Abnormal

CISO Guide to Business Email Compromise

How to Stop the $2.9 Billion Problem

The Rising Threat of Business Email Compromise

Business email compromise (BEC) is one of the most significant cybersecurity threats to enterprise organizations, with $2.9 billion lost in 2023 alone. This type of email attack occurs when a cybercriminal uses social engineering to impersonate a trusted contact—typically an executive or colleague—in an effort to steal money or valuable information. Because these emails rarely contain obvious indicators of compromise, such as malicious links or attachments, they are difficult for legacy security solutions to detect. This leaves employees—notoriously the weakest link in the cybersecurity chain—as the last line of defense.

Of the more than $12.3 billion in losses reported to the FBI Internet Crime Complaint Center (IC3) in 2023, nearly 25% were directly attributable to BEC. The $2.9 billion figure represents a 7% increase over 2022's already staggering $2.7 billion—and a total of $14.3 billion since the IC3 began including the attack in its report in 2015. Since its initial inclusion in the IC3 report, when only $264 million in losses were reported, business email compromise has skyrocketed more than 1000%.

Unfortunately, secure email gateways and other traditional security measures are unable to protect against these novel, never-before-seen attacks. Once they arrive in inboxes, your employees open and respond to them, putting your organization at risk of financial and reputational damage. Without a new approach, BEC will only continue to grow, and organizations worldwide will continue to suffer the consequences.

Business email compromise has caused

$14.3B

in total losses since 2015.

FBI IC3

Abnormal

© 2024 Abnormal Security Corporation. All rights reserved.

Types of BEC Attacks

BEC attacks can take on many forms, but they all rely on trusted relationships to complete their schemes. Here are a few ways attackers leverage social engineering to steal money and data from organizations.

Wire Transfer Requests

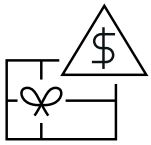
An attacker typically impersonates a well-known executive within the organization, oftentimes the CEO or CFO, and requests that an important wire transfer be completed immediately. The urgency of these requests often means that employees do not check the legitimacy of the email and complete the request—sending thousands of dollars to an account owned by the attacker.

Invoice Fraud

The target receives a fraudulent invoice from a known vendor in which the attacker changes the bank details to an account in their control. In some cases, this occurs when a vendor account has been compromised, but it can also be done through display name deception in hopes that the victim will not examine the email too closely.

Payroll Diversion

In these emails, the attacker impersonates someone at your company and emails a finance or HR employee to ask them to switch their payroll information to an account owned by the attacker. Oftentimes, the person being impersonated does not even realize that their payroll has been diverted until their paycheck does not appear in their account at the end of the month.



Gift Card Requests

Especially prevalent around the holidays, these attacks are similar to wire transfer requests but threat actors instead ask employees to buy gift cards for an employee or customer appreciation event. After making the purchase, the attacker asks the victim to send the gift card numbers to them.

It's worth noting that business email compromise attacks can take many forms and often do. These attacks can be part of larger credential phishing or account takeover schemes and can have dire consequences for both employees and their organizations.

Abnormal

© 2024 Abnormal Security Corporation. All rights reserved.

Impact of BEC Attacks

The most recent FBI IC3 report revealed that there were 21,489 victims of business email compromise attacks in 2023, costing organizations an average of more than $137,000 per attack. It's important to note that this number only includes successful attacks where victims are conned into sending money, which means the true impact of BEC could be considerably larger.

According to research from Abnormal Security, BEC attack volume increased by 108% between 2022 and 2023. While most employees may be able to spot a BEC attack and react appropriately—for example, by verifying with the requester via an alternative method before completing the fraudulent request—this isn't always the case.

108%

Increase in BEC attack volume between 2022 and 2023

28%

Median open rate for text-based BEC attacks

15%

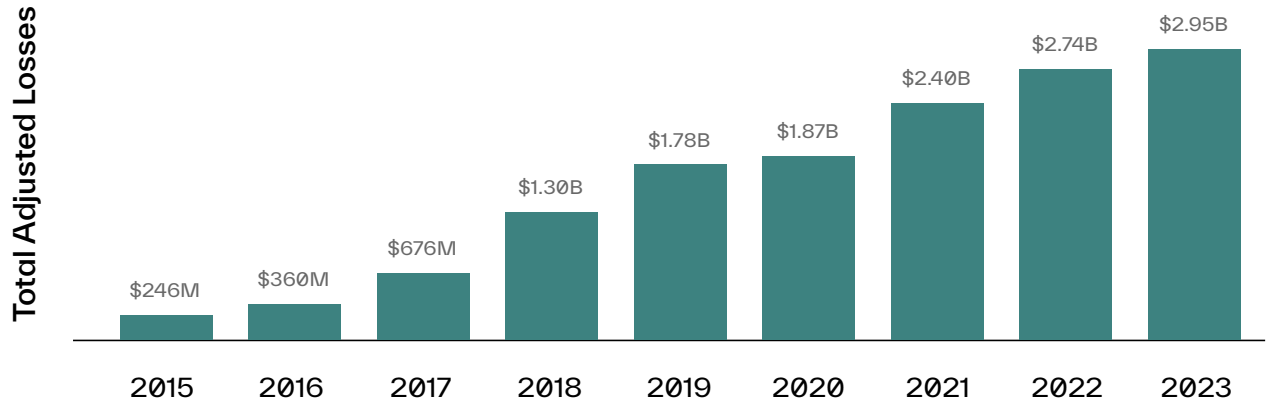
Percentage of BEC attacks that are read and replied to

Abnormal found that the median open rate for text-based business email compromise attacks is nearly 28%. And of the malicious emails that were read, an average of 15% were replied to. Unfortunately, it only takes one successful BEC attack to lose millions.

Even if employees are trained on how to detect an attack and respond appropriately, cybercriminals constantly revise their schemes. Threat actors are committed to staying ahead of changes in technology and training—and their efforts are often successful.

Losses from BEC Attacks Continue to Grow

2023 FBI IC3
Mar 2024



Abnormal

© 2024 Abnormal Security Corporation. All rights reserved.

Why BEC Attacks Are Successful

To stop business email compromise, there must be a fundamentally different approach to the problem. The standard approach of implementing a secure email gateway no longer works, particularly because of the way BEC attacks are conducted.

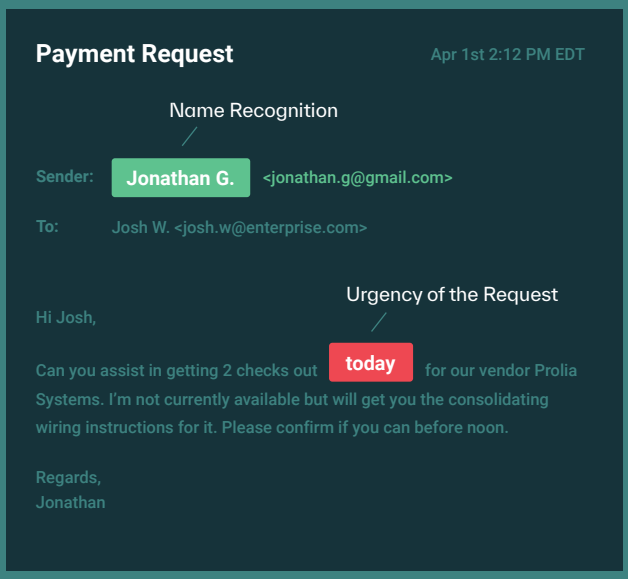
Secure email gateways (SEGs) flag emails based on known indicators of compromise. Since BEC attacks are text-based and generally lack malicious URLs or suspicious attachments, they bypass SEGs to land in user inboxes.

Threat actors leverage social engineering to trick employees, usually impersonating a trusted colleague or executive. These impersonation attacks slip by traditional email security layers since they look inconspicuous on the surface.

If you look at a real-world example of an attack that bypassed the SEG, you can see why traditional defenses fail.

When these attacks land in inboxes, they rely on name recognition and urgency of the request. By encouraging their victims to move quickly, they successfully trick people into making mistakes. And based on the number of successful attacks, more people fall for it each year—despite an increase in security awareness training. Because BEC attacks typically contain no traditional indicators of attack, it's only by understanding the context and intent that we can determine if an email is malicious.

There is little denying that these attacks are incredibly difficult to detect, by both traditional defenses and humans. As BEC grows in severity, it's increasingly obvious that these attacks must be stopped before they can trick your employees.



Suspicious Domain?

No. This email is using Gmail—a legitimate domain that millions of people use every day.

Malicious Links?

No. This is a purely text-based email with no links.

Corrupt Attachments?

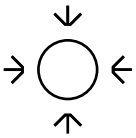
No. This email doesn't have any attachments to scan.

Abnormal

© 2024 Abnormal Security Corporation. All rights reserved.

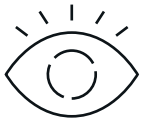
How to Stop BEC Attacks

To counter these highly sophisticated attacks, large enterprise organizations need the right security platform. The next generation of email security includes:



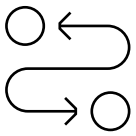
API Architecture

A solution that connects to Microsoft 365 and Google Workspace via an API and in doing so, provides access to the signals and data needed to detect suspicious activity. This includes unusual geolocations, dangerous IP addresses, changes in mail filter rules, unusual device logins, and more.



Behavioral Data Science Approach

The solution should use a fundamentally different approach that leverages behavioral data science to profile and baseline good behavior and detect anomalies. It should use identity modeling, behavioral and relationship graphs, and deep content analysis to identify and stop emails that include suspicious information or requests.



Organizational Insights

The solution should understand both formal and informal organizational hierarchies. It should map internal as well as cross-organizational relationships to understand typical communication patterns and behavior, and then detect, log, and remediate all email threats.

Without each of these capabilities, BEC will continue to outpace security measures—making it even more difficult to prevent these attacks from reaching employees, creating financial loss, and causing reputational damage.

© 2024 Abnormal Security Corporation. All rights reserved.

Conclusion

With each new development in the attack landscape, it becomes increasingly evident that legacy systems like secure email gateways (SEGs) are ill-equipped to prevent advanced threats from reaching employee inboxes. And any time an employee has to assess whether or not an email is safe is an opportunity for them to make a mistake. Unfortunately, the data shows that employees are notoriously bad at distinguishing malicious messages from legitimate ones.

While security awareness training can help reduce the risk of employees engaging with a threat actor, it's even better to minimize the number of attacks they receive in the first place. Thus, the most effective way to protect your workforce is to invest in a modern email security solution that proactively blocks attacks.

Unlike a SEG, an API-based security solution uses AI-native detection engines to ingest, analyze, and cross-correlate behavioral signals to spot anomalies in email patterns that indicate a potential attack. It then remediates malicious emails in milliseconds to prevent end-user engagement. Implementing modern email security technology that pairs advanced behavioral science with risk-adaptive detection is the only surefire way to safeguard your organization and keep your employees from making a catastrophic decision.

© 2024 Abnormal Security Corporation. All rights reserved.

Abnormal

Abnormal Security provides the leading behavioral AI-based email security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails and messages—all while providing visibility into configuration drifts across your environment. You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly, with additional protection available for Slack, Teams, and Zoom.

Ready to Stop Business Email Compromise?

Request a Demo →

See Your ROI →

© 2024 Abnormal Security Corporation. All rights reserved. v1.2/Apr. 2024