CYBERTHREATS TO LAW FIRMS

Executive Summary

Law firms represent high-value targets, given the breadth and sensitivity of the information they possess, and are therefore likely to be frequently targeted by a variety of threat actors—particularly cyberespionage actors and cybercriminals. Cyber4Sight notes that tactics, techniques, and procedures (TTP) used to infiltrate law firm networks often involve social engineering and spear phishing. Various surveys and threat-intelligence reports suggest that cyberthreats to law firms have increased over the last 5 years, and that many law firms—particularly localized and smaller firms—are still behind in implementing robust cybersecurity measures. In some cases, even though larger firms have adopted stronger measures, the local litigation counsel they often work with are a weak link in the data chain, allowing threat actors to gain access to their data, according to Jay Edelson, a plaintiffs lawyer specializing in privacy violations.1

In 2016, Cyber4Sight identified four notable cyber incidents involving law firms. In February, a Ukrainian outlined plans to conduct a spear-phishing scheme against several U.S.-based law firms to steal information for insider-trading purposes. In March, Cyber4Sight identified a new ransomware, dubbed "Cryptohasyou," that targeted an Indianapolis-based law firm through a spear-phishing email message impersonating the U.S. Postal Service. Further, the Wall Street Journal reported that unspecified hackers breached the networks of named U.S. law firms. Finally, in early April, news broke that 2.6 TBs of data reportedly were stolen via unspecified means from Panamanian law firm Mossack Fonseca. An insider may have leaked the stolen data, but lax security measures suggest a potential external attacker.

Cyber4Sight anticipates that attacks on law firms are unlikely to decrease in the next year, given overall trends in law firm attacks and the Mossack Fonseca incident, which demonstrated the potential windfall from a successful law firm breach. Following the release of the Panama Papers, Cyber4Sight assessed that the more damning elements of the leak would almost certainly raise the target profile of law firms, possibly spurring retaliatory cyber attacks from various kinds of threat actors against individuals and organizations accused of corrupt behavior.

Threat Actor Overview

From a cybercriminal perspective, data on business dealings can be used for insider trading or sold to others interested in similar activities. Additionally, cybercriminals could hold law firm data hostage and attempt to extort a ransom from either the law firm itself or the affected clients. These schemes likely would involve a ransomware infection or blackmail in which the cybercriminals successfully exfiltrate and threaten to publicly leak the data, which could cause reputational damage or business losses to the victimized firms. Attackers probably perceive law firms to be inherently more vulnerable to such extortion schemes, given the sensitive nature of client information and high stakes involved. Such schemes would also be attractive to hacktivists looking to make political statements or pressure companies to make certain concessions or change perceived damaging policies.

Cyber-espionage threat actors, including state-sponsored hackers, have aimed to access and steal firms' confidential client information to gain insight into business dealings and acquisitions, either to gain a competitive advantage or to disrupt perceived threatening activities. In September 2015, a senior managing director at the U.S.-based corporate investigations and risk consulting firm Kroll commented that the company has "investigated a number of law firm data breaches in which hackers targeted sensitive data about pending mergers, litigation strategies, and intellectual property.2 Many such attacks

© Booz Allen Hamilton, Inc., 2017. All rights reserved.

Any conclusion or recommendation by Booz Allen Hamilton as contained in this report should not be viewed as any guarantee or opinion of any future events or future outcomes. Booz Allen Hamilton undertakes no obligation to update any conclusions or recommendations to reflect anticipated or unanticipated events or circumstances in this report. Booz Allen Hamilton does not guarantee that this document has identified all cyberthreats, or that a security incident or security breach will not occur. Booz Allen Hamilton takes no responsibility and is not liable for reliance by anyone on the information contained in this report, and any reliance is at the sole risk and discretion of the recipient of this report.
are linked to Chinese state-sponsored hackers, according to a March 2015 Bloomberg article citing FireEye's chief security strategist. The strategist noted that any law firm doing business in China or representing clients in China probably would be hacked.

Regardless of the motivation of the threat actors, Cyber4Sight notes that cyber attacks against law firms potentially could result in cyber attacks against the clients themselves—such as the previously mentioned extortion schemes. Further, threat actors may obtain sensitive client data allowing for more tailored spear-phishing email messages.

**Trend Data**

Various surveys and threat intelligence reports suggest that cyber threats to law firms have increased over the last 5 years, and that many law firms—particularly localized and smaller firms—are still behind in implementing robust cybersecurity measures.

According to various legal industry news sites on 6 April 2016, insurance company QBE—which insures more than 1 in 10 law firms in England and Wales—reported that more than USD 120M has been stolen across the legal profession in the past 18 months. QBE estimated 150 successful "raids" on its clients' accounts during that time as well as at least 1,500 failed attempts. Further, the firms recovered only a small portion of the stolen money.

On 24 February, IT security company TruShield reported that, based on its collected data set of nearly 50 billion events, the legal industry was the third-most-targeted sector in January 2016, after the retail and financial sectors.

According to Cisco Systems Inc.’s 2015 Annual Security Report, the legal industry is the seventh most-vulnerable industry to malware.

The American Bar Association's (ABA) 2015 Legal Technology Survey Report found that 15 percent of law firms overall—and 25 percent of law firms with at least 100 attorneys—have experienced a breach due to a hacker, website attack, physical break-in, or lost or stolen computer or smartphone. In 2012, just 10 percent of law firms overall experienced a breach, demonstrating that the threat has increased over time, albeit at a slow pace. The ABA's 2015 report surveyed about 90,000 attorneys in private practice. Sixty percent of the attorneys said that a security breach led to no significant business disruption or loss. However, perhaps more disconcerting, 47 percent said their firms had no response plan in place to address a security breach, and only a little more than half (55 percent) of the largest firms (with 500 or more attorneys) had a security breach response plan in place.

In 2012, Mandiant reported that 80 percent of the 100 biggest law firms in the United States had been hacked, although neither the survey nor Mandiant gave any further explanation on how the supposed attacks were carried out or what information was accessed.

**Notable Cyber Attacks**

In 2015 and 2016, Cyber4Sight did not identify many reported law firm breaches or attacks. If a breach were to occur at a law firm, the fact would not necessarily become public knowledge. There are more than 50 distinct data breach notification laws in the United States, many of which require the breached party to notify the affected individuals directly. That said, there are also a number of exceptions under many of these laws that would exempt breached firms from notifying their clients. Law firms, having far smaller client bases than financial institutions or retailers, could also likely notify any affected customers without the knowledge necessarily becoming widespread, given that neither the firm nor its client would be incentivized to broadcast potentially damaging information.
The following is a list of notable reported cyberthreats against law firms:

- **2 April 2016:** The U.S.-based International Consortium of Investigative Journalists (ICIJ) coordinated the publication of an extensive array of investigative reports in multiple countries, examining in detail some 2.6 TBs of information leaked through unspecified means from the Panama-based law firm Mossack Fonseca.\(^{10}\) The ICIJ claims that its inspection of the leaked documents (referred to as "The Panama Papers") reveals that Mossack Fonseca has aided—often with the help of major banks—the creation of more than 214,000 shell corporations, implicating 140 politicians and public officials in 200 countries. According to the contents of the coordinated release, Mossack Fonseca not only helps its clients hide their money, but it has also helped them evade taxes, launder money, and circumvent international sanctions.

It remains largely unclear how the leaked documents were obtained. Cyber4Sight notes that a malicious insider may have been the prime mover behind the Panama Papers, despite Mossack Fonseca’s claims to the contrary, although multiple reports highlighting the company's lackadaisical security posture make it appear increasingly likely that an external attacker compromised the law firm's networks and stole its secrets.

- **29 March 2016:** According to unnamed sources cited in a 29 March 2016 *Wall Street Journal* report, unspecified hackers breached networks at several U.S.-based law firms, including Cravath Swaine & Moore LLP, Weil Gotshal & Manges LLP—which represent Wall Street banks and Fortune 500 companies.\(^{11}\) The timeline for the breaches is unclear, but Cravath Swaine & Moore LLP stated that its incident occurred during summer 2015. The hackers reportedly threatened to attack additional unnamed law firms in unspecified Internet postings. Further, law enforcement is still evaluating what, if any, information the hackers stole.

- **22 March 2016:** Cyber4Sight identified a new ransomware sample, dubbed "Cryptohasyou," that targeted an Indianapolis-based law firm as well as the U.S. Bureau of Labor Statistics. The ransomware is distributed through a spear-phishing email message impersonating the United States Postal Service and contains a malicious attachment. According to the ransom note, Cryptohasyou encrypts victims' files with AES256 and adds the ".end" file extension to the affected files. It is unclear whether law firms and government agencies were specifically targeted by the ransomware.

- **February 2016:** According to a 3 February 2016 Flashpoint threat alert reported by a Chicago business news website, a purported Ukraine-based individual using the moniker "Oleras" advertised his phishing services to cybercriminals on the Russian-language discussion forum DarkMoney[,]cc and listed law firms as potential targets.\(^{12}\) Oleras reportedly wanted to hire hackers to break into the firms' networks and steal sensitive information for insider-trading purposes. The named targets included 46 U.S.-based and 2 U.K.-based law firms (see Appendix for full list of named law firms). Cyber4Sight notes that this activity may be related to the breaches reported on 29 March 2016 by the *Wall Street Journal*.

- **2015:** According to the Law Firm Risk Management Blog, in 2015, hackers breached a large unnamed Polish law firm and stole sensitive documents. The hackers threatened to publish the stolen data unless the law firm paid a bitcoin ransom and published a small portion of the data to demonstrate their credibility. The hackers reportedly gained access to the law firm's servers by first breaching the services of the IT company that delivered services to the law firm.\(^{13}\)

- **1 December 2014:** FireEye reported that a new cybercriminal group dubbed "Fin4" targets Fortune 100 companies to obtain unauthorized access to merger and acquisition (M&A) information, likely in an effort to gain a market advantage.\(^{14}\) An estimated 20 percent of Fin4's
targets are law firms that are advising public companies on securities, legal, and M&A matters. The group uses custom Securities and Exchange Commission (SEC) and M&A-themed spear-phishing email messages that contain embedded Visual Basic for Applications (VBA) macros to steal sensitive credentials from targeted individuals. The group's use of investment terminology and detailed knowledge of public companies suggests that members may be current or previous employees in the investment banking industry.

- **23 June 2014:** According to a report from Bloomberg, a reported 2013 hack on an unknown hedge fund was part of a larger cybercriminal campaign that consisted of attacks on multiple hedge funds, banks, and law firms over the previous 2 years. The campaign was reportedly the work of cybercriminals based in Russia and other citizens of former Soviet bloc countries. In some cases, malware was delivered via spear phishing while other targets were compromised via drive-by-download attacks. The majority of attacks reportedly originated from Russia, Ukraine, Estonia, and Bulgaria based on analysis of the attacks and the malware involved. In one case, hackers used their access to send illicit wire transfers directly, draining a hedge fund of USD 1.5M; the cybercriminals kept each transfer to less than USD 500,000, the amount that would trip internal controls at the firm.

- **12 March 2014:** Security firm Zscaler reported that a watering-hole attack on the website of U.K.-based law firm Thirty Nine Essex Street (39essex[.]com) was conducted between 24 and 26 February. During the attack, users attempting to access the law firm's website were redirected to a LightsOut (aka Hello) exploit kit (EK) landing page hosted at swissitally[.]com via a malicious iframe injection. Based on the tactics, techniques, and procedures (TTP), the attack was possibly carried out by the suspected Russia state-sponsored group Energetic Bear as part of an economic espionage campaign.

- **Early 2013:** According to an 8 July 2015 Symantec report, the Morpho cyber-espionage group reportedly specializes in the theft of intellectual property and has not been active since early 2013, when initial campaigns were carried out against organizations across various industries and sectors, including law firms, technology and pharmaceutical companies, commodities, and government. During these campaigns, Morpho was known to use Java-based zero-day exploits to drop its malware on target computers. Morpho does not seem to be a state-sponsored group, but rather cybercriminals motivated by the financial gain of using information found in these industries for themselves, or selling it to a third party. Morpho is likely a small team of highly-skilled hackers—including some with native English speaking ability—who may be operating out of the Eastern Standard Time (EST) time zone.

- **December 2012:** Cybercriminals stole an unspecified "large six-figure" sum from an unnamed Canadian law firm. The cybercriminals obtained backdoor access to the firm's bookkeeper's computer via a virus, then obtained bank account passwords.

- **2011:** Four unnamed Canadian law firms received spear-phishing email messages from unspecified attackers that impersonated partners working on an acquisition of a Chinese company. The email messages contained malicious attachments that, when opened, reportedly infected dozens of computers at the law firms.

- **2010:** Seven unnamed Canadian law firms reportedly were targeted by hackers looking for sensitive information pertaining to a proposed USD 38B bid as part of a takeover deal between BHP Billiton and Potash Corp. The breach of the law firms' networks was attributed to China's state-owned Sinochem Group, which purportedly wanted to disrupt the bid due to business concerns.
• **Unknown Timeframe:** A partner at Steptoe & Johnson LLP stated that in one instance during an unspecified timeframe, a hacker created a fake Yahoo! Email account impersonating him, then sent email messages to other lawyers at the firm with a link to a fraudulent report designed to look legitimate.\(^{22}\)

**Deep Web Activity**

Cyber4Sight notes that cybercriminals are also selling information purportedly belonging to law firms on deep web marketplaces. For example, Cyber4Sight deep web analysts identified postings from 14 November 2014 in which an individual on the closed Russian-language criminal forum novus[.]pm advertised compromised routers for sale that appeared to belong to various law firms (see below image for example of these compromised routers). The postings suggest that the compromised routers possibly would be used as SOCKS5 proxies to obfuscate activity.

**Outlook**

Cyber4Sight anticipates that attacks on law firms are unlikely to decrease in the next year, given overall trends in law firm attacks and the Mossack Fonseca incident, which demonstrated the potential windfall from a successful law firm breach. Following the release of the Panama Papers, Cyber4Sight assessed that the more damning elements of the leak would almost certainly raise the target profile of law firms and could spur retaliatory cyber attacks from various kinds of threat actors against individuals and organizations accused of corrupt behavior. The Mossack Fonseca incident very publicly highlighted the highly sensitive work that law firms engage in and the potentially embarrassing or valuable information law firms store that pertains to their clients. The Panama Papers could focus the attention of other groups that may not have targeted law firms in the past, such as hacktivists and other hacking groups interested in gathering potentially damaging information. State hacking groups may even begin to emphasize the targeting of law firms to gather intelligence about or leverage over their adversaries or even merely to monitor the behavior of businesses in their own countries.

Further, Cyber4Sight notes that law firms are experiencing increasing pressure from their clients to improve cybersecurity, which will likely have a positive impact in mitigating future cyber attacks. Reputational factors, as well as client industry regulations, are also factors driving security improvements.\(^{23}\)
Appendix

The following is a list of the U.S.- and U.K.-based law firms specified by the threat actor Oleras for a scheme to compromise the law firms' systems and steal sensitive information for insider trading purposes, according to an early February 2016 Flashpoint alert reported by a Chicago business news website:

- Akin Gump Strauss Hauer & Feld
- Allen & Overy
- Baker & Hostetler
- Baker Botts
- Cadwalader Wickersham & Taft
- Cleary Gottlieb Steen & Hamilton
- Covington & Burling
- Cravath Swaine & Moore
- Davis Polk & Wardwell
- Debevoise & Plimpton
- Dechert
- DLA Piper
- Ellenoff Grossman & Schole
- Freshfields Bruckhaus Deringer
- Fried Frank Harris Shriver & Jacobson
- Gibson Dunn & Crutcher
- Goodwin Procter
- Hogan Lovells
- Hughes Hubbard & Reed
- Jenner & Block
- Jones Day
- Kaye Scholer
- Kirkland & Ellis
- Kramer Levin Naftalis & Frankel
- Latham & Watkins
- McDermott Will & Emery
- Milbank Tweed Hadley & McCloy
- Morgan Lewis & Bockius
- Morrison & Foerster
- Nixon Peabody
- Paul Hastings
- Paul Weiss Rifkind Wharton & Garrison
- Pillsbury Winthrop Shaw Pittman
- Proskauer Rose
- Ropes & Gray
- Schulte Roth & Zabel
- Seward & Kissel
- Shearman & Sterling
- Sidley Austin
- Simpson Thacher & Bartlett
- Skadden Arps Slate Meagher & Flom
- Sullivan & Cromwell
- Vinson & Elkins
- Wachtell Lipton Rosen & Katz
- Weil Gotshal & Manges
- White & Case
- Wilkie Farr & Gallagher


