ManageEngine
AD360

The FBI's recommendations

for IT admins to prevent BEC attacks on Office 365 users

www.manageengine.com/active-directory-360/

Introduction

The U.S. Federal Bureau of Investigation (FBI) has issued a new warning that cybercriminals are currently targeting Office 365 users through business email compromise (BEC) attacks.

The FBI's Internet Crime Complaint Center (IC3) has sounded the alarm about BEC scams. According to its 2019 Internet Crime Report, between June 2016 and July 2019, it received 166,349 reports of email compromise with total losses of over $26 billion.

Since 2013, the year the FBI started tracking BEC scams, BEC scammers have targeted organizations of all sizes, in all industries, in over 100 countries. IC3 observed that between May 2018 and July 2019, losses due to BEC scams saw a 100% increase globally.

Further, BEC scams had the most damaging effects on businesses around the world last year. With 23,775 BEC victims sharing $1.77 billion in reported losses, the average loss per victim was estimated to be $75,000. To put things in perspective, losses due to BEC were $1.3 billion in 2018, $676 million in 2017 and $360 million in 2016 (with $30,000 being the average loss per victim).

According to the FBI, BEC scammers are currently targeting cloud-hosted email and productivity suites.

Between January 2014 and October 2019, the total loss due to BEC scams targeting Microsoft Office 365 and Google G Suite totaled over $2.1 billion. This is why it's imperative for organizations that use Office 365 to understand the anatomy of BEC scams to secure their Office 365 environments against them.

In this e-book, we will discuss what BEC scams are, their types, the reason behind their popularity, some recent cases of BEC scams, and the FBI's five recommendations for defending against BEC attacks. We'll take a detailed look at each of these recommendations and discuss how to implement them in your Office 365 environment using AD360, a comprehensive Office 365 reporting, auditing, management, and monitoring solution from ManageEngine.

What are BEC scams and how do they work?

BEC scams are email-borne employee impersonation scams wherein attackers aim to defraud enterprises of money through various social engineering tactics. These scams are sometimes referred to as "man-in-the-email" scams.

Although there are various types of BEC scams, there's one common element to all of them—deception. A typical BEC scam consists of impersonating a high-level executive, or anyone with the authority to make financial transactions, to deceive an unsuspecting employee into making a fraudulent bank transfer or supplying sensitive data about the company or its employees.

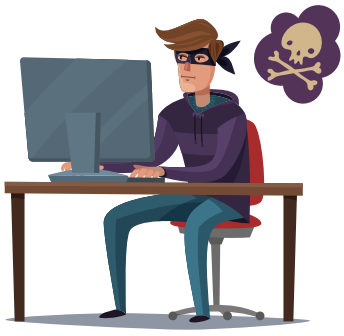
These are five common types of BEC scams:

1. CEO fraud

The attacker impersonates the CEO of a company. Fraudulent emails are then sent to an employee in the accounts department payable team requesting an urgent fund transfer to an account the attacker controls. In an attempt to please the CEO, an unsuspecting employee may readily oblige to the fraudulent request.

2. Attorney impersonation

In this type of scam, the attacker poses as an attorney or a representative of a law firm. A fraudulent request, pretending to be time-sensitive and confidential, is made to initiate the transfer of funds or sensitive information about the company. Since employees are often under the presumption that attorneys and law firms have the authority to make sensitive requests, they walk right into this trap and naively fulfill the attacker's requests.



3. The bogus invoice scheme

Companies with overseas suppliers are common victims in this type of BEC scam. The attacker impersonates one of the trusted suppliers and makes requests to transfer funds for invoice payment to a fraudulent account. This type of scam is also known as “the supplier swindle,” or the “invoice modification scheme.”

4. Data theft

The primary objective of this type of BEC scam is to extract sensitive information. Attackers try to fool the HR department or bookkeepers into providing sensitive information about the employees and executives. This information can be used in the future to conduct other cybercrime against the company.

5. Account compromise

In this type, the target account is not spoofed, but compromised. Only the accounts that have the authority to make fund transfer requests are picked as targets. Using this account, the attacker makes fraudulent payment requests to vendors. This compromised account can also be used to inject malware or steal intellectual property.

Why BEC scams will continue to prevail

Although BEC scams lack the sophistication inherent to most cybercrime, they have been growing prevalent over the years. This is mainly because these attacks embrace the philosophy that it is easier to exploit the vulnerabilities of human behavioral traits, such as trust, than software vulnerabilities.

On top of this, hackers are getting creative. Back in 2013, BEC scams began with the hacking or spoofing of the email accounts of C-suite executives, and emails with malicious links were sent requesting immediate transfer of funds. However, over the years, BEC attacks have evolved to include compromise of personal email accounts, vendor email accounts, requests for W-2 information, and so on.

Recent cases of successful BEC campaigns

In October 2019, the city of Ocala fell prey to a simple BEC campaign that stole a little more than $500,000. A senior accounting specialist working for the city of Ocala received a fraudulent email from a scammer posing as an accounting specialist from Ausley Construction. The email requested Ausley's banking information to be changed. On October 17, the scammer sent an invoice requesting payment for the service related to the construction of a new terminal at the Ocala International Airport. The payment was made the next day to a fraudulent bank account of the scammer.

On October 22, the scam came to light after Ausley Construction informed the city of Ocala that it did not receive any payments. Later, it was discovered that the email used by the scammer to send the invoice had a slight difference from the legitimate one ("@ausleyconstruction.com"). The spoofed email had an extra "s" a the end of the legitimate Ausley address (@ausleyconstructions.com).

In late September 2019, a similar scam targeted the Japanese media conglomerate Nikkei. In a report released on October 30, Nikkei America, the U.S. subsidiary of the Japanese company, revealed that an employee transferred $29 million to an account controlled by a perpetrator who posed as a Nikkei America management executive.

The unsuspecting employee thought that he was interacting with an executive who needed $29 million to be wired immediately, but it was the perpetrator who lured him into sending $29 million to an account the perpetrator controlled.

In order to safeguard your organization from such costly BEC attacks, it is crucial to have a Zero Trust approach. This means implementing appropriate security measures that would spot emails that appear to be unusual. This requires both human-centric security measures and technology-centric security measures.

The FBI's BEC defense recommendations

To safeguard your organization from the evolving threat of BEC scams, the FBI has recommended the following security measures.

1. Cautious use of social media

The success of a BEC scam is directly proportional to how credible the trap appears to the intended target. With the wealth of publicly available information on social media about C-suite executives, the perpetrator can construct near-perfect fake accounts of C-suite executives that would not arouse suspicion even to the most vigilant employee in your organization.

C-suite executives need to know that seemingly innocuous social media platforms have the potential to act as a treasure trove for attackers to collect sensitive personal information about them. suppliers of information that can be used for BEC scams.

2. Enabling MFA

One common tactic BEC scammers employ is to redirect users to a fake site that looks exactly like their Office 365 login page. This is done to compromise user credentials. Since multi-factor authentication (MFA) adds additional layers of authentication to prove the person trying to sign in is truly who they say they are, it is a brilliant fail-safe mechanism to secure accounts of users whose credentials were compromised.

Although Office 365 has native provisions to implement MFA, IT admins have to toggle between different tabs to select users and configure MFA settings. However, with AD360, IT admins can configure MFA for multiple users from a single window.

IT admins can also configure MFA for users in bulk by uploading a CSV file containing their user principal name, and assign a list of allowed authentication methods, including:

- Receiving a code via text.
- Receiving a code via phone call on a mobile or office number.
- Receiving a notification via an authentication app.
- Viewing a one-time password (OTP) in an authentication app.

3. Be suspicious of requests that evoke a sense of urgency or fear

BEC emails are drafted to create a sense of urgency. For example, the attacker can impersonate a C-suite executive to deceive employees, or partners into sending money or personally identifiable information (PII) such as Social Security numbers, credit card numbers, login credentials, and so on.

These emails can also contain subject lines with keywords traditionally used for fraudulent communications such as secret, transfer, urgent, immediate, attention, payment, and so on. This is why it's crucial to screen all inbound emails.

With AD360's pattern-based content search feature, inbound and outbound emails containing PII can be easily identified. You can also create content search profiles for keywords frequently used in fraudulent emails, and configure alerts to notify you via email when emails matching the search profile are sent or received by your employees.

4. Be vigilant about external emails

The reason BEC scams have been rampant over the years is because of their simplicity. More often than not, hackers don't even try to compromise the credentials of a C-suite executive and use their account to dupe employees. They simply modify the domain in the email address of the executive by a character. These modifications are extremely hard to detect intuitively.

For example, abc@example.com and abc@exarnple.com might appear similar, but the latter has the letter "m" replaced with "rn", in an attempt to trick you; you likely wouldn't notice it unless you were looking for it. These modified domains are called cousin domains. These domains appear to be identical to trusted domains, and are rarely spotted at a glance. Therefore, it's important to keep a close eye on all external emails.

With AD360's mail traffic reports, IT admins can analyze their organization's Office 365 mailbox traffic with vital parameters such as the volume of spam entering and leaving their organization's mailboxes, the number of emails sent and received by each employee during a specified duration, the top spam and malware recipients, and more.

This information helps IT admins effectively identify any malicious anomalies in email activity. You can also schedule these reports to run at fixed intervals, be emailed to administrators, and be exported to multiple formats such as CSV, XLS, PDF, or HTML.

5. Ensure mailbox logons are monitored, logged, and retained for at least 90 days.

Multiple failed logon attempts of a C-suite executive's account or logon attempts from multiple endpoints during non-business hours from an unusual IP or location could indicate that their account is compromised. To detect such anomalous activities promptly and respond with proactive countermeasures, the FBI recommends that mailbox logon activities be monitored, and the activity logs must be retained for a minimum period of at least 90 days.

With AD360, you can keep track of any unusual amount of failed logon attempts using the Recent Logon Failures report. This report provides information on the IP address of the device used to log on, date and time of the failed attempts, and a lot more. You can also keep track of user activities that happen outside designated business hours to ensure that employees aren't carrying out activities with malicious intent.

Unlike Office 365's native provision to store audit logs for 90 days, AD360 lets you store the audit logs for as long as you need

ManageEngine
AD360

AD360 is an integrated identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. From user provisioning, self-service password management, and Active Directory change monitoring, to single sign-on (SSO) for enterprise applications, AD360 helps you perform all your IAM tasks with a simple, easy-to-use interface. With AD360, you can just choose the components you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments from within a single console.

For more information about AD360, please visit www.manageengine.com/ad360.

$ Get Quote Download