PECB

When Recognition Matters

BUSINESS EMAIL COMPROMISE (BEC): DON'T BITE THE BAIT

The creativity and perseverance of cyber criminals know no limits. Business email compromise (BEC) is a form of online fraud that has been gradually increasing in prevalence and has become a successful tool for hackers. Earlier this year, the FBI issued a notice warning companies against this particular scam technique that is proving particularly lucrative for criminals and is growing rapidly.

Recently, the FBI reported a 1,300% increase in BEC attempts since January 2015. They also reported a 270% increase in identified victims and exposed loss from BEC events between January 2015 and April 2016. BEC attacks are most common in the US, the UK, Hong Kong, Japan, and Brazil, which the FBI reported have resulted in losses of $3 billion.

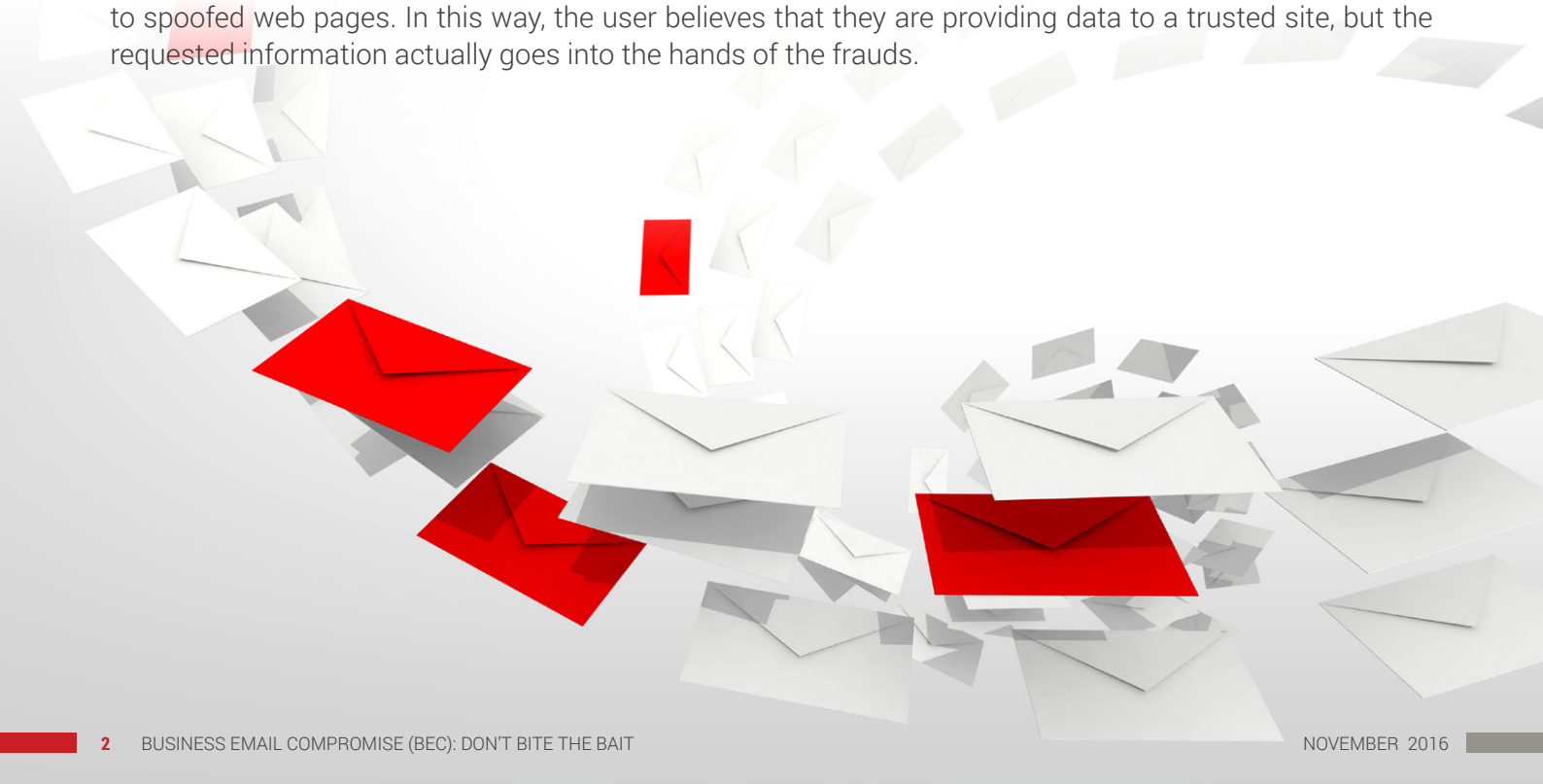
WHAT IS A BEC EVENT?

Business Email Compromise (BEC) schemes are scam techniques which are used to compromise business accounts with the intention of conducting an unauthorized money transfer. A BEC event occurs when a fraudster disguises himself as a company executive and uses what appears to be 'their' email address to instruct employees to transfer money to an account that can be accessed by the fraudster.

Usually, these email messages have a sense of urgency. They appear legitimate and look as if they originate from within the company or from a contractor/supplier of the company. Generally, the most targeted companies are those who work with international suppliers that perform remittances regularly. In most cases, the attackers mimic individuals from the organization who have access to organization's financial resources such as managing directors, CEOs, CFOs or financial managers.

For instance, a CFO of a particular organization may receive an e-mail that appears to come from the CEO of that organization, urging a payment to be made to a specified account for an apparently legitimate purpose. Another example is receiving an email that seems to come from a contractor or supplier that requests a payment for an invoice that appears genuine.

The fraudster's goal is to use the credibility to instruct the recipient to perform a task, such as a money transfer, or pass confidential information such as logins or passwords, which will give the hacker access to corporate data. These attacks are typically known has phishing scams or emails. 'Phishing' is a form of fraud which attempts to obtain a user's data, passwords, bank accounts, credit card numbers, identities, etc. The term phishing is used to refer to one of the most commonly used methods by cybercriminals to defraud and obtain confidential information which involves sending emails that appear to come from reliable sources (eg banks). To do this, fraudsters usually include a link in emails that, when clicked, leads to spoofed web pages. In this way, the user believes that they are providing data to a trusted site, but the requested information actually goes into the hands of the frauds.



HOW THESE SCAMS ARE STRUCTURED AND WHAT IS THEIR PATTERN?

Although these scams have a quite simple design, the techniques the attackers use are relatively complex because they use sentiment and appeal to people's respect for authority. Many times an employee thinks they are simply responding to a reasonable question that comes from one of his superiors. In fact, it is specifically designed to mislead the receiver.

In any case, these spear phishing attacks have a precise pattern that comprises three factors:

- The email appears sent from someone you know and trust
- The layout and content are very accurate
- The required instructions are logical and credible to the recipient

WHY ARE THESE SCAMS EFFECTIVE? RECONNAISSANCE!

The reason why these types of scams have been highly effective is because they impersonate genuine requests. The fraudsters or the designers of these scams conduct research on their potential victims, getting information on the organization, its payment methods, and its protocols and so on. Well-researched information combined with social engineering techniques such as phishing emails, that request information, are used to obtain specific details about the targeted business allowing the fraudsters to learn which persons are authorized to execute transfer payments and gaining knowledge of the protocols that the organization uses.

The FBI categorizes BEC scamming attacks into five scenarios which are listed below:

- Scenario 1: Business Working with a Foreign Supplier
- Scenario 2: Business Executive receiving or initiating a request for a wire transfer
- Scenario 3: Business contacts receiving fraudulent correspondence through compromised e-mail
- Scenario 4: Business Executive and Attorney being Impersonated
- Scenario 5: Data theft

HOW CAN WE AVOID THESE ATTACKS?

The best defensive tool against BEC scam attacks is education. Provide awareness sessions to your staff, point out the signs and indicators of such attacks. Companies should strengthen employee awareness and education but also apply different security techniques to protect themselves from these kinds of attacks.

Employee awareness and training are very important because most of the time these types of scams rely on social engineering techniques. In most cases, these BEC email scams do not involve malware which makes it harder for security tools to detect and spot these scams.

As Kevin Mitnick said: "Social engineers veil themselves in a cloak of believability. Social engineering bypasses all technologies, including firewalls."

However, there are cases when these types of email scams contain malware, most commonly key loggers. Key loggers and other forms of malware are used by criminals to compromise personal and business email IDs which allows them to steal confidential information and further advance their attacks. By doing so, criminals obtain access to authentic email threads which they can use to execute illegal transactions.

Unfortunately, many payment providers in small and large companies do not imagine that criminals can be so persistent and patient. Therefore, knowing the existence of this type of fraud is the first step towards its prevention:

- Do not post confidential information about the company on websites and social networks.
- Do not use the company e-mail service for personal use.
- Do not use the same passwords at work and at home.
- Store files on the corporate network and never solely on your computer.
- Employees shouldn't post too many details about their jobs on social media.

In addition, to stay ahead of cybercrime and prevent it, PECB training courses and certification can be your starting point to effectively and efficiently apply best practices, concepts, approaches, standards, methods and techniques in your information security framework. PECB offers its expertise in multiple fields, including ISO 27001, ISO 27032, ISO 27034, SCADA and Pen testing.

ABOUT THE AUTHORS

Artan Mustafa is a Course Development Manager for IT Security at PECB. He is in charge of developing and maintaining training courses related to IT Security. If you have any questions, please do not hesitate to contact him: itsec@pecb.com

Bevan Lane is a PECB partner and trainer. He has more than 16 years of experience as a consultant in information security, firstly with PwC and then as an independent consultant. Mr. Lane has also an extensive experience in information security risk assessment training and has implemented solutions for major organizations across the globe.

IC3, Trenmicro, Bitdefender