Cyber Security

by Gina Dollard

This article looks at how cybercriminals target employees and end-users to breach networks and how we can recognize threats and spot scams to prevent breaches from being successful.

Introduction

Today's cybercriminals are constantly evolving their tactics in order to overcome whatever cutting-edge security solutions organisations put in place to stop them. This means that although most businesses with mature cybersecurity programs are good at blocking the majority of threats that target them, there will always be a handful that manage to get through.

As the following case studies will demonstrate, there are a large number of cyber threats for which employee and end-user vigilance remains the best defence. The easiest way to breach a corporate network is through its users, but with the right knowledge and mind-set it's possible to recognise a threat when it arrives in your inbox and react accordingly.

Threats

Business E-mail Compromise (BEC) refers to a broad category of fraud in which a cybercriminal impersonates someone in an organisation – usually a senior manager or executive – and sends an e-mail to their direct reports asking them to transfer a large sum of money to a particular account or to pay an unexpected invoice. Despite its name, BEC only sometimes involves actual compromise of an organisation's e-mail system; in many cases a fraudster simply uses a lookalike e-mail address and hopes that the recipient won't notice the difference until it's too late.

Fraudsters who carry out BEC attacks often perform extensive research on the organisations they target. They will know which staff members are authorised to make payments and will have a good idea of the overall organisational structure of the company. For this reason, BEC fraud can be difficult to initially detect.

Credential phishing is still extremely common and increasingly targets users of cloud-based e-mail and office applications such as those offered by Microsoft and Google.

Common phishing e-mails for these kinds of services will claim that your account has been 'locked' or is about to be deleted and request that you login in order to prevent this from happening. You will then be shown a login page which looks identical to the real thing which will send your username and password to the fraudster. Although many cloud-based applications provide enhanced security mechanisms to protect against these kinds of attacks (such as two-factor authentication), it is common for smaller organisations in particular to not use them. This means that stolen credentials can easily be used to gain immediate access to employee e-mail accounts and documents.

Ransomware is a type of malware which encrypts files on infected systems and then demands a ransom payment (usually in Bitcoin or another cryptocurrency) before they can be retrieved. It remains one of the most immediate threats facing small and medium enterprises in particular, although it can even be devastating to large corporations.

Although some cybercrime groups have begun delivering ransomware via other means, the vast majority of ransomware incidents begin with an e-mail containing a malicious attachment or link. Once opened, the malware will begin to rapidly encrypt commonly-used files such as documents and spreadsheets. Modern ransomware can even spread automatically from one system to another, making it a particularly dangerous threat.

How to spot scams

All of the threats discussed above share a common trait: they all target end-users and employees. Most office workers receive dozens of e-mails every day. Cybercriminals take advantage of this by hoping that busy employees will click first and ask questions later. You can help to protect yourself and your organisation from e-mail-based threats by following a few simple guidelines.

Never open attachments or click links in e-mails you didn't expect to receive. This seems like obvious advice, but cybercriminals are still highly successful at tricking their targets into opening 'invoices' or other urgent-seeming attachments that arrive without warning. If in doubt, follow your organisation's guidelines for reporting potential security incidents before opening anything that you didn't expect to receive.

Always be wary of e-mails that carry an undue sense of urgency.

BEC in particular relies on the fact that employees might be used to receiving urgent instructions from company management. But you should always be wary of immediately carrying out instructions to make large payments with no notice.

The simplest method of spotting this kind of fraud is to pick up the phone and call the person who is supposedly making the request. It's not uncommon for employees to unwittingly interact with a fraudster over the course of several back-and-forth e-mails only for the fraud to come to light when they finally call the person they thought they were communicating with the whole time.

Of course, it also helps if organisations have separation of duty in place so that payments need to be authorised by a second employee who must independently verify the legitimacy of the initial request.

Carefully read e-mails that seem suspicious. Although cybercriminals have methods of making their fraudulent e-mails seem legitimate, there are often tell-tale signs that can give them away. They may use look-a-like e-mail addresses which appear to come from your organisation at first glance, but which are actually coming from somewhere completely different. They can also have poor spelling and grammar, although some phishing e-mails are almost exact copies of real e-mails sent by the services they purport to be from.

It's also common for e-mails with malicious links to claim that the link is for a well-known website. By hovering over the link without clicking on it you can check where it actually leads to. If the address isn't exactly what you expected based on the link's description, don't click on it.

Be careful of unexpected phone calls and SMS messages. As well as e-mail, cybercriminals also carry out fraud using so-called 'vishing' (voice phishing) and 'smishing' (SMS phishing). These techniques can be particularly effective because they can appear more legitimate than e-mail, where most people are used to receiving a certain amount of spam.

It's generally a good idea to refrain from clicking links in SMS messages and to hang up if you feel that an unsolicited caller on the phone is asking you to do something you're not comfortable with.

Cautionary tales

In late 2018 the Dutch branch of the cinema chain Pathé suffered a multi-million-euro loss as a result of a BEC fraud. Cybercriminals impersonated an employee from the company's French parent firm and sent an e-mail to the CFO requesting that he make a transfer of €800,000 as part of a 'confidential' acquisition.

The company's CFO and CEO complied with the request and with several more that followed, ultimately sending over €19 million. Both employees were dismissed as a direct result of their actions.

This incident shows that BEC fraud can be highly lucrative if a fraudster can find the right target.

Aluminium manufacturer Norsk Hydro was forced to take many of its operational systems offline following a devastating ransomware attack earlier this year. The malware spread throughout the company's network, affecting over 100 of its plants around the world. As a result, staff were forced to manually perform work that would have normally been performed by its computer systems.

The company refused to pay the ransom, but the estimated cost of the attack still reached €45 million. That included lost revenue due to closed factories and the extensive 'clean-up' operation needed to remove the malware and restore functionality across its network. These kinds of secondary costs can often end up being enormous in cases where malware has managed to spread to many dozens or hundreds of machines.

Conclusion

The cyber-threats profiled in this article are ones that pose a major risk to virtually every organisation that has any kind of internet or e-mail presence (which is to say, almost all of them).

It can sometimes seem that major cybersecurity incidents happen out of the blue and that ordinary employees are powerless to do anything about them. Hopefully the examples provided in this article demonstrate that major cyber-threats often rely on relatively simple social engineering techniques to gain access to the organisations that they target, which means that anyone can potentially be the difference between a thwarted cybercrime campaign and a successful one.

That puts more responsibility on staff who probably don't think of 'cybersecurity' as being part of their role, but it also means that everyone has an opportunity to be the reason why their organisation avoided that major BEC fraud or ransomware attack.

"Credential phishing is still extremely common and increasingly targets users of cloud-based e-mail and office applications"

Gina Dollard,
Head of Security Operations at AIB

Gina leads a team of cybersecurity experts. The Team provide threat intelligence to highlight and mitigate cyber risks to the business; perform incident response and forensic investigations; and engage in intelligence sharing with national and international partners.