Costs & Methods of Common Business Email Compromise

February 2024 - Written by Jerry Johnson

Egis IT Security
Shielding Your Business

Introduction:

The cost of cyber threats has never been higher. Ransomware makes most of the headlines these days, but another threat is working its way through the Internet and seldom discussed – the Business Email Compromise, or BEC. A BEC can be more personal to its victims in nature because the threat actor is communicating with them directly or impersonating them using their own tools. A BEC seldom affects an entire business except by dollar cost or reputation impact. The individuals who are tricked into paying fake invoices or who fell for the initial scam often feel personally attacked or culpable due to the direct interaction with the hacker.

What it is:

A BEC begins when a hacker or their software gets access to an email account that isn't theirs. They are crafty and find new ways to do this, but often they will use phishing emails or social engineering.[1] Once they have access, they can use the mailbox in a few ways to benefit themselves and gain financially.

Goals of the BEC hackers:

When accessing a mailbox or email account, the cyber criminals will often have programs to scan them for email or files of interest. At this time, the most valuable information they can find involves financial transactions – invoices, credit cards, anything that they can tap into for money. If they find invoice information – especially where the email account is for someone in an accounting or accounts receivable role, they may attempt a conversation takeover attack. They can send email from the hacked account to anyone that owes money and ask for payment. This especially applies to invoices that are past due. They may inform the invoice recipient that since the invoice is past due there is a more urgent need to pay or face late charges or collections. Then they can provide a payment link that appears legitimate, but is a false link that sends the money to the bad actors instead.

They will also hunt for sensitive information that includes identity or social security information, or anything related to banking or investment account logins. If they can gain access to banking or investment accounts, then they will attempt to drain them of funds. If there is no information or nothing of value for them, they will often use the mailbox or email account as a waystation to send out viruses and phishing messages to their potential victim list. The victim list will now include contact information of any email messages they were able to collect along the way.

The smallest compromise that Egis consulted on in 2023 was for $16,000 worth of credit card transactions. The largest was a conversation takeover attack where the hackers got away with $180,000 by invoicing a secondary company from the hacked mailbox. Almost all conversation takeover attacks, in particular, either attempted to get or successfully resulted in the hackers taking more than $100,000 in gains.

(317) 344-2144 10255 Commerce Dr Suite 250, Carmel, IN 46032 jjohnson@egis-security.com

Costs & Methods of Common Business Email Compromise

February 2024 - Written by Jerry Johnson

Egis IT Security
Shielding Your Business

BEC attacks start this way:

Phishing Attacks – Most phishing emails contain links to sites or have virus attachments. If you open the attachment or click on the link then you may install a virus or run a malicious web browser script on your computer. The web browser scripts are especially effective, and are able to get by many regular anti-virus programs. If a phishing email tries to scam or trick you instead of using a virus, then we call that Social Engineering instead.

Social Engineering – The most common social engineering attack is a scam email or text message where the hacker tricks you into entering your credentials for them. They can have you go to a website that you think is a Microsoft login page, and put in your username and password to achieve what you assume is a real requirement. These web pages and links can even intercept your MFA (2-factor) login codes and allow the hacker access to your mailbox or cloud documents! Sometimes they send you a QR code so that you scan it with your phone, and then the fake page comes up on your phone and cannot be blocked by your computer's anti-virus software or firewall.

Email Impersonation – Sometimes the bad guys make a fake domain name that looks very similar to yours, or just modify their email information enough to appear so. They could send you a message, for example, that you mistakenly think is from your CEO when in fact it's not even from an account or computer in your business! If they have enough information about you and your clients and CEO built up, these messages could be very convincing. They can serve the same purpose as a mailbox at your company getting hacked at that point.

During the hack:

They can use automatic messaging forwarding or other Inbox rules to help hide their activities. Usually there will be a rule added so that some incoming email messages will be automatically deleted or filed into a hidden folder if they meet a certain pattern. For example, the threat actor won't want responses to their scams or conversation takeover emails to be seen in the regular Inbox by the victim.

Also, in some cases they have left rules and even installed software into the cloud environment so that if access is cut off then they will have a back door into the account and can reconnect to it later.

If they are actively draining banking or investment accounts of funds, it is not uncommon for them to send hundreds or even thousands of spam messages to the Inbox. Sometimes they will generate hundreds of spam text messages during that time. These tactics are meant to hide any real communication attempted by your bank or credit card company asking you if these are fraud transactions.

(317) 344-2144 10255 Commerce Dr Suite 250, Carmel, IN 46032 jjohnson@egis-security.com

Costs & Methods of Common Business Email Compromise

February 2024 - Written by Jerry Johnson

Egis IT Security
Shielding Your Business

How to detect or avoid a BEC:

Ongoing Security Awareness Training – Making people aware of the threats, teaching them how to avoid and understand them, monitoring metrics, and incentivizing everyone to protect their work community are keys to success. Sharing helpful security tips and information with each other and reporting observations to management and IT people should also be encouraged!

MFA / 2-factor Authentication – Having MFA, or multi-factor authentication, in place can block many threats. The MFA methods available to us are also getting stronger, and making it harder for scammers and hackers to overcome them. This should be combined with using strong passwords and avoid re-using the same password for multiple accounts!

Good Accounting Practices – Accounting and finance departments should have extra steps and procedures in place so that if a single person or mailbox is hacked, then that person alone cannot make changes to account information or perform large transactions without a second approver involved. Every communication should also be verified in person or by phone in addition to using email or text messages.

Be a good citizen – If you see something, say something. If you notice a company is sending out malicious emails and may have been hacked, alert them and their hosting company or Internet Service Provider. If you have been hacked, be sure to alert any recipients of email from your mailbox that the messages were not real and could contain viruses. If information is taken from your Inbox or cloud storage that could lead to others being victims, act proactively to reduce your liability and collateral damage.

Conclusion:

Hackers and scammers sometimes get ahead when it comes to technology. The flood of Business Email Compromise attacks that began in 2022 continued to grow in 2023 and seems ready for a tenfold increase in 2024.

In addition to good anti-virus and anti-malware software, we recommend 3rd party email filtering products to greatly reduce the levels of spam and phishing email delivered. We also offer products that monitor mailboxes and computers for activity that indicates a hacker has access to them.

Awareness through training and technology defenses keep evolving as well. Companies that take proactive measures and accept the reality of our changing risk environment are much better poised to keep doing business as usual. Preparation is key when it comes to shielding your business.

[1] *Phishing Email - https://www.knowbe4.com/phishing*
and Social Engineering - https://www.knowbe4.com/what-is-social-engineering

(317) 344-2144 | 10255 Commerce Dr Suite 250, Carmel, IN 46032 | jjohnson@egis-security.com