FEATURE, PROTECTING YOURSELF FROM RANSOMWARE AND CYBER-ATTACKS

September/October, 2016

Reporter
33 GPSolo 48 *

Author: By Wells H. Anderson

Wells H. Anderson (info@securemyfirm.com, 888/922-1120), Jd, works with solos and small law firms across North America. his company's SecureMyFirm services (securemyfirm.com) prevent costly downtime and loss of data using ultra-secure backup systems and defenses against Internet threats.

Text

[*49] To: Kim Client <kclient@mail.com>
From: Acme Law, LLC
Subject: Data Security Incident

Dear Kim:

You are very important to us. Because we value your relationship with us and your privacy, we are letting you know about a computer security incident that could involve your personal, confidential information.

It is possible that on September 1, 2016, data in our computer system was accessed and may have included your personal information such as your name, address, e-mail address, and phone numbers. It is also possible that documents exchanged between us and notes we took may have been accessed.

We greatly value your privacy and deeply regret this incident. We have taken extensive additional security measures. . . .

Whoa! This is a letter you really want to avoid writing. The risks that lead to these letters are growing. The AV-TEST Institute (av-test.org) registers more than 390,000 new malicious programs *every day*.

In this article you will learn how to recover quickly if an attack gets through your defenses--and how to strengthen these defenses to prevent ransom-ware and other malware attacks in the first place.

THE NATURE OF RANSOMWARE
The nature of malware has changed. Infected e-mails, infected websites, and criminal hackers are releasing new variants that steal client documents or encrypt entire hard drives. Ransom messages from unidentifiable sources demand large sums of untraceable money for locked or even stolen attorney files and client secrets. The plots to profit from cybercrime are evolving along with or ahead of rapid advances in legal technologies.

The following three incidents illustrate what is riding on your security defenses and backup systems.

1. Solo firm suffers loss of ransom money and two days of work (tinyurl. com/zvopgdk). Ransomware brought a Jacksonville, Florida, sole practitioner to a standstill for two days. The malware had encrypted all the firm's files so no one could get any work done. Apparently the firm's backups failed, were compromised, or were out-ofdate, so the solo consulted experts, opened a separate bank account, purchased the necessary bitcoins, and paid the ransom.

Afterward, the firm implemented better computer firewalls, switched to passphrases that are changed regularly, and began backing up files every day to an isolated server.

2. Amy W's consumer-grade backup fails (tinyurl.com/gwsurug). A small business owner took bad advice when she trusted the consumer-grade Know-How Cloud (powered by LiveDrive) as her only backup. What Amy didn't know was that LiveDrive had been sharply criticized in online reviews and consumer comments (cloudstoragebuzz.com/livedrive).

After she opened an e-mail attachment purporting to be an invoice, her computer files were promptly encrypted by ransomware. Trusting that her files were safely backed up, she had the ransomware removed and her computer reset. Afterward she contacted Know- How Cloud and was told she had 30 days of backups. In fact, the service provider had stored only two sets of worthless backups. They had both run *after* the ransomware attack so they were merely copies of encrypted files. By the time she discovered that no good backups were available, the ransom demand had expired. She lost all her files, including important documents representing years of hard work.

3. Seven-figure ransom paid to avoid publication of stolen law firm data (tinyurl.com/gwwxwx3). Austin Berglas, head of cyber-defense at K2 Intelligence, once led the New York cybercrime branch of the Federal Bureau of Investigation. According to a March 30, 2016, article in *American Lawyer*:

> Berglas said he worked with a law firm recently that faced a ransom-ware attack, something he said he's seeing more and more often. The firm did not know about the attack until the hacker sent a screenshot of the stolen data and a message that the information would be made public if the firm did not pay. This firm opted to comply and handed over a seven-figure sum, according to Berglas.

PREPARING TO RECOVER FROM RANSOMWARE

Ransomware is profitable for criminals. You, their victim, make the rational calculation of how much time and money it will take to recover files from your backup and to recreate the recent files that are not backed up. If that is a lot more than the cost of the ransom, you, like so many [*50] other victims, take a deep breath and pay the ransom. The promise of getting all your files back fast is a strong motivator.

So, what do you need to prepare in order to *avoid* paying criminals if all your files and your local backups are encrypted and held for ransom?

CONTINUOUS FILE BACKUP

Your first, most complete fallback for dealing with a ransomware attack is a continuous backup system that can quickly recover all your files and keep you working. Most backup systems in small law offices run once per night, not continuously. Nightly backups have an important place, but they are not sufficient.

Typically, the documents you need the most are the ones you have been working on currently or earlier in the day. If ransomware locks up all of today's documents for everyone in the office, work comes to a standstill. With the right system, you can begin recovery and simultaneously keep the work flowing.

POINT-IN-TIME RECOVERY

The point-in-time recovery feature goes hand-in-hand with continuous backups. It allows you to recover today's new files and any changes you have made to documents right up to the time that they are lost or encrypted owing to a ransomware attack or another computer problem.

Here is what a continuous backup system with point-in-time recovery can do for you. Instead of paying the ransom to get your files back, you open the continuous backup software or service. From the Restore menu, you select a point in time just before the ransomware encrypted your file. (Refer to the modification dates and times of your encrypted files; in Windows, right-click a file > Properties > Details.) Run the recovery process and choose the options to restore the files to their original locations.

RESTORE FEATURES

When purchasing a continuous file backup program or service, do not be satisfied with general claims such as, "We

back up your files constantly and can restore any or all files." The restore features of different applications vary widely in their capabilities. Many require complicated, extremely time-consuming steps that may not do what you need them to do. You may have a backup system that must slog through restoring every single one of your files even if you only need to restore some of them.

A clever synchronizing restore feature can skip over all the files that were untouched by ransomware and just replace the ones that were affected. This feature can dramatically cut down your recovery time because ransomware may selectively encrypt only certain kinds of files, such as Microsoft Word, Microsoft Excel, and Adobe PDF files. Or you might be able stop ransomware after it has encrypted just a few hundred of your files, leaving thousands untouched. You want a restore process that restores just the files affected by the ransomware, not all the thousands of files in your backup.

Another valuable feature of a continuous file backup program or service is the capability of immediately but securely accessing any backed-up file. With this feature, you and co-workers can continue to work on any of your documents even while a technician is busy disinfecting computers and restoring files. That beats being idle, stymied, and frustrated.

CONTINUOUS BACKUP SOFTWARE AND SERVICES

Countless backup applications and services are available, but many don't support continuous backups and fast, point-intime restores. Here are some that do:

- **SyncBackPro** (2brightsparks. com). Software with a deep set of backup, versioning, point-in-time restore, and synchronization features that are powerful and complex.

- **BackupFS** (altaro.com/professional-pc-backup). Continuous data protection software with Reverse Delta technology to save space and restore from multiple points in time with BackInTime technology.

- **SecureMyFirm** (securemyfirm. com). Cloud backup and synchronization service for solos and small law firms with clear features for immediate file access and continuous backup.

- **MozyPro** (mozy.com/product/mozy/business). Cloud backup service with option for continuous backups, point-in-time restore, and file synchronization.

SAFE BACKUP DESTINATION

Ransomware and other new forms of malware threaten not only the files on your server, but also your on-site backup files. This means it's time to rethink your entire backup system.

A common practice has been to keep regular, nightly backups on drives in the office and to rotate drives or tapes off-site once a week or once a month. Unfortunately, ransomware developers have now designed their programs to seek out files all across your network on local drives, external drives, and network drives.

[*51] As a result, you may be among the people who stand to lose an entire week or month of files. All the networked files and backups in your office can be encrypted or corrupted by new malware and viruses, so you can be left with only your last off-site backup that is a week or a month old.

A reliable online backup service will allow you to recover from an attack that affects all the files and drives in your office. Another option is to install a network-attached storage (NAS) device to store your on-site backups. With the right device and security configurations, ransomware cannot get to the files on your NAS the way it can get to files on your external and network drives. It has the advantage of supporting rapid restoration of your files, but a single NAS device won't protect you from storms, fire, and theft. For that you'll need to double your investment, placing a second NAS device in the home of a partner or administrator. It can be securely synchronized with your on-site NAS.

WHY TRADITIONAL ANTIVIRUS SOFTWARE FALLS SHORT

Traditional antivirus software identifies malware files by comparing the "digital signature" of any new file to an

enormous list of malware signatures. These signatures are downloaded periodically and stored by the antivirus program. Malware criminals responded by releasing new viruses faster than they can be added to the antivirus lists. Antivirus companies responded with new methods of recognizing and neutralizing viruses, but they are not foolproof.

Unfortunately, thieves and antivirus companies are engaged in an ongoing contest that parallels the leapfrogging efforts of lock makers and lock breakers. Keeping your security software installed and up-todate is important because it can stop many malware infections, but it is not enough. You need to change your behavior.

HOW TO PROTECT AGAINST RANSOMWARE

The most prevalent ransomware sources are spam e-mails, infected removable drives, infected software installers, and hacked web pages. Infections of mobile devices are now booming as well. What can you do to keep ransomware from successfully attacking your files?

- **E-mail attachments and links**. Don't open unexpected attachments to e-mails. Don't click on links in e-mails unless you are sure they are safe. Even if an e-mail apparently comes from someone you know, check with them before opening an attachment or clicking a link in the e-mail.

- **Links in search results**. Infected websites specialize in masquerading as popular entertainment, news, or technology websites, often with sensational headlines. Beware of eye-catching or dramatic headlines in web search results.

- **Danger signs**. If an e-mail or pop-up makes an urgent warning or intriguing offer, be suspicious.

- **Antivirus software**. Make sure every computer and mobile device has up-to-date, high-quality antivirus and antimalware protection even though even the best is not foolproof.

- **Education**. Make sure everyone in your office knows these basics of how to avoid falling prey to ransomware.

For more details on protective steps you can take, see my article, "The New Lawyer's Guide to Cybersecurity and Protecting Your Practice" in the May/June 2015 issue of *GPSolo* (tinyurl.com/gks7dt2).

CONCLUSION

Yes, it is a wild and wooly world these days. Dealing with computer threats can be daunting. Yet, taking action to prevent ransomware and other malware attacks is doable. So is rapid recovery if your defenses are breached.

A recap:

- Continuous on-site backups with point-in-time recovery keep your practice up and running.
- A secure cloud backup service protects all your files on all your drives.
- Top-rated antivirus and antimalware software provides important protection.
- Addressing the human factor is vital. Inform everyone about criminal tricks and encourage them to think about what they see on their screens before making reflexive clicks.

By following some basic precautions and by taking advantage of new defenses and backup systems, you can work confidently. You will have lowered your risks and beefed up your ability to recover quickly.