February 2021 ♦ Issue 2

Solutions

INSIDE THIS ISSUE

1-2 Business Email Compromise (BEC),
3 Vishing-Just as Dangerous as Phishing Scams

Business Email Compromise (BEC)

CEO Fraud, also known as Business Email Compromise (BEC), is a type of spear-phishing email attack in which the attacker impersonates a company's CEO or other senior executive. It is not new, and unfortunately will continue to evolve. In 2019, the FBI reported that more than half of all cybercrime losses were due to BEC scams, with businesses losing over $1 billion dollars; and in 2020, the average dollar request in a BEC attack increased from $48k to $75k. Cybercriminals have learned that exploiting unaware employees can sometimes have the biggest payoff. When an email looks so legitimate that it can fool an employee, it can have significant consequences. However, there may not always be a malicious email with an infected attachment or link to detect, posing a big challenge to security experts.

"In 2019, the FBI reported that more than half of all cybercrime losses were due to BEC scams, with businesses losing over $1 billion dollars; and in 2020, the average dollar request in a BEC attack increased from $48k to $75k."

In BEC attacks, the cybercriminals send an email to staff members to try to trick them into doing something they should not do. These types of scams are extremely effective because the cybercriminals meticulously research their victims before launching their attack so that it can seem more believable. They search an organization's website for their locations, who the executives are, and who they do business with. The cybercriminal then learns everything they can about the organization's coworkers on sites like LinkedIn, Facebook, or Twitter. Once they know the organization's structure, they begin to research and target specific employees, picking targets based on their specific goals. If the cybercriminals are looking for money, they may target staff in the accounts payable department; if they are looking for tax information, they may target human resources; if they want access to database servers, they could target someone in IT.

Continued on page 2

AaSys®
Solutions are our Business

Once the cybercriminals determine what they want and whom they will target, they begin crafting their scheme. Most often, they use spear phishing. Spear-phishing is similar to phishing; however, instead of sending a generic email to millions of people, they send a custom email targeting a very small, select number of people. These spear-phishing emails are extremely realistic looking and hard to detect. They often appear to come from someone you know or work with, such as a fellow employee or perhaps even a manager or higher up. The emails may use the same jargon your coworkers use; they may use an organization's logo or even the official signature of an executive. These emails often create a tremendous sense of urgency, demanding immediate action and discretion.

A successful execution of a BEC scam creates a significant burden for the both the company and the employee involved and can be very costly. So how do you protect yourself and your organization? Educating employees about the dangers of these types of attacks and using good judgement is the best defense. If an employee receives a message from a supervisor or a colleague and it does not sound or feel right, it may be an attack. Clues can include a tremendous sense of urgency, a signature that does not seem right, a certain tone you would never expect, misspellings or the name used in the email being different from what the person actually calls you. The attacker may use an email address that is similar to the legitimate email or use a phone number or email address you have never seen before. When in doubt, call the person at a trusted phone number or meet them in person (don't reply via email) and confirm if they are the sender.

Every organization has policies that define proper procedures for authorizing the transfer of funds or the release of confidential information and those processes should never be bypassed. If a request to do something outside normal procedure is received, regardless of the source, it should be considered suspicious and be verified immediately before any action is taken. Contact a supervisor, the help desk, or your information security team right away.

BEC attacks don't always get the same amount of attention as ransomware attacks, however it should. The reality is every day new threats arise and evolve, and organizations must always try to stay one step ahead. Having a combination of employee cybersecurity training, best practices against email threats as well as security technologies that can detect these types of scams is a good way to protect against BEC attacks.

Sources:
https://venturebeat.com/2016/09/19/6-critical-steps-to-avoid-ceo-fraudnow/
https://www.knowbe4.com/ceo-fraud
https://www.trendmicro.com/vinfo/us/
https://threatpost.com/email-security-attacks-bec/163869/

Vishing

Just as Dangerous as Phishing Scams

There is no shortage of phishing scams being perpetrated every day, but one that has continually flown below the radar is vishing scams, also known as voicemail scams. Just like phishing emails, a vishing scammer tries to persuade you into divulging sensitive information for their ultimate benefit.

Vishing involves cybercriminals calling potential victims, sometimes even leaving voicemails, to fraudulently attempt to steal credit card information, financial details or any other confidential information, by pretending to be a reputable organization. Cybercriminals use social engineering to get people to share personal details, such as social security numbers or passwords. By using voice over internet protocol (VoIP) technology hackers can call hundreds of people at a time and make the caller ID appear to come from a trusted source, such as your bank. But the hackers also realize that most people will not answer their phones if an unknown number pops up on their caller ID, and many mobile users will automatically program those numbers to go straight to voicemail. Therefore, they also utilize the voicemail system to perpetrate their crimes. Once an automated voicemail is left by the cybercriminal, it provides the phone users with choices when they play back the message, for instance pressing 1 or staying on the line. By choosing one of the options, the victim is essentially being prescreened by the cybercriminal. This method saves the hacker lots of time my narrowing down who is more susceptible to take the bait.

Vishing does not only affect average citizens; in fact, many well-known organizations have also fallen victim to these scams.

FBI uncovered a massive coordinated vishing campaign directed at trying to gain access to company databases by way of employee VPN credentials. Once inside the system, the cybercriminals stole customer information to be used as leverage in future attacks. The FBI put out a warning urging everyone to be vigilant and provided suggestions to help mitigate the threat.

Here are some things to look out for:

- ***Claiming to be from a government entity*** - If a caller claims to be from a government entity, like social security, the IRS or Medicare, be very skeptical, especially if they are trying to sell you something.
- ***Abnormal sense of urgency*** - Scammers will try to tap into your sense of fear, using threats of arrest warrants and problems with your account. If you get one of these phone calls, don't give out your information. Hang up, perform your due diligence, and do your own investigation.
- ***Request for personal information*** - If you get a call asking you to confirm your name, address, birth date, social security number, etc., it is most likely a scammer trying to trick you into divulging sensitive information.

How to protect yourself:

- ***Hang up immediately*** if you suspect it is a vishing phone call and block the number. Don't feel obligated to listen or have polite conversation with an unknown caller.
- ***Do not pick up the phone if it is an unknown number,*** simply let the call go to voicemail. Caller IDs can be faked, so do not always rely on that. Listen to your messages and then decide whether to call back.
- ***Do not press buttons or respond to prompts on a live call or a voicemail message.*** If you get an automated message that asks you to press buttons or respond to questions, don't do it. Scammers can record your voice and use it when navigating voice-automated phone menus linked to your accounts.
- ***Verify the caller's identity.*** Just because a person provides a callback number, does not mean it's legitimate; it may be part of the scam. Do not use the callback number provided by the caller, instead search for the company's official public phone number and call them back using that number.

Sources:
FBI warns of voice phishing attacks stealing corporate credentials | WeLiveSecurity
What is Vishing (Voicemail Phishing)? | Barracuda Networks
Naked Security – Page 6 – Computer Security News, Advice and Research (sophos.com)