EXECUTIVE BRIEF

PREPARING FOR BUSINESS EMAIL COMPROMISE ATTACKS IN 2017

- Insights for busy professionals
- Read in less than 10 mins
- Knowledge without the fluff

insight brief
RESEARCH. DISCOVERY. INSIGHTS.

proofpoint

THIS EXECUTIVE BRIEF IS A SUMMARY OF THE WEBINAR:

How To Prepare For Cyber Threats In 2017

CLICK TO ACCESS THE WEBINAR

INTRODUCTION

- Business Email Compromise (BEC) and impostor fraud grew significantly in 2016. Recent FBI estimates conservatively suggest these attacks have cost more than $3 billion globally in 2016, and the UK National Fraud Intelligence Bureau has reported a single attack which incurred losses of £18 million.
- There was an explosion in ransomware use in 2016. Messages distributing ransomware accounted for 80% of all malicious message volume. Cyber-criminals were observed to be switching to using ransomware during the year because of its larger potential target audiences and subsequently higher rewards.

IMPORTANT DATA

- BEC attack payments average $140,000 and total losses in the last two years are $3.1 billion. This is much higher than ransomware attacks where single losses average $700. Greater rewards for attackers mean BEC use is likely to grow in 2017 despite additional controls being put in place across EMEA.
- 2016 saw a significant increase in the use of malicious documents and email attachments, accounting for 20% off all emails sent. This represented a 600% increase on 2015.

KEY POINTS

- 2017 will see an evolution in BEC fraud, which attempts to trick users into sending money or confidential information without using malware or malicious URLs. A recent PwC survey of 50,000 CCOs and CIOs had 43% stating that BEC attacks were a growing risk and phishing was their biggest risk.
- The first rule to defend against an evolving threat landscape is "assume your users will click". Verizon's 2016 Data Breach statistics found that 30% of users open phishing emails and 12% click on the links; an increase from 2015. So, whilst staff training is important, investing in security technology is vital.
- An example of a targeted attack deployed on less than 100 organizations in the UK involved a fake traffic violation email containing a link. This took users to a different URL where they were encouraged to download photographic evidence of the offense, but actually downloaded a Javascript.js file, which ultimately infected their machine with a banking trojan.

KEY POINTS (cont.)

- Mobile security is likely to be targeted more in 2017. Mobile spyware such as Pegasus exploits vulnerabilities in Safari to download fake Apps and gain access to a device's communications data, while SMS Phishing attacks also offer opportunities to social engineer users and access confidential information.

IMPORTANT FINDINGS

- Cyber-criminals tactics evolve in response to their effectiveness. For example, a BEC attack spoofing emails from the CEO is less effective when sent to the CFO than to other staff members. Cyber criminals learn fast and have reduced spoofs from CEO to CFO by 39% during the last 5 months of 2016.
- There were far fewer machine-based exploits targeting things like browsers and add-ons in 2016. This is because cyber-criminals now know it is easier and more reliable to use human-based exploits and trick users into infecting their own devices.

NEW INSIGHTS

- BEC attacks using Display Name Spoofing will increase in 2017. These are false emails where the visible sender name is legitimate but the email address is not. They rely on users checking their email on mobile devices which do not display the email address by default.
- BEC attacks using partner spoofing are expected to rise in 2017. These attacks use emails from trusted domains of business partners to trick internal employees into sharing confidential data or money.
- BEC attack trends differ in the US and Europe. In Europe, they are more targeted at smaller organizations which often haven't invested in security solutions. This makes them more vulnerable to attacks like domain-spoofing. In the US, increased security take-up means more advanced tactics such as partner-spoofing are being used.
- Exploit kits are a type of malicious toolkit used to exploit security holes found in software applications for the purpose of spreading malware. In 2017, these kits are expected to be used in more sophisticated attack campaigns, focusing on specific locations and systems to lower the risk of detection & increase potential returns for cyber-criminals.
- The use of a new phishing attack called Angler Phishing will increase in 2017. This utilizes fake social media accounts for services like banks and retailers to intercept genuine consumer-to-business communication, engage with customers, and attempt to learn credit card details and other confidential information.

NEW INSIGHTS (cont.)

- In 2017, Angler Phishing is expected to become more sophisticated and less manual. Attackers will implement automation and natural language processing to understand and reply accurately to customer communications before seeking to harvest their details, without any manual interaction being needed.
- Social media scams are expected to become more sophisticated in 2017. There will be an increase in fraud and counterfeiting using fake social media accounts and also more integrated fraud attacks, which combine fake social media accounts with fake apps and impostor emails.
- State-sponsored cyber-attacks declined in 2016 but are expected to grow in 2017 thanks to geo-political changes such as Brexit. Attacks are likely to come from a wider range of countries and use email as their main vector. As well as industrial espionage, objectives will include data theft and embarrassing disclosures.

TAKEAWAYS

- Partnering with threat intelligence services can give organizations an insight into the types of attacks being encountered by themselves and their sector. Early insight can offer an opportunity to defend against future attacks which makes threat intelligence a business priority as well as an IT and security priority.
- Automated email threat defenses are important because 90% of attacks organizations face originate from emails. They can block dangerous phishing attacks before they even reach users, offering bullet-proof defenses against the evolving threats from phishing and BEC attacks.
- Email authentication is effective in tackling over 60% of BEC attacks. It gives full visibility over your email ecosystem and allows anything that fails authentication to be blocked. Email authentication is so important that the UK NCSC and EU CERT both recommend implementing it.
- To protect against Mobile Security threats, businesses should employ Mobile Device Management (MDM) solutions and also invest in data-driven solutions working alongside the MDM. These can expose application behavior on a device and help to identify and remove rogue apps to cut the risk of data loss.
- Businesses must protect both their brand and their customers from social media fraud using fake accounts. To do this requires a robust social media security solution which scans all platforms, not just standard ones, ensuring full visibility and enabling fake accounts to be identified and shut down.

DEFINITIONS

- **Business Email Compromise (BEC)** is defined by the FBI as a sophisticated scam targeting businesses working with foreign suppliers and businesses that regularly perform wire transfer payments. Formerly known as Man-in-the-Email scams, these schemes compromise official business email accounts to conduct unauthorized fund transfers. (Source: fbi.gov)
- **Ransomware** is computer malware that installs covertly on a victim's device and that either mounts the cryptoviral extortion attack from cryptovirology that holds the victim's data hostage, or mounts a cryptovirology leakware attack that threatens to publish the victim's data, until a ransom is paid. (Source: wikipedia.org)
- **Locky** is a new ransomware that has been released (most probably) by the Dridex gang (source). Not surprisingly, it is well prepared, which means that the threat actor behind it has invested sufficient resources for it, including its mature infrastructure. (Source: proofpoint.com)
- **Threat actor,** also called a malicious actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact -- an organization's security. (Source: techtarget.com)
- **Exploit kits** are a type of malicious toolkit used to exploit security holes found in software applications (Adobe Reader, etc) for the purpose of spreading malware. These kits come with pre-written exploit code and target users running insecure or outdated software applications on their computers. (Source: malawarebytes.com)

Click or scan to access the webinar

CLICK TO ACCESS THE WEBINAR

proofpoint

Proofpoint, Inc. helps the most successful companies in the world protect and govern their most sensitive business data. Proofpoint is an innovative security-as-a-service vendor that delivers data protection solutions that help organizations protect their data from attack and enable them to effectively meet the complex and evolving regulatory compliance and data governance mandates that have been spawned from highly publicized data breaches.

insight brief
RESEARCH. DISCOVERY. INSIGHTS.

Our team produces short documents for busy professionals, summarising longer reports and research papers so that readers can swiftly become acquainted with a large body of knowledge and decide whether or not to read the full source document(s).

We vet and qualify reports for relevancy and value to its intended audience before creating an InsightBrief document. Our editorial team is independent from the originator of the report, ensuring that the insights exclude sales or vendor centric messaging, thereby creating real value for our time-poor readers.