FORTRA™

WHITE PAPER (EMAIL PROTECTION)

BEC: Why This Basic Threat Is Difficult to Detect

Business Email Compromise (BEC) is "one of the most financially damaging online crimes" according to the FBI[1]. It is a cunning form of email impersonation that, when combined with human error, can be incredibly disruptive and damaging.

Understanding Email Impersonation

Modern email impersonation attacks exploit the identity of trusted colleagues and brands. There are a variety of ways identity-based email attacks work and each varies in the tactics and techniques used. Understanding these differences is critical in defending against these attacks effectively without disrupting legitimate email communications. To decipher BEC from other email impersonations, here are two additional ways cybercriminals attack.

Customer Phishing: Cybercriminals use brand impersonation techniques, such as domain spoofing and malicious content including phishing URLs, to evade security controls and trick their victims. Also, keeping content generic while launching scattershot attacks allows cybercriminals to reach as many recipients as possible.

Account Takeover (ATO)-Based Email Attacks: Cybercriminals use a multi-step process that initially compromises a previously established, credible email account to launch subsequent targeted attacks such as BEC, spear phishing, or ransomware. ATO-based email attacks exploit the existing trust between the compromised account and its known contacts, which increases the cybercriminal's success rate.

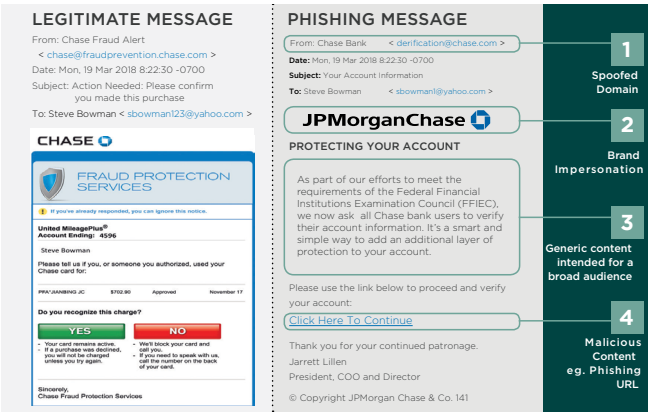

Figure 1: A comparison of a legitimate message and a possible phishing message.

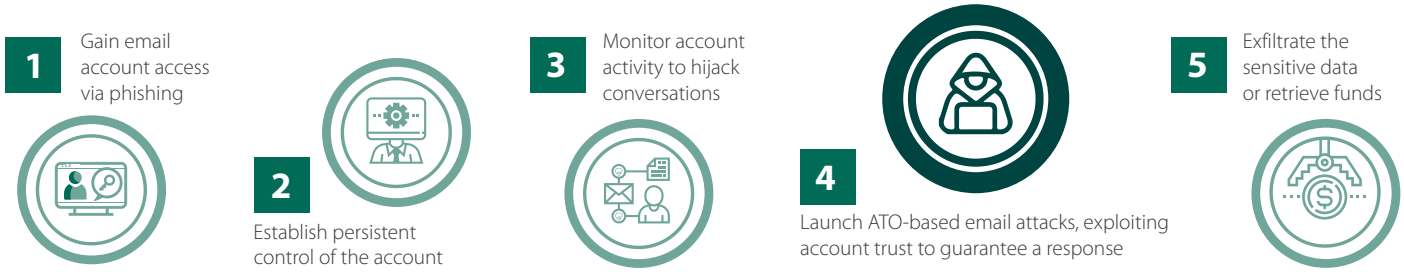

Figure 2: The phases of an account takeover.

Why BEC Is a Formidable Threat

BEC uses social engineering to masquerade as executives, colleagues, and third-party vendors – tricking victims into believing they're interacting with a trusted sender. Unlike email threats that incorporate malicious attachments or links, BEC relies purely on sender impersonation and social engineering to deceive recipients. With no malicious code or links, BEC can more easily bypass traditional email security solutions. A successful BEC attack can lead to the illegitimate transfer of funds, data breaches, or other harmful actions against victims and their organizations.

Stages of the Attack

There are various ways BEC attacks can be deployed, but the phases of the attack are similar.

Research: Cybercriminals research their targets by **reviewing information** found on the web and social media and may also take advantage of sensitive data available through previous breaches. They **study relationships** within the targeted organizations and with their third parties (such as vendors). The purpose of this is to find relationships that can be exploited via email impersonation and social engineering.

Preparation: The cybercriminals then **define their target lists, craft their messages**, and **set up infrastructures** that may be necessary to impersonate the legitimate senders. This could include establishing email accounts and lookalike domains to facilitate the social engineering ploy used in the BEC attacks. It also includes setting up financial accounts or other assets in order to monetize successful attacks.

Execution and Deception: Cybercriminals launch BEC campaigns, **sending emails** to the targeted lists. The emails lack known indicators and often use spoofed or lookalike domains. The cybercriminal will also **impersonate** people of authority (CEO, CFO, etc.) to bolster the importance of the request.

Action: Believing they are interacting with a trusted individual, the unsuspecting recipient proceeds with the request, leading to **financial loss** or **data breaches**. Some of these can include wire transfers or gift card scams.

Just How Effective Is BEC?

From afar, BEC attacks may look obvious and easy to avoid, but these attacks can be cultivated and methodical. In late 2022, Fortra™ reported that 97% of email threats involve email impersonation. So, it's no surprise that BEC was the third-highest response-based threat in volume. The report also found that 21% of reported emails were either malicious or considered do not engage. This is the highest percentage of malicious and do not engage emails recorded in nine quarters.[2]

As long as cybercriminals continue to find success with fraudulent emails such as BEC, security teams should anticipate these threats will persist. In fact, Cybersource reported in their 2022 Global Fraud and Payments Report[3] that eCommerce revenue lost to payment fraud increased in every major global region from 2021 to 2022. In the same report, phishing remained the most utilized vessel for fraud attacks globally.

Why Is BEC So Difficult to Combat?

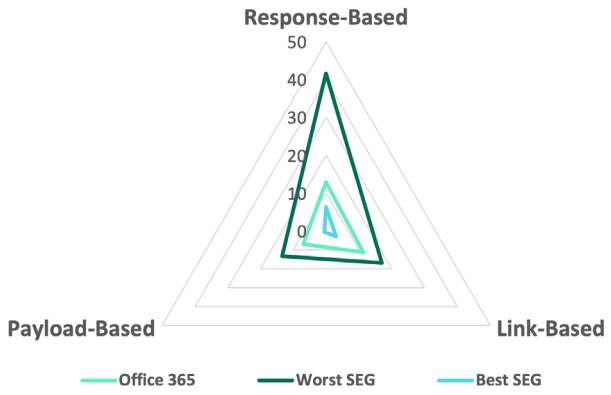

Figure 3: Fortra research shows impersonation techniques evaded SEGs most often requiring users to report them.

Email impersonation attacks, such as BEC, are particularly successful in bypassing security controls because:

1. They lack threat indicators such as payloads, blacklisted URLs, etc., that would normally be flagged by traditional security controls.
2. Targeted social engineering content can be convincing to users and renders signature-based detection ineffective
3. Cybercriminals abuse legitimate mail services to avoid blocklists and ensure deliverability.
4. Spoofed or lookalike domains aid deliverability and make these attacks more difficult to detect.

What Does This Mean for Your Organization?

Cybersecurity teams cannot depend on traditional signature-based email security controls to detect BEC. While there are no perfect remedies, many organizations have implemented additional layers of email security to minimize the risk posed by BEC. These solutions take advantage of machine learning innovations, stronger authentication mechanisms, threat intelligence, and automated threat response to prevent, detect, and respond to BEC and other advanced email threats. In our next article, we take a closer look at these solutions and how they better protect organizations from BEC attacks.

Solve your BEC worries with confidence.

READ ARTICLE

Sources

[1] "How We Can Help You" – Scams And Safety. FBI.
https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise

[2] Fortra's Suspicious Email Analysis

[3] Global Fraud and Payments Report 2022. CyberSource.
https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2022.pdf

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.