5 Ways to Stop Business Email Compromise from Attacking Your Business

impelix™ in partnership with CHECK POINT™

Executive Summary

- Business Email Compromise (BEC) attacks are some of the most popular and financially damaging attacks in the cyberworld
- Easy to pull off and tough to stop, these attacks are gutting organizations for massive amounts of money
- Without specific and proper protections for BEC, organizations will have a difficult time defending against these attacks
- There are ways to prevent BEC attacks from entering your ecosystem

Introduction

Business Email Compromise attacks are the hottest trend from cyber attackers.

These seemingly simple attacks are doing major damage. In 2021, according to the FBI, Americans lost $2.4 billion to BEC attacks. That's up from $1.8 billion in 2020.

The Internet Crime Complaint Center (IC3) found 847,376 complaints about losses, a 7% increase from 2020. Of that, BEC attacks accounted for 19,954 of the complaints.

In fact, BEC ranks ahead of ransomware in complaints. The IC3 received 3,729 ransomware complaints, resulting in a $49.2 million loss.

Gartner found that BECs increased by nearly 100% in 2019 and through 2023, predicts that BEC attacks will continue to double each year, at a cost of over $5 billion to its victims. It affects organizations of all sizes, in all industries, and it victimizes executives and regular employees alike. BEC has fooled Google and Facebook for $100 Million and a small church in Ohio for $1.8 Million. Sequoia Capital was breached via a BEC. It's hard to avoid these days.

What, exactly, is a BEC attack and why has it taken over the entire cyber world?Avanan research, 8.14% of phishing emails ended up in the user's inbox due to an Allow or Block list misconfiguration. When using an SEG like Mimecast, that number rises to 15.4%.

It's a simple attack. The basic ones start with someone compromising or spoofing a high-level executive. The "executive" asks an underling for an urgent favor. The email is the first step. Usually, the executive will ask the recipient to send over their cell phone or WhatsApp number. The scammer uses this technique as a way to establish authority and encourage cooperation; they usually will never call the recipient. From there, the "executive" will ask for the recipient to buy gift cards, or send them over other financial or personal information.

There are also higher-level attacks, whereby the recipient has to send over wire transfer instructions. These attacks can be used to send personally identifiable information, fake invoices and more.

Further, this is more of a long-term game; a rapport will be developed before the ask is made. Spoofed emails can be incredibly difficult to detect. This attack works because it tends to be casual and personable, no different than any other email a user would receive. But it has real effects. The hacker can gain access to an account, request credentials or protected information from an organization, or use it to infiltrate other accounts.

While these attacks seem like they would be noticeable and easy to detect, they actually aren't.

They rely on a few key strategies. For one, they are fairly simple to execute. Though they require some research on the part of the hacker–i.e., finding the name of the executive to spoof–they are easy to send. There is no malware or malicious URL that would be stopped by traditional security scanners.

Further, when a lower-level employee sees an executive emailing them, especially with urgent language, they are likely to engage and follow up, even if it may seem odd.

These attacks will continue as long as they are successful. And they will continue to cause major organizational damage.

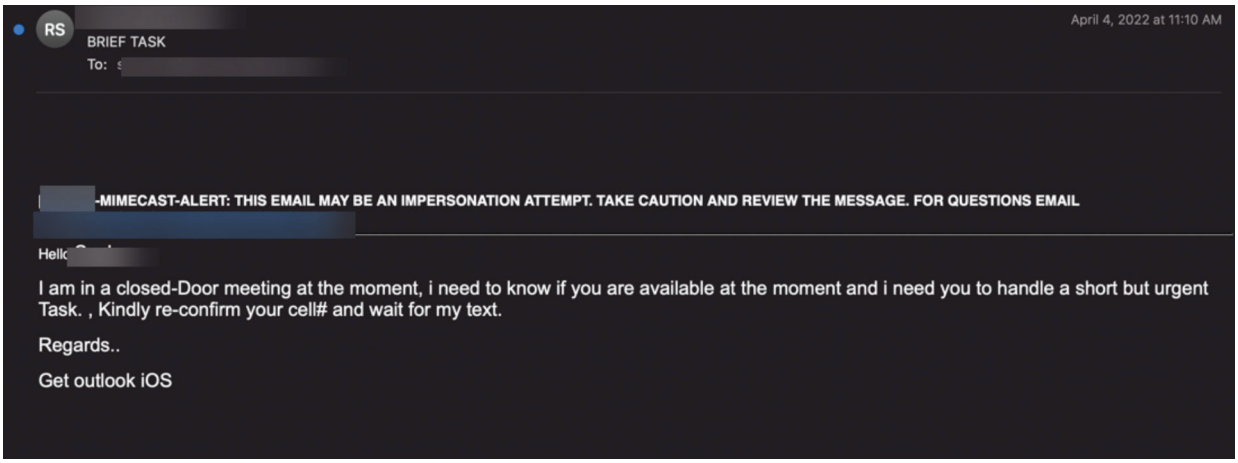
Though they are difficult to stop for default security, there are ways to control the BEC problem.

In this whitepaper, we'll go over what a few typical BEC attacks look like, and offer 5 actionable strategies that you can implement that will drastically reduce your risk.

The Attacks

BEC attacks tend to look similar, but there are some differences. In general, though, they follow a similar playbook, which has an executive being spoofed or outright compromised. From there, they will ask for something urgent. That urgency is where the end-user gets caught. After all, it's difficult to say no to an urgent task from an executive.

Here's what they look like in the wild:



The CEO's name in this company was spoofed, as the sender address is different.

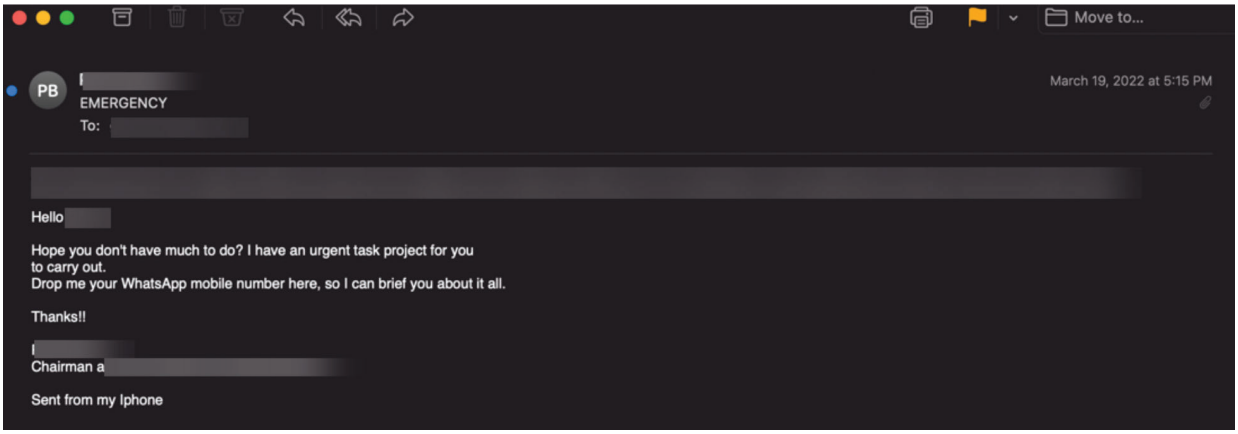
You'll notice the subject line–BRIEF TASK. It's a subject that would gain notice from any employee.

The ask is simple: The CEO needs something from you–a chance to be the hero! Once you respond with your cell, they will begin texting you, likely asking for gift cards.

Why gift cards? Physical cards, however, or at least the photo of the code, can be sold for fifty cents on the dollar on the dark web.Gift card BEC scams are actually quite popular. The Internet Crime Complaint Center tracked a 1,240% increase in 2018 of these types of attacks. And at the beginning of the COVID-19 pandemic, scammers were asking victims to buy gift cards to help purchase PPE.

You'll notice the banner at the top. This email was from a company that runs Avanan behind Mimecast. Mimecast did not stop this email; instead, they injected a warning banner at the top. (Avanan confidently stopped this at phish.) Though that banner may cause pause for some, it might not be enough. Further, even if the end-user follows basic cybersecurity hygiene and checks the sender address, there still can be reason for doubt. Maybe the CEO is using their personal email address?

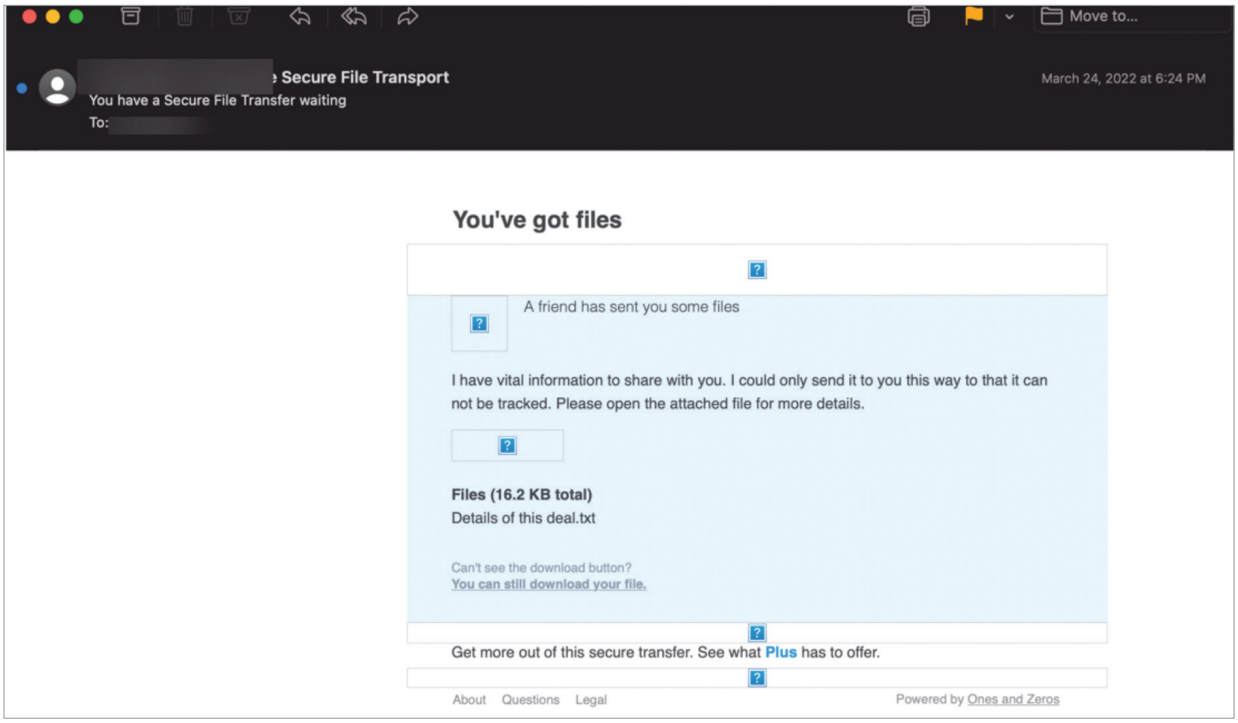
You'll see another variant of this attack below.



The idea is the same, except the scammer asks for a WhatsApp number. WhatsApp is also one of the more impersonated brands in the world. The scammer could also take your WhatsApp number and use it for future attacks.

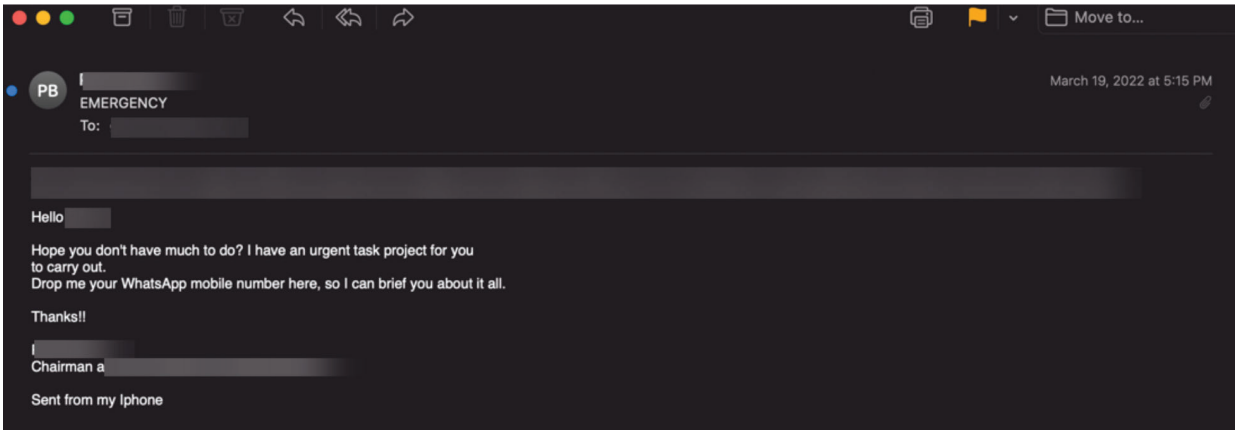
In this next section, we'll see a few higher-level BEC attacks.

This one below isn't just plain text, but it still follows the same general template. Someone says they are sharing "vital information" so important that it needed to be sent in a way that couldn't be "tracked." This is a different take on the BEC, as it attaches a .txt file. But the idea is the same.



Finally, here's an attack that represents a potential evolution of BEC attacks. In this email, the "CFO" asks for a few reports, including one of all "outstanding invoices."

That is a potentially dangerous request. All outstanding invoices can add up to a lot of money.



What all these attacks have in common is a sense of urgency. Yet since there is nothing inherently malicious about the email, security solutions have a tough time stopping these and identifying them properly. That's part of the reason they are so successful–they are tough to stop.

In this next section, we'll discuss the five things that are necessary to prevent BEC attacks from infiltrating and infecting your organization.

5 Ways to Stop BEC Attacks

1 INTERNAL CONTEXT

The most important part of stopping BEC attacks is internal context. What does this mean? It means that the security solution has an understanding of the context of conversational relationships within an organization. If a solution monitors only inbound email, when they see an email from the 'CEO' to the 'CFO', it will be the very first time it has seen such a conversation. For an email solution that is deployed inside the cloud email server, it will see thousands of similar real, internal conversations. From there, the solution can understand if this is a typical conversation or not. Within hours of the first deployment, Avanan's AI scans a year's worth of email conversations to build a reputation network, the type of internal context that alerts the AI to something suspicious. That gives Avanan an idea of what's normal and what's not.

Avanan also scans and quarantines internal email and files in real-time, protecting against east-west attacks and insider threats.

2 LOCAL AI

For AI to work effectively, it needs to be trained on the best data set. For email security, it must be embedded within the cloud suite via API. Once embedded, the data set of cloud email security solutions is much richer. By being embedded, Avanan understands who the people being emailed are, the social graph, internal email, geo-suspicious login events, and more. Beyond that, as an inline security solution, Avanan's security layers run after Microsoft and Google's default security filters. That means Avanan's AI is trained on the specific attacks not caught by Google or Microsoft. In our model, we're constantly training and tuning our AI on the specific tenant. We have separate training sets for Office 365 and Google and separate models based on the direction of mail (inbound, outbound, internal). We use best-in-class AI algorithms and put our own inputs into them. By applying custom threat profiles for each organization, we can better tune our AI and keep phishing out. Instead of applying a one-size-fits-all approach, Avanan trains its AI on the specific tenant.

Both Microsoft and Google have the internal access required to prevent BEC attacks and many of their anti-spoofing tools do a good job at blocking basic attacks but their infrastructure cannot perform the per-customer contextual analysis required for most BEC attacks. They work with far too many companies and customers to properly monitor all internal accounts and understand an organization's relationship and reputation patterns.

3 ACCOUNT TAKEOVER PROTECTION

With BEC, sometimes the executive is spoofed and the sender address is different than the actual one. But other times, the account can be fully taken over. In that case, full-throttled account takeover protection is needed. With our anomalies engine, we can determine whenever there is a foreign login. We can notify admins or send notifications to SIEMs/orchestration systems to disable an account until an MFA and/or password reset is made. Beyond that, our event analysis algorithm identifies behavior that can be a sign of account takeover. We do a historical scan that monitors over 100 event indicators and correlates them to identify previously compromised accounts. Among the many things we monitor:

- New logins from new devices, locations or browser
- Suspicious mailbox configurations
- Disabling of multi-factor authentication
- Multiple password resets in short periods of time

By coordinating these indicators, we can understand when an account might be in the process of being taken over, and block it accordingly.

4 FULL-SUITE SECURITY

When Avanan published an attack brief in early 2022 about hackers posting malicious chats in Microsoft Teams, one threat researcher dubbed it as the new business email compromise. Why? Because the same principles for BEC apply to chat applications. In fact, the FBI report on BECs notes that there's been an increase in using such apps for these schemes. As they write: "They do so by compromising an employer or financial director's email, such as a CEO or CFO, which would then be used to request employees to participate in virtual meeting platforms. In those meetings, the fraudster would insert a still picture of the CEO with no audio, or a "deep fake" audio through which fraudsters, acting as business executives, would then claim their audio/video was not working properly. The fraudsters would then use the virtual meeting platforms to directly instruct employees to initiate wire transfers or use the executives' compromised email to provide wiring instructions."

If someone is duped into sharing a spreadsheet over Teams with sensitive info (e.g., credit card numbers, SSNs, etc.), we would stop that traffic. Further, the Teams and Slack anomaly engine monitors all Teams logins and events for suspicious activity.

If you don't have security for all your apps, hackers will eventually ply their wares where they won't be stopped.

5 FULL INTEGRATION WITH AZURE ACTIVE DIRECTORY/GOOGLE DIRECTORY

Avanan automatically integrates with Azure Active Directory or Google Active Directory. Typically, IT admins have to manually update the active directory integration whenever there are job changes, employee turnover and more.

Avanan automatically integrates, constantly updating employee names, email and job titles. Because of its complete AI integration, Avanan knows your employees by name—even nickname–and role, so that it can identify when messages are attempting to impersonate someone real.

Avanan also uses the hundreds of thousands of data points it collects to undergo impersonation analysis, scanning the sender and message content for impersonation. The algorithm looks for user impersonation, and whether a single sender exists in the organization with a different address. Avanan can do that by cross-referencing several fields, such as sender and signature.

Conclusion

BECs are the most popular and damaging cyberattack in the game right now. These are fairly easy to pull off and even easier to fall for.

As Gartner has noted:

> "...due to the rise in business email compromises, account takeovers and other sophisticated attacks, many times some malicious emails are actually missed by MSDO, and in fact by any other email gateway solutions. Therefore, organizations should strongly consider integrating third-party solutions to strengthen their email security capabilities."

With some easy-to-implement policies, such as internal context, strong AI, full-suite security, account takeover protection and automatic active directory integration, these attacks don't have to cause your business harm.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com