TRAVELERS

TRAVELERS CYBER BULLETIN MAY 2020

Covid-19

Since the Coronavirus outbreak, there has been a significant increase in cyber-attacks. Cyber criminals are using the pandemic as a platform to launch new and sophisticated attacks – typically through phishing campaigns.

The phishing attacks encourage users to click on malicious links or files by offering information about the pandemic, which allows the hackers to steal sensitive data or distribute malware. As the pandemic continues, more and more people are searching online for information regarding COVID-19. Attackers are capitalising on this and are sending emails pretending to offer health advice from reputable organisations such as the World Health Organisation (WHO), when in fact it is a phishing attack. Other attacks include providing files on coronavirus 'hotspots' and offering donation links to COVID-19 charitable causes. The attacks are often a mix from both financially motivated criminals to nation-state supported hackers who are exploiting the global health crisis. As the pandemic goes on and more people are using the internet to work and socialise, there are more opportunities for cyber criminals to attack. Users should protect themselves by remaining vigilant, practicing good cyber hygiene, and getting news updates about the pandemic from reputable sources.

Cyber Security Risks of Remote Working

Globally, businesses, including law firms, are being severely impacted by the Coronavirus. The pandemic has caused a shift in normal working practices resulting in an increase of home and remote working. There are various cyber security risks associated with remote working and combined with the disruption and panic caused by the pandemic, the risk of cyber-attacks on remote workers has significantly increased. The adjustment to mass remote working has resulted in vulnerabilities which cyber criminals are taking advantage of.

Due to the nature of remote working, more law firms are being forced into sending multi-media files and documents via email. This results in the data being more exposed, especially if the network used by remote workers is not secure and encrypted. Cyber criminals can use this to their advantage, posing as a trusted entity and making requests which appear legitimate. For example, posing as a senior executive authorising a fund transfer or requesting financial information. Due to the working from home conditions, it is harder to verify requests and therefore easier to make mistakes.

Mass remote working has left law firms at higher risk for cyber-attacks. Firms should implement strategies to protect themselves and employees. This can be achieved through training, using Virtual Private Networks, two-factor authentication, and consistent telephone communications.

IN ASSOCIATION WITH

xcyber®

THE HUMAN SIDE OF CYBER®

VPN Vulnerabilities

Since the Coronavirus outbreak, numerous organisations and their employees are now operating remotely. As a result, Virtual Private Network (VPN) programs have become paramount in the secure running of organisational tasks. A VPN is a private network that connects remote sites or users together. It allows for employees to remotely access resources from their company network whilst encrypting data as it travels from one place to another over the internet.

Due to the increase in VPN usage, cyber criminals have begun looking for vulnerabilities in VPNs which they can capitalise from. There have been several security flaws found in popular corporate VPNs which can be used to silently break into a company's network and steal sensitive data.

In January this year, warnings were issued following reports of particular VPN services being unpatched. Any unpatched VPN systems pose a serious risk to the security of a business, and allow cyber criminals to gain access to remote networks where they can then carry out attacks such as ransomware. Firms should ensure that the VPN service they are using is patched and up to date to ensure the upmost protection against attacks.

Managed Service Providers

Managed service providers (MSPs) have become a key focus for cyber criminals. An MSP is a company which remotely manages customers' IT infrastructure. Numerous organisations use MSPs as they are often more cost effective, have readily available infrastructures and allow access to highly qualified and experienced IT personnel. Typically, MSPs have access to the systems of multiple customers, enabling attackers to launch malicious attacks on numerous organisations with just one hack. Once an attacker has infiltrated an MSP, they are able to move laterally within the MSPs large network of customers and exfiltrate data. A report on 'The State of MSP Cybersecurity 2019' showed that 74% of MSPs reported being victim to at least one cyber-attack in 2019. One of the main roles of an MSP is to protect and secure their customers data. However, they can often overlook their own security. Gregg Lalle (Connect Wise Senior VP) compared it to "the cobbler who builds shoes for everyone, but whose son goes to school with no shoes".

MSPs provide a valuable target to cyber criminals because they have the potential to extract data from a large audience. Therefore, any companies using MSPs should be extra vigilant and ensure cyber security is of the upmost priority to them. Both MSPs and their customers must work together to rejuvenate their cyber security and have a proactive and collaborative approach to protect themselves from cyberattacks.

Dangers of LinkedIn

In today's modern society, more and more of our lives are being shared online. Social media platforms such as Facebook, Twitter and LinkedIn can reveal a lot about a person. Cybercriminals are beginning to capitalise on the information voluntarily provided by users on these sites to tailor and launch new attacks. Attackers can gather publicly available information on an organisation or employee in order to enhance a cyber-attack and increase its success rate.

Cyber criminals have been using LinkedIn, a popular social network for legal professionals, to obtain information to inform cyber-attacks. One way in which the platform is being used by cyber criminals is as a means of gathering personal information on a target such as their job role, place of work, connections, and professional history. These details can then be used to refine phishing attacks, using relevant content, and being sent from a reputable and relatable source.

Another way in which cyber criminals are using LinkedIn for planning attacks is by researching companies and finding their vulnerabilities. They can determine the structure of an organisation and then target the weakest part. For example, new joiners at a company can be identified which are an attacker's ideal prey. They are fresh to the firm, more vulnerable and will be more likely to act upon request to prove themselves. It is imperative that firms encourage safeguarding of company information and data and for employees to be mindful of the potential risks of any disclosure of personal data.

Insider Data Breaches

Internal data breaches are an increasing problem within the legal sector. Data breaches often occur as a result of cyber criminals gaining unauthorised access to a computer system and stealing confidential and sensitive data. Due to the wealth of sensitive data law firms handle, the legal sector is at higher risk for cyber-attacks that aim to exfiltrate data. Attackers often use phishing attacks to penetrate a law firm's network. They prey on human error and tailor attacks accordingly to trick users into making a mistake. According to the UK Information Commissioners Office (ICO) human error was the cause of 90% of cyber breaches in 2019.

Attackers often target vulnerable employees and use human behaviour to their advantage to engineer successful phishing attacks. Often, when sending a phishing email, attackers will add time pressure or appear to be from a higher authority to put strain on an individual to complete a task promptly and without hesitation. As a result, employees often click on malicious links or attachments without thinking, allowing the attacker access to the company's network. An 'Insider Data Breach Survey' by Egress (2020) found that 27% of respondents from the legal sector had accidentally shared or leaked company information and 29% were found to have deliberately shared company information. An effective security awareness strategy should be implemented by firms which trains employees to look out for phishing emails. The main ways to detect a phishing email include looking at the senders' email address, identifying any spelling mistakes or poorly written requests and being wary of any suspicious attachments or links.

Ransomware

It has been predicted that by 2021, globally, businesses will fall victim to a ransomware attack every 11 seconds. This is more frequent from every 14 seconds, as seen in 2019. Although the prediction is based on historical cybercrime figures, it aligns with findings from early 2020 already. Despite businesses preparing and strategising against cyberattacks, cyber criminals are equally preparing and strategising, resulting in ransomware being a prevalent issue showing no signs of slowing down.

Ransomware is already an apparent theme for recent cyber-attacks in the legal space. Two Canadian law firms fell victim to a ransomware attack in April this year which left staff without access to computer systems, and locked out of digital files, emails, and data backups. Lawyers were unable to access client lists, financial information, and other electronic files which are intrinsic to the day-to-day operations of the firm. The two firms were believed to have been infected with the ransomware by a malicious link or attachment in an email being opened, which in turn infected the entire system.

Law firms remain an ideal target for ransomware attacks as they are very dependent upon the data they hold and often this data is extremely sensitive. As a result, cyber criminals are continuously developing and improving techniques to launch successful attacks against them. It is vital that firms stay vigilant and prepared. The Solicitors Regulation Authority has told firms to ask themselves, "When will we be targeted by online criminals, not if?".

> *Comment:* Ransomware is an cyberattack which blocks access to computer systems or files until a sum of money has been paid has been paid.

Maze Ransomware

The notorious ransomware group known as Maze had a widespread ransomware campaign In January. Maze turned its efforts to the legal sector in early February, with at least five law firms being infiltrated. Maze's modus operandi was not to only encrypt the law firm's data but to also steal it, using the exfiltrated data as a leverage. They name and shame their victims by publishing the companies name on a website whilst awaiting payment. If the payment is not forthcoming, Maze often publish small portions of the stolen data on the website as proof they have the data. "It's the equivalent of a kidnapper sending a pinkie finger" according to Brett Callow (threat analyst at Emisoft). Once payment has been made, the name is removed from the website.

Two of the affected law firms had sensitive data published, including client information. It is believed Maze used malicious email attachments to infect the networks of the affected law firms. Due to the Maze ransomware being distributed via email, it is important that firms encourage staff to be cautious when clicking on links and attachments and always verifying requests that seem suspicious.

Impacts of Ransomware

Ransomware can affect businesses in various ways, with the most prevalent being the temporary or permanent loss of company data and / or the disruption to regular operations. This in turn can have a negative impact on an organisation as it can lead to financial loss, reputational damage, and complete closure of company operations. For example, in March, a legal services company (Epiq) identified a ransomware attack which resulted in the company taking its global systems offline. The company became infected with the TrickBot malware which is spread through phishing emails. Once installed, TrickBot harvests data including passwords, files and cookies before spreading throughout the network to gather more data. The ransomware attack affected the companies 80 global offices and computers. Due to the platforms being taken offline, legal clients were unable to access documents needed for court cases and deadlines.

The cost of ransomware is rising year on year and is predicted to cost $20 billion by 2021. However, the cost of a ransomware attack goes beyond the pay-out sum. The loss of data and disruption to operations can cost significant amounts, which damages the business further. The crippling effect of ransomware can be long lasting, particularly when financial and reputational damage has occurred. Law firms should protect themselves against ransomware attacks by implementing cloud-based backups, using secure systems, and working with strong cyber security teams.

Further reading

VPN & Remote Working

ZdNet.com	https://www.zdnet.com/article/covid-19-with-everyone-working-from-home-vpn-security-has-now-become-paramount/

Data Breaches

Infosecurity Magazine	https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/
SC Magazine	https://www.scmagazineuk.com/legal-sector-prone-data-breaches-ever/article/1678303

Ransomware

National Law Review	https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion
Newsbreak	https://www.newsbreak.com/indiana/evansville/news/0O51fHNl/local-law-firm-hit-with-ransomware
Bleeping Computer	https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-14th-2020-targeting-msps/
Emsisoft	https://blog.emsisoft.com/en/35486/warning-to-law-firms-a-ransomware-group-is-stealing-data-and-posting-it-online/
Security Week	https://www.securityweek.com/legal-services-firm-epiq-hit-ransomware?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Securityweek+(SecurityWeek+RSS+Feed)
SC Magazine	https://www.scmagazine.com/home/security-news/ransomware/maze-ransomware-publicly-shaming-victims-into-paying/
Safetyde	https://www.safetydetectives.com/blog/ransomware-statistics/

About Us

Solve commercial problems with state-grade intelligence expertise. We are a bespoke cyber intelligence company with extensive experience in producing actionable intelligence for our clients. Our team are pioneers in cyber and the company draws its talent from former members of the UK's Public Sector, who bring with them many years of **outcome-driven, operational cyber experience** and specialised skills working across numerous Government departments and the UK's Intelligence and Security Agencies.

We focus on producing **intelligence-led, data-driven** and **evidence-based** reporting which enables decision making across our clients' varying needs. All our intelligence is delivered in qualitative, narrative format, providing actionable information that is easy to digest.

Our clients rely on our ability to do **scalable technical work**, translate that into human-readable analysis and actionable leads, all while maintaining a team culture that - in partnership with our clients - increases value through its **candour** and **integrity**.

Our modus operandum is to be a **strategic consultative partner**, led by a team of some of the most experienced professionals in cyber intelligence across the entire world. Together they have been working to develop and deliver effective solutions to some of the most **complex and challenging cyber** problems faced in both the public and private sectors.

Our current portfolio of client intelligence requirements includes the following thematic areas, across multiple geographic regions and sectors:

- Internal investigations (including insider threat), counter-intelligence, and specialist research (including counter terrorism, unlawful activism, and election integrity);
- Online reputation and defamation investigations, intellectual property and brand infringement (including counterfeiting and responding to disinformation campaigns);
- Countering cyber-enabled fraud and criminality (investigating and lawfully disabling the criminal ecosystems);
- Cyber risk and advisory at strategic, operational and tactical levels - including data protection, privacy and security;
- Supplier and supply-chain assurance, competitor analysis, crisis and breach response, red-teaming, and personal risk reports for executives.

To learn more about how **XCyber®** can support your business and clients, please contact our London, Mayfair office on the following address:

enquiries@xcybergroup.com

Our operational requirements team will be pleased to meet you.

xcyber®

THE HUMAN SIDE OF CYBER®

If you have found this useful and would like to receive these quarterly updates direct to your inbox please **click here** to register

The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document.

TRAVELERS

Travelers operates through several underwriting entities through the UK and across Europe.
Please consult your policy documentation or visit the websites below for full information.

travelers.co.uk travelers.ie