I. Executive Summary

The third quarterly Abnormal Security BEC Report continues our examination of the business email compromise threat landscape. Starting with last quarter’s report, we set out to provide the only global measure of BEC attack volumes available to the market. As was the case in Q2, the volume of BEC attacks continues to trend upwards, with a 15% increase from quarter-to-quarter.

For this quarter’s report, we took a closer look at BEC attack trends across eight different industries. We found that the average weekly volume of BEC campaigns increased quarter-over-quarter in six out of eight industries, with the largest increase occurring in the Energy/Infrastructure industry. The Retail/Consumer Goods & Manufacturing and Technology industries tied for the highest volume of BEC campaigns received each week.

We also closely track BEC attacks based on goals. During Q3, attackers continued to focus primarily on BEC campaigns with a goal of invoice and payment fraud, as we saw a 155% increase from Q2 to Q3. We also saw a corresponding decrease in social engineering BEC attacks with a goal to impersonate internal employees and VIPs or external partners.

Understanding who is being targeted during BEC campaigns is critically important to tuning email defenses and conducting tailored security awareness training. In Q3, we saw a change in the trend toward finance employees being the primary targets, illustrating how attackers constantly shift their tactics. While invoice and payment fraud continues to increase, threat actors have shifted their focus from the C-suite to individual finance employees and now to group mailboxes.

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 third 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
II.
Key Takeaways

**BEC Attack Volumes Continue to Increase**

Ongoing quarterly increases in BEC attack volumes should be a top concern to enterprises, with a 15% increase from Q2 to Q3. Since BEC attacks are targeted and sophisticated, this increase could indicate an ability for threat actors to scale that may overwhelm some businesses.

**BEC Campaigns on the Rise in Nearly All Major Industries**

BEC campaigns targeting Energy/Infrastructure increased 93% from Q2 to Q3, while Retail & Manufacturing, Technology and Media received the highest volume of attacks during the quarter. BEC campaign volume increased in six out of eight industries tracked by Abnormal Security.

**Invoice and Payment Fraud Remains the Predominant Goal**

Q3 was marked by a 155% overall increase in incidents of BEC attacks with a goal of invoice or payment fraud across industries. This trend was particularly notable for Retail/Consumer Goods & Manufacturing.

**Attackers Shift Their Sights from Finance Employees to Group Mailboxes**

While attacks on the C-suite have continued to stay flat, the amount of attacks targeting employees in finance departments dropped by 53% from Q2 to Q3. Attackers shifted tactics by increasing email attacks to group mailboxes by 212%.

**COVID-19 Related Attacks Decrease (Except for Invoice and Payment Fraud)**

While credential-phishing COVID-19 related attacks decreased by 82%, invoice and payment fraud that continues to leverage the fear, uncertainty and doubt of the pandemic increased by 81%.

**Most Impersonated Brands Return to Pre-Pandemic “Normal”**

In Q3, Zoom dropped away from the top spot, replaced by DHL and followed by Dropbox and Amazon. Rounding out the top five were iCloud and LinkedIn.
BEC Attack Volumes Continue to Increase

Beginning in Q2, 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.

We continue to see BEC attack volumes increasing quarter-over-quarter. This upward trend remains concerning, as unlike other attacks, BEC is highly-targeted in nature and more sophisticated in order to land bigger payouts.

Key Finding

The median number of BEC attacks received per company each week increased 15% from Q2 to Q3 (Figure 1).

Median Weekly BEC Campaigns per 1,000 Mailboxes Against Clients

Figure 1: Median Weekly BEC Attacks Increased 15% from Q2 to Q3
BEC Campaigns on the Rise in Nearly All Major Industries

Examining BEC attack trends across industries provides additional insight into where the volume increases are occurring. Abnormal Security tracks BEC campaigns across eight major industries, including Retail/Consumer Goods & Manufacturing, Technology, Energy/Infrastructure, Services, Medical, Media/TV, Finance and Hospitality (see appendix for more detail on industry subsegments).

During Q3, we found that BEC campaign volume increased in six out of eight industries, with Energy/Infrastructure seeing the highest jump of 93% from Q2 to Q3.

Campaign volume declined in Retail/Consumer Goods & Manufacturing and Technology. Despite this drop, these two industries tied for the highest overall volume of campaign attacks during the quarter.

Key Findings:

• Similar to previous findings elsewhere, Retail/Consumer Goods & Manufacturing was a primary recipient of BEC attacks during both Q2 and Q3. In Q3, Retail/Consumer Goods & Manufacturing and Technology sectors were effectively tied for average weekly BEC campaigns received per 1,000 mailboxes.

• Out of the eight industries sampled, six experienced an increase in BEC campaigns in Q3 relative to Q2.

• The 93% increase in weekly BEC campaigns targeted at the Energy/Infrastructure industry was driven by increases in all BEC attack categories (Figure 2). This included BEC attacks with a goal of paycheck fraud (or social engineering BEC, through which an internal employee is being impersonated) and invoice and payment fraud BEC (wherein either an internal or an external party is being impersonated, typically external).

• The 53% drop in weekly BEC campaigns targeted at the Retail/Consumer Goods & Manufacturing industry was driven by a decrease in BEC attacks with a goal of engaging the employee, which dropped by 84%. BEC campaigns targeting this sector with a goal of invoice or payment fraud, however, increased significantly.

• In addition to growth of in Energy/Infrastructure, BEC campaigns increased in Q3 in the following industries:
Average Weekly BEC Campaigns

Figure 2: Average Weekly BEC Campaigns Across Industry. 93% increase from Q2 to Q3 in Energy and Infrastructure Industry.
Invoice and Payment Fraud BEC Remains the Predominant Goal

Q3 was marked by a 155% overall increase in incidents of BEC attacks with a goal of invoice or payment fraud across industries. This trend was particularly notable for Retail/Consumer Goods & Manufacturing.

The unabated growth in invoice and payment fraud is simply due to the fact that it represents the greatest opportunity for attackers. Fraudulent invoices delivered by attackers have resulted in some of the largest financial losses from BEC. With thousands of vendors and thousands more invoices to manage, it becomes extremely easy for attackers to get lost and fraudulent invoices to be paid time and again.

Key Findings:

• Q3 was marked by increasing incidents of BEC attacks with a goal of invoice or payment fraud. Across all industries, the average rate of invoice and payment fraud BEC campaigns received each week increased 1.6 times the weekly rate in Q2 (155% quarter-over-quarter increase). This trend was particularly notable for Retail/Consumer Goods & Manufacturing.

• Throughout 2020, Retail/Consumer Goods & Manufacturing saw a trend of decreasing social engineering BEC attacks and increasing invoice and payment fraud BEC attacks.

• The weekly median rate of BEC campaigns with a goal of invoice or payment fraud received by Retail/Consumer Goods & Manufacturing organizations increased by 94% in Q3 as compared to Q2 (Figure 3).

• Correspondingly, across all industries, the average weekly rate of social engineering BEC campaigns, which impersonate an internal party, dropped by 38% (Figure 4), while the rate of campaigns impersonating an external partner increased by 21%.
Median Weekly Invoice / Payment Fraud BEC: Retail, Consumer Goods and Manufacturing

Figure 3: Median Weekly Invoice / Payment Fraud BEC for Retail, Consumer Goods and Manufacturing increased by 94% in Q3 2020.

Median Weekly Social Engineering BEC: Retail, Consumer Goods and Manufacturing

Figure 4: Median Weekly Social Engineering BEC for Retail, Consumer Goods and Manufacturing fell by 38% in Q3 2020.
Examples of Invoice Fraud

INVOICE UPDATE!

[REDACTED]  <[REDACTED]@[REDACTED].com>

Wednesday, August 6, 2020 at 4:08 AM

***NOTICE*** This came from an external source. Use caution when replying, clicking links, or opening attachments.

Dear Partner,

We’re currently undergoing an annual bank reconciliation audit and reviewing the company outstanding balances with all our esteemed partners, therefore re-concern with us as your records show.

1. Please send us a list of the open invoices and outstanding payments according to what your records show.

2. Hold on with any payment just to avoid credit issues as a result of the ongoing audit with our bank account.

We apologize for any inconvenience at this time and thank you in advance for your cooperation and understanding in taking the time to consider the above email.

Should you need any further information, please do not hesitate to contact me for further assistance. For all international correspondence, please feel free to write in English, German or French.

RS: With the daily increase in the spread of COVID-19, we urge you to be safe and keep safety all time.

Sincerely Yours,

[REDACTED]

This e-mail is confidential. If you are not the intended recipient you must not disclose, distribute or use the information in it as this could be a breach of confidentiality. If you have received this message in error, please advise us immediately by returning e-mail and deleting the document. The address from which this message has been sent is strictly for business mail only and the company reserves the right to monitor the contents of communications and take action where and when it is deemed necessary. Thank you for your cooperation.

Figure 5: Example of COVID-19 Related Invoice Fraud Email

RE: Statement from [REDACTED] Company

To: [REDACTED]@[REDACTED].com
Cc: [REDACTED]@Account Receivable

Thursday, September 24, 2020 at 4:48 PM

[REDACTED]  <[REDACTED]@[REDACTED].com>

15.9 KB  A...

Download All + Preview All

CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Moving forward we would like payments to be made via ACH directly if this is not possible then Wire, kindly find the attached bank letter. If you can also advise all on the expected payment date of all outstanding invoices so I can note this on my AR report for this month.

[REDACTED] Credit and Collections Manager

Figure 6: Example of COVID-19 Related Invoice Fraud Email
Attackers Shift Their Sights From Finance Employees to Group Mailboxes

During the first half of the year, attackers increasingly targeted BEC attacks at finance department employees, while targeted BEC attacks on the C-suite dropped off and plateaued.

In Q3, the rate of C-suite attacks remained flat, but we also observed that BEC attacks on finance department employees decreased by an average weekly rate of 64%. This drop was driven by a sharp decline in social engineering BEC attacks, which have goals such as gift card fraud, engagement and paycheck fraud, and impersonate an individual internal to the company.

Conversely, invoice and payment fraud BEC attacks against finance increased by 54% on average per week from Q2 to Q3. It’s important to note that the highest rates of invoice and payment fraud BEC attacks targeting employees in finance observed thus far by Abnormal occurred during Q4 2019. This may indicate a seasonality to these types of attacks. If this is the case, we should see a significant spike in such attacks in Q4 of this year.

As invoice and payment fraud continues to increase, we are observing threat actors shifting their tactics to target group mailboxes, which received the most invoice and payment fraud attacks, followed by C-suites.

Key Findings

- The overall rate of BEC attacks on finance employees dropped 64% on average per week in Q3, driven by a sharp decline in social engineering BEC attacks, while attacks on the C-suite remained flat
- Invoice and payment fraud BEC attacks against finance employees increased by 54% on average per week
- Invoice and fraud attacks targeted to group mailboxes increased by 212% from Q2 to Q3
COVID-19 Related Attacks Decrease (Except for Invoice and Payment Fraud)

While Q1 and Q2 saw spikes and overall increases in COVID-related attacks, Q3 saw a marked decline in all categories for these campaigns except in one key area – invoice and payment fraud.

Over the course of Q3, the average weekly attack rate of COVID-related invoice and payment fraud BEC increased at a rate of 81%. Conversely, COVID-related credential phishing campaigns, which had been a major source of these attacks in Q2, declined by 82% in Q3.

In Q2, invoice and payment fraud BEC appeared, leveraging uncertainty of the pandemic to impersonate some form of financial disarray, resulting in “audits” and changing banking details.

Key Findings
- COVID attacks were mostly flat or declining in Q3, with volumes greatly diminished from Q1 and Q2.
- Weekly attack volume of COVID-19 related attacks decreased overall in Q3, except for invoice and payment fraud attacks, which increased by 81% (Figure 7); credential phishing attacks related to COVID declined by 82%.
- Invoice and payment fraud attacks continue to leverage uncertainty during the pandemic to incite “audits” and urging recipients to change banking details.

COVID-19 Related Attacks - Credential Phishing BEC Fraud

COVID-19 Related Attacks - Invoice and Payment BEC Fraud

Figure 7: COVID-19 Related BEC Attacks involving Invoice and Payment Fraud Increased 81% in Q3
Most Impersonated Brands Return to Pre-Pandemic “Normal”

In Q2, Abnormal began monitoring the brands that were the most impersonated in BEC attacks. As noted, these attacks typically leverage the zeitgeist, following trends and shifts each quarter. In Q3, Zoom dropped away from the top spot, replaced by DHL and followed by the file sharing platform Dropbox (Figure 8).

Amazon remained in the top three this quarter, maintaining ecommerce’s attractiveness to cyber criminals as a strong attack impersonation vector. Rounding out the top five were iCloud and LinkedIn.

The shift to file sharing and social networking brand impersonations is notable in a couple of areas. First, with the continued predominance of remote work and learning, file sharing and other new applications could open up channels like iCloud and Dropbox for more users. Additionally, with continued economic uncertainty, employment networking sites such as LinkedIn also pose an attractive threat vector to bad actors.

Key Findings:

- In Q3, the top three most impersonated brands included DHL, Dropbox and Amazon, followed by iCloud and LinkedIn
- These attacks continue to follow the zeitgeist and will undoubtedly shift as we move into election and holiday season

Most Impersonated Brands Q3 2020

Figure 8: DHL replaced Zoom as the most impersonated brand in Q3 2020
IV. Predictions

Each quarter, we look at data to predict where the state of BEC will lead. Here’s how our Q3 predictions panned out and what we see ahead for Q4:

**Prediction:** BEC in general will continue to rise as attackers persistently find success with socially engineered techniques that evade traditional email security defenses  
**Reality:** Unfortunately, we were all too right about this prediction as BEC attacks rose an alarming 15% in Q3 over Q2.

**Prediction:** COVID-19 related attacks will continue to trend downward with credential phishing accounting for a significant percentage of these attacks  
**Reality:** We did see these attacks trend downward in all areas, except for invoice and finance fraud attacks.

**Prediction:** Supply chain attacks targeting finance departments with invoice fraud will continue to increase as a security threat to organizations.  
**Reality:** While BEC attacks targeting finance employees declined overall in Q3, invoice and payment fraud attacks continued to increase (by 54% quarter-over-quarter).

**Prediction:** 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  
**Reality:** Q3 saw Dropbox gain as a most impersonated brand, indicating this trend continues, while mainstay brands including Amazon and DHL continue to be impersonated.

**Prediction:** Upcoming U.S. elections will put a target on state and local election administrators’, candidates campaign budgets as well as confidential data  
**Reality:** While our research has yet to find a marked increase in these attacks, we anticipate Q4 will see a rise in election-related BEC.
Our predictions for Q4:

- BEC will steadily rise as attackers continue to have success penetrating secure email gateways.

- COVID-19 related threats involving invoice and payment fraud will persist as the virus remains a factor in Q4 and into early next year.

- Invoice and payment fraud, both impersonating 3rd party supply chain vendors and internal employees will continue to be the biggest BEC threat to businesses.

- All industries will be affected by BEC with retail, consumer goods and manufacturing seeing an increase in attacks as we head into the holiday season.

- Invoice and payment fraud attacks targeting group mailboxes for finance and accounts payable departments will continue to persist into Q4 and beyond.
### Appendix

Industries included in each industry category considered in this analysis:

<table>
<thead>
<tr>
<th>Industry Category</th>
<th>Sub-Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail/Consumer Goods &amp; Manufacturing</td>
<td>Retail, Wholesale, Consumer Products, Manufacturing, Manufacturing - Durables, Manufacturing - Non-Durables</td>
</tr>
<tr>
<td>Technology</td>
<td>Technology, Computer Software, Social Media</td>
</tr>
<tr>
<td>Energy/Infrastructure</td>
<td>Energy / Utilities, Logistics / Transportation, Telecom / Communication Services</td>
</tr>
<tr>
<td>Services</td>
<td>Services, Professional Services, IT Services, Consulting</td>
</tr>
<tr>
<td>Medical</td>
<td>Medical Devices, Healthcare/Medical/Pharma, Hospitals / Health Care, Pharmaceuticals</td>
</tr>
<tr>
<td>Media/TV</td>
<td>Broadcast Media, Entertainment</td>
</tr>
<tr>
<td>Finance</td>
<td>Finance, Financial Services, Banking, Holding Companies, Venture Capital &amp; Private Equity</td>
</tr>
<tr>
<td>Hospitality</td>
<td>Casinos &amp; Gambling, Lodging, Restaurants</td>
</tr>
</tbody>
</table>