LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 15
Date: December 19, 2017

Law Firms are Cybersecurity Targets

Roy Moore Scandal Used for Phishing Schemes Aimed at U.S. Law Firms

- This podcast was inspired by an article from cyberscoop.com that not only shows that law firms are a target by nation states, but the attackers also keep up with current news.
- The cybersecurity firm FireEye released a report disclosing that, since at least June of 2017, Chinese hackers have been actively targeting a shortlist of multinational law firms in an apparent effort to spy on lawyers and steal confidential information.
- The hacking group is known as APT19. APT, as we all know, is an acronym for advanced persistent threat, which is a phrase that was pretty much coined for Chinese attackers years ago. APT was one of the "sexy" acronyms that many security vendors were using extensively a few years ago. The APT hacker groups are followed so closely that we actually give them names, however the names just aren't really creative, as the name "APT19" demonstrates. Their methods of attack (as this article shows) can be creative. Regardless of names and creativity, the groups are very skilled and can be difficult to detect. When we discuss "dwell time" of attackers that can be months before detected, APT type groups are what we are referring to.
- The APT groups go-to attack vector is often well-designed phishing campaigns that contain references to pertinent, high-profile U.S. news stories. Most recently, these booby-trapped emails have separately mentioned U.S. Senate candidate Roy Moore, disgraced Hollywood producer Harvey Weinstein, and former presidential candidate Hillary Clinton. While I have seen a lot of APT phishing schemes in my career, this was definitely a fresh approach.
- FireEye says APT19 crafted the subject line "FW: Roy Moore scandal ignites fundraising explosion for Democratic challenger Doug Jones" to seemingly capitalize on the contentious campaign to fill the vacant senate seat in Alabama.
- FireEye has evidence of at least three law firms being repeatedly and continuously targeted as part of APT19's latest activity. These organizations are based in the U.S. but have offices globally, including in China. All three firms boast business internationally, offering various legal practices.
- In each case, the emails carried malware inside a Microsoft Word document. When opened, the document would covertly download an open-source backdoor onto the victim's computer before then establishing a connection to the attacker's own server. This backdoor can provide APT19 attackers with wide access to a compromised device, as well as the network it is connected to.
- At that point, they look like valid users who work to elevate privileges, then work tirelessly for days, weeks, and months to pilfer valuable information that law firms possess.

Takeaways

- Law firm data breaches are not often in the news, but they are happening at an alarming rate. The reason we don't hear about them is that they do not have a duty to disclose to the public, in most cases, when they do experience a compromise and subsequent breach.
- However, firms are and will continue to be a ripe cybersecurity target for a couple of key reasons.
    - The first reason is that they possess very sensitive and valuable M&A information involving companies in foreign nations, which is likely what the objective of this "Roy Moore" campaign was.
        - However, there are numerous other sources of extremely valuable and sensitive information, such as financial fraud and tax evasion from the Panama Papers hack, New York City firms breach seeking insider trading information that involved Cravath and Weil, the Weily Rein attack in 2012, in which the Chinese group (may not have been naming them then) wanted information related to SolarWorld, the German-based manufacturer that produces solar panels, or even smaller firms we are working with that are being targeted—and falling prey to—expense business email compromise attacks. (Links in references below)
        - In addition, law firms may also store payment- and HIPAA-related information, along with valuable patents. Yes, law firms are juicy targets for valuable information.
    - The second reason most law firms do not take cybersecurity seriously enough is that there are no specific compliance requirements for them to do so. Their customers are the ones putting pressure on them to demonstrate the strength of their cybersecurity posture.
- I have been giving cybersecurity talks and developing newsletters for the legal community for more than 10 years that address the cybersecurity risks to law firms and actions that should be taken.
- All the way back to 2010, law.com was publishing articles such as "Firms slow to awaken to cybersecurity threat," and the FBI has been working to raise awareness for law firms since 2009 after a high-profile breach of a law firm in 2008. Links to both articles are in the references below.
- The truth is that law firms experience the same types of attacks from skilled groups as many other industries. The same frameworks and approaches are just as valuable to them to help build the needed resiliency.
- These are some of the same steps we discussed in the recent podcast Episode 13 — "Information Security Questions for SMBs."

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC's security services, he is also the practice lead for the organization's incident response, forensics, and litigation support practice.

References:

https://www.cyberscoop.com/roy-moore-scandal-phishing-attacks-apt19-fireeye-harvey-weinstein/

http://www.abajournal.com/magazine/article/law_firm_hacking_history

https://www.forbes.com/sites/jasonbloomberg/2016/04/21/cybersecurity-lessons-learned-from-panama-papers-breach/#65bdfaf52003

https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504

https://www.law.com/nationallawjournal/almID/1202445679728/?slreturn=20171106214416

http://www.nbcnews.com/id/33991440/ns/technology_and_science-security/t/fbi-hackers-targeting-law-pr-firms/#.WiirLLQ-fq0