egress

CISO STRATEGY GUIDE

Business email compromise

How to detect and neutralize BEC in Microsoft 365

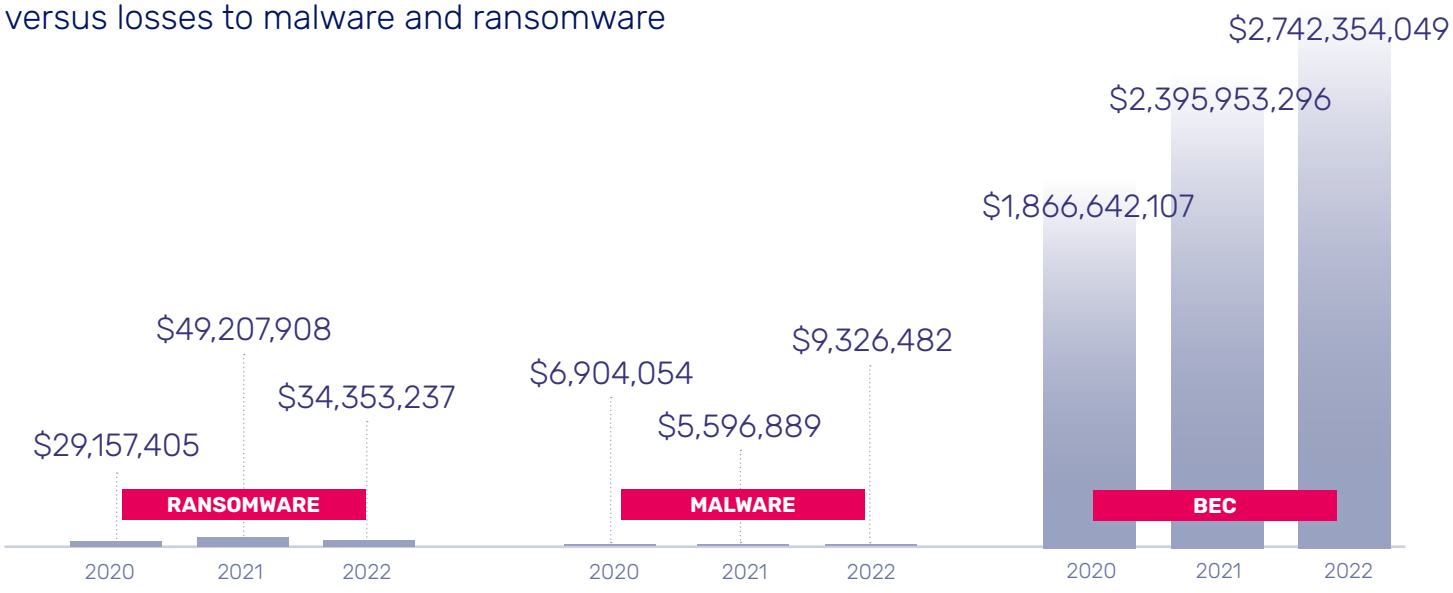
Business email compromise: a multi-billion dollar problem

Business email compromise (BEC) is one of the most prevalent and financially damaging forms of cybercrime. The number of successful attacks continues to rise year on year, and for 2022, the FBI's Internet Crime Complaint Center (IC3) reported adjusted losses of over $2.7bn from the incidents it investigated, making BEC the second costliest form of cybercrime and marking a 47% increase in lost funds since 2020.[1]

The goal of a BEC attack is to defraud an organization or individual, most frequently through the transfer of funds or payment of gift cards. A form of advanced phishing, BEC attacks are highly targeted and utilize impersonation and other social engineering tactics to manipulate victims. While cybercriminals continue to use display name and domain spoofing, increasingly BEC attacks are sent from compromised supply chain accounts.

As they do not normally contain a malicious payload (URL or malware attachment) and can be sent from compromised trusted accounts, BEC attacks have a high success rate for bypassing technologies that rely on signature-based and reputation-based detection, such as Microsoft 365 native controls and secure email gateways (SEGs). Once in the inbox, these attacks can easily trick their victims due to their highly targeted nature and social engineering techniques. Only by using intelligent cloud email security that combines advanced detection capabilities, behavior-based security, and real-time teachable moments can organizations change this narrative.

Last three-year BEC complaint loss comparison versus losses to malware and ransomware



Year-on-year adjusted annual losses reported to IC3

1 Data taken from the Federal Bureau of Investigation Internet Crime Report 2022

How a BEC attack plays out

BEC attacks have two repeated characteristics: they appear to come from a trusted source and they result in financial losses for the victim. However, cybercriminals carry out multiple steps as part of a successful BEC attack.

1. Reconnaissance

Convincing impersonation attempts require research into their targets. Open-source intelligence (OSINT) provides cybercriminals with insights into factors such as organizational structure and reporting lines, new employees, and even customer-supplier relationships.

2. Weaponization

The cybercriminal designs their attack, leveraging insights gained during reconnaissance combined with any other 'useful' information, such as trending news stories. During this phase, the cybercriminal may use scouting attacks and other tactics (e.g. vishing) to test the organization's defenses and the victim's responses, or to groom the victim prior to the attack.

3. Delivery

The BEC attack is sent to the victim, bypasses existing defenses and tricks the victim into believing they are interacting with a legitimate contact.

4. Transfer of funds

The victim carries out the intended action, for example a wire transfer into a bank account controlled by the cybercriminal.

Prevalent methods for defrauding victims

Invoice fraud

Wire transfer

Gift card purchase

Updated bank details

Cryptocurrency exchanges or payments

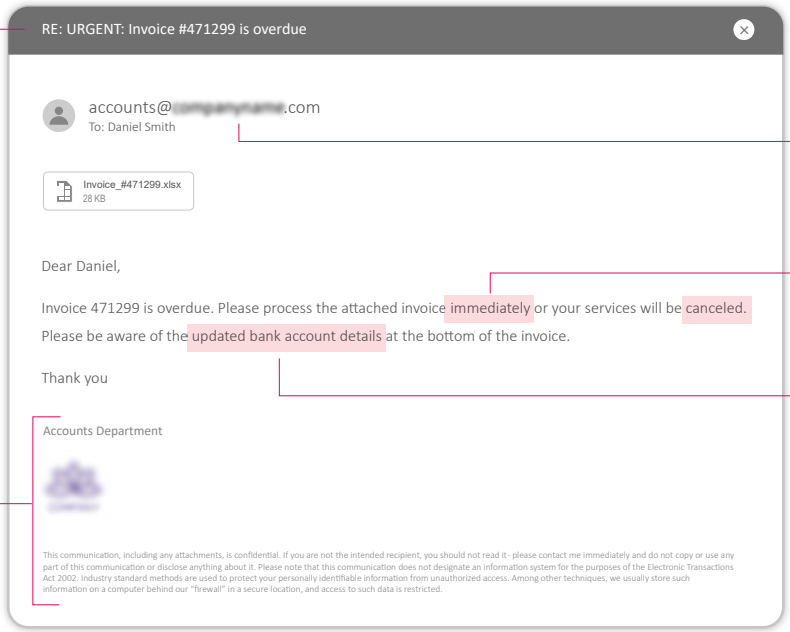
Anatomy of a BEC attack

In addition to a financial subject matter and aim of defrauding their victims, BEC attacks include several repeated characteristics.

While some might be opportunistic, the most realistic and therefore effective BEC attacks are highly tailored and leverage impersonation tactics. During reconnaissance, the cybercriminal will develop an understanding of their target's supplier ecosystem, intending to 'hide' their new payment request among the routine admin of the relationship. Domain spoofing, lookalike domains, and display name spoofing are common technical measures used by cybercriminals to impersonate suppliers. Increasingly, cybercriminals are taking over accounts of a supplier organization before launching an attack on their intended target.

Additionally, BEC attacks include social engineering tactics to psychologically manipulate their target. By creating a sense of urgency and increasing the pressure on the victim, the cybercriminal intends to move them into Type 1 thinking, a state where they are prone to acting quickly and irrationally, without questioning their actions or seeking outside counsel to validate their choices.

The below is a redrawing (for anonymity purposes) of a BEC attack sent from a compromised Accounts Payable email address and detected by Egress Defend. In the actual attack, more than 6,000 emails were sent within a 48-hour window after the original account takeover (ATO) attack, bypassing Microsoft 365 native security and SEGs in the recipient organizations.



The limitations of traditional technology and training to detect BEC attacks

The threat of BEC continues to grow as organizations struggle to effectively detect the attacks targeting them using traditional technology and training approaches. Several factors can ensure high delivery and success rates for attacks.

The limitations of signature-based and reputation-based detection

Signature-based and reputation-based detection is used as part of Microsoft's native security controls and in SEG detection. As BEC attacks aim to defraud an organization, they do not usually contain a malware attachment or phishing hyperlink payload – meaning there is nothing for these technologies to detect. Instead, BEC attacks rely on the text within the email body and file attachments that contain fraudulent invoices and alternative payment details but appear 'benign' on inspection due to the lack of malware.

Where hyperlinks are used (for example, to link to payment pages), cybercriminals can dynamically create new links that are not yet recognized by definitions libraries or use legitimate but compromised websites that don't have a bad reputation at the time of email delivery.

If a spoofed domain has been used to send the attack, dedicated cybercriminals can take steps to ensure it passes basic email hygiene checks, including SPF, DKIM, and DMARC. Alternatively, using a compromised email account from a legitimate supplier can ensure delivery.

No spike in inbound email volumes

As BEC attacks are usually highly targeted, they do not rely on a "mass mail" approach. Instead, an entire attack can play out across one or two emails, meaning there's no spike in inbound mail flow to detect.

Social engineering results in high success rate

The power of a BEC attack lies in its ability to deceive its victim. Advanced attacks are highly targeted and well-crafted, appearing like legitimate, everyday requests that should not arouse suspicions.

While organizations have delivered training to end users and may implement policies to reduce their exposure, it is unrealistic to assume employees will detect every attack or will follow every process.

Strategic CISO: AI-driven and behavior-based security that detects BEC attacks

Organizations need a new approach to detecting and neutralizing BEC attacks. In the 2023 Market Guide for Email Security, Gartner® makes two recommendations:

"Supplement the native capabilities of your existing cloud email solutions with third-party security solutions, to provide phishing protection for collaboration tools and to address… BEC-type phishing scenarios."

"Use email security solutions that include anti-phishing technology for targeted BEC protection that use AI to detect communication patterns and conversation-style anomalies, as well as computer vision for inspecting suspect URLs. Select products that can provide strong supply chain and AI-driven contact chain analysis for deeper inspection and can detect socially engineered, impersonated, or BEC attacks."

Categorized as integrated cloud email security (ICES) solutions, AI-driven anti-phishing technology enables organizations to detect the attacks that get through signature-based and reputation-based email security and layer their defenses in Microsoft 365 for robust protection.

Models such as natural language processing (NLP) and natural language understanding (NLU) are used to detect the linguistic anomalies present in social engineering attacks, including BEC, that deviate from expected behavior. These detection capabilities are not reliant on a payload to be present, but instead analyze the email body and attachments. Time-of-click analysis and link rewriting for any hyperlinks present can further reduce an organizations' exposure to post-delivery weaponization.

Additionally, ICES solutions can be used to support an organizations' zero-trust posture. By analyzing the content of every inbound email, regardless of sender domain reputation or established relationships, these solutions can detect highly effective impersonation attacks, including those sent from compromised supply chain accounts.

This approach is the only way for organizations to tackle the multi-billion dollar problem of BEC.

Bring integrated cloud email security to your organization with Egress Defend

Learn how Egress Defend uses AI to detect BEC.

Request demo See how

About Egress

Egress makes digital communication safer for everyone. As advanced and persistent cybersecurity threats continue to evolve, we recognize that people get hacked, make mistakes, and break the rules. Egress's Intelligent Cloud Email Security suite uses patented self-learning technology to detect sophisticated inbound and outbound threats that protect against data loss, resulting in the reduction of human activated risk. Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.

www.egress.com