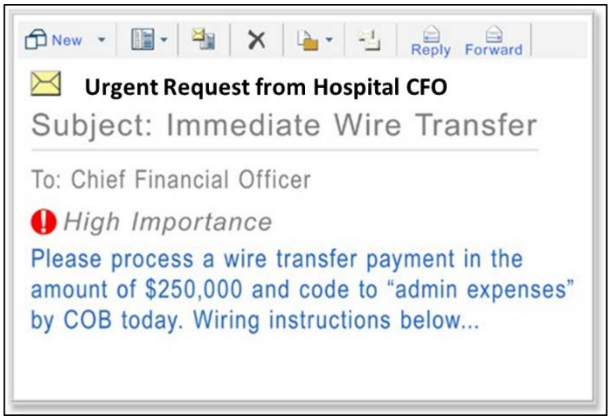
Business Email Compromise (BEC): Deception and Theft
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV
Date: March 13, 2019

EXECUTIVE SUMMARY:

Business email compromise (BEC) is a scheme in which cybercriminals send out targeted email messages to personnel with finance or resource roles within an organization in order to trick them into transferring funds to the cybercriminals. BEC is different from phishing, however, as the cybercriminals are not sending email messages with malicious links or attachments, but rather exploit human nature with seemingly legitimate requests. These requests contain nearly perfect spelling and grammar, and are used to convince individuals to send funds or sensitive information to the cybercriminals. Frequently, the BEC emails are made to look like they are from senior executives within an organization or trusted vendors to increase the urgency for victim individuals. BEC scams are a critical threat because they are mostly not caught by security solutions and employ a combination of extensive research on the target and sophisticated social engineering techniques (oftentimes including a phone call before and after an email) to exploit human nature. From October 2013 to May 2018, BEC scams victimized 41,058 US organizations across the US economy, and resulted in nearly $600M per year in losses.[i]

Healthcare and Public Health Sector (HPH) sector entities are encouraged to understand the unique BEC threat landscape and to train employees to recognize BEC scams, especially personnel with the ability to facilitate financial transactions or that handle sensitive data and PHI. Organizations should consider instituting a two-step verification process, as well as other methods discussed later, prior to executing funds transfers to confirm that the request is legitimate.



Urgent Request from Hospital CFO
Subject: Immediate Wire Transfer
To: Chief Financial Officer
High Importance
Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...

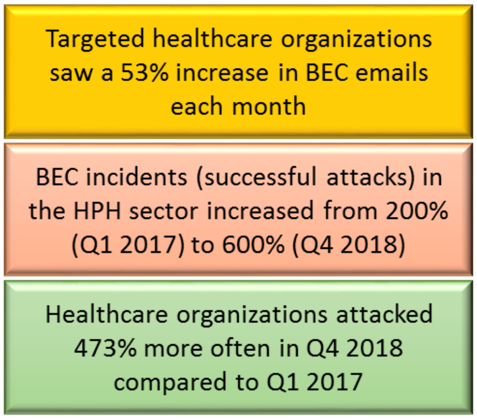
Figure 1: Example BEC email targeting the HPH sector.

BEC & THE HPH SECTOR

BEC is growing in popularity for a multitude of reasons, one being that it allows cybercriminals to focus less on technical capabilities and techniques, and more on target research and social engineering. BEC attacks are increasing in sophistication, impersonating (spoofing) more identities from personnel across the targeted organization and victimizing more people from different business departments within the organization to facilitate fraud, or any desired criminal activity. There are two main methods that cybercriminals use in BEC scams: spoofing healthcare employees - either by using compromised email credentials or manipulating the email “display-names” and domains - along with leveraging “lookalike” domains.**Error! Bookmark not defined.**

In spoofing, the attacker seeks to make the email appear to come from someone the recipient already trusts and/or regularly communicates with for business purposes. When a cybercriminal has access to an email account, they can download the mailbox to better understand how and with whom the target communicates, simply monitor the inbox and sent folder, and hijack threads to make the fraudulent request.

In a recent analysis of 450 healthcare organizations, the average targeted organization received roughly 96 BEC attacks[ii] targeting 65 different staff members in Q4 2018.[iii] In these attacks, the targeted staff members received BEC e-mails from an average of fifteen different spoofed identities.[iv] Larger healthcare organizations were targeted more frequently than smaller healthcare entities, with wire-transfer fraud being the most common type of BEC attacks.[Error! Bookmark not defined.]



Targeted healthcare organizations saw a 53% increase in BEC emails each month

BEC incidents (successful attacks) in the HPH sector increased from 200% (Q1 2017) to 600% (Q4 2018)

Healthcare organizations attacked 473% more often in Q4 2018 compared to Q1 2017

Figure 2: Statistics of BEC attacks in the HPH sector since Q1 2017.

From Q1 2017 to Q4 2018, of all observed BEC attacks targeting healthcare organizations, 95% occurred using the organization's (own) trusted domain (meaning the email accounts of employees were compromised and leveraged to send BEC emails).[iv] Lookalike domains (wherein the attackers register web and email domains that are deceptively similar to legitimate healthcare domains by, for example, using the number "0" instead of the letter "o") were used in nearly 67% of the BEC attacks against healthcare organizations.[iv]

Prior BEC Campaigns in the HPH Sector

Although many BEC scams are successfully blocked or ignored by users, there are a number of instances where cybercriminals have successfully stolen funds from the HPH sector. The following are examples of BEC campaigns targeting the HPH sector over the last several years:

In 2015, a cybercriminal leveraged compromised account credentials belonging to a local medical center and attempted to take out a large line of credit with a pharmacy to purchase prescription drugs. Given the size of the order, the pharmacy contacted the local medical center in this case center to confirm the order for over of over $500,000 worth of prescription drugs.[v] The medical center had not placed that order, and it was determined to be fraudulent. The pharmacy had only called the medical center to clarify because the shipping address for the medical center was different from that which they had on record; however, all the other certificates and credentials were accurate and accounted for including: the Drug Enforcement Agency (DEA) ID number, doctor licenses, and pharmaceutical certificates.[v]

Over a two-week period in 2016, a series of BEC campaigns was observed targeting 17 healthcare institutions in the US, ten in the UK, and eight in Canada, with the organizations ranging from general hospitals and pharmaceutical companies to specialty care and walk-in clinics.[vi] Although the intention and effectiveness of this campaign is unknown, security researchers did reveal two main techniques leveraged by the cybercriminals in these campaigns against healthcare institutions. In the first technique, the cybercriminals spoofed the "From" field in the emails to make the message appear as if that the email came from the CEO or executive, while the "Reply To" field was populated with the cybercriminals' email address. In the second technique, the cybercriminals used copycat domain names, where the scammer uses a domain name that's very similar to the target healthcare institution.[vii]

In 2017, a Wyoming-based healthcare system fell victim to a BEC campaign after a hospital staffer responded to an email from an attacker that impersonated a hospital executive. Ultimately, the W-2 tax form data of 1,457 hospital employees was given to the attacker.[viii] In this example, no PHI for the employees or the patients was given to the attacker. However, it was tax season and the attacker was only interested in W-2 data in order to likely conduct identity fraud.

In 2018, it was reported that a Missouri-based Children's hospital nearly fell victim to a BEC campaign, but was able to foil the malicious activity before the cybercriminals sent out the specially-crafted messages. Initially, the cybercriminals sent phishing email messages to numerous hospital staff, and successfully tricked five of the recipients to enter their email credentials into fake login pages on phishing websites. The cybercriminals were then able to login to the accounts and download the entire mailboxes of four of the five employees, obtaining a range of PHI belonging to 63,049 patients.[ix] The cybercriminals then prepared and were about to launch a BEC campaign from those accounts before the unauthorized access to each of the five email accounts was detected and blocked. The cybercriminals were unable to complete the BEC attack.

The HPH sector, in a sense, is like the other sectors in that cybercriminals can target organizations with BEC attacks to conduct criminal activities of transferring funds and obtaining PII such as W-2 tax data. However, the HPH sector is unique to other sectors because it deals not only with transferring of funds and PII, but also (PHI) and goods like prescription drugs – all of which can be targeted and obtained via BEC.

HOW BEC SCAMS WORK

Believability is the key for all BEC campaigns, meaning the fraudulent email messages must appear to come from the legitimate source and be sent to a legitimate, reasonable destination to not raise suspicion.[x] The cybercriminals invest a significant amount of time and resources into researching and establishing organizational hierarchies, including staff positions, email addresses, and common business processes. Using these approaches, BEC attacks have evolved to become highly persistent and evasive, leading to large financial fraud losses for businesses as well as data breaches for healthcare and government organizations.[xi] With this extensive research and information at hand, the archetypical BEC campaign would look like the following:

- **Initial Approach:** The BEC emails are sent to the targets either directly from a compromised account or spoofed to appear to be from known contacts in the target's network;
- **Targeting and Research:** The cybercriminals will often mimic previous conversations or insert themselves into current conversations between trusted partners, executives, or regular business email users;
- **The BEC "Attack":** While impersonating a known or trusted contact, vendor, partner or executive, the cybercriminals make the request for a payment be sent to an "updated" bank account number/sensitive data (PHI, W-2s)/line of credit for prescription drugs;
- **Continuous Monitoring:** Mail filters (rules) are created for the compromised email account to ensure that communications are conducted only between the cybercriminal and the victim and to monitor a compromised user's inbox.

In most BEC campaigns the cybercriminals will include a simple subject line to convey a sense of urgency and to encourage the recipient of the spoofed email to act quickly. The push for quick action, coupled with the fact that the email appears to be sent from a high-level member of their company, intends to discourage the recipients (employees) from taking the time to consider and verify that the details of the request are legitimate.**Error! Bookmark not defined.** Examples of the subject lines commonly used in BEC schemes include: *Extremely Urgent*; *Treat as Urgent*; *Due Payment*; *Urgent Payment*. Because the BEC email messages appear to come from a high-ranking individual (executive, manager, or trusted partner), the targeted employees naturally place high importance on responding. The targeted employees, wanting to do their job well and efficiently, will tend to want to act quickly to make the wire transfer or share the sensitive data without first verifying the requestor. In addition to using certain subject lines to convey a sense of urgency, the

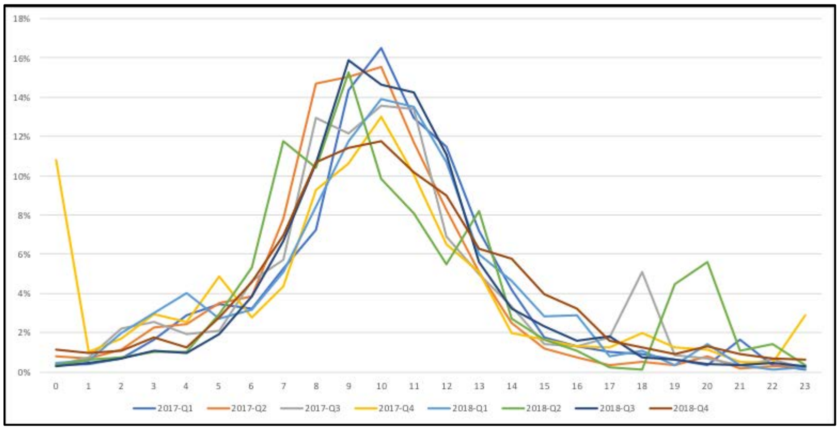


Figure 3: Most BEC email messages are sent to the targeted organizations between 8 and 10 in the morning.

cybercriminals behind BEC campaigns evidently believe that timing of email delivery is of importance. Since Q1 2017, the majority of BEC email messages were delivered between eight and ten in the morning, which suggests the cybercriminals are intending to exploit the targets during a busy time of responding to other emails and meetings.[Error! Bookmark not defined.]

BEC: LUCRATIVE AND SIMPLE

In July 2018, the Internet Crime Complaint Center (IC3) published an alert detailing the criticality and scope of the BEC threat. From October 2013 through May 2018, there was a total of 78,617 domestic and international incidents (41,058 US victims) costing approximately $12,536,948,299 USD for domestic and international victims ($2,935,161,457 total cost for U.S. victims).[xii] In 2017, the IC3 received 15,690 complaints of BEC attacks, which totaled losses of more than $675 million USD in the U.S. alone.[xiii]

The BEC technique is simple in that it involves taking over or impersonating a trusted user's email account to target organizations with intentions of fraudulently diverting/obtaining funds, sensitive data, or material goods. BEC campaigns are largely reliant on extensive research and social engineering, making it attractive to cybercriminals because it requires little or no technical knowledge, malware or special tools.[xiv]

- **BEC emails do not contain malware.** The majority of BEC attacks normally don't contain malware.
- **BEC emails (largely) bypass detection**. Successful BEC attacks are well-crafted with no spelling or grammatical errors. As a result, and in addition to the fact that the email messages do not contain attachments or links, they are often able to bypass many (or most) spam filters and other automated detection tools.
- **BEC emails are well-crafted and highly-personalized.** Cybercriminals conduct extensive research on the victim well before the BEC attack is launched, searching and collecting information from public websites, social media, and even the dark web forums to find specific data, including names and background information of company executives. With this information and with knowledge of an executive's writing style, the BEC emails will appear highly authentic.

Cybercriminals are attracted to BEC because the attack is relatively simple and fast, and the victim organization that falls for the scam might have a difficult time recovering the lost funds or containing the stolen data. The stolen funds are typically laundered almost instantaneously, as in one recent example where a cybercriminal group requested, received, and converted $1,800 in Apple iTunes gift cards into $700 in bitcoin in less than two and a half hours.[xv]

PROTECTION STRATEGIES FOR BEC

Organizations across the HPH sector must be aware of the BEC threat and train employees to recognize BEC scams, especially personnel with the ability to facilitate financial transactions or handle PHI and other sensitive data. Although all employees should be aware of the BEC risk, the training should focus on the individuals with the ability to move the resources that the cybercriminals are targeting, such as PHI, W-2 data, pharmaceuticals, and funds.

Nontechnical Protection Strategies

Because BEC campaigns rarely include malware or malicious links, the well-crafted and targeted email messages evade detection by antivirus (AV) and other security solutions. Healthcare organizations can drastically reduce the risk of email fraud and the associated financial losses and reputational damage with training to identify BEC campaigns. In addition to training, organizations are highly encouraged to establish a protocol for a two-step verification process for all requests regarding finances or sensitive data.

To counter the risk posed by BEC attacks, organizations should introduce policies that ensure that no one person or single email request can authorize large transactions or sharing of sensitive data.[xvi] Rather, organizations should institute a mixture of communication channels for verifying any request for confidential or financial information. The human element plays the most significant role in BEC, and the primary prevention starts with developing a security policy. The process for carrying out requests must require a two-step verification, and never rely on or trust a request sent via email is legitimate without following up.

If a request is sent from a company executive, the recipient should simply contact the sender by phone to help make sure the request is legitimate, and it is important that HPH sector executives are supportive of establishing this two-step verification policy. Employees within the HPH organizations should be encouraged to call – despite the email being marked *urgent* or *critical* – or if the email states the requester is on vacation or unreachable. This policy of following up with the requesting individual either in-person or via a known phone number will mitigate most of the BEC campaigns from being successful.

Technical Protection Strategies

In addition to the employee BEC awareness training and implementing a two-step verification process, there are more technical options to detect, identify and investigate potential BEC campaigns on a network. Monitoring the logins and login attempts to an email account, or any new inbox rules that are created, could help system administrators identify potentially malicious activity and BEC attempts. Cybercriminals behind BEC campaigns will often set up inbox rules on compromised email accounts so that every email received by that employee (or every email that contains certain keywords) will be automatically forwarded to the attacker, so it is imperative to have insight into this activity to potentially mitigate a compromised account and BEC.[xvi]

SUMMARY

Business email compromise (BEC) is one of today's greatest cyber threats impacting HPH organizations of all sizes across the globe. BEC fraud attacks are socially engineered to target people, rather than technology, and the cybercriminals aim to exploit the human nature of healthcare organizations' staff, patients, and business associates to defraud health care programs, produce fake insurance cards, steal health information, and obtain/divert prescription drugs.[xvii]

With the significant increase in BEC campaigns targeting healthcare organizations (473% increase in targeted BEC campaigns in 2018 compared to 2017[Error! Bookmark not defined.]) the HPH sector needs be thoroughly aware and vigilant of the BEC threat and act to mitigate the risks of transferring funds or turning over sensitive information to cybercriminals.[Error! Bookmark not defined.] Nontechnical mitigations (BEC awareness training for employees and two-step verification for completing requests) and technical mitigations – monitoring mailbox activity, such as login data and mailbox rules – can help HPH organizations minimize the BEC threat.

REFERENCES

[i] "FBI: BEC Losses in 2017 Shot Up to Over US$675 Million," Trend Micro, 21 May 2018, accessed 28 Feb 2019; https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fbi-bec-losses-in-2017-shot-up-to-over-us-675-million

[ii] Jessica Davis, "Email Fraud Attacks on Healthcare Jumped 473% Since 2017," Health IT Security, 11 Feb 2019, accessed 25 Feb 2019; https://healthitsecurity.com/news/email-fraud-attacks-on-healthcare-jumped-473-since-2017

[iii] "REPORT REVEALS 473% INCREASE IN HEALTHCARE EMAIL FRAUD ATTACKS IN 2 YEARS," The HIPAA Guide, 20 Feb 2019, accessed 27 Feb 2019; https://www.hipaaguide.net/report-reveals-473-increase-of-healthcare-email-fraud-attacks-in-2-years/

[iv] Mackenzie Garrity, "Email fraud in healthcare up 473% — 6 things to know," Becker's Hospital Review, 12 Feb 2019, accessed 28 Feb 2019; https://www.beckershospitalreview.com/cybersecurity/email-fraud-in-healthcare-up-473-6-things-to-know.html

[v] "Business Email Compromise: In the Healthcare Sector," CIS, accessed 21 Feb 2019; https://www.cisecurity.org/blog/business-email-compromise-in-the-healthcare-sector/

[vi] "CEO email scam targets 17 US healthcare organizations in 2 weeks," Becker's Hospital Review, 28 Nov 2018, accessed 19 Feb 2019; https://www.beckershospitalreview.com/healthcare-information-technology/ceo-email-scam-targets-17-us-healthcare-organizations-in-2-weeks.html

[vii] Ryan Flores, "CEO Fraud Email Scams Target Healthcare Institutions," Trend Micro, 23 Nov 2016, accessed 21 Feb 2019; https://blog.trendmicro.com/trendlabs-security-intelligence/ceo-fraud-email-scams-target-healthcare-institutions/

[viii] HIPAA Journal, "Tax Season Triggers Wave of W-2 Business Email Compromise Attacks," HIPAA Journal, 27 Jan 2017, accessed 26 Feb 2019; https://www.hipaajournal.com/tax-season-triggers-wave-w-2-business-email-compromise-attacks-8669/

[ix] titanadmin, "Children's Mercy Hospital Phishing Attack Highlights Need for Effective Anti-Phishing Protections," SpamTitan, 5 Jul 2018, accessed 25 Feb 2019; https://www.spamtitan.com/blog/childrens-mercy-hospital-phishing-attack-highlights-need-for-effective-anti-phishing-protections/

[x] Kevin Townsend, "New Variant of BEC Seeks to Divert Payroll Deposits," Security Week, 15 Jan 2019, accessed 25 Feb 2019; https://www.securityweek.com/new-variant-bec-seeks-divert-payroll-deposits

[xi] Brad Wyro, "Business Email Compromise – The 12 Billion Dollar Threat to Your Business," MDaemon, 13 Nov 2018, accessed 19 Feb 2019; blogs.mdaemon.com/index.php/2018/11/13/business-email-compromise-the-12-billion-dollar-threat-to-your-business/

[xii] "BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM," FBI IC3, 12 Jul 2019, accessed 23 Feb 2019; https://www.ic3.gov/media/2018/180712.aspx

[xiii] "FBI: BEC Losses in 2017 Shot Up to Over US$675 Million," Trend Micro, 21 May 2018, accessed 28 Feb 2019; https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fbi-bec-losses-in-2017-shot-up-to-over-us-675-million

[xiv] Alexandrea Berninger, "IBM X-Force IRIS Uncovers Active Business Email Compromise Campaign Targeting Fortune 500 Companies," IBM X-Force, 21 Feb 2018. accessed 26 Feb 2019; https://securityintelligence.com/ibm-x-force-iris-uncovers-active-business-email-compromise-campaign-targeting-fortune-500-companies/

[xv] Crane Hassold, "Scarlet Widow Bombs Nonprofit Directories to Run BEC Scams," AGARI, 27 Feb 2019, accessed 28 Feb 2019; https://www.agari.com/email-security-blog/scarlet-widow-bombs-nonprofit-directories/

[xvi] "Top Phishing Attacks: Discovery and Prevention," AGARI, 2017, accessed 1 Mar 2019; https://www.agari.com/phishing/solution-briefs/top-phishing-attacks-discovery-and-prevention.pdf

[xvii] "Healthcare Email Fraud Report," proofpoint, February 2019, accessed 25 Feb 2019; https://www.proofpoint.com/us/resources/threat-reports/healthcare-email-fraud-report