

Email Threat Report

# Brute Force Attacks and Account Takeover Attempts Rise 671%, Reaching Unprecedented Levels

/ Q3 2021

Key Takeaways and Trends

# Abnormal

# Executive Summary

There is little doubt that business email compromise and other advanced email threats are causing significant damage—both financial and reputational—to organizations worldwide. Because these never-before-seen attacks contain few indicators of compromise, they evade secure email gateways and other traditional email infrastructure, landing in inboxes where unsuspecting employees fall victim to their schemes.

## Looking for the Keys to the Kingdom

Email-based scams are not new, but they are evolving. Over the course of the quarter, we saw a significant increase in credential phishing and brute force attacks—both of which are attempts to gain access to email accounts. Once accessed, these accounts can be leveraged to send additional attacks on coworkers, partners, and vendors, and provide the credentials necessary to infiltrate other parts of the organization.

## Impersonating the Powerful

Unfortunately, phishing isn't the only issue. Impersonation is on the rise, with threat actors using both well-known brands and internal automated systems to trick their victims into submitting credentials, revealing sensitive data, or sending money. This increase in specific types of impersonation shows the extent to which cybercriminals are willing to change their tactics, and underscores the need for an email security system that will detect ever-changing attacks.

## Key Takeaways

137

number of account takeovers per 100,000 mailboxes for members of the C-suite

61%

of organizations received a vendor email compromise attack this quarter

22%  $\Delta$

increase in business email compromise attacks since Q4 2020

46%  $\Delta$

rise in impersonation of internal automated systems over the past two quarters

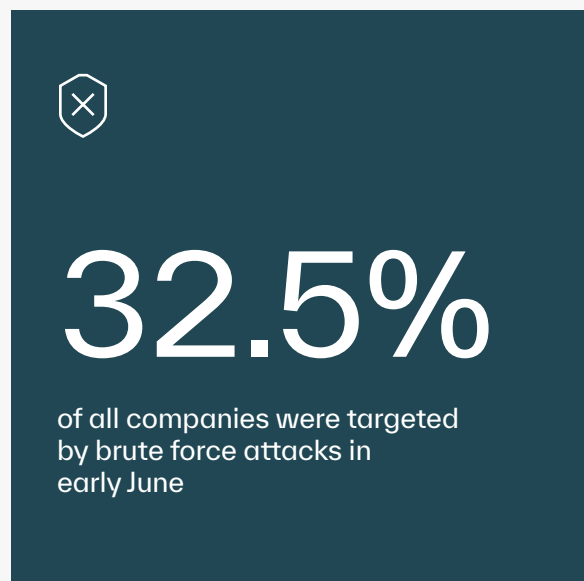
# Never-Before-Seen Surge in Brute Force Attacks and Account Takeover Attempts

While we typically only focus on business email compromise and vendor email compromise in our quarterly reports, account takeover attempts drastically increased in Q2 2021—something we've never seen to this extent. These attacks are particularly dangerous because they give threat actors full access to entire email accounts.

Some email accounts become compromised when a victim inserts their credentials into a phishing website following a credential phishing email—a type of attack that increased this quarter. Once the attacker has the credentials, he can use them to access the email account, see ongoing email conversations, and send additional attacks from the account itself. These attacks are highly effective because they come from a real person at the organization, using a real email address, and oftentimes as part of an ongoing email thread. In many cases, these account takeovers are especially damaging because traditional security infrastructure doesn't scan internal, east-west traffic, meaning threat actors can target organization employees with highly-effective attacks.

However, there are other ways to gain access to an account, without being certain which set of credentials is correct. The most common of these is a brute force attack, when cybercriminals target an account and programmatically test character combinations to determine the account password.

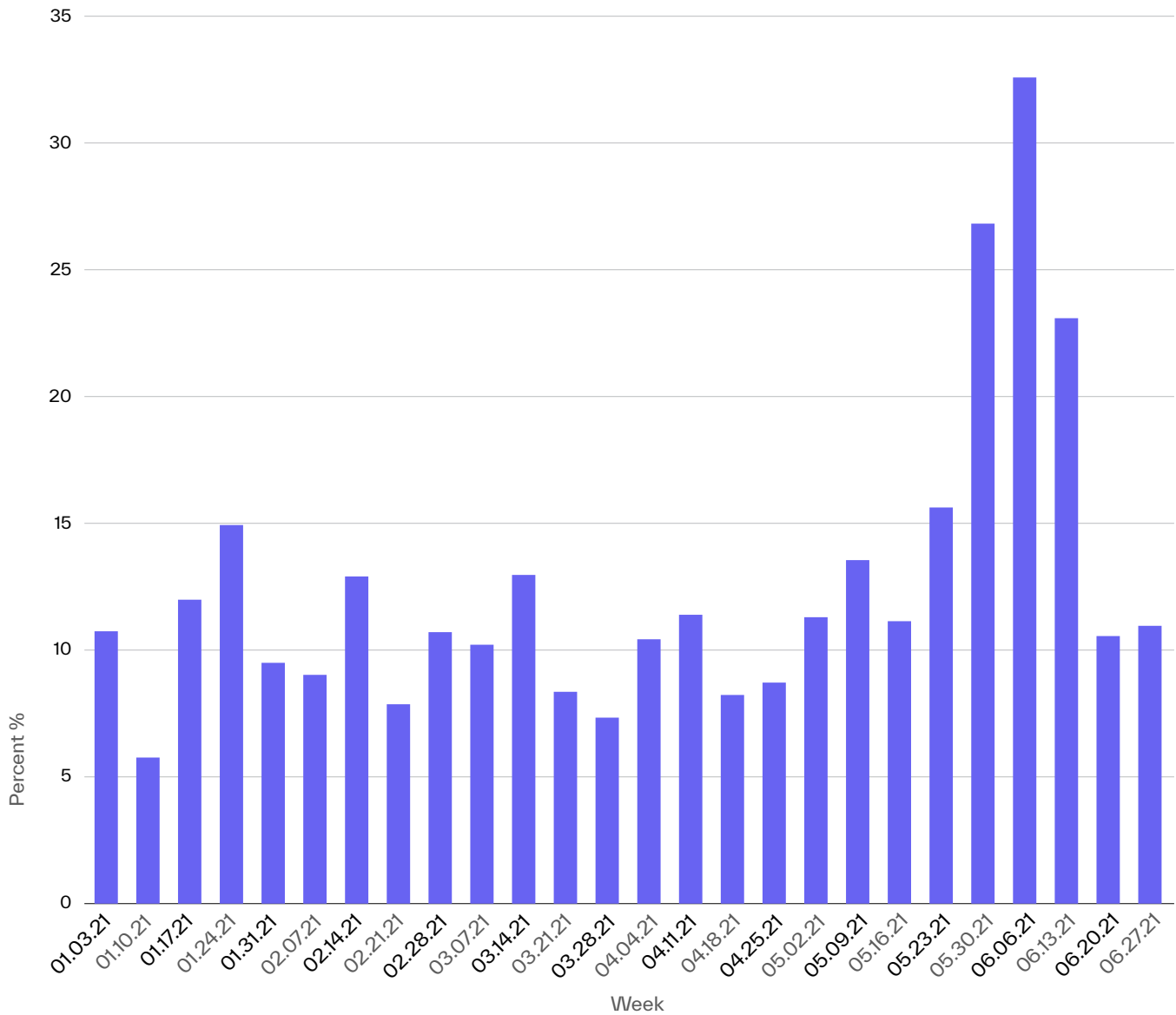
In a typical week, we observe brute force attacks targeting about 10% of companies. However, starting in May and ending in mid-June, the percentage of attacks increased by 160% to the highest-ever recorded weekly average of



26%. This means that a quarter of all companies were being targeted by brute force attacks on a weekly basis as cybercriminals attempted to take over their email accounts.

Perhaps most interestingly, during the peak of activity in the week of June 6, 2021, the rate of those attacks rose 671% over the previous weekly average as threat actors targeted 32.5% of all organizations with brute force attacks. Account takeover attempts reached unprecedented levels this quarter before returning to the normal average at the end of the month.

# Weekly Percentage of Companies Targeted by Brute Force Attacks



While we can't determine the exact reason for this increase, it corresponds with the increased attention around credential phishing and account takeovers as a result of the Colonial Pipeline and USAID attacks. We believe that new attackers may have been testing their luck with infiltrating email accounts in a similar fashion, before ultimately returning to their tried and true methods.

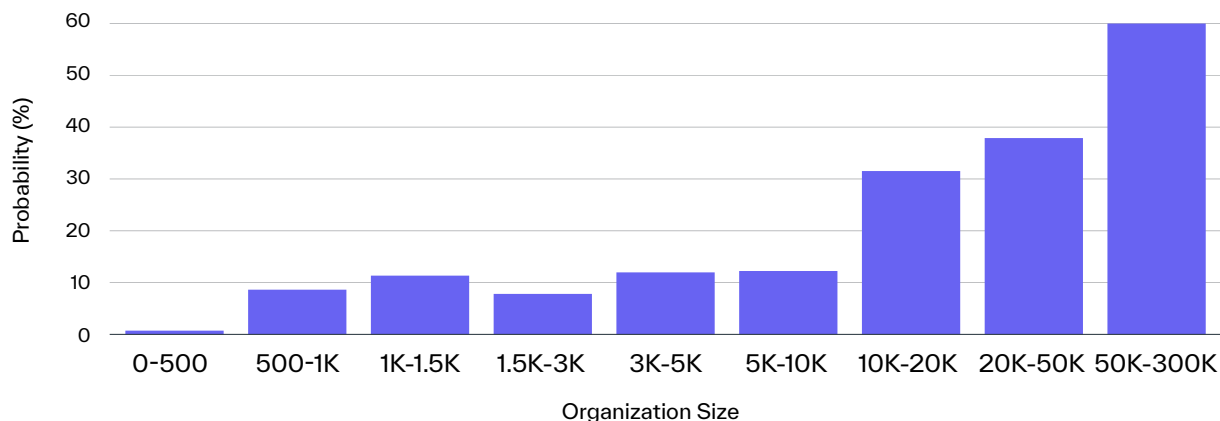
## Large Organizations at Risk for Successful Takeovers

While failed brute force attacks increased for companies of all sizes and industries in Q2, this luckily did not translate to an increase in successful account takeovers—at least for most organizations. The notable exception was for companies with fewer than 2,000 employees, which suffered both a larger increase in brute force attacks and an increase in successful account takeovers.

These small to mid-sized companies were 43% more likely to experience at least one successful account takeover this quarter. While we can't determine why this occurred, it could be due to the fact that larger companies are more likely to have stricter security procedures, including password managers, two-factor authentication, and/or more stringent password policies. Without these protections in place, smaller organizations are more likely to fall victim to brute force attacks, particularly when they increase to this extent.

That said, large organizations are still at an increased risk of account takeovers due to the sheer size of the organization. When looking at the likelihood of suffering a successful account takeover, there is a near linear relationship in which the probability increases alongside the size of the company. For example, while organizations with fewer than 500 employees have only a 1% chance of a successful account takeover, that number jumps to 60% for organizations over 50,000 employees.

### Average Weekly Probability of Suffering an Account Takeover by Organization Size



This 60% probability for large organizations showcases the need for advanced email security infrastructure. Once an attacker has gained access to an account, which they do three weeks out of every five, they have full access to internal and external contacts, historical email conversations, and ongoing email threads. In some cases, they can use this control of the email account to gain access to other systems including SharePoint, OneDrive, and Microsoft Teams.

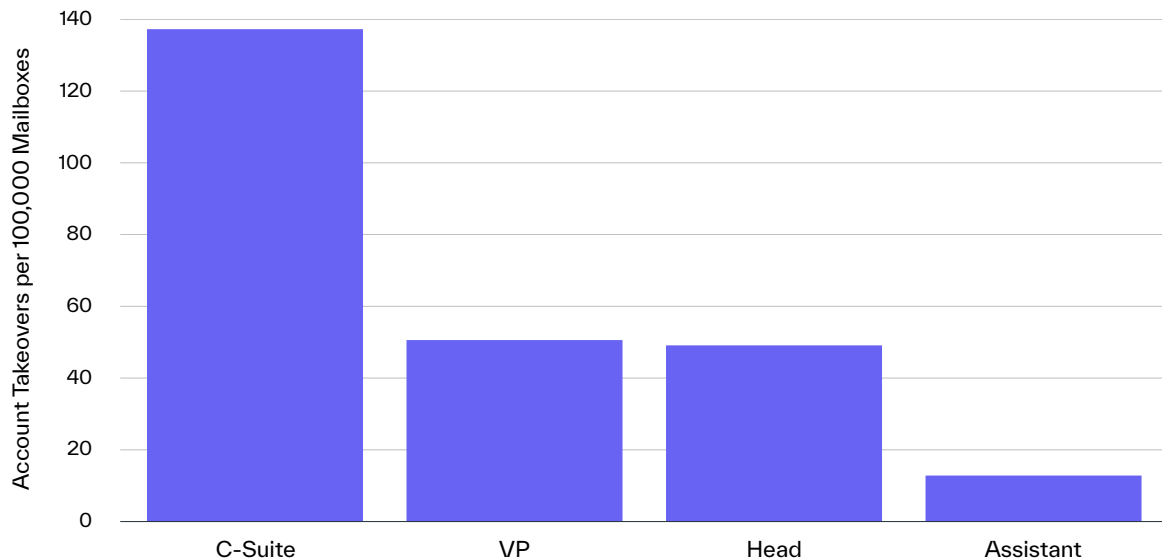
# 60%

chance of a successful account takeover each week for organizations with 50,000+ employees

## VIPs Most Targeted by Takeover Attempts

In the same way that executives and other high-level employees are more likely to be impersonated in a business email compromise attack, they are also more likely to be the victim of an account takeover. Although they comprise an extremely small number of email accounts within an organization, members of the C-suite experience nearly three times the risk of account takeovers than vice presidents—the next most targeted group. Relative to the number of people at each level, there were 137 successful account takeovers per 100,000 mailboxes for members of the C-Suite, with VPs at 50 successful account takeovers. Those with the term “Head” in their title were not far behind, with 49 successful account takeovers per 100,000 mailboxes.

## Successful Account Takeovers Relative to the Number of People at Each Level



That said, due to the small number of individuals within the C-suite, only about 1% of all successful account takeovers happen to these high-profile executives, while a full 14% of all takeovers are accounts owned by department heads. One interesting thing to note is that executive assistants are also highly targeted by account takeovers—almost certainly due to the fact that they are privy to nearly as much sensitive information as the executives who hire them.

With the increase in account takeover attempts, it is becoming even more important for those high-level roles to ensure that their accounts are secure and passwords are extremely difficult to crack. As the data shows, all it takes is an easily guessed or reused password to gain access to an entire organization.



# 137

successful C-suite account takeovers per 100,000 mailboxes

# Vendor Email Compromise Rises to Highest Level Yet

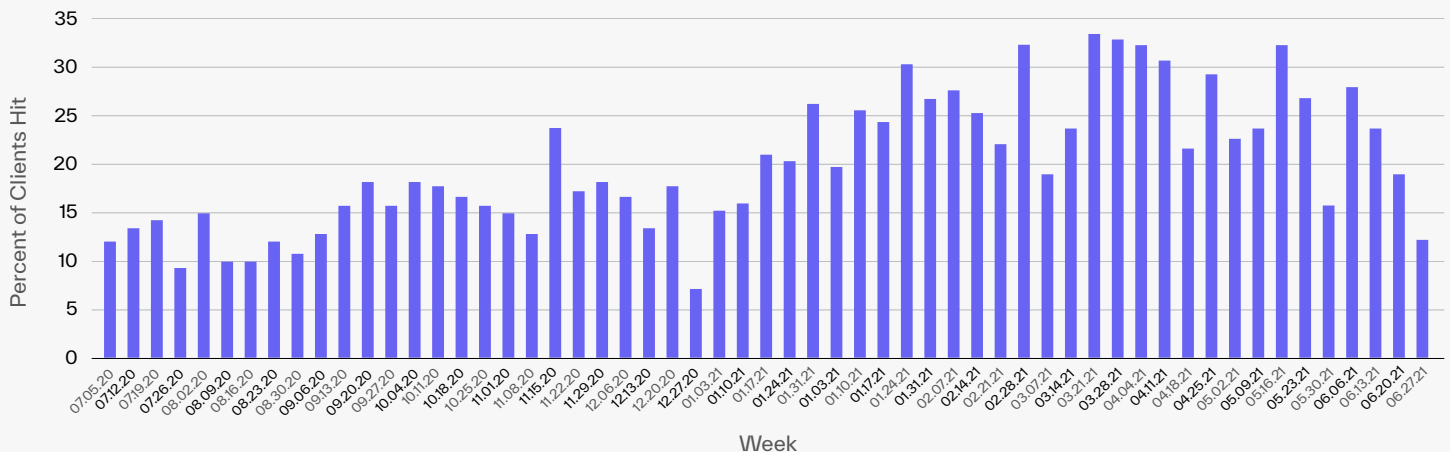
A new star on the cybercrime scene, vendor email compromise continues to rise every single quarter for the last year. Since we began tracking VEC in Q3 2020, we've seen continuous growth as more threat actors take advantage of poor security measures throughout the supply chain.

## VEC Threat Continues to Increase

Vendor email compromise is slightly different from traditional business email compromise in that it requires an attacker to have full access to a vendor email account, from which he or she launches attacks on customers. The typical attack includes a request to update bank details or to pay a fraudulent invoice, but these attacks can also take the form of RFQ scams or generic invoice inquiries.

Over the last quarter, this problem has increased, with Abnormal Security customers now receiving a median of 4 attacks per quarter. This means that your chance of receiving a VEC attack has risen 96% over the last year—a trend we expect to continue, especially given the increase in brute force and credential phishing attacks, both of which provide the necessary access to email accounts.

Percentage of Abnormal Customers Targeted by a VEC Attack Each Week

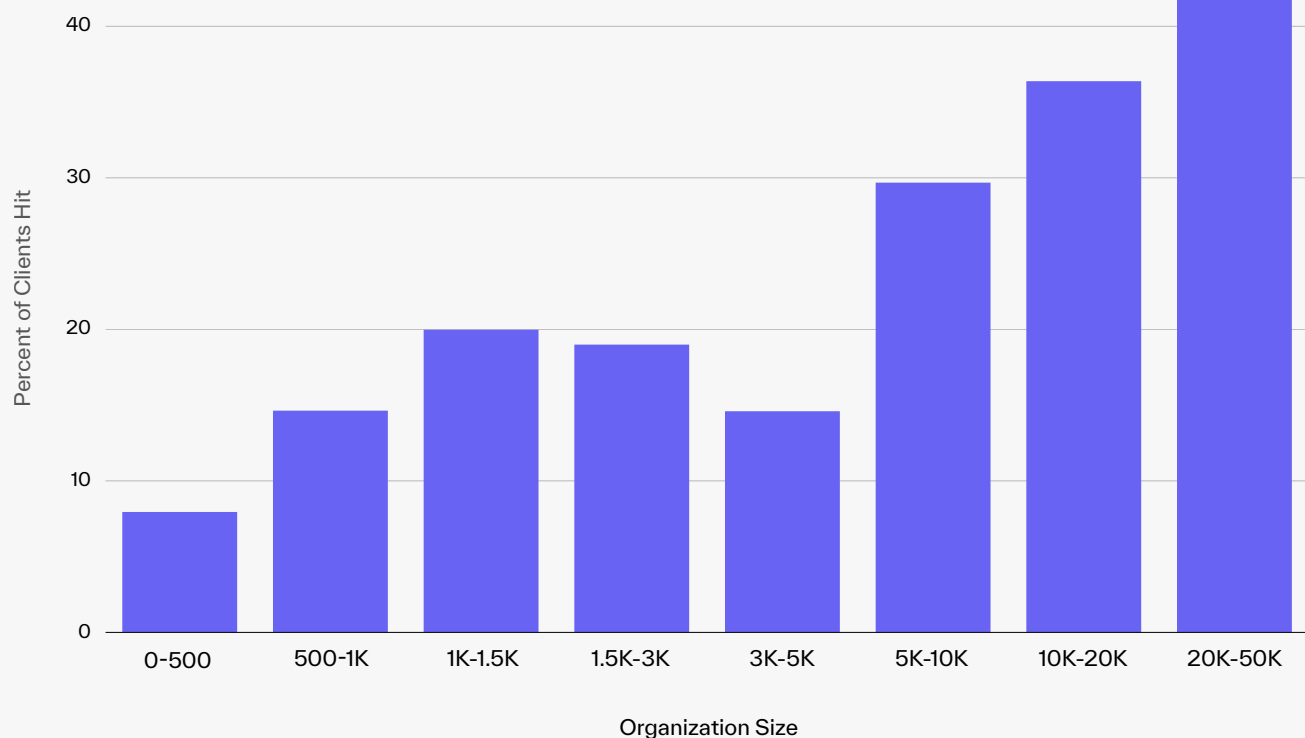


While four attacks per quarter may not seem that many, it is vital to remember that these attacks are using compromised accounts. Because they come from real vendor accounts, referencing real vendor information, they are particularly hard to detect and thus, very lucrative for cybercriminals. With an average request of \$183,000, four successful attacks each quarter could cost you millions each year.

## Large Organizations at Higher Risk

When it comes to company size, vendor email compromise tends to target larger organizations, with those over 20,000 employees having the highest probability of receiving a VEC attack. Organizations under 5,000 employees experience VEC attacks only once every five weeks, but that number shoots up to nearly every other week for organizations over 20,000 employees. This could be because these larger organizations have more vendors and thus more opportunities for compromise.

Average Weekly Probability of Receiving a VEC Attack by Organization Size



Over the course of the last year, Abnormal has stopped hundreds of VEC attacks for our customers. The single highest requested amount remains at \$1.6 million from an attack first seen in late 2020. With this attack type continuing to increase, we expect that number to grow in coming months, particularly if threat actors continue to target large organizations with thousands of vendors and massive budgets.

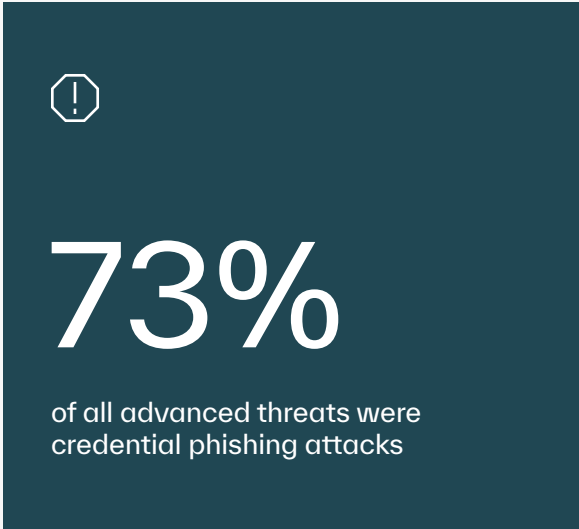


# High Effort, High Reward: Business Email Compromise Grows

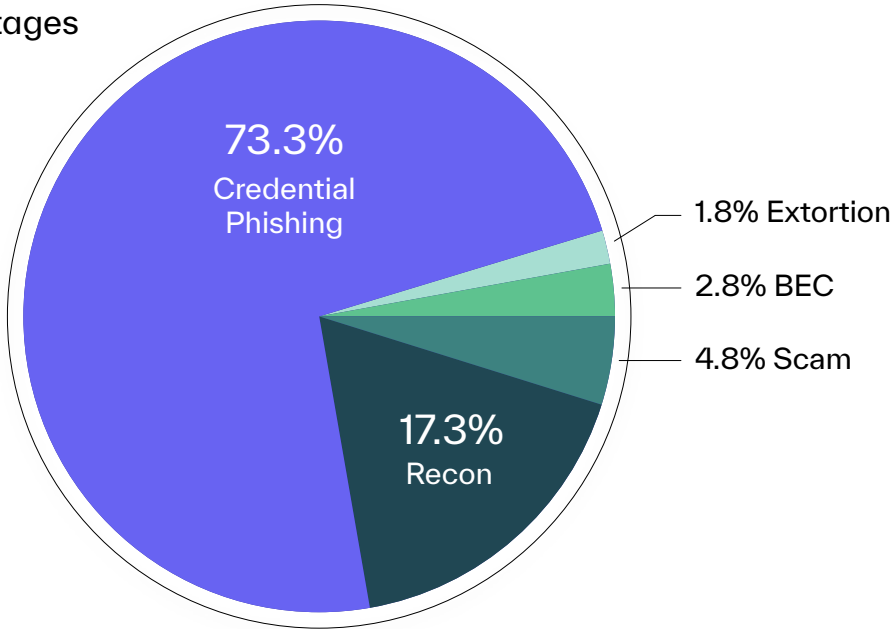
We know from the data released in the 2020 IC3 Internet Crime Report that cybercriminals are moving away from low-impact spray and pray methods and toward more targeted attacks. It appears that 2021 will be no different.

## Credential Phishing and BEC Attacks Increase

Our new data shows a substantial increase in credential phishing and business email compromise attacks, as attackers move away from reconnaissance. In fact, credential phishing continues to make up a growing share of advanced attacks, from 66% of advanced attacks in Q4 2020 to over 73% of attacks in Q2 2021.



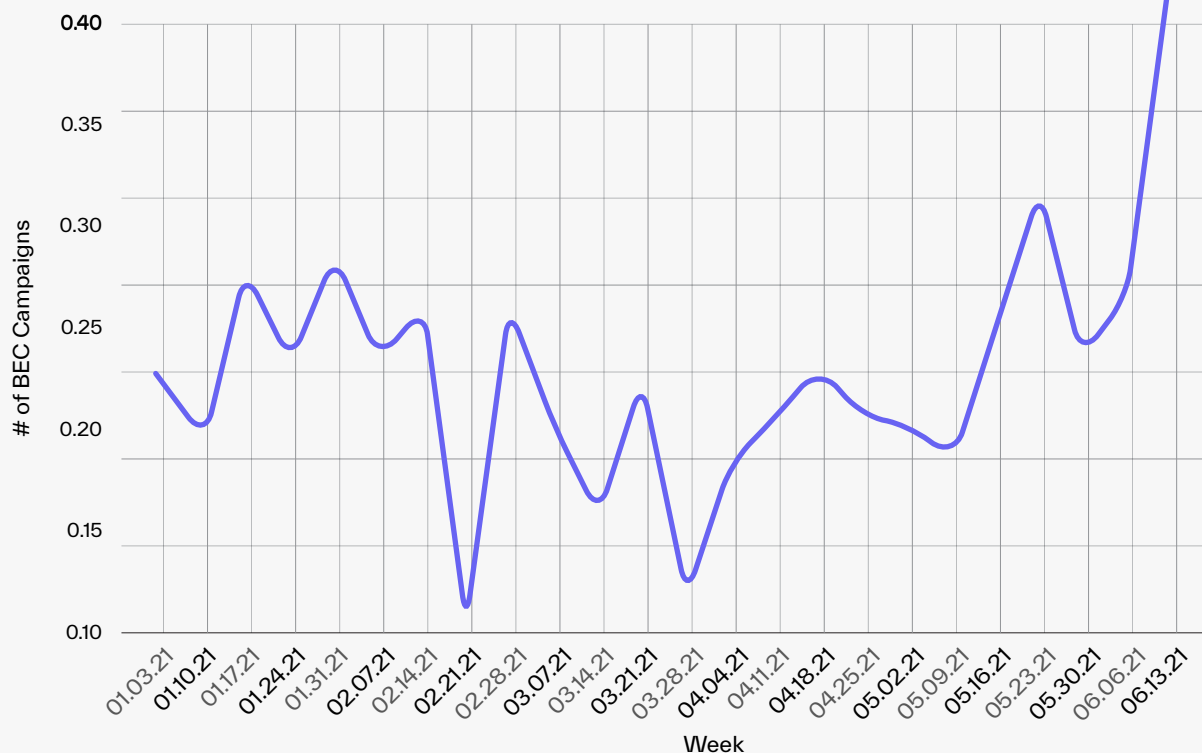
Q2 Advanced Attack Percentages



We also saw an increase in the percentage of business email compromise attacks, rising from 2.3% at the end of 2020, to 2.8% this quarter. While BEC attacks make up only a small percentage of all advanced attacks, they are especially concerning because they require impersonation of an employee to establish rapport with the victim and convince them to engage in actions such as paying fake invoices, buying gift cards, or sending sensitive data. This upward trend has continued since we started tracking BEC attacks in late 2019—an unsettling fact given that BEC is highly targeted, very sophisticated, and tends to land larger payouts.

After a relatively slow start to the year with a median of only .2 campaigns per 1,000 mailboxes, we saw a significant rise in attacks as threat actors came back from their winter holiday. It picked up in the spring, before spiking in mid-June, doubling in attack numbers and hitting its peak of .41 campaigns.

### Median Weekly BEC Campaigns per 1,000 Mailboxes



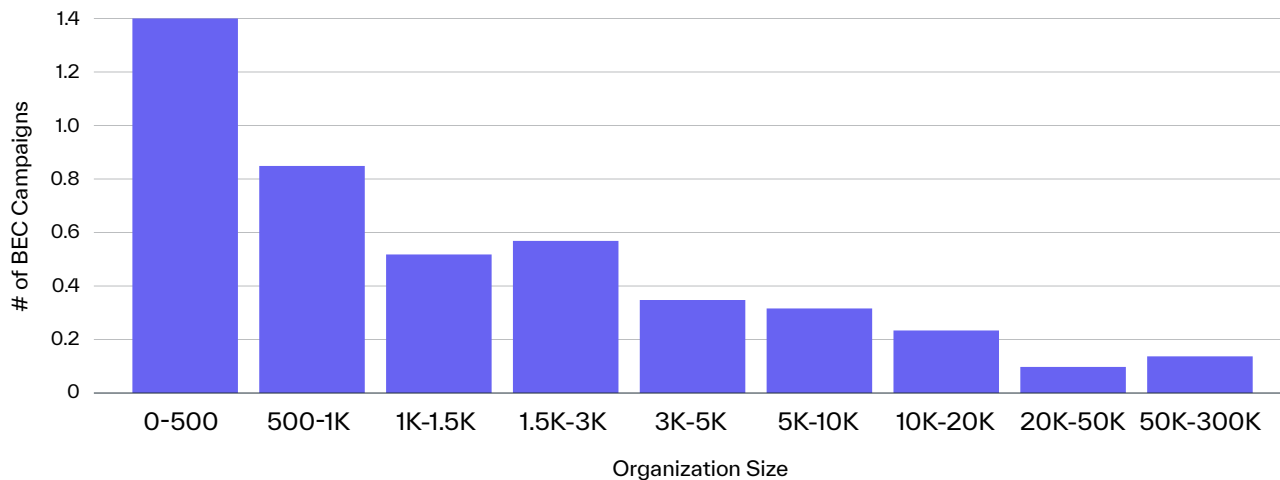
While we expect some fluctuation in attack volume week-over-week, the fact that it doubled over the half indicates the sheer volume of the BEC problem—and the fact that it won't be going away anytime soon.

And for those who believe that .41 campaigns is nothing to be concerned about—after all, that's still less than one BEC campaign a week—it's important to remember that we're tracking BEC data by campaign rather than by attack. This means that one campaign could be sent to 500 employees, giving all 500 people the opportunity to interact with that email.

## Size Matters, At Least for BEC

It's logical to think that larger organizations receive more BEC attacks, but the data states otherwise. The weekly BEC attack rate—or the number of campaigns per 1,000 mailboxes—is highest for small organizations and then drops continuously as organization size increases. In fact, the median number of campaigns per 1,000 mailboxes is 1.4 for companies with less than 500 people, but hovers around 0.1 for organizations over 20,000 employees. This pattern where the number of BEC attacks does not necessarily grow alongside the size of the organization likely indicates that attackers are targeting specific roles—something we expect to see with business email compromise.

### Median Weekly BEC Campaigns per 1,000 Mailboxes by Organization Size



For example, there is only one Chief Financial Officer at each organization, no matter the size. If cybercriminals are targeting only that role, we would expect to see this exact trend where attack numbers do not rise as the number of employees increases.

The good news for small organizations is that while they do receive more BEC attacks per employee, they are less likely to receive attacks on a consistent basis. Organizations under 500 employees have only a 42% probability of receiving a BEC attack each week, but that probability drastically increases once employee size grows.

Those organizations in the 500-5,000 employee range have a 60-70% chance of receiving a BEC attack each week, and that number increases again for organizations from 5,000 to 50,000—each with a 79-85% chance of receiving a BEC attack.



Organizations under 500 employees receive

1.4

BEC campaigns per week

But while size may matter for BEC attacks, the same does not necessarily hold true for credential phishing –the most popular type of attack by sheer volume. In fact, nearly all companies receive a phishing attack each week, regardless of company size.

Smaller organizations under 500 employees have only a 92% chance of receiving an attack, but the data doesn't vary much after that. All larger organizations have at least a 95% chance of receiving a credential phishing message on any given week, showcasing the need for a solution to block these emails before they reach employee inboxes.

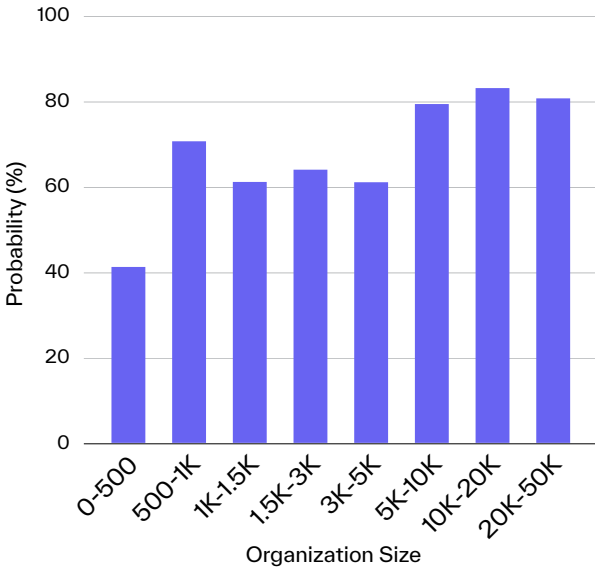


Organizations over 5,000 employees receive a median of

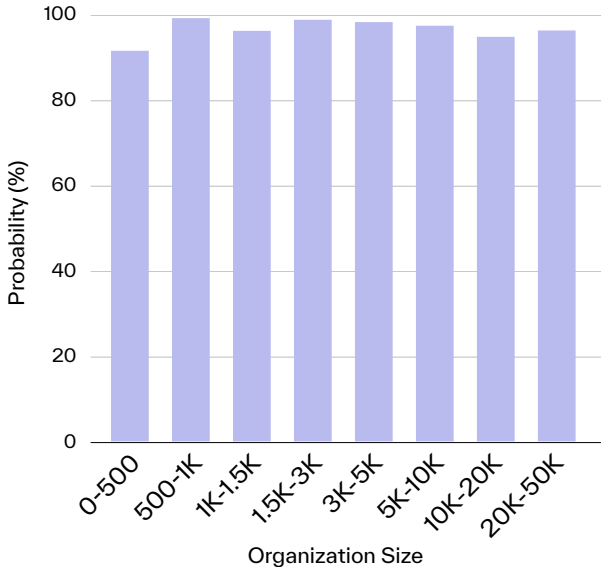
# 96

credential phishing attacks per week

Average Weekly Probability of Receiving a **BEC Attack** by Organization Size



Average Weekly Probability of Receiving a **Credential Phishing Attack** by Organization Size



Organizations with fewer than 5,000 employees see a median of 16 phishing campaigns per week, with larger organizations receiving a median of 96 attacks. The largest organization sees an average of 2,182 BEC campaigns per week.

## Education and Religious Organizations Targeted Most

Examining BEC attack trends across industries provides additional insight into where volume increases are occurring, and which industries should be particularly cautious moving forward.

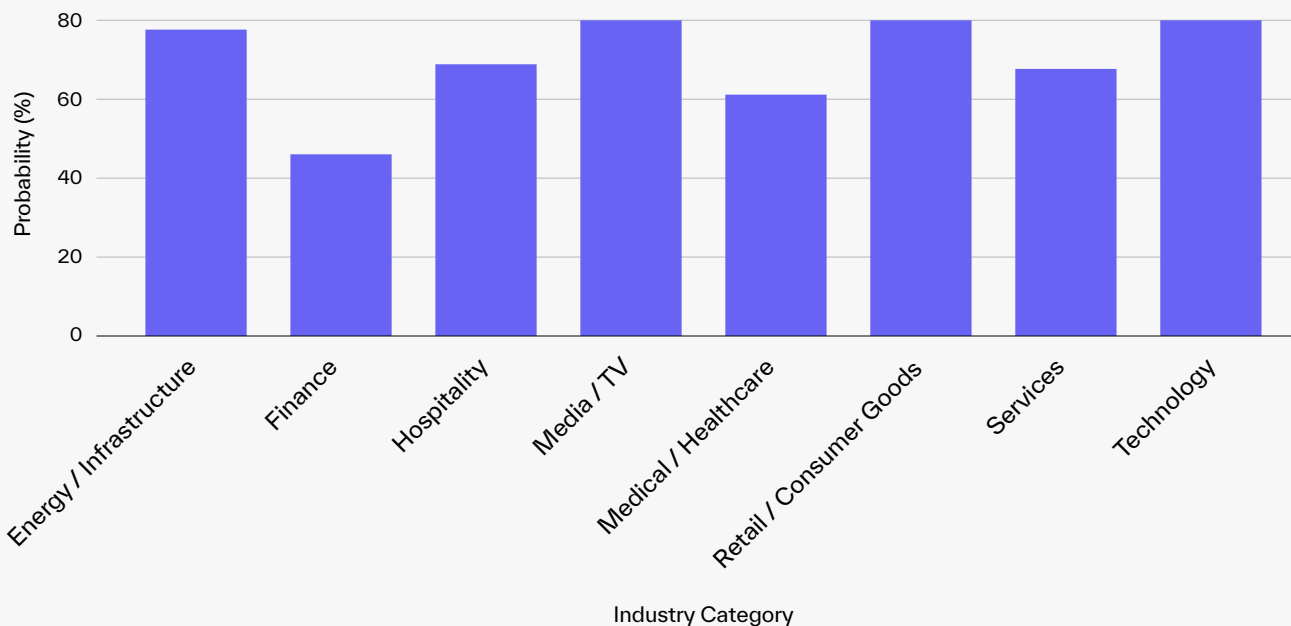
When it comes to probability of attack each week, education and religious organizations are most likely to be targeted with an 86% chance of attack. Multiple other industries tie for second with an 80% probability of attack—or four attacks every five weeks—as BEC actors target retail and consumer goods companies, technology corporations, and media and television organizations.



# 80%

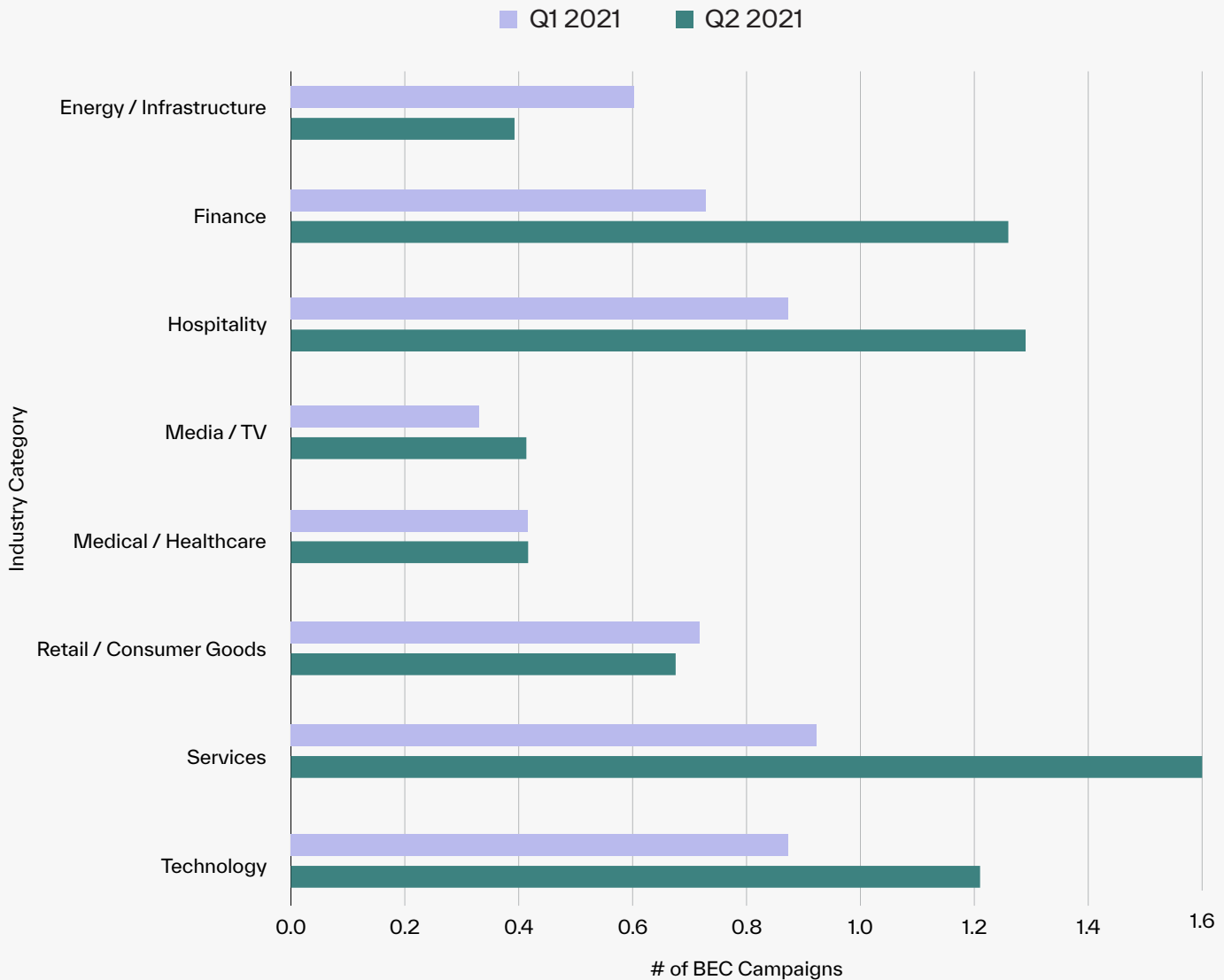
80% probability of attack each week for retail and consumer goods, technology, and media and television companies

## Average Weekly Probability of Receiving a BEC Attack by Industry



In an interesting turn, finance—one industry that we expect to be regularly attacked—had only a 50% chance of receiving a BEC attack on a weekly basis. Nonetheless, attacks are still hitting rapidly, nearly doubling in number over the last quarter.

# Average Weekly BEC Campaigns per 1,000 Mailboxes




This dramatic increase holds true for the hospitality sector and the services industry as well, with technology companies also seeing a significant increase in activity. And despite being most likely to be attacked, energy/infrastructure and retail/consumer goods both saw their actual attack numbers drop this quarter—a refreshing change after previous quarterly increases.

## Guess Who? Surge in Known Impersonation

The success of BEC has much to do with the impersonation of known individuals—typically a trusted executive, colleague, or vendor. In fact, not much has changed over the past three quarters when it comes to employee and VIP impersonation, as cybercriminals continue to take advantage of unsuspecting employees.

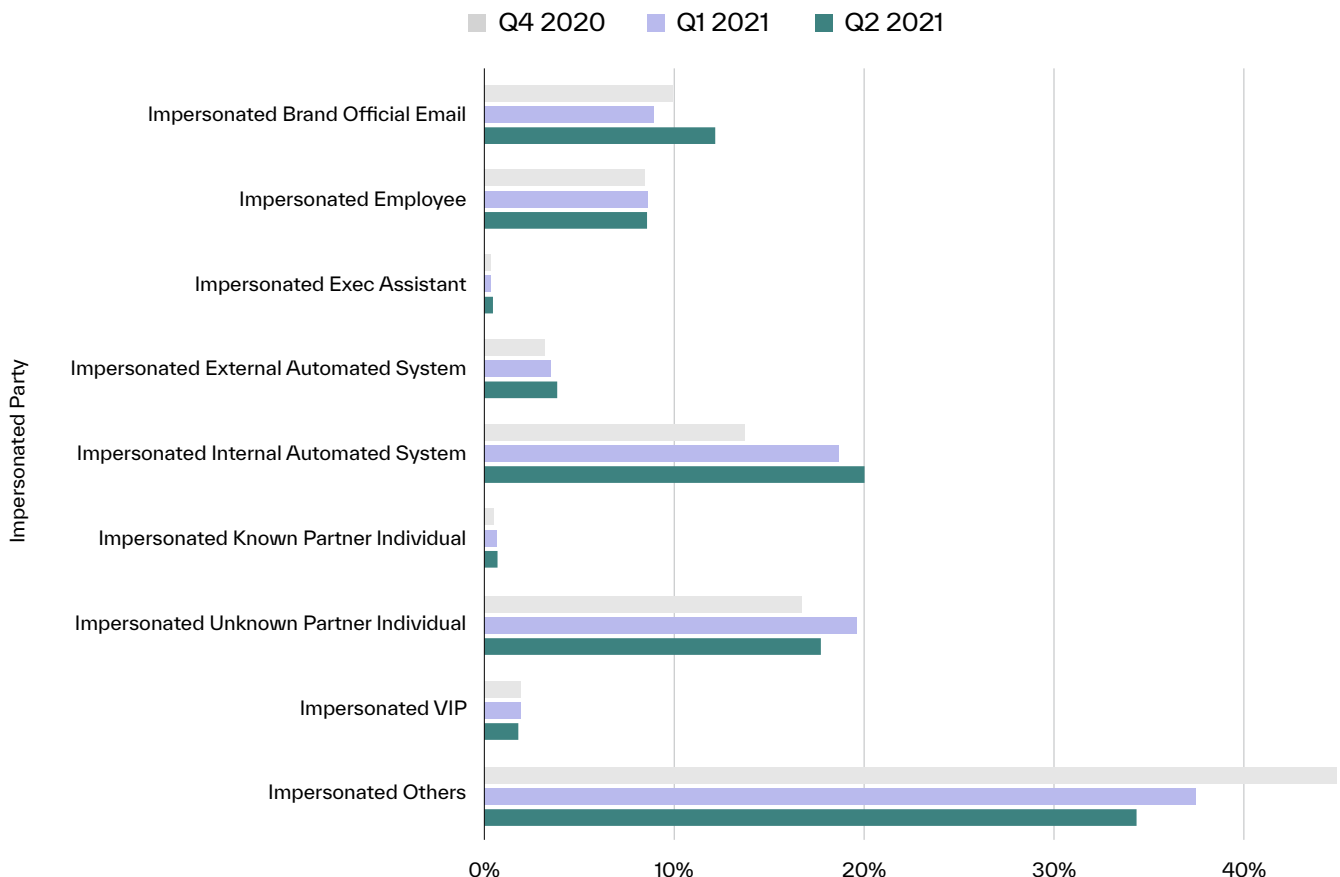
That said, we've seen a significant decrease in the number of attacks that are impersonating random individuals, as those attacks dropped from 45% to 34% of all BEC attacks over the past two quarters. Where we did see the biggest increase is in impersonation of official brands and internal automated systems.



# 46%

increase in impersonated internal automated systems

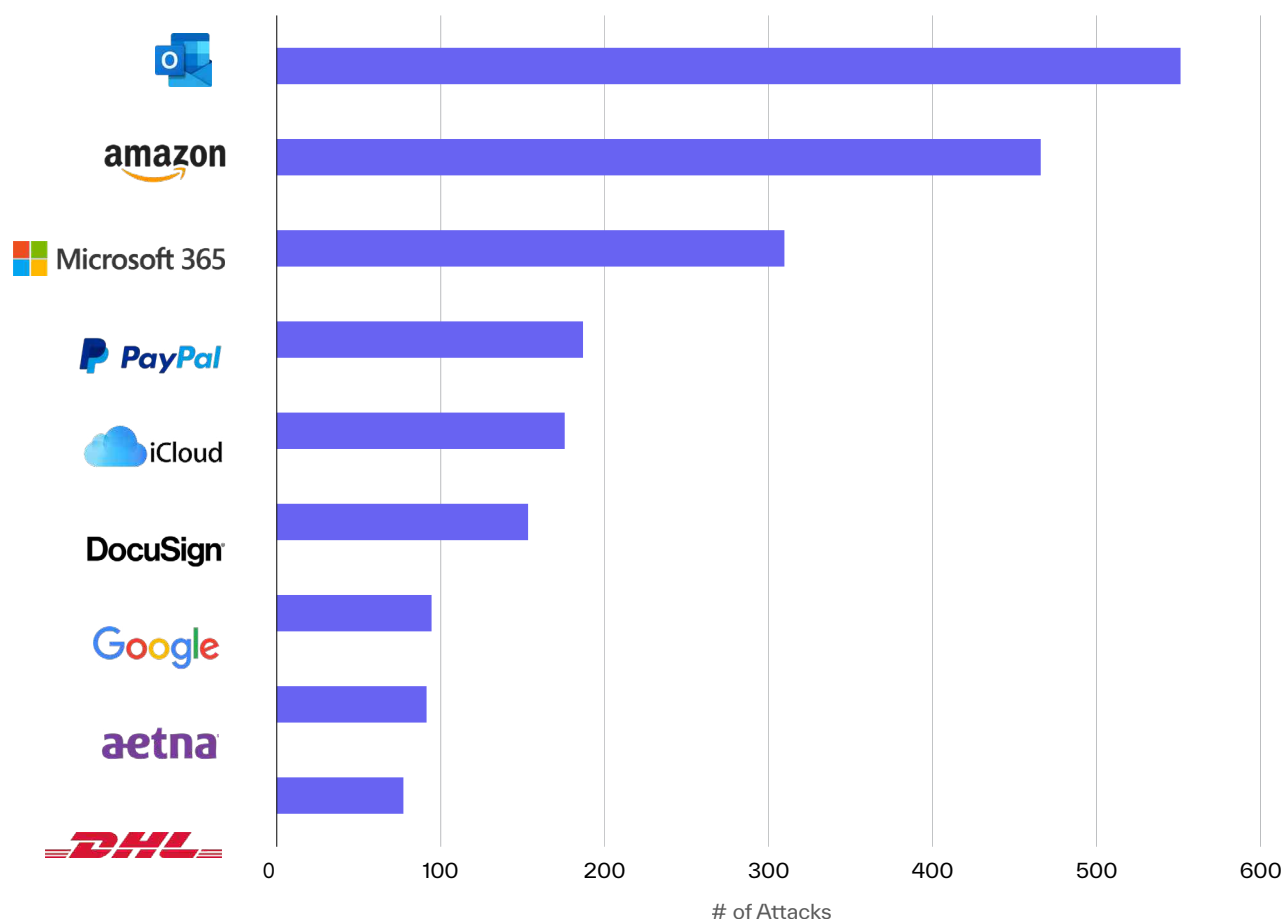
## Quarterly BEC Campaigns Percentages by Impersonated Party



For those brands who were used to run BEC attacks, Microsoft Outlook won the top spot—unsurprising given that many threat actors wish to gain access to Outlook accounts. The easiest way to do so is to impersonate the brand and they did so with over 500 separate BEC campaigns over the twelve weeks between April and June.

Following Microsoft, we saw over 450 campaigns impersonating Amazon, and then another 300 impersonating various Microsoft programs. Other significant impersonations include PayPal, iCloud, DocuSign, and Google—all of which can and are used for business purposes.

### Number of BEC Campaigns by Impersonated Brand



Perhaps the most interesting development over the last few quarters is the drop in impersonation for shipping services. DHL was the most impersonated brand in late 2020, but DHL impersonation campaigns dropped 68% over the last few months, with only 75 campaigns sent this quarter.



When it comes to internal impersonations, there was a 46% increase in spoofs of automated systems, with emails typically coming from aliases like IT Support or IT Help Desk. These generic emails encourage people to download additional software, click on a link, or enter information into an external website. Each method creates an opportunity for cybercriminals to gain access to internal accounts or organizational systems, from which they can launch further attacks.

In this example stopped by Abnormal, a threat actor has impersonated the internal IT system, hoping to trick unsuspecting employees into clicking on the link to update their VPN. Once

they click the link and enter their password, that cybercriminal has access to their entire account, and potentially any others that use the same username and password.

As more organizations and employees become aware of BEC attacks impersonating their executives and coworkers, cybercriminals are changing their tactics. In a remote-first world where millions of people are still working from home, this system-based impersonation seems to be working—at least for now.



Subject: [VPN] configuration secured link

Sender: remote\_access\_vpn@ [redacted] <57e13c35476e47f78c2812ee23f4737b@ [redacted]>

Recipient: Emily Whitaker <EWhitaker@[redacted]>

To: Emily Whitaker <EWhitaker@[redacted]>

Apr 3rd 10:52 AM EDT

---

New VPN configuration home access is now required.

[http://portal.remoteaccess.\[redacted\]/vpnconfiguration](http://portal.remoteaccess.[redacted]/vpnconfiguration)

Login with your email and password.

Thanks,

IT Support

[redacted]

# Advanced Email Threats Will Continue to Increase

Advanced email attacks like credential phishing, business email compromise, and vendor email compromise are increasing in popularity, in large part due to their success. Because they typically lack traditional indicators of compromise, they are difficult to detect and even harder to prevent. Once they reach inboxes, the last line of defense is your employees, who are prone to error when confronted with a socially-engineered email designed to take advantage of their emotions. And when attackers have access to full email accounts through brute force attacks, they have the keys to the entire cloud kingdom in their hands.

While we anticipate that these attacks will continue to increase, both in volume and in repercussions, they can be stopped. With the right solution—one focused on understanding the normal to prevent the abnormal—you can ensure that your employees, and your entire organization, are protected from the most dangerous email threats.



Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially-engineered and never-seen-before email attacks that evade traditional secure email gateways. Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, ransomware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

To stop account takeovers and other advanced attacks at your organization, visit:

Follow us on Twitter: