InfoTrust

mimecast

EXECUTIVE SUMMARY

UNDERSTANDING AND SECURING AGAINST EMAIL ATTACKS

To find out more contact an InfoTrust representative

+61 2 9221 5555

info@infotrust.com.au

Email is one of the leading communication tools for businesses and, as such, is a primary attack vector for cybercriminals to get their hands-on sensitive data and company funds. And email attacks are showing no signs of slowing down. Not only does the volume of attacks continue to rise, but attacks are becoming ever more sophisticated, deceiving even the most astute of business professionals.

HOW **EMAIL ATTACKS WORK**

73% OF IMPERSONATION ATTACK/BEC VICTIMS FACED A DIRECT FINANCIAL LOSS

Report Reference: Mimecast 2019 State of Email Security Report

Cybersecurity practitioners know that email attacks aim to either deliver malware, lure victims to malicious websites or steal valuable or sensitive company data. They rely on the general belief that email inboxes are secure and aim to trick recipients into clicking links, downloading files or entering information. While it would be nice to think that email accounts are relatively trustworthy, 3.4bn fake emails are sent out daily. And, although these fraudulent emails can sometimes be easy to spot, the methods being used are becoming increasingly sophisticated in a bid to trick even the wariest of recipients. Unfortunately, the success of email attacks is far more due to the manipulation of weaknesses in human psychology than technological sophistication.

Today, targeted email attacks are incredibly advanced in their methods, using social engineering to bypass existing security controls and secure email gateways (SEGs). Attacks are often identity-based, impersonating reputable senders and containing no malicious code or links. As many identity-based attacks lack detectable URLs, they can be difficult for SEG's to detect. When trusted people are impersonated by email, recipients can find themselves making payments and sharing sensitive data without a second thought. The advanced methods of attack are made even more successful when organisations think they have the necessary security protocols in place. Email threats are versatile and varied, often evolving faster than email defences themselves. By using trust, authority and familiarity, hackers are able to fool recipients and make huge financial gains. According to Mimecast's 2019 State of Email Security Report, 73% of impersonation attack/BEC victims faced a direct financial loss.

THE COST **OF AN EMAIL ATTACK**

Data breaches are one of the biggest threats to today's businesses, and email continues to be the number one threat vector. In the first half of 2019 alone, more than 3,800 publicly disclosed data breaches, exposed an astonishing 4.1 billion compromised records worldwide. Of the 3,800 breaches, 70% involved email and 65% passwords.

It's not only the frequency and volume of data breaches that are on the rise, the total cost is escalating too. According to IBM, the average data breach now costs companies more than $3.92 million. And the cost of an email attack is more than the immediate financial loss, the reputational fallout and impact on consumer confidence is significant too.

THE KEY **TYPES OF EMAIL ATTACK**

UNDERSTANDING THE DIFFERENT TYPES OF EMAIL ATTACK AND THE CHAIN OF EVENTS THAT UNFOLDS IN EACH CASE, BUSINESSES CAN BE MORE PREPARED FOR WHEN THEY HAPPEN

There are many types of email attack, continually evolving in variety and sophistication. However, there are four fundamental types that businesses should be aware of and have a plan for both defence and remediation: ransomware, phishing, business email compromise and account takeover. While all of these attacks generally start with a spoofed email being sent to a victim, they then

take different courses to reach their goal. Some use social engineering techniques to trick the victim into supplying sensitive personal or business information; others aim to extract a ransom from a victim by locking their files and demanding a payment to regain access. By understanding the different types of email attack and the chain of events that unfolds in each case, businesses can be more prepared for when they happen, aware of the inherent dangers and prepared for how they'll respond to minimise the damage in the event of an attack.

1 RANSOMWARE **ATTACKS**

53% OF ORGANISATIONS EXPERIENCED A BUSINESS-DISRUPTING RANSOMWARE ATTACK IN 2019, UP 26% FROM A YEAR AGO

Report Reference: Mimecast State of Email Security Report

Ransomware is the oldest and most commonly known type of email attack and has been used since the 1980s to blackmail recipients into giving cybercriminals money. Ransomware has continued to surge in popularity amongst cyber threat actors, 53% of organisations experienced a business-disrupting ransomware attack in 2019, up 26% from a year ago (Mimecast State of Email Security Report). Organisations are falling victim to ransomware every minute of every day, and that doesn't look likely to change.

While ransomware can spread across the internet without specific targets, the nature of the file-encrypting malware means that cybercriminals are also able to target their victims personally. Ransomware continues to be a significant threat to businesses in all sectors. However, ransomware attacks via email are often targeted at organisations that have small (or no) security teams, that will be willing to pay quickly due to the immediate requirement for their files, or that hold sensitive data that could result in legal controversies. Ultimately, it's all about getting the highest payout for the least effort.

THE CHAIN OF EVENTS IN A RANSOMWARE ATTACK

Although there are several ways that ransomware can infect a person's computer, malicious email is the most commonly used method. While every attack is unique, there is a commonality in their behaviour. The goal, of course, is to demand a ransom, which involves the following chain of events:

1. **Email Received** - this is the distribution stage of the software to potential victims. A spoof email will be sent which appears to be legitimate, either impersonating a trusted institution, colleague or friend.
2. **Victim Responds** - as the victim believes the email to be trustworthy, they fall for the trick and open the email attachment or click the URL which links to a drive-by-download.
3. **File Passes Secure Gateway** - the victim has unwittingly consented to the download, and the file passes the secure email or web gateway, rendering the business' key defences worthless.
4. **Endpoint is Infected** - once the malware has been downloaded it copies itself, and the malicious payload is executed. This means that the ransomware has unpacked itself onto the local machine and has performed reconnaissance on the system.
5. **Files are Encrypted** - all the files discovered during the reconnaissance stage are encrypted and the original data deleted.
6. **Ransom is Demanded** - once the encryption work is done, the ransomware displays instructions on the screen for extortion and ransom payment, threatening the destruction of data if payment is not made.
7. **Business Responds** - organisations can choose to pay the ransom and hope their files are actually decrypted, usually by receipt of a link that they can use to download a key or decryption program. However, there is always the chance that their files won't be decrypted regardless of payment. Alternatively, they can attempt recovery by removing infected files and systems from the network and restoring data from clean backups. Some types of ransomware are pre-configured to have timeout thresholds, meaning that the ransom price can increase over time or the software begins to delete encrypted files if payment is not made by a specific time.

2 PHISHING **ATTACKS**

Phishing is a cyberattack that uses email to target an individual, gain their trust and then ask them to provide sensitive information. If users are fooled by a phishing email, they will end up passing over the information that is requested, be it credit card numbers, account details, usernames or passwords.

What makes phishing attacks really stand out, or not as the case may be, is their ability to masquerade as a trusted entity, plausible person or company that the target does business with. According to the latest Verizon Data Breach Investigations Report, nearly a third of all data breaches in 2019 involved phishing. With 94% of organisations experiencing a phishing attack of some kind in 2019 (Mimecast State of Email Security Report) The reason this type of attack is so popular amongst cybercriminals is due to its success rate, but also how simple it is to accomplish. Even those with minimal technical skills can purchase phishing kit bundles giving them the website resources and tools they need to install it on a server. All the attacker then needs to do is to find their targets and send the email.

94% OF ORGANISATIONS EXPERIENCED A PHISHING ATTACK OF SOME KIND IN 2019

Report Reference: Mimecast State of Email Security Report

THE CHAIN OF EVENTS IN A PHISHING ATTACK

There are a variety of techniques that can be categorised as phishing. The purpose of the phishing attempt can either be to access sensitive information or to infect the user's computer with malware. What every type of phishing email has in common is the element of disguise and deception. In the case of a phishing email that aims to get the victim to hand over sensitive information, a chain of events unfolds:

1. **Email Received** - the victim receives an email from a spoofed email address appearing as if from a trusted entity. The spoofed emails that are sent are either softly targeted, perhaps aiming for people that hold a specific role within their organisation, or they aren't targeted at all. Often phishing emails are sent to millions of potential victims to improve the odds of a response.
2. **Victim clicks URL** - there are several potential scams that are used to encourage recipients to click the URL within a spoof email, but each will have a hook and a sense of urgency. For example, the recipient is told their account will be deactivated if they don't update their details, encouraging them to take fast action.
3. **Link Passes Secure Email Gateway** - as the victim clicks on the link, they have consented to go to the related website, overriding the secure email gateway.
4. **Victim Visits Fraudulent Website** - fraudulent websites will aim to look almost identical to the one that the victim is used to. Cybercriminals use foreign character sets to disguise URLs. This works because some alphabets contain characters that look very similar to Latin letters when displayed in Unicode within a browser.
5. **Victim Hands Over Sensitive Information** - if the website has succeeded in deceiving the victim, they will enter their details. In the case of a bank, a commonly used entity for phishing emails, once entered the attacker can then use their details to access their account. The victim is then redirected to the legitimate bank website to avoid any further suspicion.

3 BUSINESS **EMAIL COMPROMISE**

Business Email Compromise (BEC), takes phishing attacks to the next level. These types of phishing attacks aim to deceive specific people, and attackers dedicate a lot of time and energy into doing so. Ultimately, the people chosen have been selected because the potential rewards are significantly higher than a wider-spread phishing attack. There are two key types of BEC to be aware of:

- **Spear Phishing** - an email is created to appeal to a specific individual. In terms of the fishing reference, the attack is aimed at a specific fish, rather than throwing bait in the water in the hope that anyone bites. Spoofed addresses are used to make the email look credible, often appearing to come from senior management to the recipient.
- **Whaling** - this is the next level of spear phishing, where the target is a very big fish. Usually whaling is aimed at CEOs or other high-value targets such as company board members within an organisation. Aiming at high-value target will take a lot more time, but the potential rewards are significant.

Since their inception in 2013, BEC attacks have become increasingly popular amongst cyber attackers. The FBI's most recent Internet Crime Report (ICR) reported losses amounting to $1.3 billion in 2018, double the volume of the preceding year. And 45% of organisations noting they saw a significant increase in targeted spear-phishing attacks in 2019 (Mimecast State of Email Security Report). As with many of the email attack techniques, BEC attacks don't discriminate based on size of business. Anyone can fall victim, and small businesses with one person responsible for multiple transactions can be easier targets than big corporations.

THE CHAIN OF EVENTS IN BUSINESS EMAIL COMPROMISE

What all BEC attacks have in common is the level of personalisation that is involved. The attacks aren't sent out to a wide pool of potential victims. Instead, direct analysis is carried out of the organisation and the potential targets to make a realistic ask that will fool even the most senior of employees. A BEC attack will unfold as follows:

1. **Target Organisation Infiltrated** - the first step in a BEC attack is for the cybercriminal to carry out in-depth reconnaissance of the target organisation. Frequently used websites will be used to harvest employee account credentials and gain access to mail servers. Attackers will then research payment processors and vendors and spend time sifting through emails. It can take weeks for hackers to build up a profile of interactions so they can effectively mimic their behaviour.

AS WITH MANY OF THE EMAIL ATTACK TECHNIQUES, BEC ATTACKS DON'T DISCRIMINATE BASED ON SIZE OF BUSINESS

2. **Email Received** - the spoofed email will be sent to the victim. Spoofing means that the email header will be falsified to include the supposed sender's name and address and the formatting will replicate that of a legitimate source. Emails are often sent to junior staff who are more likely to surrender to the demands of what they believe to be a senior employee or the CEO without question.
3. **Request Placed** - BEC attacks will often go undetected by security systems as they don't use detectable payloads like URLs and attachments. Instead, the email will ask the user to provide information or to pay an invoice. There is often a level of urgency to the request and paperwork found during the reconnaissance stage will be included to add further validity.
4. **Request Processed** - whether a BEC attack comes from a forged invoice, a compromised account of an actual employee or a fake email address, they can look incredibly realistic. By their nature, BEC attacks have no payloads, malicious attachments or URLs, that can be detected and blocked, which allows them to evade most existing security technology. Organisations are left vulnerable to attacks and their traditional defences rendered ineffective.

4 ACCOUNT **TAKEOVER ATTACKS**

An Account Takeover-based email attack involves cybercriminals gaining access to a trusted email account, and then using it to launch further attacks. What is different about this type of attack is that the emails originate from the actual email accounts of trusted senders, which have been compromised by unauthorised access. As there is already pre-existing trust with the recipients, there is a tremendous success rate, and the validity of the source outsmarts traditional security controls.

Before 2017, Account Takeover attacks were pretty much non-existent. However, as with the other forms of email attack, this method has gained a huge amount of popularity amongst cybercriminals. Agari conducted research finding **a 126% increase of Account Takeover attacks** every month in 2018.

This type of attack has a few distinct advantages for cybercriminals. Firstly, the accounts being used are legitimate and established, so there is no need to leverage impersonation techniques such as spoofing emails to bypass security controls. Secondly, there are pre-existing trust relationships between the account holder and their contacts. This makes the emails in an account takeover attack extremely convincing and makes it much more likely for the recipient to release funds.

THE CHAIN OF EVENTS IN AN ACCOUNT TAKEOVER ATTACK

The chain of events in an Account Takeover attack is longer than that of the other email attacks. Ultimately, this is because a spear phishing or

malware-based attack is needed first to obtain account access. The alternative point of entry is for cybercriminals to purchase account credentials from the dark web, and then immediately use the account as a launchpad for targeted attacks. However, once the cybercriminal has account details, the attack will unfold as follows:

1. **Account access gained** - the attacker will gain the login details to a legitimate account by launching a phishing attack or purchasing credentials, as discussed.

2. **Account control established** - this may involve creating audit rules to delete the malicious activity, setting up forwarders to silently monitor users' communications, or increasing password change processes to maintain control. The longer the attacker has control of the account, the more successful their attack is likely to be

3. **Internal reconnaissance** - the attacker determines the best way to exploit the account, finding out if the user credentials give direct access to monetise data and whether the contacts will allow them to compromise higher-value accounts. Sometimes attackers lay dormant for some time, observing communication with the plan to hijack at the optimum moment.

4. **Fraudulent request made** - this is the targeted email attack against the contact list of the controlled account. It can either be a BEC type request where payment is demanded or can include a phishing link, giving the hacker the chance to gain a deeper foothold on the organisation.

WHAT CAN **ORGANISATIONS DO TO PREVENT EMAIL ATTACKS**

As cybercrime has quickly become a top priority for organisations, IT professionals have stepped up their game to invest in network defences to try to protect their systems. Although a wide range of security tools may be deployed to safeguard email accounts, the majority still focus on protecting the network. With the sophisticated techniques being used today, such as phishing scams and account takeovers, standard defences aren't enough. Solutions that were successful just a few years ago can be rendered useless under the likes of ransomware, phishing and Business Email Compromise. When cyber scams bypass defences and hit organisations where they are most vulnerable, their employees, they often don't stand a chance.

To be in with a chance of preventing email attacks, firms need to do more than throw money at cybersecurity. It's vital to understand where the attacks are coming from to be able to implement the right measures. Cybersecurity involves having a comprehensive strategy in place to protect the whole email ecosystem. What this means is addressing the whole attack chain, from proactive prevention to real-time response. A security strategy should be designed to protect both the email ecosystem and its users from the wide variety of threats they face.

Users need to be educated to help them be less easily fooled by emails impersonating credible senders. From Mimecast's research, human error ranks highest for cyber risk, with it being a

CYBERSECURITY INVOLVES HAVING A COMPREHENSIVE STRATEGY IN PLACE TO PROTECT THE WHOLE EMAIL ECOSYSTEM.

contributing factor in more than 90% of breaches. Businesses using cloud-based systems need to understand the extent of their built-in security solutions and take a proactive approach to stopping attacks, monitoring risk, and responding when attacks happen. With a combination of education, awareness, technologies and processes, organisations can be better placed to ward off attacks and the financial fallout that results.

The unfortunate truth is that email attacks have become so widespread that every business of every size is at risk. But there are some key steps that can be taken to mitigate the threats.

1. **Enforce email authentication** – SPF, DKIM, and DMARC are all free to use standards that can be utilised by your organisation to strengthen your email security posture.

2. **Deploy any available advanced impersonation or sandboxing controls** – any Next-Gen Secure Email Gateway worth its salt will offer these out of the box, ensuring these are configured correctly is vital.

3. **Security awareness training** – teaching your users and then testing their knowledge is an important part of your security strategy.

4. **Check your web gateway configuration** – if you are able to deploy web threat isolation and ensure your HTTPS traffic is being inspected.

5. **Incident response (IR) planning** – creating, and most importantly rehearsing your IR plan is key to maturing your business' cyber resilience.

6. **Backup your business-critical data** – should the worst happen; ensure you have a backup that meets your RPO and RTO objectives.

ABOUT **INFOTRUST AND MIMECAST**

InfoTrust is a specialised cybersecurity practice, founded in 2014 by Dane Meah and Simon McKay, who identified a gap in the market where partners could provide more value to customers other than just the solutions and services they were delivering. Today this has come to be what we know as the "InfoTrust Way", at every stage of the customer's journey InfoTrust provides added value in the form of health checks, assisted implementation, managed services and complimentary operational reviews. InfoTrust prides itself in working with best-in-breed technologies to deliver successful business outcomes to customers, which made it an easy choice to partner with next-generation email security vendor, Mimecast.

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email profoundly safer, restoring trust and bolstering business resilience. Known for safeguarding customers against dangerous email, Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, awareness training, data protection, to uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.

Our customer engagement teams and Security Operations Center help organizations of all sizes with proactive support and actionable intelligence. Our easy to use and deploy cybersecurity platform with open APIs makes customers' existing investments more valuable and teams smarter. The collective intelligence gathered across our global customer base and strong partner network provides a community defense that helps make the world a more resilient place.

To find out more about how InfoTrust and Mimecast can help your organisation prevent and prepare for email attacks, sign up for our free email security workshop.

REFERENCES

Mimecast – State of Email Security 2019 Report

Techradar - One trillion phishing emails sent every year

Forbes - Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019

IBM Study – Data Breach Costs on the Rise; Financial Impact Felt for Years

Agari – Protecting against ATO Attacks

InfoTrust