



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 who'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 billion¹ 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 our [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 identified and stopped **nearly 5 million** (4,987,526) BEC attacks — many of which were missed by legacy secure email gateways and cloud email suites.



THE AVERAGE BEC REQUEST WAS
\$1.5 MILLION

IN 2021, AREA 1 SECURITY
IDENTIFIED AND STOPPED NEARLY
**5 MILLION BEC
ATTACKS**

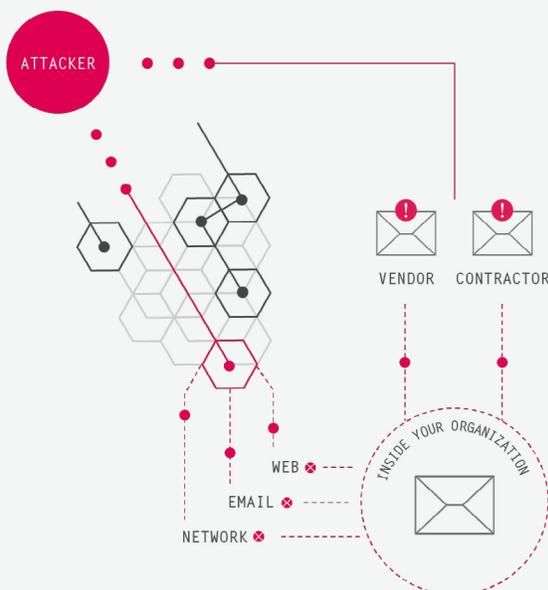
¹ <https://www.ic3.gov/Media/Y2020/PSA200406>

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 <u>impersonated</u> 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 <u>attack</u> 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 <u>duped</u> into transferring ¥4 billion (approximately \$37 million) in a BEC scam.
Scoular	\$17.2 Million	2014	US commodities trading company Scoular <u>wired</u> \$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 <u>transferred</u> \$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 4 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

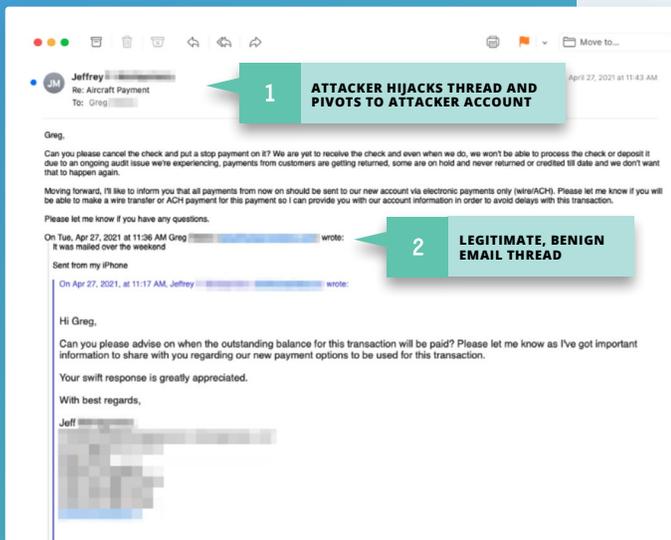
Here are the top industry sectors Area 1 saw being targeted for BEC attacks in 2021.

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		



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.

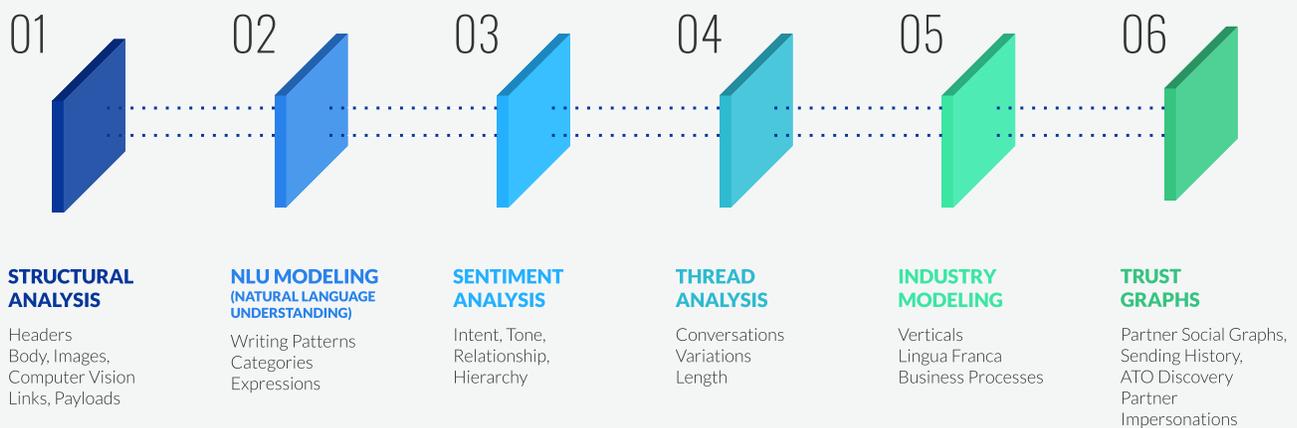
What's Next?

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

Area 1 Security has always been focused on stopping phishing attacks – the single largest cyber threat vector – including BEC attacks. Our cloud-native platform uses sophisticated contextual analysis to detect all types of BEC attacks, as well as other targeted threats such as ransomware.

ADVANCED TECHNIQUES USED TO DETECT AND STOP BECs

Area 1 uses various proprietary technologies to detect a comprehensive range of advanced attacks, including BECs. Our cloud-scale platform integrates with and supports organizations of all sizes.



To see how we detect and stop sophisticated BEC attacks, please [request a demo](#).