Ransomware

The Currency has Changed, but the Threat is All the Same

BY SCOTT GREENE AND JEFF MARTIN

Ransomware is a type of malicious software, often referred to as malware, that restricts access to computer files, systems, or networks and demands a ransom payment to restore access. Incidents of ransomware attacks are on a steep rise. According to cybersecurity company SonicWall, the first three quarters of 2021 saw a 148% surge in global ransomware attacks, with a predicted record-breaking 714 million attacks by the end of the year. This is of particular concern in the United States, which leads the world in the number of attacks. The sophistication and variety of attacks are constantly growing, making this a top cyber security issue to be aware of and protect against.

Types of Ransomware

Traditionally, single extortion attacks such as locker ransomware and crypto ransomware have been used to ransom data. Locker ransomware encrypts the entire computer system, while crypto ransomware encrypts all or some files on a computer system to block authorized users' access.

Double extortion ransomware involves a two-tiered attack where threat actors not only encrypt files but also export the encrypted data. The threat of publishing the stolen data is then used to pressure firms to meet ransom demands. The stolen data is usually published or further ransomed on the dark web to the highest bidder. This type of ransomware has become increasingly popular.

Grubman Shire Meiselas & Sacks fell victim to this type of ransomware in May 2020. The entertainment and media law firm's computer system was encrypted, and files also were stolen. The ransomware group REvil, which carried out the attack, demanded payment in the form of $42 million in cryptocurrency. In this case, double extortion ransomware was used to force payment after the firm attempted to negotiate with the ransomers. The criminal group leaked 2.4 gigabytes of the stolen data onto the darknet to strongarm the firm into paying.

The Proliferation of Cryptocurrency and Bitcoin

Cryptocurrency provides a level of anonymity that is nearly impossible to achieve with traditional forms of monetary transactions. Unlike traditional banking, there is no personal identifiable information attached to the destination address tied to the ransom. As the most popular and accessible cryptocurrency, Bitcoin has become commonplace in ransomware attacks. Threat actors therefore heavily rely on this means of payment to remain anonymous and ensure that their victims can comply with their demands.

Although Bitcoin transactions are transparent by design to allow for transaction validation, threat actors have employed available services to limit the risk of exposure. Cryptocurrency tumbling services provide an extra layer of anonymity by mixing funds that are potentially identifiable with a pool of other funds. This process is random, which makes tracing the source of the transaction difficult because the amount of funds and the number of times the funds are mixed is arbitrary. Law enforcement experts are left with a complex transaction trail that can be nearly impossible to trace.

Why are Law Firms Ripe for the Picking?

The very nature of attorney–client relationships involves the exchange of personal identifiable information and other sensitive information such as trade secrets, potentially damaging information regarding the client's criminal activity, or tax return information relevant to business operation. As a matter of professional ethics, attorneys are required to keep this information confidential. Law firms are therefore prime targets because the highly sensitive and valuable information becomes a commodity to threat actors, who leverage legal and ethical obligations to force ransom payments.

Due to the impact of COVID-19, law firms, like many businesses, made the abrupt transition to remote work. The surge in the use of cloud computing and remote servers to facilitate this transition increased points of entry for potential ransomware actors to exploit. Employees who use their own equipment due to the transition can put the entire company's security at risk if they do not employ cybersecurity measures consistent with what was in place in the office.

The presumption that a law firm will have weaker cyber security measures also increases the likelihood they will be targeted.

The vast majority of attacks arise from poor cybersecurity practices, and many small and midsize firms have not historically prioritized this area. But there have been encouraging trends that point to increased awareness around these types of attacks. According to the American Bar Association (ABA), 36% of US law firms obtained cyber insurance policies in 2020, up from 33% in 2019. However, the aggressive rate at which cyber threats have increased far outpaces the legal industry's shift to greater protection. Coveware's 2021 first-quarter report revealed that the professional services industry was affected the most by ransomware attacks. Within this industry, small and midsize law firms accounted for the majority of ransom attacks. A 2021 study by Capterra revealed that one in three law firms of this size had suffered cyberattacks in the last 12 months.

A recent case resulted in the ransomware actors gaining access to an entire computer network and encrypting all files. Without a backup of the data, the firm was forced to engage in negotiations. The initial request of seven Bitcoin was negotiated down to three—still a hefty sum at Bitcoin's current rate of nearly $50,000. An additional threat that was leveraged in these negotiations was sending all payroll documents to the other employees at the company, which would have allowed everyone to see each other's pay rates. This particular firm did have cyber insurance, which meant that professional negotiators handled the back and forth with the threat actors. Those negotiators generally act as though they are employees of the company so as to not tip off the hackers that there is cyber insurance at play. The decryption key was sent in that case, and access was restored. Unfortunately, the process took multiple weeks, resulting in a large loss of business productivity and income—something that's generally not covered by cyber insurance policies.

An Attack Happened—Now What?

When data is stolen during ransomware attacks, it is usually held hostage until the firm complies with ransom payments. According to Coveware, nearly 70% of law firms paid ransoms to regain network access or retrieve stolen data. Unfortunately, the risk of being double-crossed by ransomers is high. This report also highlighted that one-third of the parties who complied have never recovered their files.

The increased use of double extortion ransomware means that a firm's troubles far exceed restricted access to their network or encrypted files. Threat actors have posted client information on the dark web to journalists, press outlets, and other third parties to serve their purposes. In general, the extent of the data breach can be difficult to determine, as other bad actors often resell or exploit the information for identity fraud and other purposes.

Beyond the immediate consequences resulting from a successful attack, there are further legal and general business ramifications a law firm may face. If the attack is due to inadequate cybersecurity measures and deemed preventable, there may be civil litigation or, at a bare minimum, serious implications regarding their three ethical obligations:

- confidentiality—client's personal information no longer protected;
- competence—failing to maintain security competence to the detriment of their client; and
- professional judgment—deciding whether to disclose the breach to their client.

These types of attacks, if disclosed, can do enormous damage to a law firm's reputation. Privacy protection is of top importance when selecting an attorney, and a firm that has had that type of information stolen in the past will be regarded with increased scrutiny.

The increased use of double extortion ransomware means that a firm's troubles far exceed restricted access to their network or encrypted files. Threat actors have posted client information on the dark web to journalists, press outlets, and other third parties to serve their purposes. In general, the extent of the data breach can be difficult to determine, as other bad actors often resell or exploit the information for identity fraud and other purposes.

Negotiating with Bad Actors

Prior to negotiating with the threat actors, a firm must first decide whether to engage in these discussions at all. The FBI advises against negotiating with these hackers and argues that by negotiating and paying their ransom, it further encourages this type of criminal behavior. Some businesses have found that even after paying, the hackers don't make good on their promise to deliver the encryption key and actually may sell the data regardless. These are all important considerations a compromised law firm must take into account.

While cyber insurance is an important tool to protect a firm's interests, the knowledge that the firm has cyber insurance can hamper negotiations. Threat actors know that insurance companies have deep pockets and the contractual obligation to fulfill the ransom ask, and this bolsters their unwillingness to come down from their initial ransom request. Some hackers specifically target companies with cyber insurance, and even if they aren't aware of a policy prior to the attack, they may find the documents proving this in the firm's stolen data. If they understand the deductible and other terms, they may realize that they can push for a much higher ransom.

Once ready to negotiate, it is imperative to understand exactly what was stolen or encrypted, and how much that data is realistically worth. Some firms may have strategies to recover it, and, armed with the knowledge that the data may be sold despite a ransom payment, will choose to pay nothing to the attackers. In cases where the data is worth the ransom, a key to negotiating is discovering as much information as possible about the attackers, their sophistication, and their past negotiating strategies. This provides insight into how they've been talked down or finessed before—and whether they've upheld their end of the bargain once paid off.

Protecting Your Firm in This Dangerous Age

Within any business, the weakest link remains the same—the individual employee. Access to systems is often gained by phishing, usually via spoofed emails that appear to belong to a reputable person or company. That email could contain dangerous attachments or links meant to trick users into inputting their username and password. Phishing emails used to be easier to spot, with grammar/spelling errors that are apparent to native English speakers (as many of the attacks originate outside the country). However, the hackers have grown more sophisticated and now will pay native speakers to write flawlessly constructed emails. Recognizing fake emails now requires more knowledge: calling to confirm emails sent with attachments that were not expected, hovering over links to see where it is trying to take you, clicking "reply all" to see if it reveals a phony email address, and doublechecking the email signature to ensure the details are all correct. It is also imperative to keep in mind that legitimate companies will not send emails requesting sensitive information, and anything with a heightened sense of urgency should be regarded as suspect.

Keeping employees up to date and educated on the latest phishing strategies is paramount to maintaining security at a firm. People also should be instructed to follow best practices regarding password creation. Passwords should be updated frequently, at least 10 characters in length, and contain characters from upper case, lower case, numbers, and non-alphanumeric special characters ($, %, #, etc.). They should not contain the user's name or other easily identifiable pieces of information (or information easily gleaned from social media accounts) like family names, pets, addresses, and special dates. In addition, we are now able to enable two-factor authentication and even three-factor identification on many platforms, and this should be taken advantage of when available.

On a firmwide scale, trusted IT professionals should be employed to implement best practices with firewalls, server security, anti-malware programs, and thorough employee education. Of particular importance as it relates to ransomware is ensuring regular and comprehensive data backups. With the sensitive information that a firm possesses, the threat of it being sold is still of huge concern, but a lot of power is taken out of the hacker's negotiation if the target already has the capability to restore what was stolen and encrypted.

Cyber insurance can be of significant value to an attacked firm, although having a policy in place does not abate the need for solid cybersecurity protocols, as cyber insurance providers require certain measures to be in place prior to backing the policy. Ransomware claims will cause a firm to be difficult or highly expensive to insure moving forward, and even with insurance there can be significant financial consequences to an attack, including temporary stalls in business, damage to a firm's reputation, and insurance policy deductibles. Therefore, it is in a firm's best interest to ensure that it employs rigorous cybersecurity safeguards even after acquiring this type of insurance.

On a firmwide scale, trusted IT professionals should be employed to implement best practices with firewalls, server security, anti-malware programs, and thorough employee education. Of particular importance as it relates to ransomware is ensuring regular and comprehensive data backups.

Yet, the Future Looks Bright

The pervasive nature of ransomware both within and beyond the legal industry has not gone unnoticed. The federal government as well as regulatory bodies such as the US Securities and Exchange Commission have now prioritized the displacement of ransomware actors.

The US Department of Justice (DOJ) has likened its priority to combat ransomware attacks to its effort to fight terrorism. The government's multilayered approach focuses on the disruption of ransomware infrastructures, increased cyber protection and cooperation through notification and information sharing among national agencies as well as on the international front.

In its effort to disrupt ransomware actors, the DOJ has established the National Cyber Investigative Joint Task Force to "enhance coordination and alignment of law enforcement and prosecutorial initiatives." Federal agencies such as the US Cyber Command and National Security Agency have committed manpower, technology, and expertise to better understand this threat and present options for combatting ransomware actors.

In 2021, the FBI announced that it had traced and recovered 63.7 of the 75 Bitcoins paid to hackers by the company Colonial Pipeline, although they declined to detail how exactly this was achieved. There are now several startups devoted to tracking Bitcoin and analyzing the blockchain for suspicious activity, helping spot potential criminal transactions. In the United States, the increasing legitimization of the currency prompted laws that mandate that crypto exchange companies require identity validation to sign up, meaning users must upload government identification documents.

While the proliferation of ransomware has caused some leaders to call for a ban on cryptocurrencies entirely, it seems unlikely to be embraced on the global scale that would be needed to thwart these types of attacks. The threat is likely to continue growing unless or until more effective tracking strategies can be developed and easily accessed. In the face of so many uncertainties, it falls to individuals and business owners and managers to safeguard against these types of attacks through education and a commitment to best practices and incident response plans. We must protect our computers and data in the same way that we secure the doors to our home, and we must behave in ways that protect us against the risks and threats that come with technology. CL

This article first appeared in the March 2022 issue of Arizona Attorney Magazine. *It is reprinted here with permission.*

Scott Greene has been helping lawyers, business owners, courts, CEOs, and IT departments understand data for over 35 years. He collects, analyzes, and explains complex electronic evidence in plain English. Today, he is an affiliated professional member of the ABA and heads the digital forensics division of Evidence Solutions, working as an expert witness and forensics professional. His extensive and diverse experience allows him to be an expert in many facets of digital technology. **Jeff Martin** started his IT career as a small-business consultant, where he was quickly identified as someone who had the knack for explaining technical information to nontechnical audiences. He became a director of IT in the financial industry, and then spent five years solving crimes as a digital forensic analyst for the Michigan State Police—also becoming an adjunct instructor at Northern Michigan University after obtaining a master's degree in cyber security. He is now an advanced digital forensics examiner and expert witness at Evidence Solutions, working with attorneys and individuals to discover and explain complex electronic data.

Coordinating Editor: James R. Paravecchio, jvecc13@yahoo.com