TLP WHITE

Cyber threats to the legal sector and implications to UK businesses

Contents

Executive summary

The legal sector is a vital component of UK business and government infrastructure, holding personal, business critical and commercially sensitive information. As such CERT-UK assesses that it presents an attractive target to malicious actors in order to:

- Attack the law firms directly; seeking to extort and defraud through ransomware and phishing campaigns
- Target client's data; where the law firm represents the weakest point in the cyber security chain or utilise a network or relationship in order to conduct a third party or supply chain attack

CERT-UK judges that law firms are an attractive target in their own right and as a means of accessing their clients. Despite this, the awareness and resilience within the sector does not match the threat, with 62% of law firms estimated to be the victim of a cyber-attack in the last year, whilst only 35% of law firms have a mitigation plan in place in the case of an attack.

In particular there has been an increase in the number of malicious actors seeking to extort or defraud law firms as cyber criminals have begun to identify the legal sector as a vulnerable and profitable industry. In tandem with this, more traditional surveillance and disclosure attacks have continued.

This paper provides an overview of the trend of attacks against the legal sector, including motivations and methodologies as well as some symptomatic case studies.

Introduction

Confidentiality is integral to the business model of any law firm. The information held by the legal sector is often highly personal, business critical or commercially sensitive, and is consequently clearly valuable. As much of this data is hosted both on- and off-site, robust cyber-security is critical to retaining confidentiality, integrity and availability.

The last 12 months have seen several law firms suffer high profile breaches, indicating perhaps, that the cyber-security standards of the sector are not in line with the threat, something which has not escaped the notice of threat actors themselves. Legal organisations in the UK should be aware that they are a high value target and therefore need to make additional efforts in order to increase their cyber resilience and reduce the impact of a cyber-attack.

62%

The number of law firms victim of cyber-attack

4.5%

of all UK data breaches occur in the legal sector

In 2015 the PWC annual law firm survey reported that 62% of law firms had been a victim of cyber-attack, showing an increase of 17% from 2014[1]. The Information Commissioner's Office (ICO) also reported a 32% increase in data breaches from the legal sector in 2015, which now account for 4.5%[2] of all UK data breaches.

As an industry, the legal sector has come under increased scrutiny. Cisco ranked law firms as the 7th most vulnerable industry to malware in 2015[3], the first time the sector appeared in the ranking. Critically, law firms are not legally required to disclose data breaches to the public and, as such, it is assessed that the number of reported cases represent only the tip of the iceberg. This is already starting to have a commercial impact on the sector, and in February 2016 Elite insurance announced its withdrawal from the solicitor's professional indemnity market, citing concern about increased risk of cyber-attack[4]. If professional industries are spooked, how long until clients begin to turn away?

An attack on a law firm would not impact the legal sector alone; law firms are integral to almost every industry in the UK. Larger corporations in particular should be aware that if they have invested heavily in their own cyber-security, the law firms they employ may represent the weakest link in the cyber-security chain and a potential avenue for a supply chain or third party attack. If you are unsure or concerned about the cyber-security of your suppliers you can refer to the CERT-UK paper on cyber-security risks in the supply chain, and seek assurances from your suppliers that they adhere to a professional standard, such as Cyber Essentials.

Is the legal sector being targeted?

The nature of the everyday business conducted by the legal sector requires large numbers of documents to be created, circulated and contributed to across an organisation. Files such as PDFs, Word documents and Excel sheets are critical to the digital fabric of any effective law firm. However, file attachments as a threat vector are on the rise, in particular through macro delivery and phishing. Therefore, as document transfer is vital to the operational infrastructure of law firms, it is critical to invest in cyber-security resilience. In particular organisations should consider extensive user education on the risks associated with opening email attachments from unknown senders, and in particular of allowing attachments from unknown senders to run macros which may download malware without user knowledge.

This challenge is compounded by the nature of the working environment in the legal sector whereby remote working and 24/7 contact with clients may be required. As a result, lawyers are perhaps more tempted to operate on unprotected connections and on less secure devices. The use of multiple devices can make the implementation of effective patch management extremely difficult, leaving the network exposed to vulnerabilities. Organisations should consider employing device management software which allows oversight and control over

[1] http://www.lexology.com/library/detail.aspx?g=62a99a2e-cff3-4e2d-a047-11a4adac64f6
[2] http://www.lexology.com/library/detail.aspx?g=62a99a2e-cff3-4e2d-a047-11a4adac64f6
[3] http://www.bloomberg.com/news/articles/2015-03-11/most-big-firms-have-had-some-form-of-hacking-business-of-law
[4] http://www.scmagazineuk.com/cyber-security--kryptonite-for-lawyers/article/489116/

endpoints, or if employees are using their own devices, introducing clear bring your own device (BYOD) policies which dictate appropriate work place use.

> "A number of law firms believe they were too small or obscure to warrant the interest of professional hackers"

Oversight is an issue which extends beyond individual organisations and their devices. Cisco has observed that although solicitors and barristers are regulated by several authorities, including the ICO, Solicitors Regulations Authority (SRA), Bar Council and Law Council, the language used prefers "should" over "must"[5] leaving greater opportunity for non-compliance. This is in stark contrast to organisations such as the Financial Conduct Authority (FCA) which adopt a much harder line[6] in both language and approach to regulating cyber resilience.

The final factor is employee education and organisations' perception of the threat. In a 2011 report PwC found that "a number of law firms believe they were too small or obscure to warrant the interest of professional hackers"[7]. For many SMEs cyber resilience is not featured on their risk registers and so has limited engagement at senior level[8]. This is underpinned by Legal Week's Benchmark survey, which found that only 35% of law firms had a response plan in place for cyber-attacks, compared to 52% of non-legal professions[9]. In a recent Managing Partner Survey[10] it was found that only 22% thought cyber-security should be the responsibility of the managing partners and less than a quarter (24%) believed that it was the responsibility of all employees. As a result, user education and training is often limited and viewed as a compliance exercise.

35%

the amount of law firms that have a response plan in place for cyber attacks

CERT-UK recommends that cyber resilience should be considered at all levels up to board level responsibility.

Why the legal sector is a valuable target

The information held by law firms is sought out by a swathe of malicious actors with a variety of motives and objectives. CERT-UK has identified several key reasons for malicious actors to target the legal sector.

[5] http://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf
[6] https://www.axelos.com/CMSPages/GetFile.aspx?guid=994a0a2e-c566-4633-a5be-457a5401812d
[7] https://www.pwc.com/us/en/law-firms/assets/pwc-safeguarding-your-firm-from-cyber-attacks.pdf
[8] https://www.schillingspartners.com/news-and-opinion/cyber-attacks-on-the-legal-sector
[9] http://www.legalweek.com/digital_assets/6602/013-024_LW_0305_Benchmarker_FINAL_for_WEB.pdf
[10] http://www.managingpartner.com/news/risk/uk-law-firms-are-failing-tackle-their-greatest-risk-cybercrime

Profit

This is the primary driver for cyber criminals and extends beyond direct theft to include fraud by collaborating with a wider criminal network and extortion through withholding or threatening to release client data. Economic espionage group Wild Neutron (AKA Jripbot, Morpho and Butterfly) is assessed to target law firms as part of broader campaigns to reach their intended final victims.

Known to use a combination of exploits, watering holes and multi-platform malware, Wild Neutron's activities became notorious in 2013 when they successfully infected companies such as Apple, Facebook, Twitter and Microsoft[11]. The group is assessed to be financially motivated and serves as a sobering example of the advanced capabilities at the disposal of threat actors targeting the legal sector.

Theft

Law firms are increasingly the victims of theft directly, with cyber criminals attacking them in order to commit financial fraud. Insurance Company QBE have reported that £85 million[12] has been stolen from British law firms in the past 18 months. Hackers have learned that law firms often transfer funds on a Friday (the day when housing deals tend to complete) and 150 law firms were successfully targeted by "Friday Fraud" with many more attempts unsuccessful. It is interesting to note that this attack method is not new, only the cyber element is innovative, in the past criminals would conduct similar social engineering fraud over the phone.

£85,000,000 has been stolen from UK law firms in the past 18 months

Fraud

Law firms play an integral part in commercial enterprise, specifically regarding litigation, mergers and acquisitions. As such, cyber criminals seek to exploit this data through fraud such as insider trading or selling information to a third party.

In early 2016, a cyber criminal posted their intent to infiltrate 48 law firms' networks, including several which are headquartered in the UK with the stated aim to acquire information about merger agreements, letters of intent, confidentiality agreements and share purchase agreements[13] in order to facilitate what would likely become an insider trading enterprise. The post also included a list of potential targets for a phishing campaign targeting law firm employees by sending them a phishing email appearing to originate from a trade journal asking to feature them for excellence in M&A[14].

[11] http://www.kaspersky.com/about/news/virus/2015/Wild-Neutron-Mysterious-Cyber-espionage-Actor-Returns-with-New-Tricks-and-Victims
[12] http://www.ft.com/cms/s/0/2c5340fe-f0fa-11e5-9f20-c3a047354386.html
[13] http://www.chicagobusiness.com/article/20160329/NEWS04/160329840/russian-cyber-criminal-targets-elite-chicago-law-firms
[14] http://www.chicagobusiness.com/article/20160329/NEWS04/160329840/russian-cyber-criminal-targets-elite-chicago-law-firms

Extortion

Another avenue of approach is the use of extortion in order to extract payment. This can be achieved by either preventing firms from accessing data through the use of ransomware or by leveraging sensitive data directly by employing blackmail. In May 2016 CERT-UK received several reports of a highly targeted and persistent phishing attempt against UK law firms and UK organisations' legal departments. Figure 1 is an example of an email targeting a legal department.

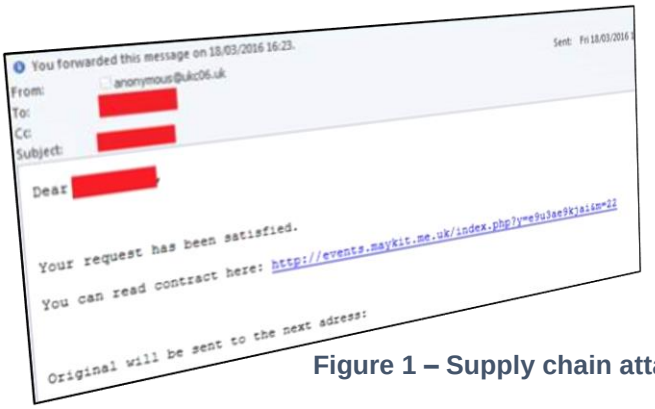

Figure 1 – Supply chain attack

It attempts to lure the target into opening an attachment suspected to contain Locky ransomware. In this case the attack was not successful. The encryption, and potential loss of data could be ruinous and as such it is vital to have a comprehensive back-ups procedure. CERT-UK recommends regular back-ups and tested restore procedure covering the entire estate in order to prevent an effective ransomware attack. Malware is not the only means of extortion; CERT-UK have been made aware of SQL injection attacks being used in conjunction with brute force attacks to compromise law firm's extranets, allowing the attacker to access the client view of case statuses. This type of breach is often accompanied by extortion demands and the threat to release client case details online.

Information

Valuable assets in the form of Intellectual property and patents are another commodity which are particularly sought out by APT groups. Organisations that operate abroad should consider that in some regions, cyber reconnaissance will be conducted in order commit intellectual property theft, corporate espionage or simply due diligence. In some cases this activity may be supported by both the state and the private sector.

Law firms may represent the weakest link in the chain to reach their clients' data

Many UK businesses employ law firms and are often a trusted partner with high levels of access within an organisation, making them a perfect vehicle for supply chain and third party attacks. In 2013 BAE systems identified a legal firm which was being used in a "watering-hole" style attack; an infiltration method wherein a legitimate site is compromised in order to deliver malware to visitors of the site.

The activity was attributed to a well-publicised cyber espionage group, known as Havex (AKA Energetic Bear) where a compromised website belonged to a London based barrister's chambers. The group were known to be targeting the energy sector, with a focus on the UK market in particular, and it is possible that the barrister's chamber in question were targeted

due to information related to a specific case or their expertise in the energy sector. This example serves to highlight that legal companies themselves may not be the target of a cyber-attack, but that they represent the weakest link in the chain to reach their clients' data.

Exposure

Law firms often hold their clients' data over a period of many years, sometimes decades. Much of this information can retain its potency and be personally, politically or commercial sensitive regardless of how much time has passed. In 2012, AntiSec, a division of the hacktivist group Anonymous hacked a US based law firm in order to expose the "rich and powerful oppressors"[15].

Whilst these types of attacks may have little impact on the functionality of a law firm, the impact on brand and reputation can be catastrophic. On 3 April 2016 the German newspaper Süddeutsche ZeitungIn published a series of documents belonging to the law firm Mossack Fonseca. These documents were a small proportion of the significant data breach known as the Panama Papers, which collectively describes 11.5million leaked documents detailing financial and attorney client information that dates back as far as 1970s. At 2.6 terabytes, this was the largest data breach in history.

Founding partner Ramon Fonseca has stated that the incident was "an unauthorised breach of our email server" and not an "inside job"[16], whether or not this is accurate, increased scrutiny of Mossack Fonseca's security has revealed concerning cyber-security weaknesses. It is highly unlikely that these weaknesses are unique to Mossack Fonseca, but rather, are representative of some systematic cyber weaknesses which exist across the entire sector.

The Mossack Fonseca client portal had not been updated since 2013 and contained several security weaknesses. One such vulnerability was DROWN, a well-publicised exploit targeting servers supporting SSL v2 protocol. Furthermore the client portal used an outdated version of the Drupal open source CMS platform, which is known to contain at least 25 vulnerabilities including an SQL injection vulnerability which allows a malicious actor to remotely execute arbitrary commands[17]. The website was also running one of the most common WordPress vulnerabilities (Revolution Slider) and, at the time of the data breach, not securing the web server behind a firewall[18].

> The critical lesson is to ensure a patching policy is in place

The key point is that organisations must ensure a patching policy is in place. In the case of Mossack Fonseca it was possible for the attacker to remove huge amounts of data without raising any security flags. Organisations should be aware of normal traffic flows, base-lining traffic as a metric to identify where increased data flow may indicate a data exfiltration attempt.

[15] http://www.lexology.com/library/detail.aspx?g=62a99a2e-cff3-4e2d-a047-11a4adac64f6
[16] http://www.bbc.co.uk/news/world-latin-america-35975503
[17] http://www.wired.co.uk/article/panama-papers-mossack-fonseca-website-security-problems
[18] https://www.wordfence.com/blog/2016/04/mossack-fonseca-breach-vulnerable-slider-revolution/

Conclusion

The threat from APT groups seeking to extract client data remains prevalent, but organisations should be aware that criminal groups are now also seeking to extort law firms, and the rising trend of ransomware should be of particular concern. As cyber-security has become part of the operational fabric of large organisations such as banks and those involved with critical national infrastructure, threat actors are being forced adopt innovative and less direct attack vectors. A cyber-attack on a legal institution could have a significant impact, to an organisation and their clients, who may be the intended targets. Client data in particular may be the target of sophisticated and persistent threat actors.

CERT-UK assesses that the current cyber resilience of the legal sector does not match the threat. It is likely that a significant breach in this sector will occur if cyber-security is not a board level priority and employee education is introduced across all levels of an organisation, indeed it is likely that several breaches may have already happened. CERT-UK recommends following the 10 Steps to Cyber Security as a starting point and ensuring that any organisations who hold your organisations data do the same.

www.cert.gov.uk
@CERT_UK

A CERT-UK PUBLICATION