CLOUDFLARE
AREA 1 SECURITY

WHITEPAPER

How to Stop Business Email Compromise Threats

Advanced techniques for fighting financial phishing fraud

Overview

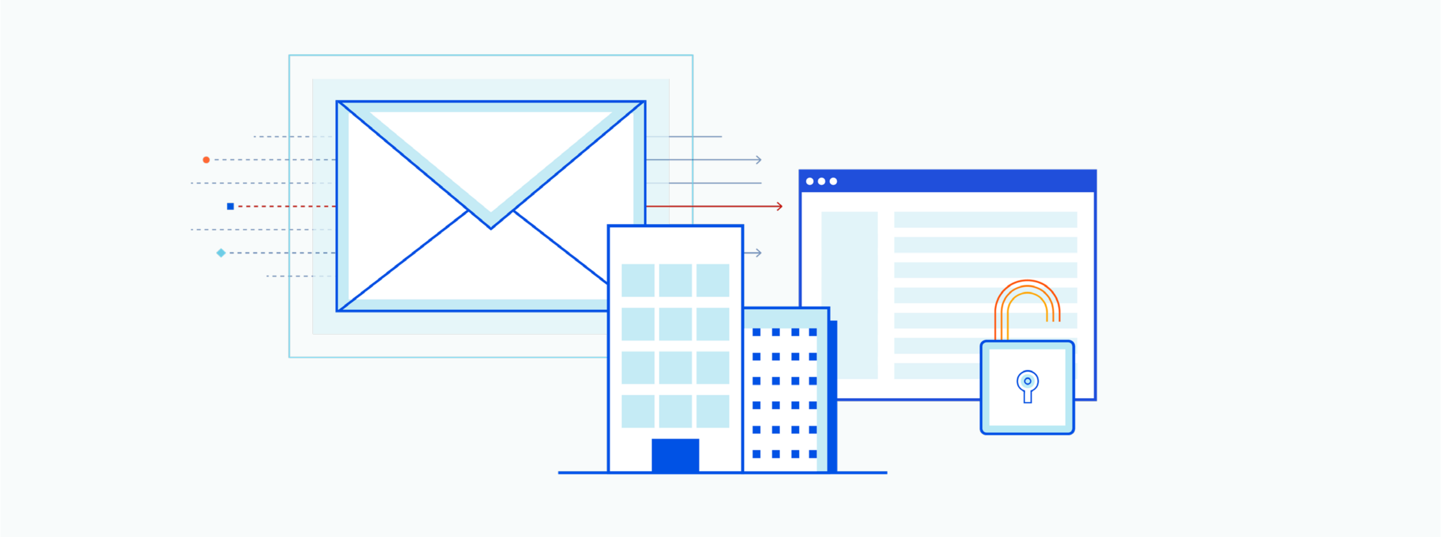
Exploiting an existing relationship between a victim and organization, Business Email Compromise (BEC) attacks are a specific form of financially motivated phishing attacks. In our third annual update on the state and evolution of BECs, we find that BECs have remained the most costly cyber attack, resulting in millions in damages, and surpassing reported costs from ransomware attacks.

By now, BEC has become a fairly well-recognized term in many industries so we will omit a detailed breakdown of BEC types in this report. (For those who are interested, we've previously broken down the various BEC types in our previous ebook, "BEC in 2021: Supply Chain-Based Phishing Attacks on the Rise.") Law enforcement has also made progress in bringing BEC actors to justice. Recently, several perpetrators of international BEC rings have been apprehended, including participants in a $10 million laundering operation and SilverTerrier, a large Nigerian cybercrime gang that's amassed over 800,000 stolen passwords from 50,000 targets.

Yet despite the many years they have been in the public purview, these phishing attacks, ranging from the absurdly simplistic to well-researched "long cons," BECs continue to evade security systems and reach victims.

Why? Much of this is due to the still constantly evolving nature of BECs and threat actor techniques. We've previously reported on attackers abusing COVID-19 vaccine availability and other timely events as lures. The relative ease, low cost to execute and profitability is also attractive for cyber gangs, including nation-state hacking groups looking to "broaden their horizons."

For more about the current state of BEC attacks and how to effectively stop them, read on.



BEC – just as (if not more) impactful as ransomware

While staggering ransomware demands tend to hog the headlines, BEC is one of the most financially damaging cybercrimes according to the FBI, resulting in more than $2 billion in reported losses.

Yet organizations tend to underestimate the severity of BEC attacks. This is due in part to most companies failing to report BEC incidents. Additionally, unlike ransomware, where the attack is very obvious, some organizations may not even know they were a victim of BEC fraud until a later audit or third-party reporting. After all, BEC money transfers are typically approved by a legitimate employee!

Despite the under reporting, according to the 2021 Verizon Data Breach Investigations Report2, BEC attacks compromised the second most common form of social engineering attack, with 95% of financial losses falling between $250 and $984,000 per incident.

Our own data from the 2021 Email Threat Report showed that the average BEC request was $1.5 million. The median was $260,000.

While BECs make up just 1.3% of attacks, the fact that they are easily missed by many traditional security tools can mean steep financial consequences. In 2021, Area 1 Security (acquired by Cloudflare) identified and stopped nearly five million (4,987,526) BEC attacks — many of which were missed by legacy secure email gateways and cloud email suites.

Average BEC request intercepted by Area 1 = $1.5 Million

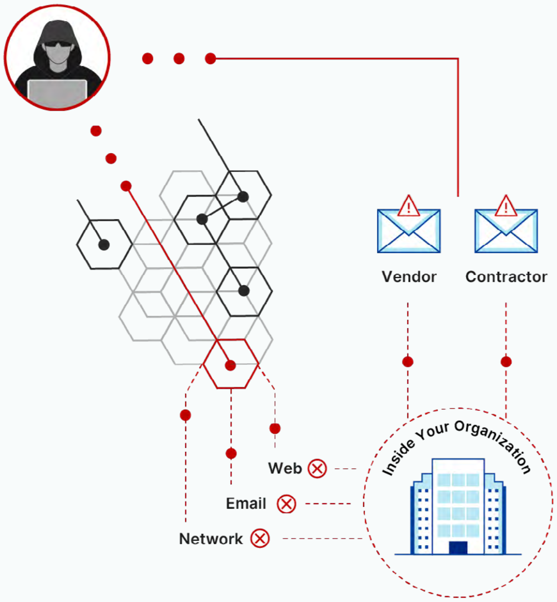
In 2021, Area 1 identified and stopped nearly 5 million BEC attacks

[1] https://www.ic3.gov/Media/Y2020/PSA200406
[2] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

BEC “Worst Hits”

Here are some of the most [in]famous BEC attacks hitting major brands and costing millions in damages.

Victim	Loss	Year	What happened
Facebook and Google	$123 Million	2019	A Lithuanian scammer impersonated Quanta Computer, an electronics supplier for Facebook and Google. Facebook and Google paid $123 million in fake invoices to the scammer.
Crelan Bank	$75.8 Million	2016	Belgian-based Crelan Bank lost over €70 million (roughly $75.8 million) to fraudsters who compromised the CEO’s email account. The attack was later discovered in an internal audit.
Toyota Subsidiary	$37 Million	2019	A European subsidiary of the Toyota Boshoku Corporation (subsidiary of the Toyota Group) was duped into transferring ¥4 billion (approximately $37 million) in a BEC scam.
Scoular	$17.2 Million	2014	US commodities trading company Scoular wired $17.2 million to a fraudulent offshore account after receiving a fake email from the CEO.
Mattel	$3 Million (recovered)	2016	A financial executive at Mattel transferred $3 million to a fraudulent account after receiving a spoofed email appearing to be from the CEO.



Why are BEC attacks still so successful?

BEC attacks can be notoriously difficult to detect and therefore stop. These attacks rely on authenticity and a deep understanding of the target’s behaviors and business processes. That knowledge extends to compromising the target’s supply chain and partners as well. Other email security solutions, including cloud email providers and secure email gateways, are unable to accurately identify these emails as malicious messages (more on how attackers “Phish with the Cloud” here).

The top four reasons victims fall for BECs

01

BEC uses social engineering instead of malware.

Instead of including malicious links or weaponized attachments, BECs are usually short, text-only messages. They rely on our tendency to follow social etiquette, like lending a hand to a coworker, or power dynamics, like complying with an urgent request from an executive, to trick victims into sending money to fraudulent accounts.

Traditional email security tools that rely on scanning a malicious link or attachment for known signatures will miss BECs.

02

Attackers use legitimate domains.

With cloud-based email providers, it's easy and inexpensive for anyone to get a legitimate email domain. Attackers regularly take advantage of a free or low-cost Gmail domain, for example, to send phishing emails. It's also trivial for an attacker to purchase a legitimate "lookalike" domain similar to their target victim's domain.

By using legitimate and/or newly created domains, phishing emails can pass email authentication checks. Solutions that rely on domain reputation alone to determine maliciousness can also miss these BECs.

03

BECs are low volume but highly targeted.

Our 2021 Email Threat Report showed that BECs made up only 1.3% of attacks and an even smaller percentage of total email volume. However, BECs are extremely targeted —attackers will research targets and intended recipients to craft messages that appear personal and legitimate.

Security tools that rely on baselining what "normal" benign messages look like, or require a higher volume of threats to create a signature, fail to detect BECs accurately.

04

Victims are usually unaware of account takeovers or compromised credentials

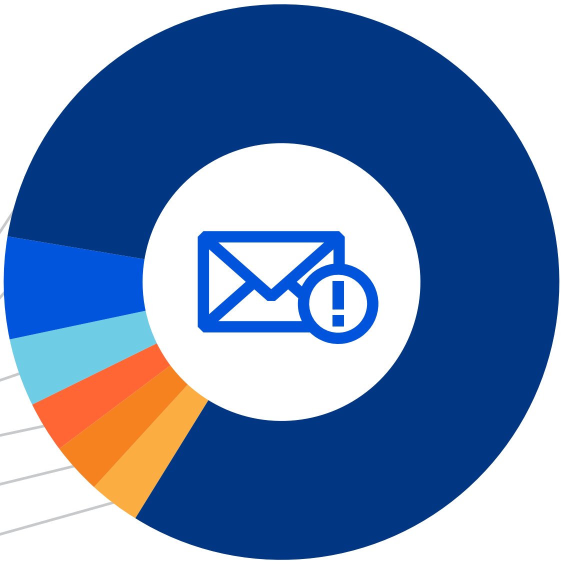
Type 4 (as defined by Gartner's "Protecting Against Business Email Compromise Phishing" report), the most sophisticated BEC, often leverages account takeovers, where an attacker has hijacked a legitimate user's account. The attacker silently observes ongoing email threads (sometimes for several months), before inserting themselves in the conversation at the critical moment to divert a payment.

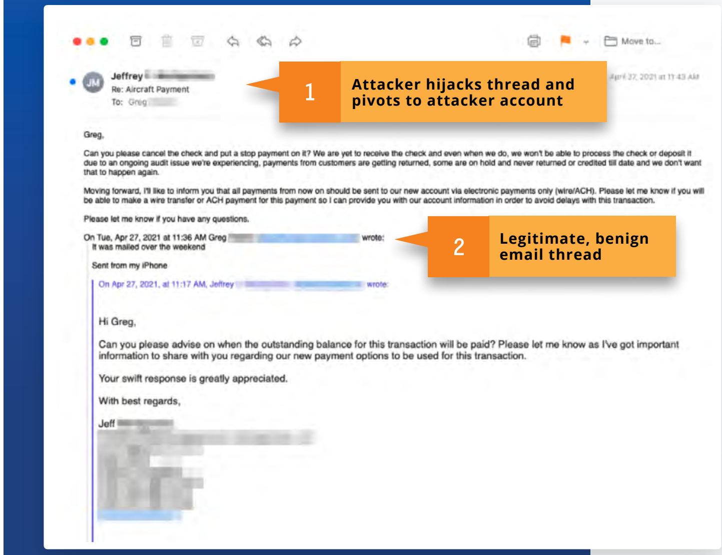
Only advanced detection techniques using contextual analysis can catch these sophisticated compromised vendor attacks.

Top BEC targets

Here are the top industry sectors Area 1 saw being targeted for BEC attacks in 2021.

Repair & Maintenance Services	87.65%
Non-Government Services	3.8%
Soap & Cleaning Compound Manufacturing	2.09%
Other General Manufacturing	1.74%
Retail Trade	1.31%
All Other Industries	




Move to...
1
Attacker hijacks thread and pivots to attacker account
2
Legitimate, benign email thread

Jeffrey [redacted]
Re: Aircraft Payment
To: Greg [redacted]
April 27, 2021 at 11:43 AM

Greg,

Can you please cancel the check and put a stop payment on it? We are yet to receive the check and even when we do, we won't be able to process the check or deposit it due to an ongoing audit issue we're experiencing, payments from customers are getting returned, some are on hold and never returned or credited till date and we don't want that to happen again.

Moving forward, I'll like to inform you that all payments from now on should be sent to our new account via electronic payments only (wire/ACH). Please let me know if you will be able to make a wire transfer or ACH payment for this payment so I can provide you with our account information in order to avoid delays with this transaction.

Please let me know if you have any questions.

On Tue, Apr 27, 2021 at 11:36 AM Greg [redacted] wrote:

> It was mailed over the weekend
>
> Sent from my iPhone
>
> > On Apr 27, 2021, at 11:17 AM, Jeffrey [redacted] wrote:
> >
> > Hi Greg,
> >
> > Can you please advise on when the outstanding balance for this transaction will be paid? Please let me know as I've got important information to share with you regarding our new payment options to be used for this transaction.
> >
> > Your swift response is greatly appreciated.
> >
> > With best regards,
> >
> > Jeff [redacted]
> >
> > [redacted]

What does a sophisticated type 4 BEC look like?

$4+ million BEC fraud attempt

This attack uses a partner account-takeover to hijack a legitimate, benign conversation thread before pivoting the conversation to the attacker's account.

The attacker compromises a partner's account ("Jeffrey"), then hijacks the thread. Sending from a malicious look-alike domain, the attacker pivots the thread to the attacker's account. The look-alike sender domain is identical to the benign sender domain but ends in .co instead of .com.

This attack checks all four of the "BEC success factors" discussed previously.

Four techniques to stop BEC attacks

While some BECs can be spotted by careful recipients, most sophisticated BEC attacks – the ones that can result in substantial financial loss – typically require trained professionals and advanced phishing detection solutions. Small variations in details matter, especially in BECs that involve partner account takeovers as the attacker has the correct "login" and privileges already.

01

Sentiment analysis

Looking at message content isn't enough. Accurate BEC detection requires looking into the intent of the message. Message tone, relationship(s) between the sender and recipient(s) and any relationship hierarchy also needs to be considered.

02

Active fraud verdict escalations

In sophisticated Type 4 BECs, most of the messages within a conversation are benign. The only attacker briefly inserts themselves into the thread to divert payment. An effective BEC detection solution must include a way to escalate and notify of potential fraudulent communications happening in real time. Automatically blocking/quarantining/retracting malicious messages and kicking off a review process can prevent funds from being transferred.

03

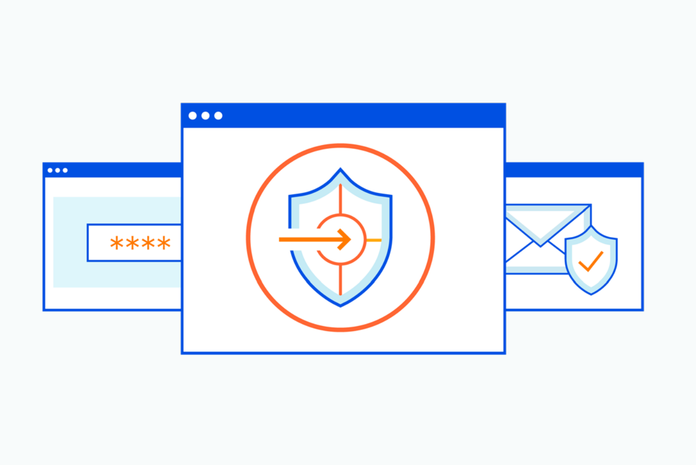
Conversation and thread analysis

Similar to sentiment analysis, conversation and thread analysis looks at intent and relationships within entire conversation threads. Nuances such as variation in message(s) within a thread and length of messages can indicate a sender is not who they appear to be, indicating account takeovers and cases where a conversation has been hijacked by an attacker.

04

Sender trust graphs

Social graphs are important in detecting BEC, especially supply chain based attacks, as it can be used to map risk exposure and trust relationships. This is key in discovering account takeovers and partner impersonations where the sender is a "trusted" individual outside of your own organization. Advanced BEC detection techniques also analyze partner social graphs and sending history.



Extending Zero Trust principles to email

As organizations look to adopt new security principles and network architectures like Zero Trust, email is a critical gap. In this ebook, we have seen how attackers steal money and data by "just asking" at the opportune time. BEC attacks don't need sophisticated malware or network intrusion to succeed – they exploit our implicit trust in email communications.

With Area 1 as part of Cloudflare Zero Trust, customers will get comprehensive Zero Trust that's inclusive of the most used and most attacked SaaS application today – email.

Here is how Area 1 helps extend Zero Trust principles to email:

Assume breach

Area 1 correctly assumes that phishing campaigns are always being set up. With massive-scale phish indexing, Area 1 scans the Internet to hunt for attacker infrastructure and proactively block phishing attacks days before they hit the inbox.

Never trust

Email is an open gate that compromises even the most ironclad Zero Trust network architectures. Area 1 doesn't trust emails just because they have email authentication set up, are from reputable domains, or have a prior communication history with the potential target. In fact, BECs are much more likely to originate from senders and infrastructure that are "trusted" by deterministic security controls.

Always verify

A fundamental tenet of Zero Trust is to continually verify every user and request, even if they are inside the corporate network. Area 1 enacts multiple protection layers before, during, and after emails reach the inbox. All types of communication (external, internal, from trusted partners) are analyzed with similar diligence. Users are protected from deferred attack campaigns – where benign links are pivoted to attacker-controlled infrastructure after they reach the inbox – by Area 1's integration with Cloudflare Remote Browser Isolation.

Understand (and share) email threat context

Email is different from every other SaaS application because of the vast array of "fuzzy" signals it generates, including email content, tone and sentiment, unexpected variations in email threads, and sender-recipient relationships. Area 1 uses sophisticated contextual analysis to parse and weigh all these signals to identify highly targeted attacks in progress – protecting users on the most used (and most different) SaaS application.

Moreover, cross-sharing of threat intelligence generated by Area 1 with the 1T+ daily DNS requests observed on the Cloudflare network will better protect customers from all Internet threats.

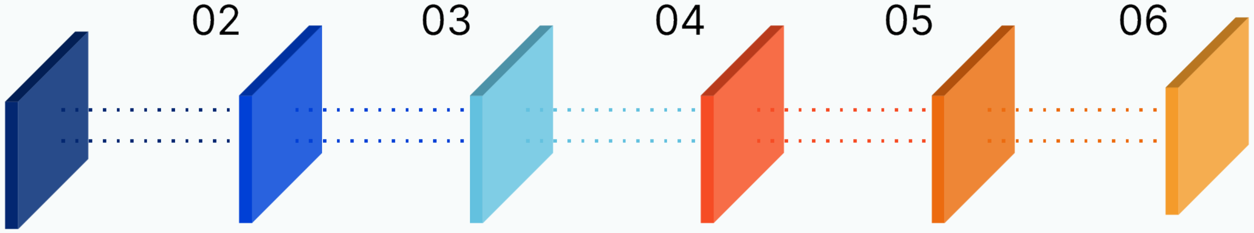
What’s next?

Business Email Compromise can cost a single organization millions in direct losses. Difficult for traditional email security tools to identify, BEC is most effectively stopped by email security solutions using advanced detection techniques.

Area 1 has always been focused on stopping phishing attacks – the single largest cyber threat vector – including BEC attacks. Our cloud-native email security platform uses sophisticated contextual analysis to detect all types of BEC attacks before they cause damage.

Advanced techniques to detect and stop BECs

We use various proprietary technologies to detect a comprehensive range of advanced attacks, including BECs. Our cloud-scale solution integrates with and supports organizations of all sizes.



01

Structural Analysis

Headers
Body, Images,
Computer Vision
Links, Payloads

02

NLU Modeling
(Natural Language Understanding)

Writing Patterns
Categories
Expressions

03

Sentiment Analysis

Intent, Tone,
Relationship,
Hierarchy

04

Thread Analysis

Conversations
Variations
Length

05

Industry Modeling

Verticals
Lingua Franca
Business Processes

06

Trust Graphs

Partner Social Graphs,
Sending History,
ATO Discovery
Partner
Impersonations

To see how we detect and stop sophisticated BEC attacks, please request a demo.

CLOUDFLARE®
AREA 1 SECURITY