Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Keeping ahead of the phishing curve

Lior Kohavi, Cyren

The Covid-19 pandemic flipped the world on its head and triggered major shifts in day-to-day activity. However, it also caused noticeable acceleration of the digital transformation already underway, forcing companies to develop and speed up their online presence in order to survive the volatile climate.

Despite the initial disruption, businesses have proven that they can maintain operations from completely remote environments, and research has shown that both buyers and sellers actually now prefer digital self-service and remote human engagement over in-person interactions.¹ For all businesses, though, large and small, there is one very real threat that can always be relied upon to make an appearance – phishing.

Phishing attacks are still the most prominent form of threat vector due to their versatile nature and ability to grant hackers access to vulnerable employees.² Since most companies have shifted to running their business almost exclusively online, they have been even more susceptible to the varying forms of phishing, including spear-phishing and business email compromise (BEC). Websites have been a big part of phishing campaigns in recent months, given the number of online businesses being set up across the globe. Websites offer companies more credibility and stronger customer trust, but they also provide criminals with a front to mask their malicious activities.

Website builders and content management system (CMS) platforms have been a valuable service to organisations and criminals alike. Their simplicity, accessibility and minimal costs make them the perfect way to set up an online presence in a short space of time. This, combined with the onslaught of phishing attacks, makes for a very real threat to online businesses.

**Threats on the rise**

New trends have emerged within the phishing threat vector, including the use of user-generated content (UGC) platforms. With UGC, criminals are able to develop their own phishing pages, or make use of compromised websites. Common website platforms, like Weebly, Squarespace and Wix, are used to help create these phishing pages, and are often overlooked by workers and security systems as they are typically used for legitimate activity.

"**Findings from Google show that two million new phishing sites were created in 2020, with further research revealing a 73% increase in phishing emails across the board**"³⁴

Employees being familiar with these different platforms enables bad actors to carry out their attacks, making them the ideal resource for their campaigns. To make matters worse, threat actors are also known for using a technique known as delayed activation, meaning that the attack does not necessarily begin when the email/malicious link enters the inbox. Victims may be directed to a phishing page that appears legitimate, but the attack does not commence until the criminal is ready. This could take minutes, hours or even days after the original message is received.

Companies are being swamped with email attacks on a daily basis, a lot of which never make it to the inbox, but there are always those that do. Findings from Google show that two million new phishing sites were created in 2020, with further research revealing a 73% increase in phishing emails across the board.³⁴ It has been so easy to communicate and complete business with customers and partners online that criminals have jumped on the chance to exploit these channels.

**Recognising past attempts**

Such is the way with cyber security, businesses often don’t know which avenue criminals are going to take until it’s too late. But good practice is to keep tuned in with what the latest criminal trends are so that we can better understand which defence solution is needed. Here are three examples of how criminals have used UGC platforms for their attacks.

Known for using all resources at their disposal, cyber criminals will often make use of compromised web pages to carry out their attacks. WordPress is a particularly popular target, as there are common exploits that allow adversaries to set up malicious content which would go on to infect the victim’s device. Additionally, the site is often used to link to phishing pages where data and credential theft could take place. This could include a fake Microsoft log-in page which would record user credentials and send them straight through to the bad actor in order to carry out further exploitation.

In other instances, however, criminals...
will often set up their own phishing pages using cheap and easy website builders. One such attempt used Wix, where the target was sent a fake verification email for one of their online accounts. The link took the user to the disguised phishing page and any credentials submitted were given to the criminal.

These types of attacks can also be taken further with multiple stages. These multiple stage/phase attacks often appear far more sophisticated and so can be harder to identify. One attempt used two site builders, Weebly and Zyro. The victim received an email with a link to a newly shared encrypted document. The link, however, took them to the first stage of an attack, in the form of a SharePoint site created using Zyro. Once the user clicked ‘preview document’, they were taken to the final stage of the attack, which was a fake Outlook365 page. From there, any passwords and credentials given would be sent to the attacker.

User training

A lot of companies resort to security awareness training (SAT) as one of their primary defences against phishing attacks. SAT focuses on advancing employee knowledge of the cyberthreats that wait just outside their inboxes. There is no doubt that maintaining good awareness over what techniques are being used by criminals gives workers a fighting chance at spotting them before they do any damage. But is this really enough?

As we’ve seen, phishing techniques are rapidly growing in sophistication, with many attempts successfully making it past the security defence line. By using legitimate web builders and cunning social engineering techniques, criminals are able to create a convincing facade that they work on behalf of a legitimate source.

Unfortunately, the artificial training commonly used as part of SAT is no longer sufficient for strengthening business cyber defences. The training is often applied in an ad hoc manner, meaning that the knowledge gained is unlikely to take hold for any meaningful length of time. Further, SAT is repeatedly positioned as being a solution to the main problem – ie, employees. Creating the mindset that each employee is a threat to business security is a counterproductive activity as workers will become less motivated about protecting the company and will be more focused on impressing their employer.

Crowd-sourced approach

The answer is quite simple. If positioning employees as part of the problem fails to work, then make them part of the solution. Knowledge about cyberthreats is good but providing employees with the necessary tools to stop these threats in their tracks is far more effective.

A crowd-sourced approach does just that – it provides employees with the ability to scan their inboxes and verify and report any suspicious emails. Rather than sending any questionable emails through to the IT team to check, workers are able to do so themselves. Only once a malicious email has been detected by the scan does it get sent to security teams for further investigation.

Additionally, the data received from these scans is then circulated round the entire business so that every user can benefit from the findings. All reports go towards automatic detection and remediation of similar attempts. This entire process can take place without disrupting individuals’ busy work schedules, but equally makes them feel like they are contributing to the wider business security strategy.

Each time the crowd-sourced technique is used, a company’s defence line will strengthen as the data piles up to feed the machine-learning system that monitors the rest of the business inboxes. Beyond the initial click of a button, there is no further need for human interaction from employees, meaning they can continue with their more strategic and high-value tasks without unnecessary disruption.

Salvation and downfall

An online presence could be both the salvation and downfall for businesses. It opens up vast areas of opportunity for flexible working, increased activity and overall business continuity. Yet there lurks an evil hiding in the digital background, waiting and ready to exploit any weakness it can find.

Armed with cheap and accessible UGC, phishers are prepared to target any and every company, hoping to make it past email security defences and fool naive employees with social engineering. Employers need to be ready to take up arms against the onslaught of attacks, but they need to bring in the entire company.

“Bad actors will always find a way to breach your network, of this we can be certain. It is therefore imperative that employers establish a new line of defence”

A crowd-sourced approach to SAT will allow the company to build a bank of data, at the press of a button, to help defend against different forms of phishing attacks. Bad actors will always find a way to breach your network – of this we can be certain. It is therefore imperative that employers establish a new line of defence to help their businesses survive and thrive in the expanding digital world.

About the author

Lior Kohavi was appointed Cyren’s chief strategy officer and EVP for advanced solutions in May 2019, having previously served as Cyren’s CTO for six years. His more than 20 years of experience as a technology executive includes work as a business strategy architect at Microsoft, and as vice-president of product management and strategy at Whale Communications. He led the development of cryptographic security at Cylint and served as head of the Israeli Air Force’s Network and Operations Systems Department.
The cost of cybercrime in the US healthcare sector

Jesse Abulencia

The US healthcare system is burdened with the highest costs in the world, and they are still rising as a result of the system itself, its own inefficiencies and government politics. However, there is yet another factor coming more and more into play, adding additional costs and risks to stakeholders in the healthcare system, affecting patients, employees, governments and the doctors themselves. While digitisation and technology provide vast benefits for the quality and efficiency of the work of medical professionals and care of patients, cybercrime in the healthcare sector has risen as well.

Currently, cybercrime against the US healthcare system is at an all-time high. In the period between 2014 and 2017 alone, the occurrence of cyber-related attacks on organisations relating to medicine and healthcare increased 300% compared to previous years.¹ According to a survey conducted by SANS in 2014, about 94% of healthcare providers or organisations had become a victim of cybercrime at some point in their operating history.²

The motives of cybercrime perpetrators are similar to the motives of ordinary criminals, and can involve the illicit gain of money, information and/or intellectual property. The cost of cybercrime worldwide is estimated to be upwards of $575bn.

Specifically with regards to the healthcare sector, the primary motive has been monetary gain. From the point of view of the attackers, healthcare is considered to be relatively attractive due to the nature, quantity and value of stolen data, and the fact that targets in healthcare are relatively easy to attack and not hardened against many common attack methods. In fact, the healthcare system was such an attractive and valuable target that in the year 2015 alone, the data of more than 110 million patients was compromised.

Highly vulnerable

Due to how much the US healthcare system has been targeted – and successfully – and the extent of damages and costs in recent years, this sector can be considered to be highly vulnerable. A multitude of factors have resulted in this situation. One obvious direct factor is simply the relative lack of cyber security experts to identify and resolve vulnerabilities in systems. The concept of market supply and demand comes into play; with relatively few cyber security professionals willing and able to handle the security needs of organisations, along with the high demand for their services, high market rates exist to recruit and hire prospective employees. Contrary to expectations, even though the US boasts the highest healthcare costs in the world, many medical organisations are strapped for cash in various departments, resulting in them being unable to afford cyber security experts at the market rate.

Limited resources are also prevalent within the healthcare industry, preventing workers from placing their focus on security-related tasks at a time when caring for patients is the primary concern. Furthermore, this patient-first culture can hinder effective cyber security practices, as medical providers work to make sure patients are taken care of first, even at the expense of security. For example, in many

References

1. Bages-Amat, Arnau; Harrison, Liz; Spillecke, Dennis; Stanley, Jennifer. ‘These eight charts show how COVID-19 has changed B2B sales forever’. McKinsey, 14 Oct 2020. Accessed Oct 2021. www.mckinsey.com/business-functions/marketing-and-sales/our-insights/these-eight-charts-show-how-covid-19-has-changed-b2b-sales-forever.
2. ‘Cyber Security Breaches Survey 2021’. Department for Digital, Culture, Media & Sport (DCMS), 24 Mar 2021. Accessed Oct 2021. www.gov.uk/government/statistics/cybersecurity-breaches-survey-2021/cyber security-breaches-survey-2021.
3. Chandler, Simon. ‘Google Registers Two Million Phishing Websites In 2020’. Forbes, 25 Nov 2020. www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/.
4. Coker, James. ’HMRC Records 73% Growth in Email Phishing Attacks During #Covid19’. Infosecurity, 19 Nov 2020. Accessed Oct 2021. www.infosecurity-magazine.com/news/hmrc-growth-email-phishing-attacks/.