Enterprise Network Protection Against Cyberattacks Primer: Business Email Compromise

A TrendLabs℠ Primer

Business Email Compromise (BEC) involves **email scams** that are far simpler than the technically advanced business threats such as data breaches and targeted attacks. The targeted emails come in the form of familiar business interaction—plain text from supposedly a highly revered executive or an established business contact—typically without malicious links or attachments, so it can bypass security measures. Touching base with the company via social engineering techniques, the scams ultimately lead to fraudulent transfers resulting to hundreds of thousands of dollars in losses.

The figures released by the **FBI** show that BEC schemes have been increasingly successful, as they have become more pervasive. BEC has resulted to at least $5.3 billion stolen, with an average exposed loss of $132,000 per incident, from reportedly 131 countries from 2013 to 2016. The agency also reports that the identified exposed losses to BEC have increased by 2,370% from 2015 to 2016.

In this primer, we will discuss how Business Email Compromise makes inroads in small- to medium-sized businesses and enterprises today, and how to avoid being a victim of this billion-dollar scam.

Swindling and Defrauding Businesses across the Globe

Business Email Compromise (BEC) usually targets employees in organizations who regularly perform wire transfer payments. By impersonating communications from high-level executives and business contacts, cyber crooks can lure employees—typically from the finance department—to initiate fraudulent wire transfers to foreign accounts. Cybercriminals can follow up their emails with a phone call to give further urgency, or coincide requests with the executive's business travel so that it would be harder to verify on the employee's end.

Most of the BEC incidents involve posing as the Chief Executive Officer (CEO) or president of the target company. This is why the commonly known scheme is called "CEO Fraud". The authority gives an air of legitimacy to send out an email for conducting a wire transfer that can involve a hefty amount of money.

Although CEO Fraud is the form of BEC scam usually perpetrated, the FBI has identified four other methods by which the scam can be carried out:

- The Bogus Invoice Scheme – Fraudsters pose as a company's foreign supplier and communicate via phone, fax, or email to transfer funds for invoice payment to an alternate account controlled by the fraudsters.
- Account Compromise – This scheme is not about spoofing emails, it involves hacking employee accounts. Requests for invoice payments to fraudulent bank accounts are sent from the employee's email to multiple vendors in the employee's contact list.
- Attorney Impersonation – Fraudsters identify themselves as lawyers or law firm representatives, claiming to handle confidential and time-sensitive matters. The request, typically done through phone or email, can also be timed to occur by the end of business day or week when contacted employees are more pressured into acting quickly.
- Data Theft – Role-specific employee accounts (typically human resources and bookkeeping) are targeted for requests—not for wire transfers, but for personally identifiable information (PII) or tax statements of employees and executives. This can serve as a jumping-off point for future BEC attacks against the company.

Based on Smart Protection Network (SPN) feedback, our analysis showed that BEC schemes often targeted Chief Financial Officers (CFOs) more than any other company position. Since CFOs handle the finances of an organization and are normally responsible for processing transfer requests, it just makes sense that fraudsters direct their scams to them.

Figure 1: Distribution of target positions by BEC

On the other hand, CEOs are most commonly spoofed in BEC scams, followed by managing directors. This is probably to create a sense of urgency in the intended recipients and consequently lure them into making the money transfers.

Figure 2: Distribution of spoofed positions by BEC

On a global scale, BEC schemes have been found to be active in different parts of the world. Our Smart Protection Network data showed that the highest number of BEC attack attempts in the first half of 2017 were in the United States, Australia, United Kingdom, Norway, and Canada.

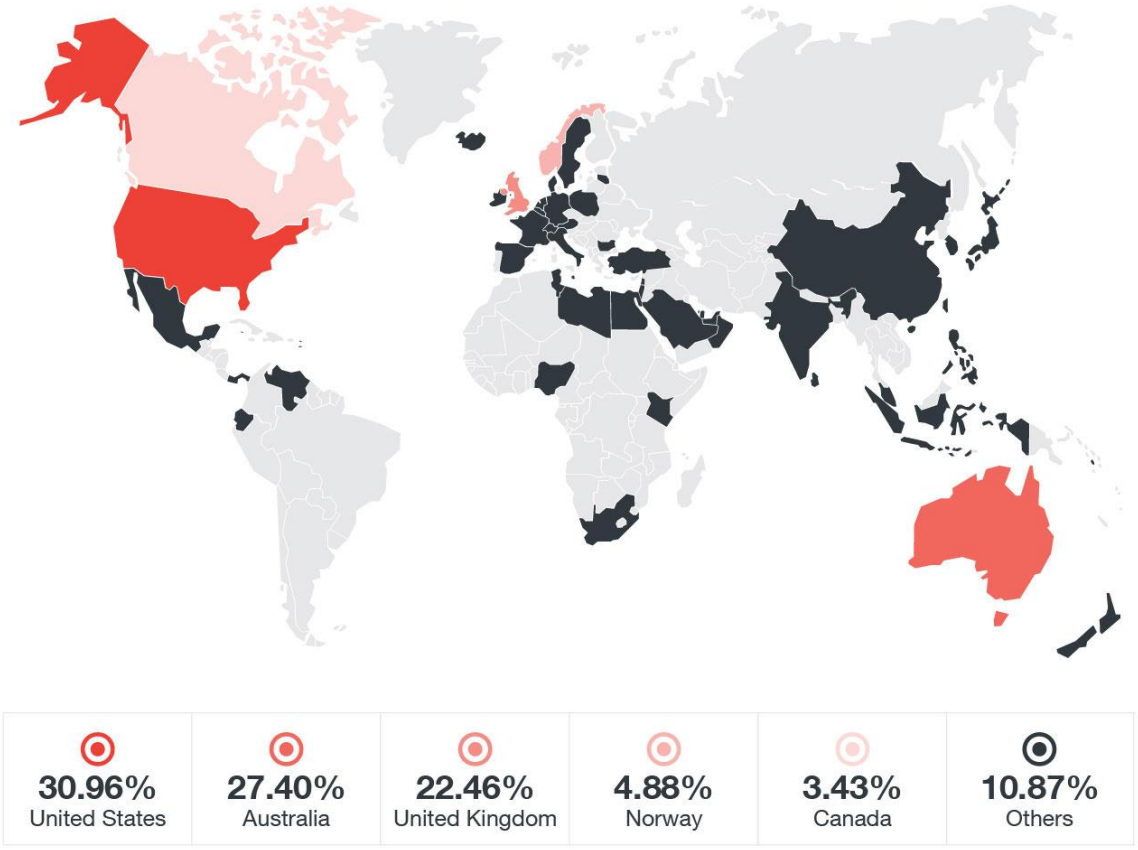

Figure 3: Countries with the most number of BEC attack attempts in 1H 2017

Simplicity and Social Engineering at Play

Business Email Compromise is unlike the other moneymaking schemes that involve malware. While some BEC incidents include **malware** to funnel money, normally the cybercriminals just trick the victims into doing the transfer for them.

BEC schemes keep things simple. Most email subjects contain single- or few-worded subject lines. Subjects also usually have the following words: request, payment, transfer, urgent, remittance, invoice, and acquisition instructions, among others. Simple and innocuous email subject lines are less likely to raise doubt, thus making it harder to be filtered.

The schemes heavily bank on social engineering tactics to compromise legitimate corporate email accounts or convincingly spoof an email account. In order to do this, the perpetrators monitor and study their victim organization to successfully identify their unwitting target employees and the protocols necessary to perform the wire transfers. They may also request a transfer that is similar to the usual business transactions so as not to raise any suspicion.

For example, an accountant who frequently works with the senior management may receive a well-worded email, with familiar or identical format and communication style, from purportedly the CEO. The email contains a request to make an urgent wire transfer, accompanied by the bank account details. The email can bear the company logo and even the signature of the CEO. Considering that the email looks legitimate and comes off with the usual tone of the CEO, the accountant can be duped into transferring funds.

Cybercriminals can also exchange several emails with their targets to gain their trust. This makes the communication seem sound. Crimeware such as the simple **HawkEye** keylogger can be planted using social engineering. This was the case with the Nigerian cybercriminals that were willing to play the long game and took their time with gathering intelligence on their targets. Only after several emails did the cybercriminals send the keylogger. This ensured the success of their targeted scams more.

Malware utilized in fraudulent emails, such as in the abovementioned incident, can be purchased online for a cheap price. The steepest price could average at $50, while some can even be obtained for free.

Solutions and Recommendations against Business Email Compromise

Helmed by social engineering, Business Email Compromise is a threat that is trickier to detect. Since BEC attacks do not normally use malicious attachments or URLs, they can evade traditional security solutions that only look into suspicious content and behavior. BEC mail, then, can be sent straight through company email accounts and result in significant monetary losses.

This is where employees will be a crucial line of defense. Since BEC does not require advanced technical components, strengthened employee awareness—from the newest recruit to the CEO—and understanding how BEC scams work will help deflect BEC attempts and protect businesses against a fraud incident.

Employees should check whether the wire transfer request is consistent with the previous ones or not—considering the timing, sender and recipient, and country to which the prior wires have been sent. They should be able to confirm transfer details through a two-factor verification system, where there is an established other communication channel (such as for phone calls) available for double-checking. Phone verifications should also be done using previously known numbers, not the numbers indicated in the email request.

It would also be helpful to assess the content of the email. Carefully look at email addresses. Scammers can mimic legitimate email addresses by constructing an address that can be off by only one letter. Creating intrusion detection system rules that can flag emails with extensions similar to the company email as fraudulent can be especially helpful.

One can also ask if the request is unusual of the requester's typical behavior. Does the text contain phrases or anomalies that could mean fraudulent email request? Or does the email involve urgency that is out of the ordinary? Be wary of requests that entail secrecy or pressure to take action immediately. Organizations may consider holding requests for an additional period of time to verify the legitimacy of the request.

The May 2017 **public service announcement** of the FBI Internet Crime Complaint Center (IC3) also has provided other actionable security strategies that include:

- Establishing a company domain name: Use a registered company domain name for employee emails instead of using open source email services.
- Staying away from spam: Do not open spam email or click on links and attachments from unknown sources. Unsolicited emails should be immediately reported and deleted as these can contain malware.

- Using Forward instead of Reply: Use the “Forward” option and type in the email address from the company address book to ensure legitimate correspondence. Using the “Reply” option can leave unsuspecting employees to respond to fraudulent business emails.

Harnessing both employee and technology defenses are the most effective protection against BEC schemes. Having educational resources and intelligent solutions that go beyond the malware-only protection can prevent this business-crippling, email-borne threat.

Trend Micro is able to provide protection for both small to medium-sized businesses and enterprises against BEC-related emails through our **social engineering attack protection**. This technology, integrated with the **Trend Micro™ Email and Collaboration Security**, including **Smart Protection for Office 365**, utilizes the following techniques:

- Social engineering attack protection (SNAP) combines expert rules and machine learning technologies to identify and filter BEC-related email behavior and characteristics (from mail header to body) such as a forged sender and a known malicious email service provider. A rule is triggered once any of the known BEC-related tactics is seen. The email’s content is also checked and verified through machine learning.

- Email reputation-based technologies (for blocking known malicious IP addresses and analyzing email sources and email correlation combinations)

- Antimalware which uses both predictive machine learning and heuristic-based scanning technologies

- Sandbox-based technologies for behavioral analysis of possible malicious file attachments or embedded URLs

To learn more about Business Email Compromise and how organizations can defend themselves, read **Billion-Dollar Scams: The Numbers Behind Business Email Compromise**.

Created by:

TrendLabs

The Global Technical Support and R&D Center of Trend Micro

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**

Securing Your Journey to the Cloud

www.trendmicro.com