Big Game Hunting

Cybercriminals Set their Sights on Treasury

Corporate systems and data are increasingly being held to ransom by cybercriminals. The modus operandi of these underworld gangs is also rapidly evolving to exploit vulnerabilities in remote-working set-ups on the back of Covid-19. As such, treasurers must be more aware of – and prepared for – cyber-attacks than ever before. Here, two senior leaders from Barclays highlight the latest cyber traps to avoid and outline how treasury departments can shore up their digital defences.

While it was 'memorable' for many reasons, 2020 was also a record-breaking year for cyber-attacks and data breaches[1]. With the onset of the Covid-19 pandemic, and widespread moves to remote working and learning, the world also witnessed an explosion of cybercrime. Indeed, annual global damages caused by cybercriminals are predicted to reach $10.5tr. by 2025[2].

Against this backdrop, it is understandable that 'data and cybersecurity policies' are the top regulatory concern for 32% of treasurers over the year ahead, according to TMI and Barclays' *European Corporate Treasury Survey 2021*.

Your files have been encrypted!

Currently, one of the most prevalent types of cyber-attack is ransomware, with almost 1,400 confirmed attacks in the first seven months of 2021.[3] Paul Gillen, Chief Information Security Officer, Barclays Europe, explains: "Since early 2020, so-called Big Game Hunting [BGH] ransomware attacks have been emerging as a significant threat to organisations around the world." For those who aren't familiar with the term, BGH refers to financially motivated criminal groups using ransomware tactics, techniques, and procedures (TTPs) to extort large sums of money from organisations – by essentially holding their systems and/or data hostage.

By **Eleanor Hill**, Editor

The 'bad actors' here are very sophisticated cybercriminals, who specifically select high-value targets. "Companies that are highly sensitive to downtime and/or data exfiltration are often targeted. Certain sectors such as biopharma are also under greater threat than others – due to the nature of the prize, with 'kidnapping' of intellectual property [IP] often being high on the cybercriminals' agenda," adds Gillen. "They will hunt down these targets over a matter of weeks and months to ensure the attack is successful."

To give a sense of scale here, in Q4 2020, the average downtime due to a ransomware attack was 21 days[4]. Moreover, the mean global cost of remediating a ransomware attack has risen to $1.5m this year, up from $761,106 in 2020[5]. Clearly, the threat level is by no means insubstantial.

Exposing and exploiting vulnerabilities

Unfortunately, the Covid-19 pandemic has in many ways created a perfect storm for ransomware attacks, says Helen Kelly, Head of Europe, Barclays Corporate Banking. "In early 2020, we saw organisations having to shift to entirely different ways of working, almost overnight," she notes. Employees began working remotely and businesses inevitably prioritised digital channels and direct relationships with customers. This rapid pivot in the operating environment opened up technology vulnerabilities in organisations that had not prepared for these eventualities. For example, employees in some corporates were using their own personal devices to access company systems because their organisation was not able to respond quickly enough with a corporate set-up to use remotely.

And even when remote-working software and protocols such as virtual private networks (VPNs) and remote desktop protocols (RDPs) were in place, cybercriminals quickly shifted their TTPs to maximise their chances of success. "They deliberately played on the themes of Covid-19 and working from home (WFH) through phishing emails," explains Gillen.

Some employers and their employees were in a state of turmoil at the start of the pandemic. This was an unexpected, total change in their business operations and in people's personal lives. Kelly adds: "As such, logical thinking around cybercrime was put to one side in some organisations – and people opened emails and clicked links that they wouldn't have under normal circumstances."

Uncharacteristic behaviour such as this has made phishing emails an extremely effective initial attack vector during the pandemic. "And phishing continues to be one of the main ways criminal organisations open the door into a target company," confirms Gillen.

Evolving threat landscape

Alongside successful phishing attacks, a more sinister trend is growing in the cybercriminal underworld – the rise of initial access brokers (IABs). These opportunistic groups sell access to victim organisations as a service, often collaborating with criminal groups which focus on malware development and execution.

Gillen elaborates: "Many of the major IABs started off as developers of banking trojans, gradually adding network intrusion capabilities by exploiting software and operating system vulnerabilities. IABs have been used during recent major cyber intrusion operations, and in some cases initial access may have been bought or sold by nation-state adversaries."

He also believes that ransomware operators are increasingly working with IABs and learning from high-profile nation-state cyber intrusion operations. "The latest intelligence indicates that the ransomware business model is evolving to focus on supply chain compromises and aggressive extortion tactics. Recent ransomware demands have been as high as $70m and criminal gangs are carrying out around 35 targeted attacks every week."[6]

Ransomware-as-a-service (RaaS) is another growing area of cybercrime, whereby criminals can simply pay other gangs for the services they need to perform a ransomware attack. In addition, distributed denial-of-service (DDoS) attacks have also been used against online services to force higher-value ransom payments, Gillen notes.

Treasury as a target

For treasurers, the threat here is enormous. If a ransomware attack were successful

BOX 1 WHAT IS PHISHING?

Phishing involves a fraudster, posing as a legitimate source, sending emails that aim to trick people into divulging sensitive information or transferring money into other accounts. The emails typically contain a link to a fake website, which will request that you enter financial information, passwords or other sensitive information.

Alternatively, emails may contain an attachment in the form of a document, form or notification. Equally, the email may be designed to contain and deliver malware via an attachment or a link. If the link is clicked or the attachment opened, the criminal will be able to gain access to your system.

Source: https://www.barclayscorporate.com/insights/fraud-protection/phishing/

> ***"Since early 2020, so-called Big Game Hunting ransomware attacks have been emerging as a significant threat to organisations around the world."***

HELEN KELLY

Managing Director, Head of Europe, Barclays Corporate Banking

PAUL GILLEN

Chief Information Security Officer, Barclays Europe

against a payment system, for example, the impact would be highly significant. Gillen comments: "The business would potentially face regulatory action due to compromised personally identifiable information [PII]. There could also be a loss of monetary assets through theft or ransom payment, and loss of service. In turn, this could lead to reputational damage and loss of customer trust, potentially leading to a further monetary loss through decreased revenue."

Treasurers also need to be vigilant when it comes to the potential payment of a ransom. "Of course, we do not endorse the payment of money to criminal gangs. Payment of ransoms perpetuates the ransomware business model and incentivises further attacks," comments Gillen. "But we are aware of some corporates that have paid ransoms in order to bring impacted services back online more rapidly. The issue to be aware of here from a treasurer's perspective is that some ransomware operators are internationally sanctioned. Therefore, payments to such sanctioned groups may cause an organisation to face regulatory or even legal action."

While ransomware is arguably the most rapidly evolving cyber threat for treasurers to pay attention to, other types of attacks are still out there. Take the aforementioned banking trojans, for example. "These have evolved from information- and credential-stealing malware used to conduct fraud against individuals to sophisticated network intrusion malware, which can be devastating for corporations and open up the way for silent attacks, without a ransom and with no red flags, such as the theft of IP," says Gillen.

Another for the watchlist is CEO or CFO fraud, also known as business email compromise (BEC). Kelly comments: "While this type of threat has been talked about in treasury circles for a number of years, Covid-19 has disrupted workflows to such an extent that BEC has found holes in some corporates' armour in recent months." The social engineering that informs a BEC attack is also becoming more sophisticated and intense. "Senior company executives, including the CFO, are at risk – arguably more than ever – with cybercriminals using online collection through social media and social engineering campaigns to gain personal information on them to help inform BEC attacks," she adds. "Treasury teams should be on high alert right now for BEC."

Meanwhile, invoice fraud also remains rife in treasury, with cybercriminals sending fake invoices or looking to change the bank details of an existing supplier to divert monies into their own coffers. "Unexpected changes in personnel, bank account details or telephone numbers are red flags to watch for here," warns Kelly. "Any such changes should always be double- or triple-checked with the supplier by phone, using the original contact details for them."

Being cybercrime-savvy

This simple action of picking up the phone to a business partner is a critical part of a robust cybersecurity approach in treasury. "It's a cliché, but people are one of the best defences against cybercrime and fraud," says Kelly. Gillen agrees, adding that "Cybersecurity is a team sport."

Best practice, says Gillen, is all about collaboration and trying new tactics – and this is very much the approach taken by Barclays' Chief Security Office. "Cybersecurity is not about looking at one function over another, but examining how they work together and how threats might target the organisation through different pathways. A joined-up approach to cybersecurity is essential – and this extends beyond the four walls of the organisation to trusted business partners."

A good example of this collective action is the trend for data on cyber threats to be shared among corporate communities in a secure manner. "This ultimately leads to more robust threat analysis and improved decision-making around stopping cyber-attacks and fraud," says Gillen.

In addition to collaborating in this way, Barclays also deploys the latest technology behind the scenes to analyse customer behaviour and ensure it truly is the client requesting a payment to be made, for example. Any anomalies that are detected are flagged up to the client to ensure that a fraud is not occurring.

Barclays also places a significant emphasis on education and training, often working hand in hand with organisations to help identify weaknesses in their cybersecurity protocols and bringing employees up to speed on threats to look

BOX 2 CHECKLIST: EQUIPPING YOUR TEAM IN THE FIGHT AGAINST CYBERCRIME

1. Create a programme of ongoing education and training to ensure the treasury team understand how cybercrime works and what they can and should do to protect themselves and the business.

2. Keep on top of evolving threats and communicate that throughout the business. Barclays offers regular webinars that can help as part of an awareness programme.

3. Make sure your processes are robust, that any necessary changes are noted, and that the team is informed of new requirements, for example, multi-factor authentication. Also look to automate treasury processes where possible.

4. Build a culture of openness where people aren't afraid to speak up (and there are mechanisms to enable that) and where cybersecurity is seen as a collective responsibility.

5. Regularly update anti-virus software and install any patches immediately when notified.

6. Make it clear what steps a treasury team member should take if they feel that they may have fallen victim to a cyber-attack. This can facilitate a faster response and potentially reduce exposure.

Source: https://www.barclayscorporate.com/insights/fraud-protection/cyber-crime-employee-awareness/

out for. "Knowledge is one of the most powerful tools against cybercrime and fraud – and I would encourage treasury leaders to hold regular sessions with their teams around the threat landscape," advises Gillen.

Although being up to date on the fast-moving world of cybercrime is important, so too is adhering to the basics of cybersecurity. "Although it isn't the cutting edge of cybersecurity, it is vital to continually pay attention to strong authentication, patching, monitoring, and risk oversight. Treasury will be easier to defend if everyone is taking care of these fundamentals," he notes.

Another way treasury teams can help to keep cybercriminals at bay is by automating processes. Kelly comments: "Reducing manual touch points in processes lessens the opportunities for cybercriminals and fraudsters. Robotic process automation [RPA] can be applied to low-value, repeatable, processes and then artificial intelligence [AI] can potentially be layered on top to deliver more intelligent insights, in a safer environment. It's a win-win."

> ***"Organisations need to rethink their priorities and be realistic about the threat environment they are now working in."***

Happening in real life

Having the right culture within treasury is also important, believes Kelly. "Team members, no matter how junior, need to feel able to question instructions – even if they purport to be from the CFO or CEO. Reducing any sense of urgency should also be permitted where necessary. It is far better to stop and question payment instructions, and potentially send a payment late, than to send a fraudulent payment on time. In other words, organisations need to rethink their priorities and be realistic about the threat environment they are now working in."

On the subject of reality, Gillen cautions that one of the biggest pitfalls to avoid when it comes to cybercrime is thinking that 'it'll never happen to you' – or believing that 'cyber-attacks are just something you read about in the press.' He comments: "Cybercrime is extremely real. Businesses often make the mistake of thinking they have nothing of interest to cybercriminals. They could not be more wrong. We live in a world where systems, data and IP are immensely valuable assets. Every corporate is a potential target."

This, Kelly concludes, is why "treasurers must take the lead and ensure their team is always ready to deal with the evolving threat landscape. In this digital age, cybersecurity is no longer an add-on to the treasury role; it is the backbone for best practice". ■

Notes:
1 https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=6cc0f5c358d3
2 https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
3 Cyber Defence Alliance, Ransomware-as-a-Service Alerts, 1 January 2021-31 July 2021.
4 https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
5 https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
6 https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/