks. Take time to identify the weaknesses in your computer security and fix them. If your password is hello123, it's time to change it to something stronger. If your computer is still running on Windows XP or Vista, it's time to upgrade. If your inbox is filled with spam emails, consider using a spam filter. If you're not backing up client files, start doing it now.

More information on how you can better protect client data is available in PLF's Learning The Ropes segment called, "Data Security/Data Breach: Everything You Need to Know to Protect Client Data," available at *www.osbplf.org > CLE > 2017 Learning the Ropes*.

My colleague, Sheila Blackford, has written an article called "Beware Ransomware," which covers tips on how to protect against ransomware. It is available at *www.osbplf.org > Practice Management > Publications > In Brief*.

Have a plan to respond to a cyber attack. Know whom to call when you are hit with ransomware. On your list should be the Oregon State Bar General Counsel or a private legal ethics counsel, the FBI, and an IT specialist. Use the data breach checklist, "What to Do After a Data Breach," to help you plan. The checklist is available at *www.osbplf.org > Practice Management > Publications > In Brief*.

Second, be very vigilant. Don't put your guard down just because your computer is running on the latest operating system or has the most updated antivirus or anti-malware protection. An antivirus program won't stop you from clicking on a malicious zip file; only staying vigilant can do that. Always be careful when opening emails, surfing the web, clicking on links, and downloading applications and software.

Additional Resources

ARTICLE

- What's Backing Up Your Data, www.osbplf.org > Practice Management > Publications > In Brief https://www.osbplf.org/assets/in_briefs_issues/Whats%20Backing%20Up%20Your%20Data.pdf

PRACTICE AID

- How to Back Up Your Computer, www.osbplf.org > Practice Management > Forms https://www.osbplf.org/assets/forms/pdfs//How%20to%20Back%20Up%20Your%20Computer.pdf

Hong Dao is a Practice Management Advisor with the Professional Liability Fund.