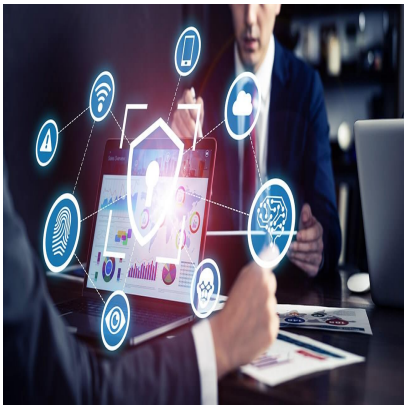


Understanding the Implications of Business Email Compromise Scams

Description

Understanding the Implications of Business Email Compromise Scams

- Prabhakaran Parameswaran â?? Cybersecurity Services Team

Enterprises and individuals alike have the potential to fall victim to more than 40 types of frauds. Out of these, frauds that take place when the attacker opts for Business Email Compromise (BEC) methods also pose a significant threat.

As per the cybercrime reports compiled by the FBI, BEC scams account for over $1.8 billion cumulative loss globally. BEC attacks are said to be around 64 times more devastating than other cybercrimes due to the losses it incurs.

What is a Business Email Compromise scam?

A Business Email Compromise belongs to the realm of cybercrime. An attacker is capable of attacking enterprises or corporate email accounts. After doing so, the attacker will move to defraud the company as a whole or individual employee. The reason for their ability to carry out this fraud is that the attacker gains access to specific sensitive information.

Mainstream media has also referred to this type of attack as the â??man-in-the-mailâ?• attack or the â??man-in-the-middleâ?• attack. The reason for this is that these attacks go undetected since the party on the receiving end thinks that they are capable of sending confidential emails to another party. However, the attacker will have gained access to all these emails.

Who do BEC attackers target?

These scams are directed towards companies the majority of the time. There are five ways this scam can take place:

Compromising the account

The hacker will gain access to a specific employeeâ??s account and, therefore, use their identity to infiltrate the databases holding sensitive information.

Fake invoice

The hacker will look to target foreign suppliers in this case. The basis of this attack requires the hacker to act as a supplier then request payments to their account.

Impersonation of an attorney

Another common tactic is taking the identity of a legal representative. Once the hacker does so, they approach the employees for a fund transfer.

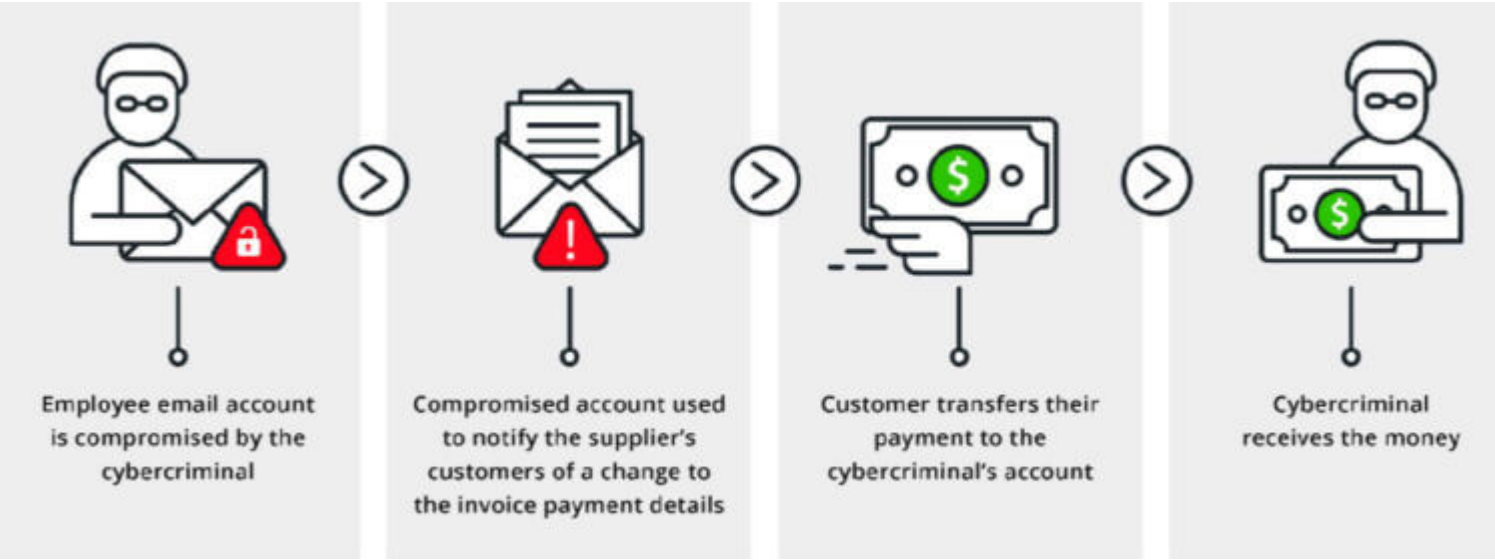
Data theft

The HR department falls victim to this kind of threat. The hacker will attain access to personal information about employees from the records. The employees are usually CEOs or higher-ups working in management.

CEO fraud

After the hacker is capable of obtaining access to CEO information, they are capable of assuming the identity of the CEO. Now, these individuals can send out fraudulent emails to the finance department.

Steps that attackers utilise



One of the best approaches to management security breaches involves tracing the steps of the attacker. This will not only help to examine the existing security measures but also predict potential

future steps that the hacker might make.

When it comes to BEC attacks, the attack takes place in the steps below:

Searching for a target

The hacker will first search for an enterprise and then a suitable employee working in the said enterprise. The hacker will attack based on one of the above methods. Hackers use various platforms like LinkedIn or company websites to search for any sort of contact information.

Sending out emails

The attacker will now send out emails to the targeted employeesâ?? email account. The emails will contain malware and will be known as phishing emails. The links in this email will redirect the employee towards a fake Outlook-365 login webpage. This webpage is created by the attacker and looks exactly like an authentic page.

Gathering information

Once the attacker plugs in their login credentials in the dummy website, the attacker can then copy down the email address and password of the employee. The next step would be to create a fake domain that resembles the company. In this domain, the hacker will enter the victimâ??s email address and surpass the web filters.

Now the attacker gains access to the email account, and the attacker will look to alter the real domain in a way that will forward all emails from the real account to the attacker. The attacker can now gather information regarding the billing or invoices and wire transfers.

Conduct social engineering

The hacker is essentially looking for emails that contain information about any kind of payment that took place between the company and the employee. These emails will be doctored so that the attacker can request payments using this email. The altered email will be sent along with the same mail chain to avoid suspicion. The money that is transferred by the employer will now reach the attackerâ??s account.

Collect financial reward

Now the attacker can finally profit off the scam. However, in the majority of these cases, the payments that take place do not undergo verification since the employer sees the same mail chain and thinks nothing of it.

How can a security team detect a Business Email Compromise Scam attack?

Detecting a security breach or, better yet, a phishing email is a best-case scenario in this case. Implementing a proper security policy should be at the forefront of a security teamâ??s efforts. A typical detection process against BEC attacks should include a series of scanning facilities or software that carries out the following:

- **Monitoring:** These facilities will provide visibility into the overall activity of the user depending on what email platform they use. This is especially useful for enterprises that deploy on a cloud.
- **Alerts:** The software or technology that is used should send out alerts to the security team when there is a login detected. In addition to this, the software can send alerts when there is an alteration in the browser in which the login took place.
- **Audits:** Regular audits will ensure that all phishing emails are removed from the inbox. The audits can be automated or manual as well.
- **Redirects and Forwards:** Emails can also be checked safely to see if the links are redirecting users to external domains. This will secure all the possible channels that hackers may utilize.

Preventive measures that security teams can implement

The detection of a BEC scam is only one aspect of the cybersecurity policy that enterprises can implement. In addition to this, there should be protective measures that prevent the attack in the first place. Enterprises should look to incorporate the following aspects:

- **Enhanced login processes**

Increasing the security around the login process can, essentially, nip the scam in the bud. A popular security measure at the moment is the incorporation of Multiple Factor Authentication. By this, an employee requires more than just their login credentials to access an account. This can also extend to making payments.

- **Detection of third-party domains**

Some enterprises introduce a marking system. According to this system, the emails that come from third-party domains will be marked with a different color to ensure that employees know it is suspicious.

- **Conduct domain name squatting**

Domain name squatting refers to the process where a party purchases an entire domain so as to prevent other parties from profiting off of said domain name. By doing so, a company can ensure that they find similar domains.

- **Spread awareness**

Since BEC attacks usually target actual people, all employees must receive some education regarding the nature of these attacks. An effective education would involve helping them detect signs in the email that may denote that it is a fake and more.

How should a team respond to a BEC attack?

In the off case that the BEC attack does take place and the hacker has infiltrated the email platform like Outlook 365, setting up a proper response can drastically reduce the damage. The security team should create a disaster management process that inhibits the chances of incurring a great loss during the attack. Therefore, the team should consider the following approach:

- **Password change**

The first plan of action would be to issue password changes to all the accounts that were involved in suspicious activity. To completely inhibit the damage, an enterprise can force all employees to change their passwords.

- **Active users**

The next step would be to kill all active sessions that may be taking place at the time. To do this, one will have to visit the Office365 admin center and follow the usual protocol that is present.

- **Removal of inbox rules**

Finally, to completely destroy the threat, the team will have to scan through the inbox rules and determine if there are any changes. In case there are certain suspicious alterations present, they will have to remove them.

BEC attacks have the potential to set back a company significantly in the financial sense. By targeting the workforce, attackers can carry out well-orchestrated attacks that prove a challenge to detect and neutralize. Therefore, every employee must make it a point to refrain from sharing important login credentials either in person or on online platforms. Finally, the best way to prevent such attacks is to be aware of them.

Category

1. Atmecs-Blog

Tags

1. Cybersecurity

Date Created
July 19, 2022
Author
admin