Ransomware 101: An Introduction for small law firms and title insurance agents

By: Terrence D. Pricher

Ransomware is the most dangerous cyber threat in the world and it is growing worse every year. Some estimates report as much as a 500% increase in ransomware over 2015. Many solo and small firm lawyers, preoccupied with legal work, often don't pay enough attention to office operations. Meanwhile, the practice of law is becoming more and more mobile and technology based. Every lawyer has a computer and / or mobile device(s) they use for legal work and email to communicate with clients and other lawyers. While nothing can guarantee never becoming a victim of ransomware, awareness and preparation are two factors that can reduce the odds.

What is Ransomware?

Ransomware fits into the general category of malware, which is the general term for many different types of bad viruses that are planted into operating systems and cause a variety of problems. With ransomware specifically, an attacker blocks access to a user's data files or entire computer, and unlocks access to the data in exchange for payment (a.k.a. a ransom payment). Once a system is infected, the victim is often left with little choice other than paying the ransom to, possibly, regain access to his or her own files.

The Targets of Ransomware

Law firms are some of the top targets for ransomware and other malware[1]. In general, the top targets for ransomware are users with a lot of money and / or

[1] Several articles have been written about law firms as targets for a ransomware attack. Two examples:
http://www.abajournal.com/magazine/article/ransomware_software_attacks_stymie_law_firms/
http://abovethelaw.com/2015/03/is-your-law-firm-a-target-for-hackers-spoiler-yes/

information, limited IT infrastructure and limited controls. The potential benefit to a cyber criminal is the amount of money and information available. Thus, cyber criminals will attack any business that they can infect, but it is obvious they will target potential big payoffs more often. Law firms have a lot of data about clients and third parties, and a lot of money. Add in limited IT infrastructure and limited controls, and small law firms are prime targets for a ransomware attack. A small law firm that handles real estate transactions is the ideal target. Other frequent targets include title and escrow companies, medical companies, franchises, small businesses, government contractors, and municipalities. Some estimates project that almost half of the world's companies have been a victim of a ransomware attack in the last twelve months. With the amount of data handled by law firms and lack of controls, especially at solo and small firms, the numbers are likely higher.

One way that lawyers make themselves known to cyber criminals is by using email addresses that contain a word such as law, attorney, legal, and so on. For example, email addresses such as Joneslaw@xzy.com, AttorneyJones@xzy.com and Joneslegal@xzy.com are easy to identify as a lawyer's account. Similar key addresses, such as JonesTitleLLC@xzy.com, identify title insurance agents (often lawyers). Once the cyber criminal knows a lawyer uses the account, the account becomes a target.

How Do You Get Infected with Ransomware?

The most frequent method for ransomware infection is via a "Trojan Horse". In this scenario, infection is secretly started by the user who opens an attachment, visits a malicious website, or downloads an infected file over the Internet.

Another method is via what's called malvertising, which is meant to look like legitimate advertising on legitimate websites. Once a user clicks on the advertisement, the malware downloads.

Phishing and spear phishing are two additional techniques often used to install ransomware. Both use email to lure the victim to click on a link within a

seemingly legitimate message that downloads the ransomware. Phishing involves sending an email to as many people as possible, hoping to lure a victim to click on a link. Consider phishing the cute cat viral video method of spreading ransomware.

Spear phishing, however, targets specific victims by personalizing an email to make it appear even more legitimate. As a result, a spear phishing attack requires some level of preparation. A sophisticated cyber criminal will take the time to carefully choose a target as well as the timing of the spear phishing attack. Some cyber criminals gather information from social media while others use information obtained from a prior victim. However, once the information is acquired, it is not always immediately used. For example, a cyber criminal that infiltrates a victim's email account now has access to the victim's entire email directory and prior emails. A prudent spear phisher may gather information and watch accounts until multiple lucrative targets are identified, then strike at an opportune moment.

The keys to a successful spear phishing attack are believability and timing. Accounts will be monitored and an attack will be launched at a time of urgency, hoping to take advantage of some chaos, which leads to a hurried decision or a failure to identify an attack. These attacks frequently occur: (1) right before a big transaction is to take place, (2) when the boss is on vacation, (3) tax season, (4) during holiday shopping. The return email address must look legitimate in order to encourage the recipient to download the ransomware. For example, in courier font, a 1 looks like a lower case l (e.g. 1 and l). Missing the difference is a simple mistake for any person, in a rush or under a deadline, to make. If the email address the user is familiar with is Joneslaw@xzy.com and the return address is, in courier font, Jones1aw@xzy.com, it may look legitimate. In this scenario, however, the "l" has been replaced by the number "1".

A link in an expected email is far more likely to be clicked than one from an unknown source. Thus, spear phishing has a high the success rate.

Elements of a successful attack

As a result, the user installs the ransomware on his own system, the ransomware locks up the user's own data files, and the cyber criminal sends a ransom demand with payment instructions. The user, hoping to regain access to his data or system, follows the instructions and pays the ransom. Once payment is received, the cyber criminal may or may not send the user instructions to unlock the data. Usually this is a numerical code to unlock the data or to activate a decryption program found on another website associated with the cyber criminal.

Preventing Ransomware Infections

To avoid infection, the first step is to keep your computer's operating system and software up to date with the latest security updates. Next, install and run self-updating anti-virus software. These first two steps are important because many ransomware attacks target older versions of software with holes in the security controls. The updates are either completely new versions, or have patches for holes that have been identified. Another reason these first two are important: even if you block websites and have firewalls in place, they do not stop anyone from opening an email attachment and inadvertently launching a ransomware virus. In this case, up-to-date anti-virus software has a better chance of helping stop the attack.

Back up your files!

In general, a multi-faceted back-up strategy executed frequently and to more than one location, is best. For example, back up all of your computers and mobile devices regularly to cloud-based backup services and/or external hard drives, with snapshots kept off site. More importantly, be sure to test that your back-up restore procedures work. As a result, if files are locked up by ransomware, a user will be able to restore locked files from backups without needing to pay a ransom.

How to respond after an attack

If you are a victim of a ransomware attack, law enforcement may not be able to help you. However, the attack should still be reported as a crime.

After you have recovered your files, even if by paying the ransom, it is very important to take immediate steps to prevent future ransomware attacks.

Once you are the victim of a ransomware attack, you become a prime target for a future attack. The cyber criminal will likely try to re-use the virus that has been installed. Often victims pay the ransom, regain access to their files, and continue with the same lack of IT infrastructure and controls that led to the first attack. Far too often, the victim doesn't wipe the ransomware virus clean from their system or patch the hole in the security system and becomes a victim again soon after.

Don't be lazy. Commit to making cyber security a top priority. The best response is too contact IT security experts and follow their advice. This will add to the cost of being a victim, but is your best approach to protecting yourself from future attacks.

If you do not have the resources to employ an IT security expert, at a minimum, you should immediately update and run all antivirus software to clean out your system, back up your files, and perhaps even reinstall your computer's operating system. Once you are the victim of an attack, prepare yourself to properly backup all of your files as soon as you regain access. If you don't have an external hard drive and / or cloud storage get them immediately, even before you pay the ransom, if possible. This way, you can immediately back up your files to multiple locations as soon as you regain access to your information. These measures are not intended to replace the advice of an IT security expert, I simply list them as the bare minimum actions that should be taken to help prevent becoming a repeat victim.

Conclusion: Avoid Being A Victim of Ransomware

Commit to slowing down and scrutinizing emails and links before clicking on items in the future. "Think before you click" is a good mantra to adopt. If

something looks suspicious, take action before you click. The cyber criminal knows whether the victim downloaded the malware attached to a video or clicked on a link sent in an email and will attempt the same method again. Do not click on a link until after steps are taken to ensure that the email is legitimate. Even if an email message appears to have come from someone you know, it's best to speak with the sender before clicking on a link.

Ransomware is one of the biggest cyber threats to law firms and title insurance agents and it is growing every year. While nothing can be guaranteed, awareness and proper preparation can reduce the odds of becoming a victim.