Abnormal Security

Abnormal Quarterly BEC Report Q2 2020

Executive Summary

The second Abnormal Security Quarterly BEC Report examines the business email compromise (BEC) threat landscape during what may be the most tumultuous quarter in modern business history: the first full quarter of the COVID-19 pandemic. After the shock of the initial shutdown passed near the end of Q1, businesses and their employees in Q2 navigated a new work-from-home landscape amid great business uncertainty.

Unsurprisingly, attackers were ready, willing and able to use the time of confusion to refine and improve strategies for compromising email accounts. COVID-19-themed attacks continued to increase week-over-week, finally peaking in the third and fourth weeks of April. On average, the weekly COVID-19 campaign volume increased 389% from Q1 to Q2, with a remarkably high volume of credential phishing attacks.

Attacks related to the pandemic weren't the only ones on the rise. As we covered in our first report last quarter, attackers have been shifting their focus away from the C-suite and towards vendors and employees in finance departments. This trend continued to play out in Q2, as campaigns leveraging payment and invoice fraud increased in frequency and used COVID-19 as cover.

Brand impersonation is a go-to tactic for attackers, especially for credential phishing and BEC attacks. The impact of COVID-19 was a major influencing factor here as well, as Zoom replaced American Express as the most-impersonated brand in Q2 (Zoom wasn't even in the top 10 in Q1). Rounding out the top five were Amazon, DHL, Intuit and RingCentral.

Since the beginning of the pandemic just a few months ago, we've seen the rapid acceleration of digital transformation trends that many once thought would take a decade to develop. While the threat landscape has shifted rapidly, with cybercriminals effectively adapting strategies and campaigns to target enterprises and their employees, organizations have not been able to respond as quickly with changes to their approach to email security. As the email threat landscape continues to evolve, it will be critical for enterprises to keep pace in the coming weeks and months.

Abnormal Security will continue to examine the evolving BEC threat landscape so that you can prepare and stay ahead of attackers. In the meantime, the following report details what we learned in the second quarter of 2020.

We invite you to share this with your colleagues and reach out to us with any feedback and questions.

Sincerely,

Evan Reiser

CEO and Co-Founder, Abnormal Security

Key Takeaways

01 COVID-19-themed email attacks peaked and plateaued mid-quarter

Mirroring the surge of the initial coronavirus outbreak itself, we observed a significant spike in COVID-19-themed attacks that started in late Q1. Attack volume peaked in the third and fourth week of April before plateauing and returning to mid-March levels. Overall, weekly campaign volume increased 389% from Q1 to Q2. For the first time, we detected a surge in payment and invoice fraud related to the pandemic.

02 BEC attack volume per company is increasing

Q2 2020 saw a surge in BEC attack volume with the number of BEC attacks per company increasing by 11% as hackers took advantage of new work-from-home scenarios.

03 Payment and invoice fraud growth accelerates

The growth in payment and invoice fraud accelerated in Q2, with attacks increasing 112% over Q1 (as compared to a 75% growth rate from Q4 2019 to Q1 2020).

04 Attackers continue shifting from C-suite to vendor and finance targets

The rate of BEC attacks targeting employees in finance departments increased by 50% in Q2, aligning with the continued increase in payment and invoice fraud attacks.

05 The most impersonated brands map to the pandemic-influenced zeitgeist

Zoom supplanted American Express as the number one impersonated brand in email attacks, followed by Amazon and DHL.

Q2 2020 State of BEC

COVID-19 Attacks Peak and Plateau

Weekly COVID-19 Campaign Volume

↑389%

Increase from Q1 to Q2 2020

In our Q1 2020 State of BEC report, we noted that COVID-19-themed attacks exploded in mid-late March, concurrent with when the world truly began to comprehend the pandemic-induced crisis. These attacks were largely tied to the news cycle, utilizing multiple techniques and capitalizing on fear and uncertainty as the world reacted to the virus's initial outbreak progression.

The surge of attacks related to COVID-19 continued In Q2, reaching its peak in the third and fourth week of April, before declining to mid-March levels and then plateauing. On a monthly basis, COVID-19 attacks decreased 70% from April to June. This may indicate that employees have "settled in" to the new normal of remote work. This could also potentially be the result of news-cycle fatigue, as attacks preying on anxiety or connecting with a news event fail to hit the mark.

Covid-19 Related Campaigns Per 1,000 Mailboxes

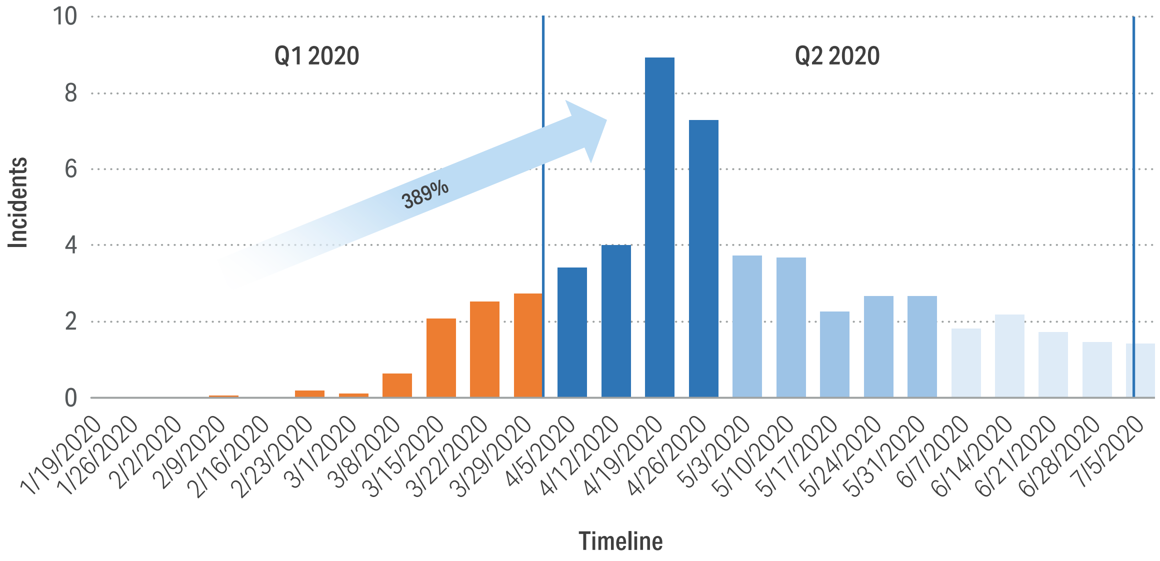


Figure 1: COVID-19 attacks increased 389% from Q1 to Q2.

In Q1, we also noted that spam was the most employed pandemic-related attack technique. This shifted in Q2, however, as we observed a sharp and surprising increase in credential phishing campaigns, overtaking spam at some points. This suggests that attackers are finding a successful footing and strong ROI with credential phishing, which we expect to continue to rise into Q3.

Covid-19 Related Campaigns Per 1,000 Mailboxes By Attack Type

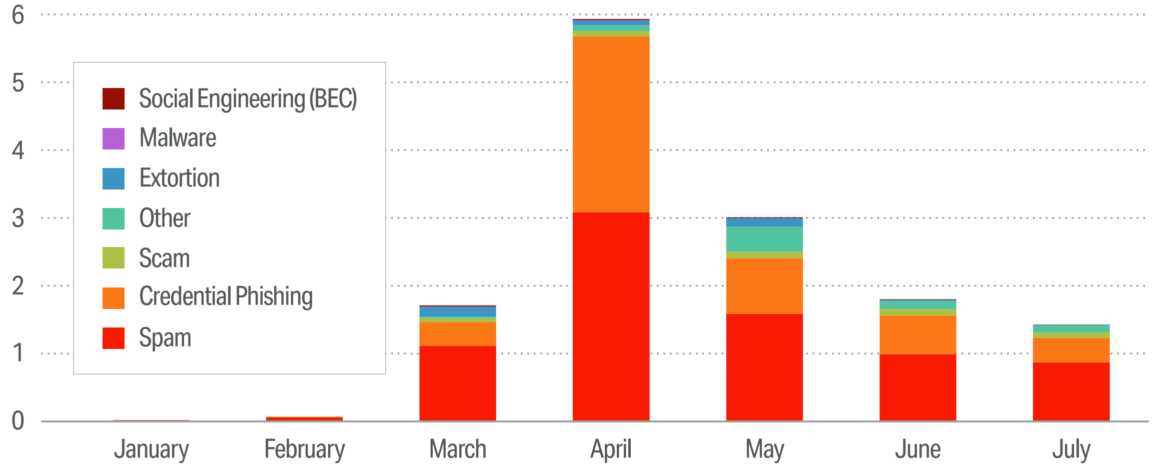


Figure 2: Credential phishing campaigns increased 195% from Q1 to Q2.

COVID-19 related BEC attacks also increased in Q2 — mainly rooted in invoice and payment fraud. These attack campaigns impersonated external parties, such as vendors, and used sympathy tactics that took advantage of slowed business processes to entice recipients to respond. This is part of a growing trend this year, but Q2 was the first time we've observed such attacks tied to the pandemic.

Key Findings

- Weekly attack volume of COVID-19 related attacks increased by 389% from Q1 to Q2
- Attacks related to COVID-19 peaked during the third and fourth weeks of April
- Credential phishing overtook spam as the most-applied COVID-19-related email security attack technique for three weeks during Q2. Overall, COVID-19-themed credential phishing attacks increased 195% from Q1 to Q2, while spam attacks grew 36%
- COVID-19 themed BEC attacks focused on invoice and payment fraud were detected as attackers attempted to gain sympathy – and funds – from employees who were possibly disconnected from typical chains of command and communication

BEC Attack Volume

In Q1, we looked at BEC attack volume, normalized by number of mailboxes. In this analysis and moving forward, we calculate the rate of BEC attacks per company, demonstrating a more robust and accurate picture of the BEC threat landscape. There is no current global measure of BEC attack volumes. Tracking data such as the FBI's IC3 report on BEC only looks at attack complaint volume, so year-over-year increases capture only victim data, not the true volume of these attacks.

In Q2, we observed an 11% increase in the volume of BEC attacks, as compared to Q1. While this number might not seem high, it's significant and somewhat alarming. BEC attacks are highly targeted, less focused on volume and more on sophistication to dupe key targets with the potential to lead to big payouts. As we noted above, the shift to remote work may be partially responsible for the increase, making employees more susceptible to BEC and giving attackers the opportunity to apply tactics likely to be successful given these working conditions.

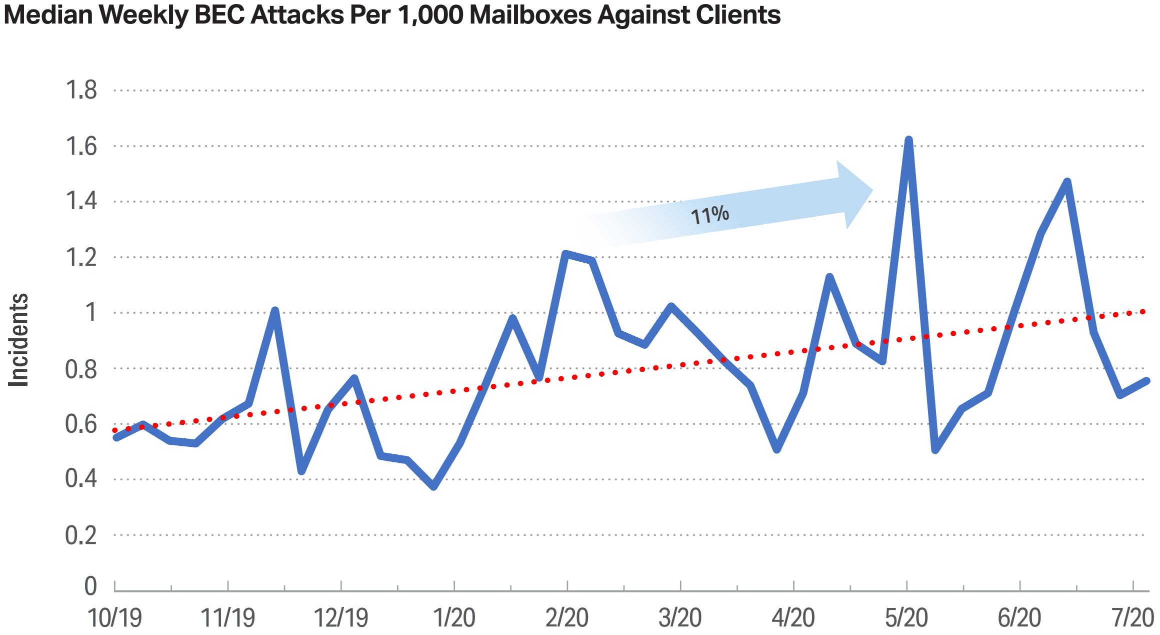


Figure 3: BEC attacks increased 11% in volume from Q1 to Q2.

Key Findings

- The volume of weekly BEC attacks per company trended upward in Q2, growing 11% as compared to Q1
- The rate of BEC attacks targeting employees in finance departments increased by 50% in Q2, aligning with the increase in payment and invoice fraud attacks. This continues a trend identified in Q1 with fewer attacks aimed at C-level employees and attacks aimed at vendors and finance employees.
- The shift to remote work presented an opportunity for BEC attack success, as employees are more susceptible to these sophisticated and highly targeted campaigns.

Payment and Invoice Fraud

In Q1, we examined several different types of BEC attacks – from engagement to gift card and paycheck fraud – and determined that while single recipient attacks decreased year over year, invoice and payment fraud attacks increased more than 75%. In these attacks, attackers hijack existing financial conversations to attempt to execute payment against fraudulent invoices or attempt to update a valid payment with fraudulent bank account details.

Appendix A illustrates an invoice fraud attack.

This trend accelerated, as we saw a substantial increase in Q2 with payment and invoice fraud attacks increasing 112% over Q1, with a spike of more than 60% in the last week of June.

Weekly Percentage of BEC Attacks Involving Invoice or Payment Fraud

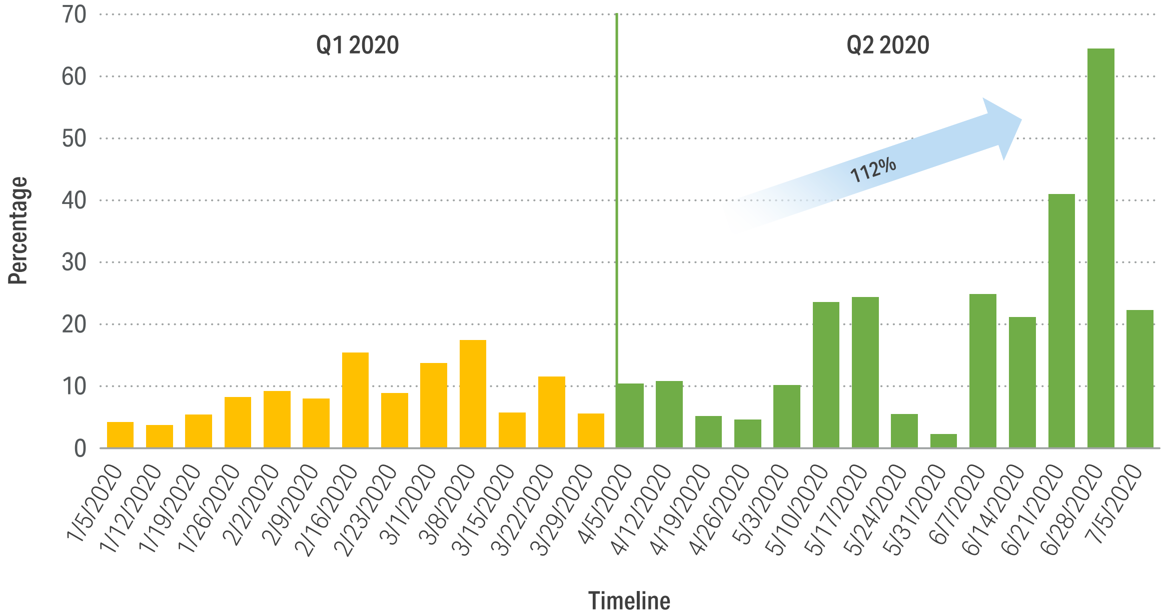


Figure 4: Weekly Percentage of BEC attacks involving invoice or payment fraud increased 112% from Q1 to Q2.

Invoice fraud attacks are largely driven by vendor fraud, where attackers compromise vendors, customers, or anyone involved in the supply chain, to leverage the "trusted" relationship and request or re-direct payments. Amidst COVID-19, businesses are relying on email for communication more than ever, creating a fruitful attack vector for scammers.

Given the significant increase from Q1 to Q2, it's likely that attackers experienced a lot of financial success and will continue investing in these types of attacks.

Key Finding:

- As the number of BEC attacks per company trended upwards in Q2, so did the number of invoice and payment fraud attacks, with an increase of 112% over Q1. This is a reflection of attackers recognizing these types of attacks and supply chain compromise producing the largest financial gain.

Most Targeted Employees

In Q1, we examined which employees were being targeted the most and identified a 37% decrease in attacks on the C-Suite year over year. Consequently, attacks on finance employees increased by 87% in the same period.

Q2 saw this trend continue, with the average weekly BEC attacks against finance roles increasing by 50%. This continued trend can likely be attributed to the significant increase in invoice and payment fraud attacks, which do not typically target the C-Suite. Attacks targeting the C-Suite ticked back up slightly in Q2 but did not return to pre-2020 levels.

Weekly Average BEC Attacks Per 1,000 Mailboxes Targeting C-Suite Executives

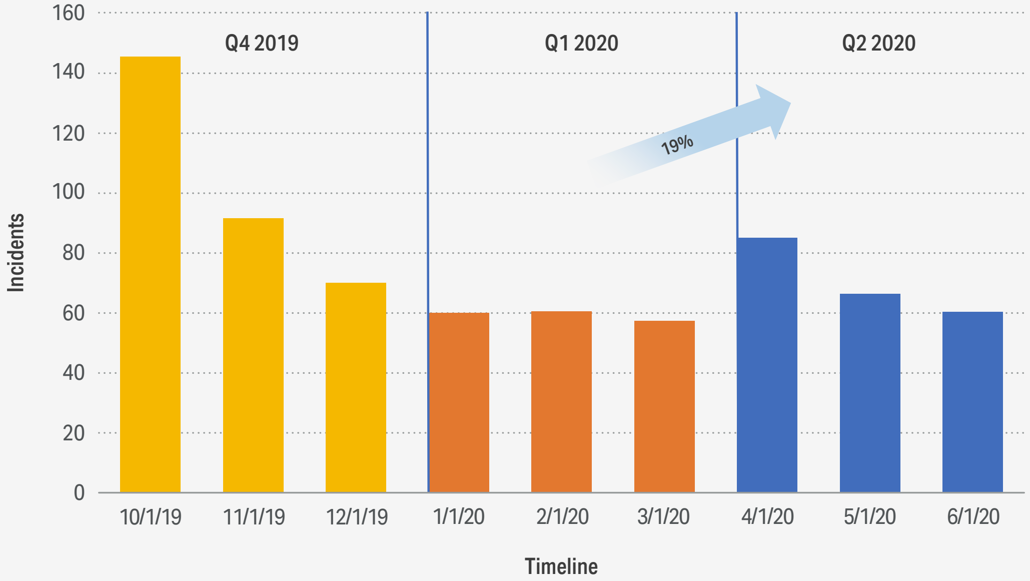


Figure 5: C-suite targeted BEC attacks increased 19% from Q1 to Q2.

Weekly Average BEC Attacks Per 1,000 Mailboxes Targeting Finance Department

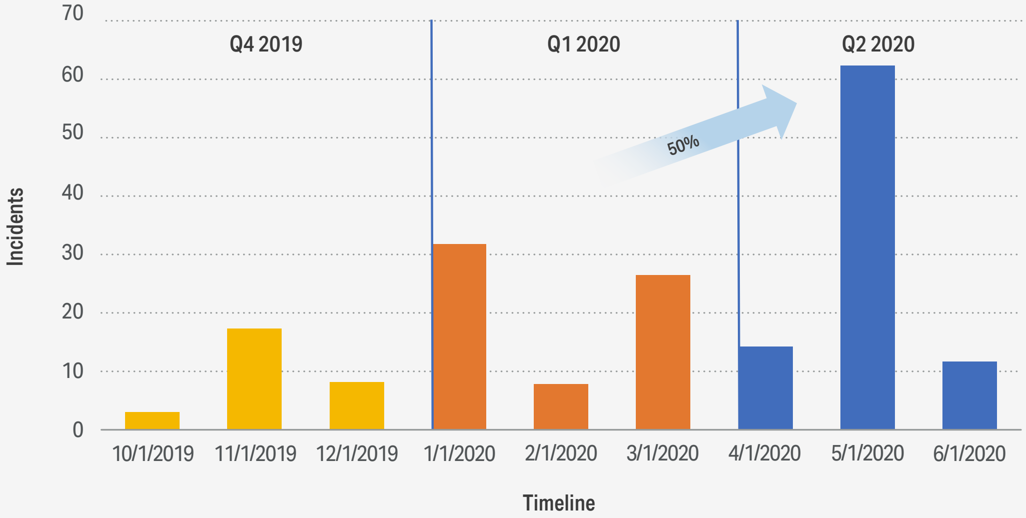


Figure 6: Finance department-targeted BEC attacks increased 50% from Q1 to Q2.

Key Findings

- The rate of BEC attacks targeting employees in finance departments increased by 50% in Q2, aligning with the increase in payment and invoice fraud attacks.
- C-suite-targeted attacks increased 19% from Q1 to Q2.

Q2 2020 Spotlight: Impersonated Brands

Impersonation attacks are a form of fraud where a bad actor assumes the identity of a trusted or known entity. Unlike common phishing attacks, which can feature spelling mistakes and tend to lack specificity, impersonation attacks are highly targeted and well-crafted to appear realistic and authentic. Attackers often research a victim, gathering information from online sources such as social media accounts, and include that information in the text of an email to lend authenticity to the message.

Attackers also leverage the zeitgeist, which drove remarkable shifts in the most impersonated brands in Q2. In particular, Zoom replaced American Express at the top of the list, as scammers took advantage of its instant pandemic-fueled popularity and ubiquity to steal employee credentials and personal information. Example attacks include scammers asking recipients to join a Zoom meeting regarding their supposed termination and impersonating a Zoom notification in order to steal Microsoft account credentials.

Rounding out the top three were two other brands very much associated with COVID-19 shifts toward e-commerce and delivery: Amazon and DHL. Intuit and RingCentral followed closely behind within the top five. By way of comparison, the top 3 most impersonated brands in Q1 2020 were American Express, Amazon and iCloud.

Most Impersonated Brands Q2 2020

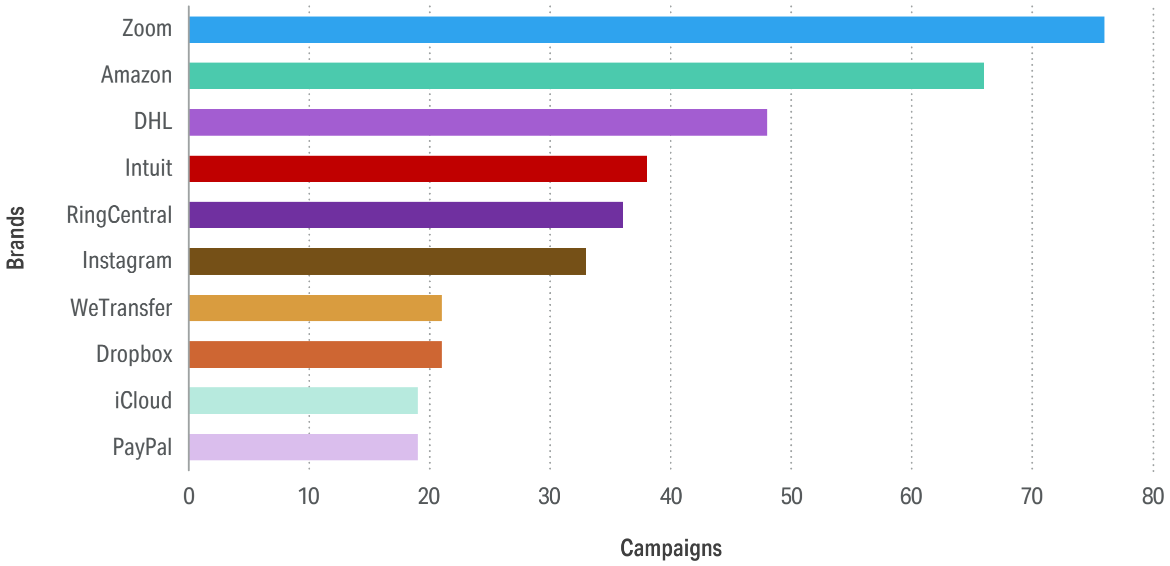


Figure 7: Most impersonated brands in Q2 2020.

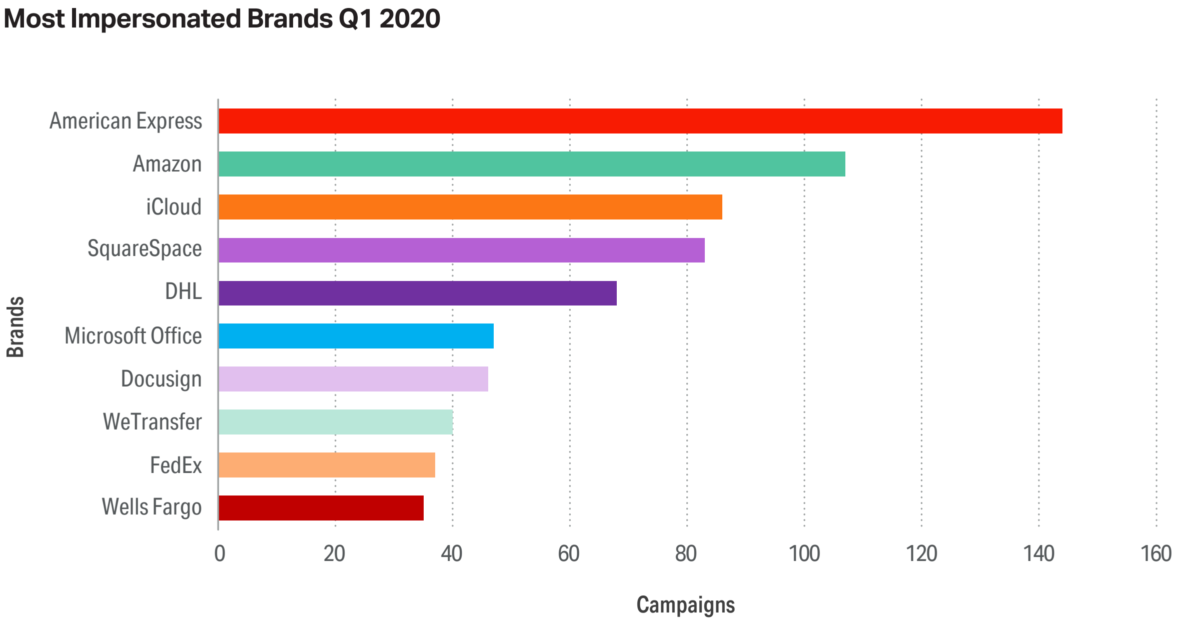


Figure 8: Most impersonated brands in Q1 2020.

COVID-19 fatigue might be setting in, but remote work isn't going anywhere, so attacks will continue to impersonate brands that facilitate remote work and contactless commerce.

IV. Predictions

As we look to Q3, we'll continue to see attackers ready to exploit today's BEC vulnerabilities. Based on Q2 and macroeconomic and geopolitical trends, here are our predictions for the upcoming quarter:

- COVID-19 related attacks will plateau or continue to trend downward with credential phishing accounting for a significant percentage of these attacks
- Upcoming U.S. elections will put a target on state and local election administrators', candidates campaign budgets as well as confidential data
- Supply chain attacks targeting finance departments with invoice fraud will continue to increase as a security threat to organizations
- Work from home will continue through Q3 and as a result collaboration technologies like Zoom will continue to be one of the most impersonated brands
- BEC in general will continue to rise as attackers persistently find success with socially engineered techniques that evade traditional email security defenses

Appendix A: Case Study

Debt Collector Impersonation / Invoice Fraud Attack

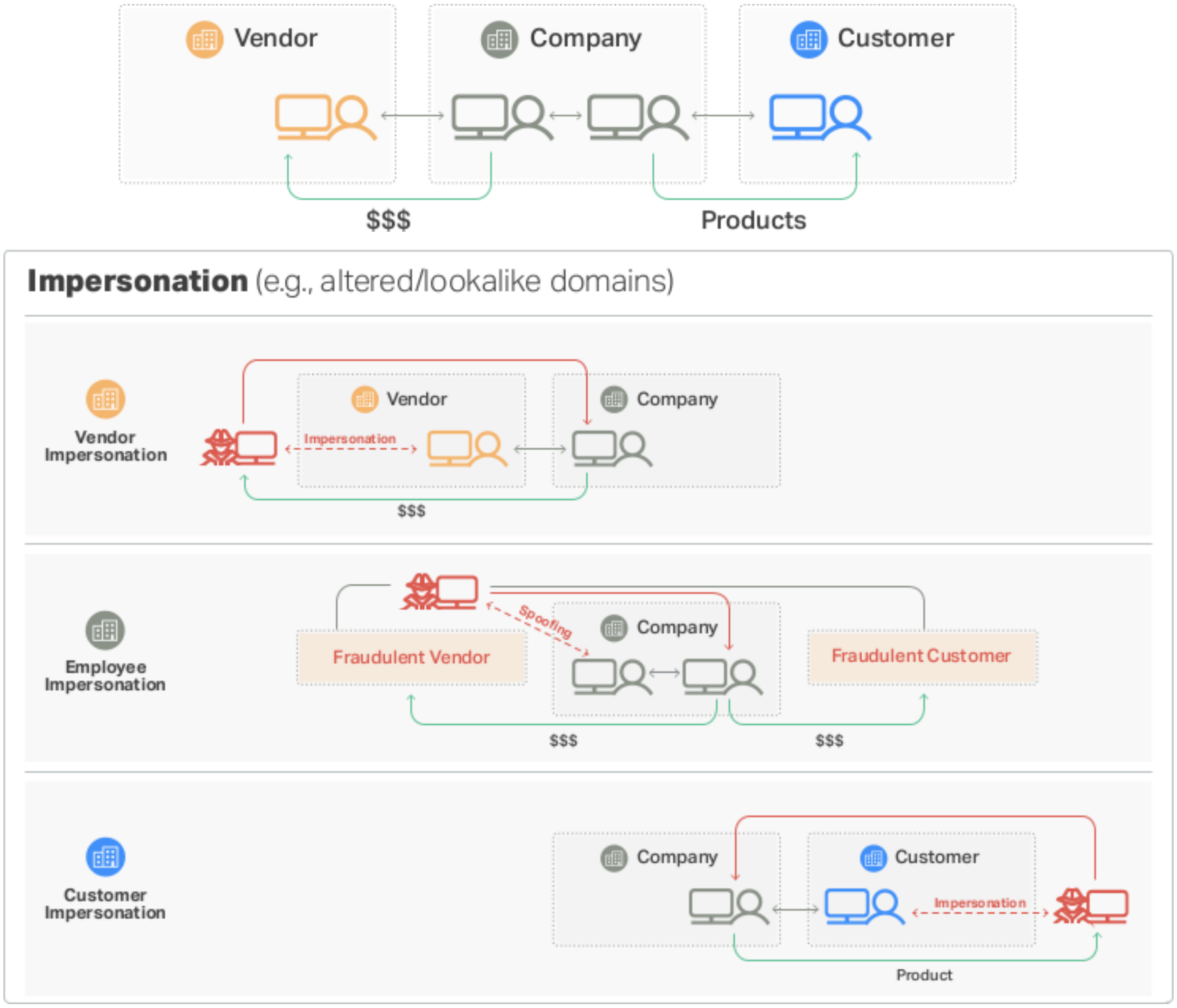
Overview

On June 4th, 2020, Abnormal Security detected and stopped an attempted invoice fraud targeting a global retailer, preventing nearly $30,000 from being stolen. This was a novel attack, which later surfaced at several other customers. The attacker's operation involved impersonating a debt collection agency claiming it was collecting an unpaid debt and then spoofing the target company's COO. The email from the spoofed COO contained the fake invoice referenced by the impersonated debt collector and claimed it was lost.

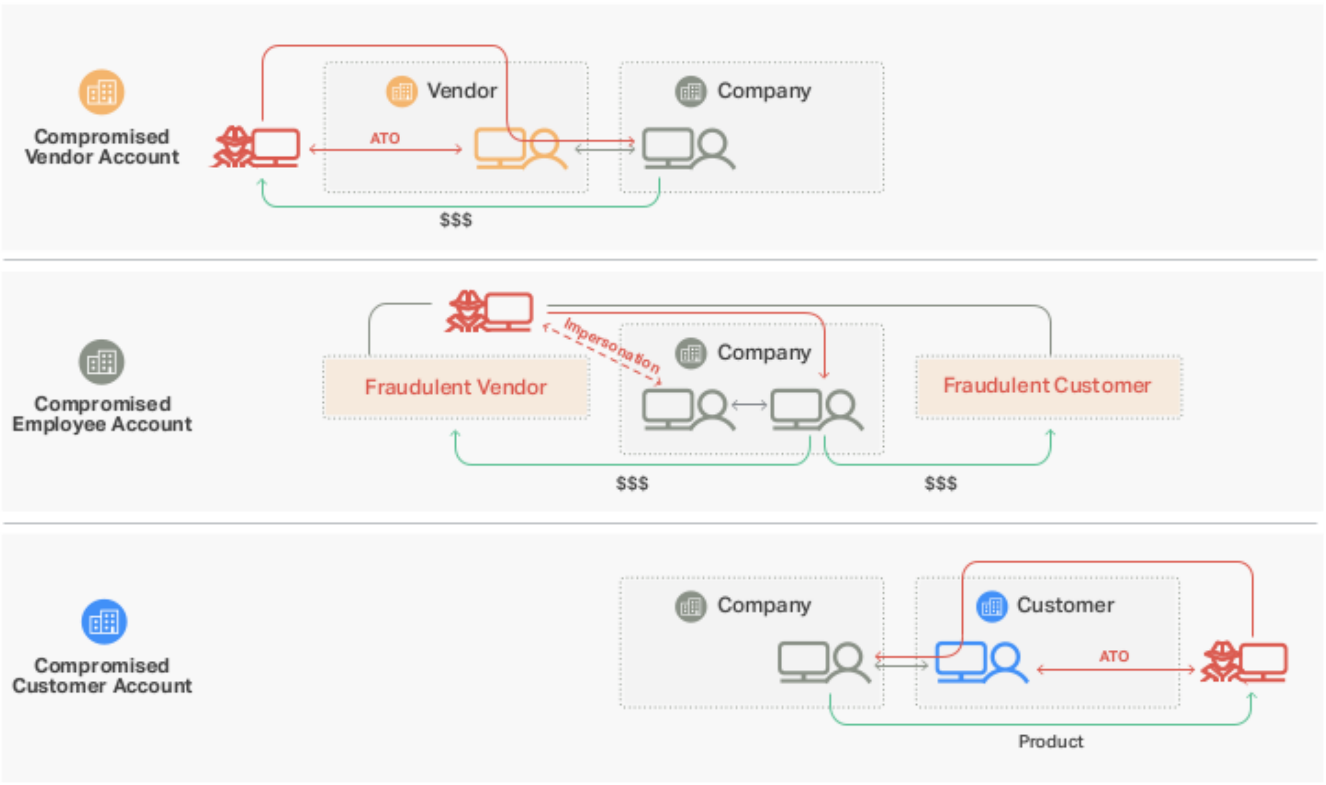
Disclaimer: All parties have been anonymized for this case study.

Types of Business Email Compromise (BEC) Attacks

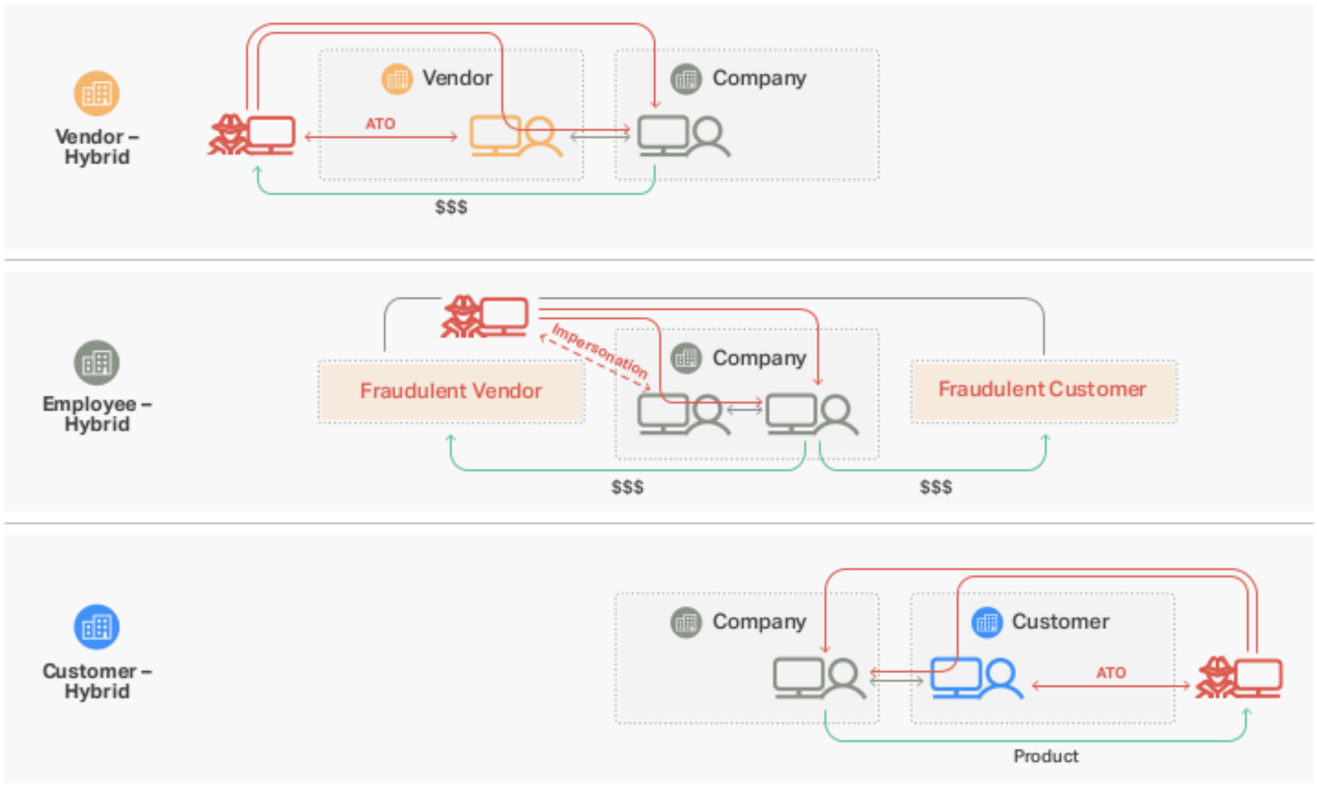
BEC attacks can be broken into 9 different categories depending on the pretext of the attacker (Vendor, Employee, Customer), along with the attack technique (Spoofing/Impersonation, or Compromised Account/Account Takeover). Attacks may also leverage a hybrid approach using multiple techniques.



Compromised Account (e.g., altered/lookalike domains)



Hybrid (e.g., altered/lookalike domains)



Attack Summary

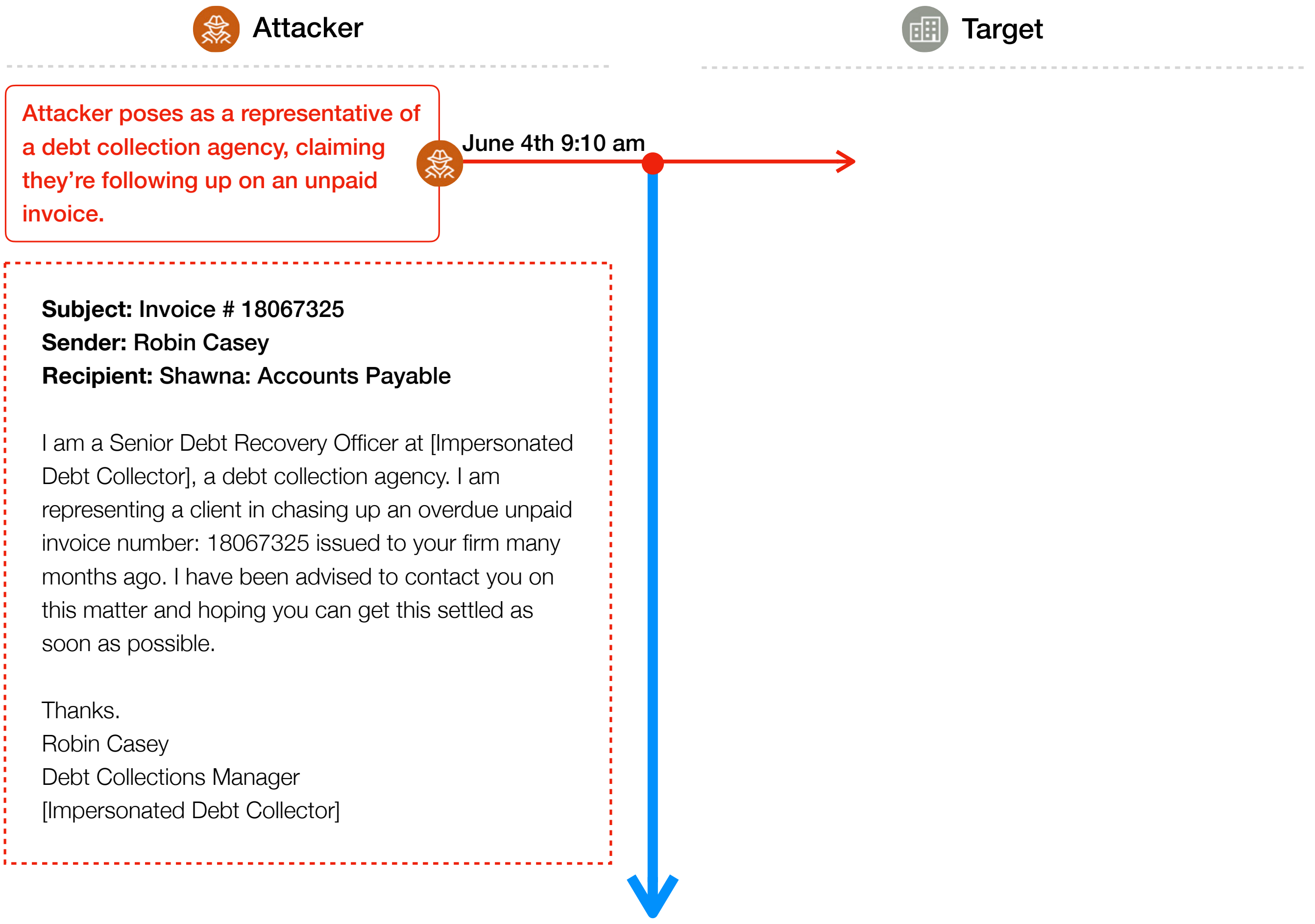
The attacker targets a retailer (henceforth referred to as “Retailer”) by impersonating a debt collection agency reaching out about an unpaid invoice for a vendor (henceforth referred to as “Vendor”). The debt collection agency is a real company, but is being impersonated by the attacker (henceforth referred to as “Impersonated Debt Collector”) using a lookalike domain. The vendor appears to be entirely fictional.

Shortly after the initial attack email was sent, the attackers spoofed the COO of the Retailer, reaching out to the same employees at the Retailer as the initial email asking for the Vendor’s invoice to be paid. Attackers were able to convince the employees at the Retailer to begin processing the invoice before Abnormal Security notified the Retailer that this was an attack and prevented payment from being made. The amount of the invoice in question is worth nearly $30,000. This attack spanned an extended engagement of six back-and-forth conversations over the course of one day.

Constituents

Attacker Personas Impersonated Debt Collector	**Attacker Personas** Spoofed Target	**Target Organization** Retailer
• Robin Casey	• Marie Macklin (spoofed COO)	• Shawna: Accounts Payable • Rebecca: Finance

Attack Timeline

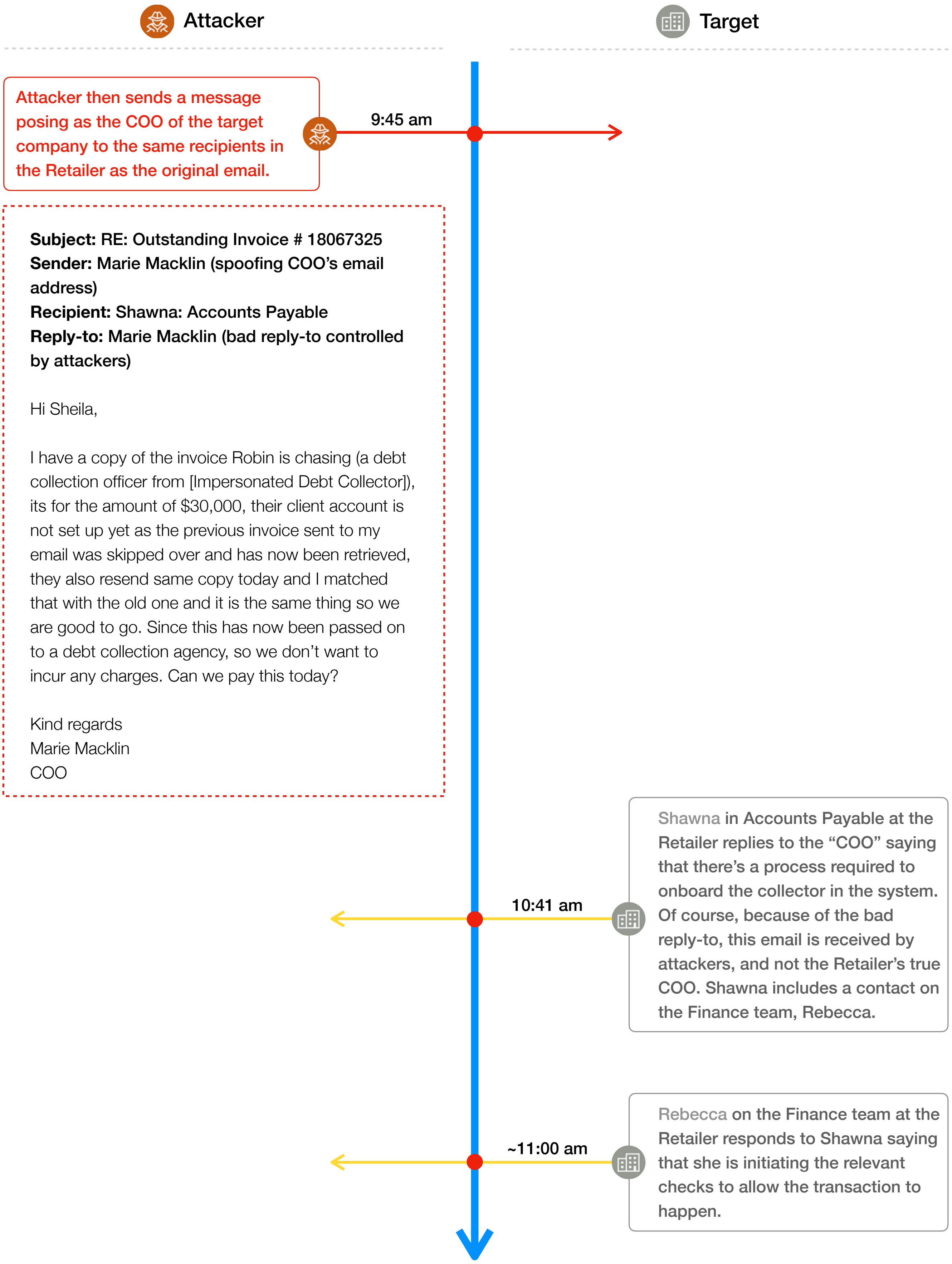


Attacker poses as a representative of a debt collection agency, claiming they’re following up on an unpaid invoice.

Subject: Invoice # 18067325
Sender: Robin Casey
Recipient: Shawna: Accounts Payable

I am a Senior Debt Recovery Officer at [Impersonated Debt Collector], a debt collection agency. I am representing a client in chasing up an overdue unpaid invoice number: 18067325 issued to your firm many months ago. I have been advised to contact you on this matter and hoping you can get this settled as soon as possible.

Thanks.
Robin Casey
Debt Collections Manager
[Impersonated Debt Collector]



Attacker

Target

Attacker then sends a message posing as the COO of the target company to the same recipients in the Retailer as the original email.

9:45 am

Subject: RE: Outstanding Invoice # 18067325
Sender: Marie Macklin (spoofing COO's email address)
Recipient: Shawna: Accounts Payable
Reply-to: Marie Macklin (bad reply-to controlled by attackers)

Hi Sheila,

I have a copy of the invoice Robin is chasing (a debt collection officer from [Impersonated Debt Collector]), its for the amount of $30,000, their client account is not set up yet as the previous invoice sent to my email was skipped over and has now been retrieved, they also resend same copy today and I matched that with the old one and it is the same thing so we are good to go. Since this has now been passed on to a debt collection agency, so we don't want to incur any charges. Can we pay this today?

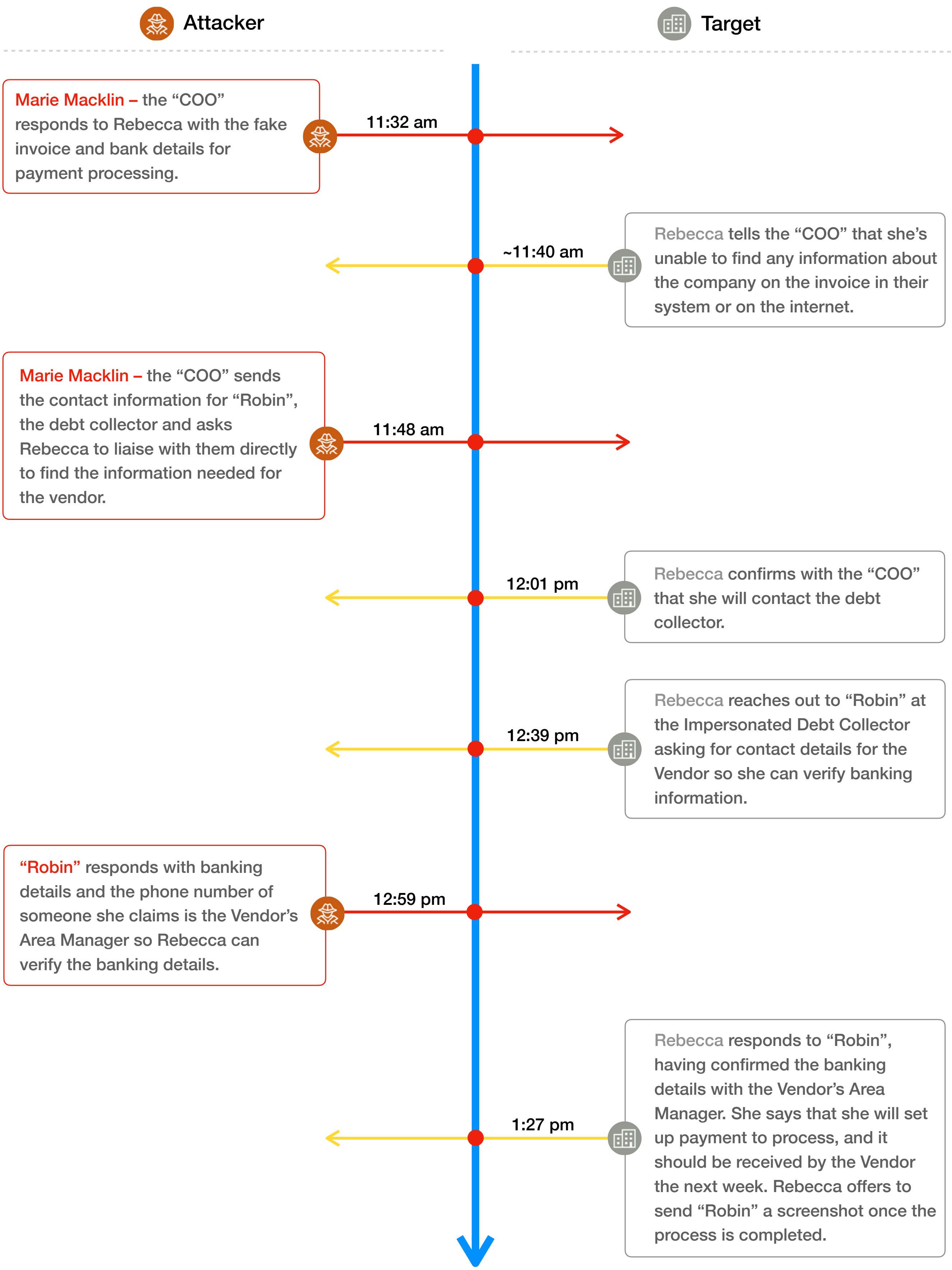
Kind regards
Marie Macklin
COO

10:41 am

Shawna in Accounts Payable at the Retailer replies to the "COO" saying that there's a process required to onboard the collector in the system. Of course, because of the bad reply-to, this email is received by attackers, and not the Retailer's true COO. Shawna includes a contact on the Finance team, Rebecca.

~11:00 am

Rebecca on the Finance team at the Retailer responds to Shawna saying that she is initiating the relevant checks to allow the transaction to happen.



Attacker

Target

11:32 am — Marie Macklin – the "COO" responds to Rebecca with the fake invoice and bank details for payment processing.

~11:40 am — Rebecca tells the "COO" that she's unable to find any information about the company on the invoice in their system or on the internet.

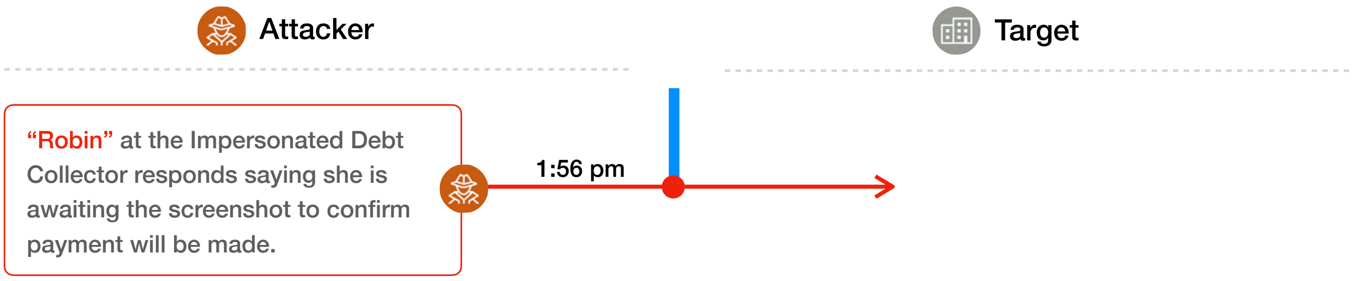
11:48 am — Marie Macklin – the "COO" sends the contact information for "Robin", the debt collector and asks Rebecca to liaise with them directly to find the information needed for the vendor.

12:01 pm — Rebecca confirms with the "COO" that she will contact the debt collector.

12:39 pm — Rebecca reaches out to "Robin" at the Impersonated Debt Collector asking for contact details for the Vendor so she can verify banking information.

12:59 pm — "Robin" responds with banking details and the phone number of someone she claims is the Vendor's Area Manager so Rebecca can verify the banking details.

1:27 pm — Rebecca responds to "Robin", having confirmed the banking details with the Vendor's Area Manager. She says that she will set up payment to process, and it should be received by the Vendor the next week. Rebecca offers to send "Robin" a screenshot once the process is completed.



Attacker

Target

“Robin” at the Impersonated Debt Collector responds saying she is awaiting the screenshot to confirm payment will be made.

1:56 pm

Subject: **RE: FW: Outstanding Invoice # 18067325**
Sender: **Robin Casey**
Recipient: **Rebecca: Finance**

Hi Rebecca,

[The Vendor’s Area Manager] just confirmed that he agreed with you for next week payment.

I now await your screen shot to confirm its processed.

Thanks.

Robin Casey
Debt Collections Manager
[Impersonated Debt Collector]

Attacker Techniques

The actor behind this attack used sophisticated social engineering techniques to collect payment on the fraudulent invoice. This attacker leveraged spoofed emails ostensibly coming from the Retailer’s COO to provide additional social proof that led employees to overlook what would have otherwise been major red flags that should have prevented them from processing this payment.

Domain Impersonation

The attacker impersonated a debt collection agency claiming to be collecting an unpaid invoice for a vendor. The debt collection agency was real, but attackers registered a lookalike domain for their emails:

- Replacing “i” with “l”
  e.g., “redbird.com” becomes “redblrd.com”
- Adding or removing an “s”
  e.g., “advancednetwork.com becomes “advancednetworks.com” or vice versa
- Adding “int” or “inc”
  e.g., “superiorpackaging.com” becomes “superiorpackaginginc.com”
- Spelling out a portion of the name that’s otherwise abbreviated
  e.g. “ihop.com” becomes “internationalhop.com”

Spoofing the COO with a bad reply-to

To add greater credibility to the initial email for engagement, the actor sent an email spoofing the COO of the Retailer. The email from the spoofed COO even included a faked thread communicating with the Impersonated Debt Collector. This spoofed COO aimed to ensure the process continued even when red flags were present, including employees finding no information about the alleged vendor either in their system or on the internet, or when employees questioned whether the payment should be sent to the Impersonated Debt Collector (which could have led the employees to contact the real debt collector and therefore realize that this was an attack) or the fake Vendor (where the attackers were hoping payment would be sent).

Urgency

The initial request came from a debt collector, which meant that employees were more likely to act quickly in order to avoid issues with further interest or penalties from accruing. Attackers leverage urgency because it often leads employees to overlook otherwise suspicious signals, or cut corners to act quickly in an effort to avoid any negative consequences.

Detection Techniques

Abnormal Security detected this attack and prevented the payment to the incorrect account from occurring. This attack was detected during an evaluation of the product in passive mode, enabling a unique view of the entire lifecycle of the attack. The core of Abnormal Security's detection is Abnormal Behavior Technology, or ABX, which combines the Abnormal Identity Model, Abnormal Relationship Graph, and Abnormal Content Analysis to arrive at high confidence decisions. A number of specific techniques in ABX were used to detect this attack, including:

Identity Modeling

VendorBase: A global, federated database on vendor to provide real-time scores of vendor risk.

Domain Impersonation: Identification of a lookalike domain raised suspicion of a potential attack.

Relationship Graph

Normalcy Traits: Geolocation and key contacts at each vendor.

Domain Analysis: Pattern and age of domain

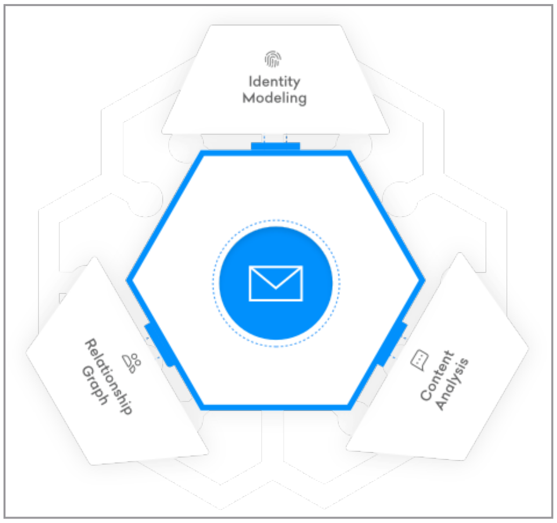
Unsafe engagements: Unusual and unsafe engagement from employees.

Content Analysis

Natural Language Processing: Text analysis to determine topic and sentiment of conversation.

Vendor Mail Detector: Model to automatically detect vendor relationships.

Invoice Processing: Detection of invoices fo invoice-specific analysis.



About Abnormal Security

The Abnormal Security cloud email security platform protects enterprises from targeted email attacks. Powered by Abnormal Behavior Technology (ABX), the platform combines the Abnormal Identity Model, the Abnormal Relationship Graph and Abnormal Content Analysis to stop attacks that lead to account takeover, financial damage and organizational mistrust. Though one-click, API-based Office 365 and G Suite integration, Abnormal Security sets up in minutes, requires no configuration and does not impact email flow. Backed by Greylock Partners, Abnormal Security is based in San Francisco, CA. Please visit www.abnormalsecurity.com and follow the company at @AbnormalSec.