BUSINESS EMAIL COMPROMISE
The Imposters Among Us

Threat Spotlight
Supplier invoicing fraud

Customer Spotlight
How Stagecoach is fighting imposter blindness

Point of View
Defending against email fraud
CONTENTS

THREAT SPOTLIGHT

P5 The Cost of BEC and EAC
P9 Understanding BEC Scams: Payroll Diversion
P13 Understanding BEC & EAC Attacks: Gift Card Scams
P16 Understanding BEC Scams: Supplier Invoicing Fraud
P22 TA2519 AKA TMT Group Arrests and New Activity
P24 You’ve Got BEC!

CUSTOMER SPOTLIGHT

P28 The Next Generation of Targeted BEC Attacks: How Stagecoach is fighting imposter Blindness

PO I NT OF VIEW

P31 Building Trust in your Business Email Communication
P32 Unmasking BEC and EAC
P38 What to Do (and what not to do) to Fight BEC and EAC
P40 Enabling your users to recognise and avoid BEC Attacks
P42 What is DMARC?
P46 The Modern CISO’s Guide to Stopping BEC and EAC
P50 Making the most of your Proofpoint Partnership

Magazine Contributors

Simon Taylor
Information Security Manager, Stagecoach

Robert Holmes
VP & GM, Products, Proofpoint

Vincent Merlin
VP Marketing APJ & EMEA, Proofpoint

Adenike Cosgrove
Director, International Product Marketing, Proofpoint

Andrew Rose
Resident CISO, Proofpoint

Rebecca Cleveland
Senior Manager, Customer Marketing, Proofpoint

Matt Cooke
Senior Product Marketing Manager, EMEA, Proofpoint

Cover Illustration
Peter Greenwood - Folio Art

Graphic Design
Chris Cooling - Broadgate Creative

NEW PERIMETERS
Here at Proofpoint, we’re proud of the community we’re building and the influence we, together, continue to have on cybersecurity. The industry now speaks our language. Terminology such as ‘People Centric Security’ and ‘Very Attacked People’ is widely recognized, and that’s your success as much as it is ours.

Following last September’s virtual ‘Protect’ customer conference, we wanted to introduce more ways to connect and bring value to our 7,100+ enterprise and 110 thousand SMB customers around the world. I believe this regular magazine is the best way to do that.

Printed sustainability with great care, I hope that ‘New Perimeters’ will serve as an antidote to the bitesize, lightning speed of the modern world – though a digital version is available if you prefer.

Whether you’re reading this online or in print, you’ll have seen our striking front cover. We commissioned world-famous illustrator Peter Greenwood, who designed the visuals for many editions of Time magazine, to create something worthy of marking our first edition.

Behind the front cover, we’re shining a light on the biggest issues in cybersecurity, covering the latest threat actors, the techniques they are using to target your people, and the controls we can leverage to stay one step ahead of the criminals.

We open our inaugural issue with what has been dubbed one of cybersecurity’s “most expensive threats”: Business Email Compromise (BEC).

The FBI’s Internet Crime Complaint Center (IC3) reports that BEC cost organizations $1.7bn last year – accounting for over half of all cybercrime losses. The insurance company AIG reported that BEC overtook ransomware and data breaches in cyber-insurance claims and that BEC-related cyber-insurance claims accounted for nearly a quarter of all claims in the EMEA region in 2019.

And attacks are on the rise, moving Gartner to list several mitigating steps in its ‘top ten security projects for 2021’.

We look at the most effective ways to defend against common BEC/EAC tactics (pg. 32), roundup some of the biggest and boldest attacks in the wild (pg. 24) and take a look at how our customer Stagecoach is fighting imposter blindness (pg. 28).

I trust you’ll find this issue packed with valuable content to help you bolster your defenses and hope it can start a dialogue around the most advantageous cyber strategies.

I invite you to continue the conversation with a virtual briefing with our executive team, a meeting with our resident CISO, or a Customer Business Review (details on how to request these on pg.50).

Finally, this is your magazine. We would love to hear your suggestions on how we can improve it, and the kinds of topics you’d like us to cover in future editions. Email rcleveland@proofpoint.com to let me know your thoughts.

REBECCA CLEVELAND
Customer Marketing Manager
Proofpoint
The Cost of BEC and EAC

Business Email Compromise (BEC) and Email Account Compromise (EAC) afflict businesses of all sizes across every industry. More money is lost to this type of attack than any other cybercriminal activity. The FBI reported that from June 2016 to June 2019, companies reported $26.2B in losses. And in 2019 alone, BEC scams accounted for more than half of all cybercrime losses — an estimated $1.77B. The average loss per BEC incident in 2019 was $74,723.

BEC/EAC are People-Centric Threats

BEC/EAC attacks rely on tricking a person into believing the criminal is someone they are not. What makes BEC/EAC attacks so effective at evading traditional email defenses is the fact that they don’t utilize traditional malware-based methods. Instead BEC/EAC attacks are crafted by people to deceive people.

Criminals use a variety of credential phishing, account compromise, identity deception and social engineering techniques to trick people into giving up confidential information or activate an unauthorized transfer of funds.

$74,723

Average loss per BEC incident in 2019

By Robert Holmes
VP and GM, Products
Proofpoint
Types of BEC and EAC Attacks

While the end goal of BEC/EAC attacks are the same — to steal your organization’s money — there are several different attack types or scams.

Here are the four current BEC/EAC attack types:

1. Payroll diversion:
   In a payroll diversion scam, a criminal sends a fraudulent email to HR or payroll employees requesting to change or update direct deposit information from a legitimate employee bank account to the fraudster’s account or a pre-paid card account. The latest FBI data shows that the dollars lost as a result of payroll diversion scams have increased more than 815% between Jan 1, 2018 and Jun 30, 2019.

2. Gift card scam:
   In this attack, the criminal poses as a supervisor or employee with authority and sends an urgent email requesting assistance to purchase gift cards for staff or clients. The email asks for serial numbers so s/he can email them out right away.

3. Supplier invoicing:
   When implementing this attack type, a criminal will impersonate a vendor your company regularly does business with and send a request to update bank information for payment of outstanding invoices. When you consider the large dollar amounts often associated with supplier invoices, this type of scam leads to the biggest losses.

4. M&A fraud:
   M&A fraud involves the fraudster pretending to be an executive of the victim company (either using impersonation or a compromised account). He or she requests that funds be transferred to a given 3rd party. For example, the email might say something like “We’re buying Company X and we need to make a payment or we risk losing the deal.”
Three Warning Signs of a Business Email Compromise (BEC) Attack

Time Sensitive and Covert Requests
When executing BEC attacks, attackers often try to elicit an emotional response from their targets. Commonly spoofing the identity of an executive or high-level manager within their target’s department, these messages will request ‘last minute changes’ or ‘personal favors’, relying on the targeted employee’s desire to help their boss or a company executive. As these types of attacks are becoming more and more refined, these requests will also come at the end of the workday and week, putting pressure on targeted employees to finish requests before the end of business hours.

Messages from Personal Mailboxes and Mobile
Another common tactic that threat actors may exploit to get around existing defenses is spoofing an executive, employee or supply chain partner’s personal mail address, such as a Gmail or Yahoo account. To give off the impression of a last-minute request, these messages can say something to the tune of “Hi <employee>., I had to leave the office on my way to the airport, but we just received a message from <critical supply chain partner> and we need to change their routing information by EOD. Can you assist while I’m traveling?” with a stock signature giving the impression it was sent from their mobile phone.

Direct Messages from Supply Chain Partners
An increasingly frequent tactic in BEC and Email Account Compromise (EAC) attacks is the use of supplier identities, whether spoofed or through compromised user accounts. Taking on the identities of supply chain partners is very effective for threat actors, circumventing any internal processes, and taking on an identity that the receiver is not as familiar with as a fellow employee. Messages that use these tactics can be identified by their direct nature - an employee may receive a request directly from the supplier to suddenly change payment routing or shipping information without going through the typical process and the proper paperwork.
TO BETTER PROTECT AGAINST THESE KINDS OF SCAMS, IT IS CRITICAL THAT SECURITY SOLUTIONS ARE CAPABLE OF USING MORE THAN JUST A PRE-DEFINED LIST OF EXECUTIVES TO DETECT IMPOSTOR EMAIL.

Four Key BEC/EAC Tactics

Proofpoint detects, analyzes and blocks millions of these BEC/EAC attacks every day. In doing so, we've observed that across each BEC/EAC attack type, fraudsters leverage four key tactics:

**Impersonation** in email happens by exploiting technical and human vulnerabilities. Not only are people wired to ignore subtle textual differences, thereby making lookalike domains a useful tool in BEC/EAC attacks, but also Simple Mail Transfer Protocol (SMTP) is, by its own admission, “inherently insecure” and therefore prone to both Display Name and domain spoofing.

**Compromised accounts** are priceless to threat actors. They afford them the ability to conduct extensive reconnaissance, and fraudulent emails sent from that account will be almost indistinguishable from legitimate emails. They will bear the same Display Name and email address; they will be sent from the same mail server; and they will pass all the email authentication protocols (SPF, DKIM and DMARC). Accounts are compromised using stolen credentials (often obtained via phishing), 3rd party application auth tokens or brute force attacks.

While every BEC/EAC attack can be mapped to at least one of the four tactics, we are seeing more and more attacks that span multiple tactics in a single attempt to steal money. For example:

- The target company’s domain is spoofed (employee impersonation) to steal credentials that gives the threat actor access to an employee’s account (employee account compromise) from which they can then conduct payroll diversion or gift carding scams.
- Cybercriminals use stolen credentials to access the account of a supplier (supplier account compromise) from which they initiate or intercept discussions with the target company’s Accounts Payable team before switching the conversation (very often by introducing the new email addresses into the Cc field) to a lookalike domain of that supplier (supplier impersonation) from which a demand for payment is made.

Siloed Defense Won’t Solve the Multifaceted BEC/EAC Problem

Because cybercriminals employ multiple tactics and combinations of impersonation and account compromise, defending against one or two of these tactics is insufficient to address the threat as a whole.

And legacy email security providers that rely only on reputation and malware sandboxing won’t help when good/legitimate email accounts are being used to socially engineer the theft of money by sending payload-less (e.g. text only) messages.

Your email security solution should invest in detecting and stopping impersonation, account compromise, credential phishing and social engineering. And let’s not forget about training your users to spot and report on these attacks/tactics too.

To build such a solution, email security providers need access to the right data sources: email traffic, cloud account activity, user data and domain data. With that information, threat analysts and machine learning models can detect the use of multiple tactics in these types of attacks and implement integrated, adaptive controls across the attack surface of email, cloud accounts and people.
UNDESTANDING BEC SCAMS

Payroll Diversion

What Are BEC Payroll Diversion Scams

BEC payroll diversion scams are similar to other BEC attacks by relying on impersonation and social engineering to convince the target victim to send money to the attackers. In this case, the attackers target the payroll process of a company or organization and attempt to redirect legitimate payroll payments from their intended destination accounts to accounts under the attacker’s control. This is different to gift card scams in that the employee being impersonated is typically not a VIP, whereas in a gift card attack the impersonated employee is typically a CEO or other high-level executive. To better protect against these kinds of scams, it is critical that security solutions are capable of using more than just a pre-defined list of executives to detect impostor email.

BEC payroll diversion scams are by necessity very focused in their targeting. To succeed, these scams must correctly identify someone in the HR or payroll department to make changes to an employee’s direct deposit information.

To understand the scope of the problem, the FBI’s IC3 reported that the dollar loss associated with payroll diversion increased 815% between Jan 1, 2018 and June 30, 2019. Proofpoint has seen and blocked more than 35,000 payroll diversion scams protecting US$2.2 M per day in the first half of 2020. Our research shows that the Monday and Tuesday are the most popular days of the week for these scams, the second and last weeks of the month are the most popular weeks for these scams, and “Direct Deposit” is the most popular lure.
How BEC Payroll Diversion Scams Work

The crux of a successful BEC payroll diversion attack is the redirection of payroll funds from their intended legitimate destination to an account under the attacker’s control. The illustration above shows the steps in a typical BEC payroll diversion attack.

BEC payroll diversion scams rely heavily on intelligence gathering. A successful BEC payroll diversion attack requires the attackers identify the correct target for their attack and demonstrate credible familiarity with the payroll process so as not to arouse suspicion. Both of these require the attackers invest time and energy into extensive reconnaissance and intelligence gathering prior to launching their attack.

Unfortunately, this type of intelligence can be gathered from publicly available sources such as a company’s website or alternatively LinkedIn.

Like many BEC attacks, payroll diversion scams rely heavily on a combination of impersonation, social engineering, and urgency.

When attackers launch a BEC payroll diversion attack, they try to convince someone at the target company or organization who can make changes to the payroll disbursement system that they are the employee they claim to be or someone authorized by the employee to make changes to their payroll information. In these exchanges, they will seek to convince their target to change the destination of payroll disbursements for the employee they’re impersonating to an account under their control. Depending on the sophistication of the threat actor, they may include a reason why reverting to a paper check sent in the physical mail is not possible.

This is used as a tactic to circumvent secondary financial controls for account information updates.

In a successful attack, the target victim will make the changes and the issue will be closed. Ideally for the attacker, the issue will be closed with little notice by the target victim. In this case, making the attack look as much “business as usual” as possible is key to a successful attack.

If the attack is successful and the changes are made, the final step is for the money to be transferred into an account under the attacker’s control at which point the attacker can retrieve the funds. This is important to note because the attack may take up to two weeks to incur financial loss after the payment instructions have been successfully updated. It’s worth noting that because of this two week delay, BEC payroll diversion attackers tend to prefer to levy their scams in the second or fourth week of the month. The FBI notes that many times the target accounts are actually pre-paid card accounts, which enables the attackers to quickly utilize the diverted funds.
How Proofpoint Protects Against BEC/EAC Payroll Diversion Scams

We provide a people-centric multi-layered solution to help organizations protect against payroll diversion scams.

First, as part of Proofpoint Email Protection, Impostor Classifier dynamically analyzes a wide range of message attributes, including the sender/receiver relationship, header information, domain, and message body to determine if a message is a BEC message. Proofpoint Email Protection delivers unique value in the following ways:

- Analyzing and blocking 15,000 BEC messages per day globally gives our customers an unfair advantage as Impostor Classifier has observed countless payroll diversion attacks to compare message body contents against.

- Being in mail flow allows Proofpoint’s BEC detectors to understand the sender/target relationship, which is a critical detection ingredient.

- Detecting impostor email isn’t limited to a pre-defined list of executives or VIPs. Because payroll diversion attacks do not typically target VIPs, preventing these attacks requires inspecting all messages. Impostor Classifier inspects all messages not just messages for VIPs.
Second, in the event there isn’t enough data to identify a message as an impostor message, we enable administrators to alert the user that the message is suspicious using email warning tags. These visual cues help users take extra precautions with the email in question. In addition to the impersonated sender alert, our email warning tags support other situations including external sender, new sender and newly registered domains.

Last, but not least, we provide security awareness training to help organizations turn users into part of their defense. Because BEC payroll diversion scams rely on social engineering to trick end users, it’s critical to train employees. As a Proofpoint customer, you can use BEC/EAC threat data to tailor that training to your specific threats. For example, you can plan training about BEC payroll diversion scams for the individuals involved in your payroll business process during the second and fourth week of the month if that’s borne out by your specific threat data. Not only can we help you teach users to spot BEC payroll diversion scams, but we can also enable those users to report those messages as suspicious and automate the investigation and remediation of those reported messages to their internal abuse mailbox.

Are You Protected?

BEC payroll diversion scams are a growing form of BEC attacks out there. However, these scams are also some of the most lucrative with Proofpoint stopping an estimated $2.2M per day in BEC payroll diversion scams. These scams are also highly targeted and require detailed knowledge to be successful. These two points are good news for defenders because it provides clear direction on what you can do to help better protect against these scams. One, you can ensure that people who have the ability to change payroll disbursement information are aware of the risks and receive additional training and protection. Two, you can work to ensure that critical information regarding payroll policies and procedures are not publicly available in a way that can facilitate these kinds of scams.
What Are BEC/EAC Gift Card Scams?

BEC/EAC gift card scams are similar to other BEC/EAC attacks by relying on impersonation and social engineering to convince the target victim to send money to the attackers. In this case, though, the attackers try to convince the target victim to send money to them using popular retail gift cards rather than through wire transfers. In gift card scams, the attackers will frequently impersonate the CEO or other high-level executive in the business as part of the scam.

Attackers abuse gift cards in BEC/EAC attacks because it is a quick and easy way to for them to get money from their targeted victims: the victims don’t have to navigate complicated wire transfer instructions, they just go and purchase gift cards from well-known, recognized and trusted retailers.

Abusing gift cards like this is also a quick, easy and simple way for attackers to effectively launder stolen money. Instead of receiving the stolen money directly, the attackers receive the money by way of the retailer whom the targeted victim purchased the gift card from.

Using gift cards has another benefit for attackers: potential victims may not be aware of the role of gift cards in BEC/EAC attacks because wire transfers are more commonly been associated with BEC/EAC attacks. With potential victims being less wary of requests for gift cards than they might be for wire transfer requests, they may be more likely to fall for this particular type of BEC/EAC attack, especially when the scam email is impersonating the CEO or other high-level executive.

Abusing gift cards like this is not something that’s new or unique to BEC/EAC attacks. Cybercriminals have been effectively using gift cards as a payment and laundering method for a number of years in other types of attacks. BEC/EAC attackers have picked up this tactic because it has worked well in other attacks and they have adopted it aggressively for their use. The FBI’s IC3 reported* 1,164 gift card attack complaints accounting for US$1,021,919 in losses between January 1st, 2017 and August 31st, 2018, representing a 1,240% increase in these kinds of complaints. They noted that over 90% of these incidents reported in the five-month period between March and August 2018 alone.
How BEC/EAC Gift Card Scams Work

BEC/EAC gift card scams are very straightforward in their approach. Like other types of BEC/EAC attacks, the attackers impersonate a trusted person like the CEO, send information to the targeted victim as that impersonated party explaining how much money needs to be transferred, why it has to be transferred and how it has to be transferred. In the case of gift card scams the “how” is by purchasing retail gift cards and sending the information on to the attackers. The illustration above shows the sequence of a BEC/EAC gift card attack.

Like all BEC/EAC attacks, gift card scams rely heavily on a combination of both authority and urgency. The illustration on the next page shows an example of this with a BEC/EAC attack email sent by an attacker impersonating the CEO of the company to an employee of the company. This email is the first of a series of exchanges that will culminate in the attacker giving the targeted victim instructions on what gift cards to purchase and how to send the relevant information to the attacker so they can cash those gift cards out.

CEO impersonation like you see in this example is a common tactic. Proofpoint research has shown that since March 2020, over 7,000 CEOs or other executives have been impersonated. In 2020 over 50% of Proofpoint customers have had some VIP impersonated. Looking at the last 90 days, on average a CEO specifically has been impersonated 102 times.
I’m in the middle of something and I need your assistance remotely. I need you to run an errand for me at any nearest Walmart, Target or CVS around you. I need some gift cards to send out to a vendor today. Can you make this happen? If yes, let me know so I can advise the quantity and denomination. I will reimburse you tomorrow.

Ron, What can I help you with?

Wednesday, 2 September 2020, 19:22 +0100 Brenda wrote:

How Proofpoint Protects Against BEC/EAC Gift Card Scams

First, as part of Proofpoint Email Protection, Imposter Classifier dynamically analyzes a wide range of message attributes, including the sender/receiver relationship, header information, domain, and message body to determine if a message is an imposter message. Proofpoint Email Protection delivers unique value to our customers in the following ways:

- Being in mail flow allows Proofpoint’s BEC detectors to understand the sender/target relationship, which is a critical detection ingredient.
- Analyzing and blocking 15,000 BEC messages per day globally gives each Proofpoint customer an unfair advantage as Imposter Classifier has a large corpus of prior BEC attacks to compare message body contents against.
- Configuring arbitrary combinations of VIP display names (e.g. Michael or Mike) doesn’t force customers to choose where to apply protections against display name impersonation attacks.

Second, in the event there isn’t enough data to identify a message as an imposter message, Proofpoint alerts the user that the message is suspicious using email warning tags. These visual cues help users take extra precautions with the email in question. In addition to the impersonated sender alert, Proofpoint’s email warning tags support other situations including external sender, new sender and newly registered domains.

Last, but not least, Proofpoint provides security awareness training to help our customers turn their users into part of their defense. Because BEC/EAC gift card scams rely on social engineering to trick end users, it’s critical to train employees about gift card scams. Not only can we help our customers teach users to spot BEC/EAC gift card scams, but we can also enable those users to report those messages as suspicious and automate the investigation and remediation of those reported messages.

PROOFPOINT PROVIDES A MULTI-LAYERED SOLUTION TO HELP PROTECT YOUR BUSINESS AGAINST GIFT CARD SCAMS.
What Is BEC Supplier Invoicing Fraud

BEC supplier invoicing scams are sophisticated and complex schemes to steal money by either presenting a fraudulent invoice as legitimate or by re-routing the payment to a bank account controlled by the attacker. When you consider the large dollars associated with supplier invoices, these scams are often the costliest for victim organizations. Proofpoint has stopped multiple supplier invoicing attempts where each incident was millions of dollars.

Similar to gift card scams and payroll diversion scams, supplier invoicing scams rely on social engineering and impersonation to convince the target victim to send money to the attackers. But what sets BEC supplier invoicing scams apart is not just the large dollar amounts often associated with these scams, but also the complex nature of these scams.

While gift card scams are relatively simple, using maybe one email targeting one employee, supplier invoicing scams are more byzantine involving compromise and impersonation of trusted vendors and carried out in multiple stages against multiple individuals and organizations. The impersonation can either be at an account level or at the domain level (e.g. domain lookalikes).
How BEC Supplier Fraud Works

Many of the BEC supplier invoicing attacks Proofpoint has observed indicate that these attacks originate from a legitimate email account that has been compromised. These compromised accounts are highly prized by threat actors. They can conduct extensive reconnaissance and fraudulent emails sent from the compromised account will pass email authentication controls (e.g. DKIM, SPF, DMARC) because they are sent from a legitimate account.

Once a legitimate transaction is identified, the threat actor “thread hijacks” an already in-progress email conversation about the transaction (step 3 in the diagram). Since the attacker’s message is part of an email thread that the target victim reasonably believes to be legitimate, their message has greater credibility. As such requests for bank account changes due to audit or COVID-19 seem more plausible. This believability and trust are key elements of social engineering. By their very nature, thread hijacking attacks are very difficult, if not impossible for users to identify, making this a threat vector where technology countermeasures are particularly needed and useful.

Figure 1: Anatomy of a Supplier Invoicing Fraud Attack
At this stage of the attack, the threat actor pivots to a supplier account impersonation tactic where the attacker inserts an impersonated account in the “reply-to” or “cc” of the email conversation. The impersonated accounts can be a lookalike of the supplier domain (e.g. supp1ier.com instead of supplier.com) or a lookalike of the account (e.g. janedoe[,]supplier[@]mail[,]com instead of jane[,]doe[@]supplier[,]com).

Why do this? The impersonation pivot allows the threat actor to maintain the email conversation with the target when the compromised account has been remediated. In many cases, the email thread continues via the impersonated account. Shifting the conversation to the impersonated account also makes it more difficult for forensics and investigations because you lose the logs in the supplier SEG.

The illustrations opposite show exchanges in a BEC supplier invoicing attack that Proofpoint stopped. The attackers in this particular attack started with the compromised supplier account where the attackers hijacked an existing email thread and utilized the “impersonation reply-to pivot” tactic. They impersonated two separate trusted individuals and targeted two separate individuals in Finance and Accounting roles to try and make the fraud seem legitimate.

In Figure 2 we see an email message from the compromised account of a trusted individual from a supplier hijacking an existing email thread about several legitimate invoices. In this message the attackers are using the trusted individuals actual account and achieving impersonation through control granted by compromising that account.
ATTACKERS WEAVE TOGETHER
IDENTITY DECEPTION,
AUTHORITY, AND URGENCY
WHILE USING TACTICS LIKE
ACCOUNT COMPROMISE AND
IMPERSONATION TO MAKE A
FRAUDULENT BANK ACCOUNT
CHANGE REQUEST SEEM
LEGITIMATE

The fraud is made more credible by the
fact that this second email references the
same invoice numbers as the first email
and both emails have been sent to one
of the target victims. These two emails
reinforce each other and that helps create
a greater sense of legitimacy that the
attackers hope will convince one of the
target victims to respond and take action.

In Figure 4 the attackers have shifted back
to the compromised supplier account
and are requesting a change of bank to
intercept the payment.

It’s also notable that this email is using
both authority and urgency, both common
social engineering tactics in BEC attacks.
Also notable is that the fraudulent emails
are devoid of any malware payload such
as an attachment or URL. There are
no links or attachments for the victims
to click.

Taken as a whole, this shows how
attackers weave together identity
decception, authority, and urgency while
using tactics like account compromise
and impersonation pivot all to make
a fraudulent bank account change
request seem legitimate so that target
will pay the invoices to the threat actor’s
bank account.
How Proofpoint Protects Against BEC/EAC Supplier Invoicing Fraud Scams

PROOFPOINT PROVIDES A MULTI-LAYERED SOLUTION TO HELP ORGANIZATIONS PROTECT AGAINST SUPPLIER INVOICING FRAUD.

First, as part of Proofpoint Email Protection, NexusAI for BEC Detection dynamically analyzes a wide range of message attributes, including header information, domain, and message body to determine if a message is an impostor message. Proofpoint Email Protection delivers unique value to Proofpoint customers in the following ways:

- The Nexus Threat Graph aggregates and correlates trillions of threat data points across email, cloud accounts, domains and more. Threat visibility across multiple attack vectors is a critical element to identify a fraudulent message from a compromised account.
- Analyzing and blocking 15,000 BEC messages per day globally gives each Proofpoint customer an unfair advantage as NexusAI for BEC Detection has a large corpus of prior BEC attacks to compare message body contents against.
- Being in outbound mail flow enables us to understand bi-directional communications and identify whether there’s an established history of communication or whether the message is from someone you’ve never communicated with but is impersonating a supplier.

Second, the Nexus Supplier Risk Explorer continuously maps your supply chain and uncovers what threats they may be sending to your organization. This visibility helps you understand which suppliers are the riskiest and allows you implement adaptive controls to mitigate that risk.

Figure 5: Nexus Supplier Risk Explorer automatically identifies your suppliers and the risks they pose
Third, Proofpoint provides incident responders with reporting to understand what type of BEC attack it is (e.g. invoicing, gift card, payroll) and who received it. This visibility is important for prioritization efforts and informs what actions should be taken. Proofpoint also helps streamline incident response with the ability to automatically find and pull back delivered messages, including forwarded mail and distribution lists.

Last, but not least, Proofpoint provides security awareness training to help organizations turn users into part of their defense. Because BEC supplier invoicing fraud relies on social engineering to trick end users, it’s critical to train employees about BEC supplier invoicing scams. Not only can Proofpoint help organizations teach users to spot BEC supplier invoicing fraud, but we can also enable those users to report those messages as suspicious and automate the investigation and remediation of those reported messages.

Are You Protected?

BEC supplier invoicing scams are not sophisticated in their goals or even their tactics. The goal is simple: convince a target victim a fraudulent invoice is legitimate, so they’ll pay it. The tactics primarily focus on spoofing and account compromise: tactics that are not technically sophisticated.

However, BEC supplier invoicing fraud weaves these tactics together in creative ways which is why BEC supplier invoicing scams continue to be successful. As we see in the example here, the end result of these tactics is a multi-layered fraud that is reasonably, highly credible.
TA2519 AKA TMT Group
Arrests and New Activity

Executive Summary

On November 19th, the Nigeria Police Force in conjunction with Interpol arrested three individuals as ringleaders of a cybercrime syndicate dubbed “TMT Group”. The TMT Group was reportedly leveraging commercial remote access trojans such as Agent Tesla, Lokibot, AzoRult, Pony, and Netwire in conjunction with bulk mailing software. It was reported that the group monetized their unauthorized access through various business email compromise (BEC) schemes. The group is suspected to have compromised government and private sector organizations in more than 150 countries. Proofpoint has attributed TMT Group activity to a cluster of activity dating back to August of 2019. Proofpoint formally tracks this activity as TA2519 and has confirmed that this group is still active despite the Interpol arrests.

Proofpoint Analysis

A review of historical threat data identified tens of email campaigns delivering Agent Tesla and Loki Bot dating back to August of 2019. The activity was observed consistently on a daily or weekly basis. The social engineering themes of the campaigns has included payments, invoices, the use of DHL package notifications and COVID-19 while impersonating the World Health Organization (WHO). The RAT payloads were often obfuscated and packed with commercial loaders such as GuLoader or CyaX. TA2519’s use of mailing software, such as Turbo Mailer and Gammadyne Mailer from their operational systems, led to the reuse of a several email sender IP addresses.

Example Attack Chain

Email

ISO Attachment w/Excel Document

Agent Tesla

Exfiltration of Credentials

BEC Campaign

Download Attach... 924.7KB
Download Attach... 1.4MB
Download All
Preview All
Agent Tesla

TA2519 leveraged Agent Tesla, a remote access trojan (RAT), in campaigns from March 2020 to July 2020. The typical attack pattern consisted of ISO email attachments that if opened led to the installation of Agent Tesla. A newer version of Agent Tesla is referred to as Origin Logger, however, Proofpoint collectively refers to this family of malware as Agent Tesla. The configuration of the Agent Tesla RAT used during this time follows.

C2 Email Address: defaultforward22@yandex[.]com
C2 Email Server: smtp.yandex[.]com
C2 Email SendTo: defaultforward22@yandex[.]com

Loki Bot

TA2519 leveraged Loki Bot, another common RAT, in campaigns from August 2019 to March 2020. The typical attack pattern consisted of ISO email attachments with embedded executables that when opened led to the installation of Loki Bot. A subset of the Loki Bot command and control (C2) URLs follows.


Financial Exfiltration

Interpol and the Nigerian Police Force have reported that TA2519 monetizes their unauthorized access through BEC schemes. Proofpoint has not been able to link the RAT activity to any of our BEC activity clusters. It is likely that specific members of TA2519 obtained harvested credentials and then handed them off to other members using different infrastructure for financial exfiltration.

Indicators of Compromise

Agent Tesla Samples

Notably, the Agent Tesla configuration for this sample includes a new C2 email address.

C2 Email Address:
ryan.sowders52@yandex[.]com
C2 Email Server:
smp.yandex[.]com
C2 Email SendTo:
ryan.sowders52@yandex[.]com

<table>
<thead>
<tr>
<th>Post Arrest</th>
</tr>
</thead>
<tbody>
<tr>
<td>f183ef50c311ce806b5eb236444</td>
</tr>
<tr>
<td>22e7dfb840c2d3aeb54651993e28b108ac81d</td>
</tr>
<tr>
<td>b77e79fedfa97c6819b7d50afe12bae96b8934391c44075cedf0dec842322fca</td>
</tr>
</tbody>
</table>

Loki Bot Sample

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>cac61face9cd1b8cedbed3592c7b18ae54</td>
<td>a6d15feb267679530a3c862911f2f</td>
</tr>
</tbody>
</table>

Sender IP Address

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>154.0.162[.]179</td>
<td>77.105.37[.]159</td>
</tr>
</tbody>
</table>

Conclusion

The recent arrest of three TA2519 members highlights the use of commercial malware in BEC schemes where we traditionally see pure social engineering techniques. Proofpoint assesses that BEC campaigns will increase in the short term and that their reliance on compromised accounts as opposed to spoofed infrastructure will increase as well. The need for compromised accounts will fuel future credential phishing and malware campaigns by traditional BEC threat actors.

Post-Arrest Activity

Proofpoint has observed additional activity related to this group’s infrastructure after November 19th when the 3 individuals were arrested. The latest campaign we observed from TA2519 was dated November 26th, 2020 and it used a DHL theme we have previously observed. This campaign leveraged a Gzipped attachment containing a CyaX packed executable file which leads to Agent Tesla.
A ROUNDUP OF THE 6 BIGGEST, BOLDEST, AND MOST BRAZEN BUSINESS EMAIL COMPROMISE SCAMS OF 2020 AND 2019

1. ‘SHARK TANK’S’ BARBARA CORCORAN

ABC-TV describes the stars of its hit show “Shark Tank” as “tough, self-made, multimillionaire and billionaire tycoons.” But that doesn’t mean they can’t be duped.

Barbara Corcoran, one of the judges on the show who decides whether to invest in the dreams of various entrepreneurs, was robbed of close to $400,000 by a BEC scam in February. Corcoran, who made her millions as a real estate broker, admitted in late February of 2020 that her bookkeeper wired money to someone posing as Corcoran’s assistant, ostensibly to pay for a real estate renovation. After the money was sent, Corcoran realized that the email address was not actually that of her assistant; it was one letter off from the real address. “There was no reason to be suspicious, as I invest in a lot of real estate,” Corcoran told People magazine.1 Corcoran’s IT staff later traced the attack to a Chinese IP address.2 Corcoran’s bank pressed the German bank to freeze the money, giving her time to prove it was fraud. That an email message seems to be routine — and, therefore, not suspicious — is one of the central design features of BEC.

2 - Ibid.
$4 Million lost in three separate BEC attacks

2. PUERTO RICO

Puerto Rico has suffered several setbacks of late, including hurricanes, a government debt crisis, a recession — and now, BEC attacks.

The Puerto Rico government lost more than $4 million in three separate BEC attacks on agencies in January 2020. The scam began when someone compromised the computer of a finance worker at Puerto Rico’s Employment Retirement System about a month earlier. Using the worker’s account, the attacker then sent emails to the worker’s colleagues in other agencies. The email instructed recipients to change the banking account number tied to remittance payments. This BEC-style attack is technically an example of email account compromise (EAC). In this case, the attacker isn’t just trying to make their email address seem legitimate — they’re using an account that is legitimate. The largest theft targeted Puerto Rico’s Industrial Development Company, a government-owned corporation investing in economic development on the island. It resulted in the loss of $2.6 million in government funds. The Puerto Rican Tourism Company was also taken for $1.5 million, while the territory’s Commerce and Export Company lost $63,000. Like most BEC attacks, Puerto Rico’s vulnerability was a human one. “Where the government failed greatly was in the procedures, not the technology,” said José Quiñones, president of Obsidis Consortia, a nonprofit cybersecurity organization in Puerto Rico, to the Associated Press.

3. RED KITE COMMUNITY HOUSING

People who have trouble paying for housing in High Wycombe, a British city outside of London, can turn to Red Kite Community Housing. The charitable housing nonprofit owns and manages more than 6,500 homes in the Wycombe area, which it rents out at below market rates.

Unfortunately, Red Kite suffered a financial setback of its own when it was hit by BEC in August 2019. Attackers stole £932,000 or $1.2 million in U.S. dollars. According to news reports, cyber attackers impersonated one of Red Kite’s suppliers by registering a lookalike domain. Using the fake domain, which closely resembled that of the real vendor, the attackers tricked the recipient into wiring money to the attacker’s bank account. The email included a fictitious email history in the message body to make it appear to be part of a long-running conversation between Red Kite executives and the vendor. Red Kite’s own security included two-factor authentication to verify changes to payments and accounts, a Red Kite spokesperson told the tech news website of Scotland-based Digit. Red Kite says its systems were never compromised. The weak spot: human error. The Red Kite worker was fooled by the email and didn’t follow normal procedures. “It is this single point of failure that we have addressed in our internal review of learning and changes required that feature in an action,” the association says. Red Kite reported the breach to its tenants (who did not bear the cost of the theft), local police, an outside cyber-forensics firm and a local agency that regulates Social Housing. The nonprofit has since upgraded its security posture, completed an audit and review of its payment processes and systems and put additional security measures in place, including staff training.

References:
6 - David Paul, (Digit). “British Charity Loses almost £1m in Domain Spoofing Scam” February 2020.
7 - Red Kite Community Housing. https://redkitehousing.org.uk/]
A rash of cyber-attacks targeted small U.S. cities, local agencies and school districts. Attackers might assume that smaller, sometimes cash-strapped local agencies have less money for cybersecurity than larger jurisdictions or the private sector. In many cases, they’re right.

But that’s only part of the story. At large and small organisations alike, people are usually the weakest security link.

Case in point: Manor Independent School District outside of Austin, Texas. The district of 9,600 students was scammed out of $2.3 million in a BEC email attack in November 2019.

The scammer emailed several district employees over the course of several months starting in November 2019, changing the payment instructions for a vendor. Just one worker fell for the email, but the damage was done. The scammers pulled off three separate transactions before someone noticed something amiss. The district expects to recover only $800,000 of the lost funds from an insurance policy, leaving it with a $1.5 million net loss.

$2.3 Million stolen in a single BEC attack

9 - Drew Knight, Luis de Len, KVUE-TV. “Manor ISD loses $2.3 million in phishing scam; police and FBI investigating,” January 2020.
$37 Million stolen in largest reported BEC attack

5. TOYOTA BOSHOKU

BEC attackers target organizations large and small. One of the biggest victims and payouts in recent months was Toyota Boshoku. The Toyota subsidiary, which supplies seats and other interior components, was swindled out of $37 million in August 2019. The attack was textbook BEC, according to news reports. Someone posing as a business partner sent emails to people in the company’s finance and accounting department, requesting payment into a the attacker’s account. The company says it became aware of the fraud quickly, reported it to authorities and is working to recover the money. The $37 million attack illustrates how social engineering can bypass even the most well-funded cyber defenses because they target people, not infrastructure.

6. RIJKSMUSEUM TWENTHE

Cyber criminals set their sights on big payoffs when they scam banks, corporations, government agencies and other targets to steal money through BEC and EAC schemes. So it should be no surprise when they set their crosshairs on art dealers and museums, which trade in highly valued masterpieces. Rijksmuseum Twenthe, a national museum in Enschede, Netherlands, lost $3.1 million to an EAC scammer posing as well-known London art dealer. The museum had been negotiating over email for months with the dealer to buy the 1824 painting "A View of Hampstead Heath: Child’s Hill, Harrow in the Distance" by English landscape painter John Constable.

Somewhere along the way, a scammer either hijacked the dealer’s email account or created a convincing lookalike - the details are the subject of an ongoing lawsuit - and waited for the sale to close. The dealer shipped the painting. But when it came time to send the payment, the museum wired the money to an account in Hong Kong — not the seller’s. The scammer had “updated” payment details in an earlier email. The museum is suing the dealer, claiming the dealer was negligent in not noticing or intervening when the scammer compromised his account. The dealer is countersuing, saying the museum should have double-checked banking details before sending payment. For now, the museum is holding the painting while litigation continues.

$3.1 Million lost to impostor art deal


The Next Generation of Targeted BEC Attacks:

How Stagecoach is fighting imposter Blindness

Imposter fraud has a long and nefarious history. But while the scam may be nothing new, the techniques involved get more advanced by the day.

Where yesterday’s fraudsters used to disguise and misdirect to fool unwitting victims, today’s cyber criminals harvest stolen credentials to ape and assume your digital identity.

Considered the most expensive cybersecurity issues, the most popular forms of imposter fraud today are Business Email Compromise (BEC) and Email Account Compromise (EAC).

A successful BEC attack sees a cyber criminal pose as a trusted contact — a colleague, vendor, or other affiliated third-party to convince a victim to wire money to a bogus account. Scammers may also compromise legitimate accounts to the same ends — known as Email Account Compromise.

Whether achieved through domain spoofing, phishing, or credential theft, the result can be devastating. An average BEC attack costs approximately $154,000 — compared to just $640 for a successful ransomware exploit.

BEC impacts not just the compromised organization but its customers, suppliers, and numerous other third parties. And it’s an issue that affects businesses of all sizes, across all sectors — with 86% of organizations worldwide suffering an attack last year.

With trust, reputation, and revenues at stake, businesses like Stagecoach, the UK’s largest bus operator, turn to cybersecurity experts for protection, guidance, and peace of mind.
Stagecoach under attack

It’s not unusual for Stagecoach to be a constant target for cyber attacks. Bad actors are forever scanning social platforms and directories for details on company executives.

These details are used to fabricate false payment emails. Stagecoach sees attempted attacks of this nature every day.

Like many other modern organizations, the company recently migrated to a flexible cloud platform, Office365. However, such migrations can result in an increased attack surface.

Stagecoach saw an immediate increase in BEC, spoofing and phishing attempts post-migration. Attackers spoofed Stagecoach and its O365 domains to try to trick employees and partners.

Stagecoach had the protections in place expected of a company with 24,000 staff based throughout the UK. However, with the volume of attacks increasing, it was likely only a matter of time before one saw success.

Gaining greater visibility

High volume attacks can stretch even the best defenses, for the simple reason that a cybercriminal only has to win once.

That’s why a successful cyber defense is multi-layered, combining people, process, and technology controls.

In its latest report, Protecting Against Business Email Compromise Phishing, Gartner laid out five key recommendations for implementing such a defense:

- Complement email security technology with user awareness training specifically to educate users on BEC phishing.
- Implement standard operating procedures to authenticate email requests for financial or data transactions and move high-risk ad hoc transactions from email to more authenticated systems.
- Upgrade secure email gateway solutions to include advanced phishing protection, imposter detection and internal email protection.
- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to authenticate email domains and minimize the opportunity for domain abuse.
- Implement multifactor authentication to protect against account takeover.

Stagecoach aligned its cyber defense with this strategy. After a comprehensive RFI process, the company implemented Proofpoint’s full Proofpoint People-Centric Security Bundle (P3).

Along with tools and controls to fight BEC and EAC, and protect cloud applications, P3 includes a comprehensive people-centric security program, ensuring all users are aware of their cybersecurity responsibilities.

As well as requiring awareness and education among end-users, implementing such a strategy also involves buy-in at the board-level.

Simon Taylor, Information Security Manager at Stagecoach: “I have been fortunate to have the support from the CISO and the board so have been able to procure and implement the full Proofpoint People-Centric Security solution.”
Eliminate blind spots with defense in depth

Since implementing its new cyber strategy, Stagecoach has seen a marked improvement in its ability to detect and prevent all manner of cyber-attacks: “Since implementing Isolation, we have had 100% protection on malicious emails!”, states Taylor after the implementation of Proofpoint Email Isolation.

With tools, solutions, and daily checks aimed at protecting Stagecoach users, data, and cloud apps, cybersecurity awareness is now higher than ever throughout the organization. In addition, the organization is working to implement DMARC to protect its 1,200+ domains — a step Taylor may have taken sooner with hindsight, although the priority was placed on mitigating a perceived higher threat from internal access to mail accounts: “Implementing DMARC has been the biggest challenge... because you risk stopping legitimate emails flowing. Had we done it first, however, we’d be in a better position now with regard to BEC, possibly.”

Stagecoach offers a great example of a multi-layered, people-centric approach. This starts with a technical combination of email gateway controls, email authentication, and content analysis, designed to ward off BEC and similar attacks. Greater visibility into cloud applications, suspicious logins, activity, and DLP alerts also allows IT teams to spot bogus access attempts and analyze the data flowing to and from the organization.

But these tools, while eliminating blind spots, are just one piece of the puzzle. As well as protecting the organization from targeted attacks, the P3 solution offers valuable insight into the methods and origins behind those attacks. This information is leveraged to train end-users on common threats in context — highlighting the very threat vectors they are most likely to encounter.

Educating users in this manner raises awareness and conveys the vital role they play in protecting the organization from cyber criminals.

The result is a cybersecurity culture where the onus for defense is not solely on IT teams but every individual.

With the Proofpoint solution in place, Taylor is satisfied to have achieved his initial goal of implementing “a layered approach, providing the best security not just from traditional attacks, but also the loss of data.”
Building Trust in your Business
Email Communication

TRUSTING COMMUNICATION IS A KEY COMPONENT IN RELATIONSHIPS. IN FACE TO FACE RELATIONSHIPS, TRUST IS EARNED THROUGH OUR WORDS, ACTIONS, AND EYES. IN SOCIAL MEDIA, BRANDS OR NOTABLE INDIVIDUALS OBTAIN OUR TRUST EARNING THE VERIFIED STATUS TICK MARK, FOLLOWING THE SOCIAL PLATFORMS VERIFICATION PROCESS.

Your business communicates to customers, supply chains, and business partners through email. So how do you establish trust? With email being inherently easy to spoof, do your employees and business partners trust that the emails they receive are from who they appear to be from?

Deploying DMARC
Deploying Domain-based Message Authentication Reporting and Conformance (DMARC) is a great start to ensure the emails you receive are trustworthy. DMARC allows users to reveal what an email from your organization looks like, allowing them to authenticate any message that looks like it’s from you and automate taking appropriate action.

Many businesses are now promoting the benefits of DMARC to their supply chain and business partners, encouraging (some mandating) its use. DMARC is an unforgiving technology that demands perfection to authenticate messages, but we don’t live in a perfect world, far from it.

Proofpoint gives you the visibility and service experience to guide you through your own DMARC deployment. Moreover, it gives you visibility of the DMARC journey of those businesses you communicate with, allowing you to adapt your policies in line with how perfect or not their DMARC implementation has been. This level of visibility allows the messaging and security teams to add value back to the business, increase trust, and manage the risks of your business relationship emails through visibility and control.

Authenticating email upfront can help remove the risk of spoofed messages, thwarting attacks like business email compromise, or credential phishing attempts.

However, in the same way we can’t always trust the content that’s tweeted out from a verified twitter account, we can’t assume trust in an authenticated email. Email accounts can be hijacked just like twitter accounts, and it’s a growing threat.

Scrutinize your email gateway’s ability to detect imposter activity from legitimate authenticated email. Proofpoint’s imposter classifier takes a dynamic approach to detecting fraudulent email patterns and blocking messages to reduce your risk of exposure to BEC and other attacks using compromised accounts in your supply chain and business partners.
EC and EAC are growing problems that target organisations of all sizes and across every industry worldwide - in all 50 states and in 177 countries. They share a similar playbook and are often linked (the FBI tracks them together). But they have key differences that are important to understand when building out a defence strategy.
Japanese media giant Nikkei isn’t the stereotypical victim of financial fraud.

It’s one of Japan’s biggest media conglomerates, the owner of London’s the Financial Times and its namesake stock index on the Tokyo Stock Exchange.

That sheer size and financial heft made it an especially lucrative target of scammers.

In September 2019, an employee of its U.S. subsidiary, Nikkei America, transferred $29 million based on instructions from an email that appeared to be from an executive at the parent company.

Unfortunately, the email was from someone merely posing as the executive. (Some reports suggested that the attacker may have actually taken over the executive’s account,12 which would make it an EAC attack; the media company and authorities have provided few details publicly.)

---

BEC and EAC attacks are inherently focused on people, rather than technical vulnerabilities. That shift renders traditional infrastructure-focused defences useless against them. Unlike large-scale attack campaigns, BEC and EAC attacks are specific and highly targeted. So they go unnoticed by security tools that look for network traffic patterns and other detection techniques.

Because BEC and EAC rely primarily on social engineering and human psychology, there are no malware attachments or malicious URLs to be analysed. In fact, malicious emails sent from compromised accounts usually pass authentication and even content-analysis checks.

BEC/EAC attacks are complex, using multiple techniques. There are several reasons why point products working independently from one another cannot do the job.

Advanced BEC and EAC attacks are often blended

Bad actors use many techniques that span multiple technologies and channels. Today’s threats often combine email and cloud vectors, including apps and services such as Amazon Web Services, Box, Google G Suite, Microsoft 365 (Office 365), Slack and others.

By getting corporate users to respond to a single malicious email, attackers can infiltrate a cloud account. This can then lead to phishing or email fraud both internally and across supply chains.

Attackers are constantly shifting tactics and always evolving. This may leave you exposed to other advanced deception techniques you may not even be aware of.

If you’re solving for techniques in a siloed manner, your security tools might miss important signals from other channels.

For example, financial requests from the CFO that might appear routine in isolation can take on new significance if you know that person is being targeted with account takeover attempts such as credential phishing.
Preempting BEC: first steps

There are some things you can do to prevent the potential damage that can be done by BEC and EAC attacks. These recommendations may seem obvious at first, but they can go a long way toward safeguarding your organisation.

Change your financial processes

Start by tightening the reins on who can process and authorise wire transfers. Minimise the number of people involved and make sure authorised employees stick to process and learn to recognise suspicious requests for wire transfers.

Another step in the right direction is to use multiple verification steps for wire transfers. For example, if a transfer exceeds a certain amount, you might want to require authorisation by someone higher up in the chain of command. And because BEC and EAC attacks use email, you can use other means of verification such as an old-fashioned phone call.

For example, some attacks ask the targeted employee to change account information. Again, you can confirm with a phone call. Just make sure the phone number is legitimate and not spoofed.

Deloitte suggests that changes to the workplace culture, such as instilling the importance of following corporate protocol, can also head off BEC attacks. In a recent article, the global professional services network offers this piece of advice.

An effective compliance culture supports employees with the protocol they need to follow up with confidence. Without the internal isolation BEC criminals depend on, their attacks are more likely to fail.

Deploy multifactor authentication

Another useful tool to prevent some account takeovers is multifactor authentication (MFA), which asks users to provide two or more ways to identify themselves. Just about everyone is familiar with logging into a bank account first with a password and followed by entering a numerical code that is sent to their mobile phone.

MFA provides an extra layer of security against account takeovers. But it doesn’t do anything for BEC attacks. And even in EAC attacks, it isn’t bulletproof.

Deploy an Email Security Solution Purpose-Built to Fight BEC and EAC

BEC and EAC are complex issues, and there is no single approach that can protect against every kind of impostor attack. A security tool may stop one or two tactics but still leave you exposed to a multitude of others.

That’s why you need a solution that addresses every angle of these sophisticated and complex threats. Your BEC/EAC defence must address all attacker tactics. It must provide visibility into malicious activities and user behaviour. And, for the most effective BEC/EAC defence, it should automate detection and threat response.
Helping security leaders meet the challenge head on

A truly purpose-built solution will help CISOs, CIOs and other security leaders achieve the following:

- Minimise the risk of BEC and EAC by protecting against a wide range of attacker tactics and techniques.
- Gain visibility into who receives impostor email and into who sends these emails using your company’s domain. That includes both trusted third-party senders and compromised accounts.
- Strengthen overall security by blocking impostor email and fraudulent use of domains by accurately detecting compromised cloud accounts.
- Understand and clearly communicate the risks to the board of directors. That starts with identifying and describing the human attack surface. You should know who your Very Attacked People™ are, who is being attacked with credential phishing and impostor emails, and who is vulnerable to credential theft.
- Reduce costs and improve operational effectiveness by consolidating security vendors and products.
- Make your security team more effective and efficient.

A solution built expressly to stem the tide of BEC and EAC threats will enable your security team to:

- Cut through the noise. The team should be able to prioritise incidents and investigate potential threats by accurately blocking impostor emails, detecting suspicious cloud account logins and activity, and stopping attempts to steal account credentials.
- Train users how to recognise, reject and report BEC and EAC attempts.
- Prevent fraudulent use of your organisation’s legitimate domains.
- Provide actionable insights into who is being attacked with impostor emails and credential phishing. Based on that insight, provide risk-based security controls to those users, such as isolating access to unknown websites and targeted security awareness training.
- Reduce manual work, save time and accelerate threat response. Automate detection, investigation and remediation.

Attackers will never stop looking for ways to exploit your users and prey on human nature and business processes. But with an effective BEC/EAC solution, you can greatly reduce the chances of impostors reaching your users — and your users from falling for tricks that cause lasting damage.
## Putting the pieces together

### THE COMPONENTS OF AN EFFECTIVE BEC/EAC DEFENCE

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Cloud Application</th>
<th>Automated Remediation</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block attacks that use display name spoofing, spoofed domains and lookalike domains</td>
<td>Authentication</td>
<td>Identify and remove suspicious emails that have entered the organisation</td>
<td>Assess user vulnerability to BEC and EAC threats</td>
</tr>
<tr>
<td>Analyse message headers to identify anomalies</td>
<td>Identify suspicious cloud account activity and compromised accounts</td>
<td>Remove unwanted email from internal accounts that are compromised</td>
<td>Train users on how to identify threats and credential theft</td>
</tr>
<tr>
<td>Analyse all email content with machine learning</td>
<td>Detect brute-force attacks</td>
<td>Force password resets and disable accounts that are compromised</td>
<td>Simulate real-world BEC and phishing attacks</td>
</tr>
<tr>
<td>Enforce email authentication policy</td>
<td>Build policies to prioritise</td>
<td>Use an account authentication solution to re-authenticate sessions</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Web Access</td>
<td>Investigate account compromise incidents</td>
<td></td>
</tr>
<tr>
<td>Create global email authentication policy (DMARC) and enforce it on an Internet-wide basis</td>
<td>Isolate access to unknown websites</td>
<td>Automate abuse mailbox process</td>
<td></td>
</tr>
<tr>
<td>Block all attempts to send unauthorised emails from your trusted domains</td>
<td>Provide read-only access until security analysis is complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report on lookalike domain registrations</td>
<td>Control content entering your organisation through personal webmail accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visibility</td>
<td>Automated Remediation</td>
<td>Education</td>
<td></td>
</tr>
<tr>
<td>Identify VAPs</td>
<td>Identify and remove suspicious emails that have entered the organisation</td>
<td>Assess user vulnerability to BEC and EAC threats</td>
<td></td>
</tr>
<tr>
<td>Provide user-centric visibility into account attacks</td>
<td>Remove unwanted email from internal accounts that are compromised</td>
<td>Train users on how to identify threats and credential theft</td>
<td></td>
</tr>
<tr>
<td>See which users are being attacked with impostor and phishing attack</td>
<td>Force password resets and disable accounts that are compromised</td>
<td>Simulate real-world BEC and phishing attacks</td>
<td></td>
</tr>
</tbody>
</table>
What to Do (and what not to do) to Fight BEC and EAC

When you receive an email

**Do:**
- Do look carefully at the sender’s email: Accounts are often created to look similar to a trusted source
- Do review the email for grammar and spelling: Cyber criminals have improved over the years with this, but continue to look for abnormal spacing and misspellings
- Do inspect links: Attackers usually embed malicious links into their emails. You can use your mouse to hover over the hyperlink to see if there is an embedded URL
- Do be cautious about opening attachments: Attackers might be able to then get into your email account through you opening or downloading the email attachment
- Do report impersonated or suspect emails: Before giving out any sensitive information, forward the email to your security team

**Don’t:**
- Don’t trust the sender: Anyone can use a trusted domain to send an email
- Don’t click on attachments or links: These can contain malware giving access to your mailbox
- Don’t click on “verify your account” or “login” links in any email: Always open a new window and type in the URL or type in the official home page to log into an account
- Don’t be embarrassed: There’s a reason why the financial losses from these attacks are on the rise - they are easily disguised. Contact your security team ASAP if you do fall victim to an attack

Before you reply to an email

**Do:**
- Do use good judgement: If a trusted person has never requested sensitive information from you before, you should be skeptical
- Do validate the request via another channel: Pick up the phone to verify any requests from the trusted person
- Do open a new window to check out the website: Instead of clicking on the URL, open a browser and type it in

**Don’t:**
- Don’t be so quick to reply: Sometimes the attacker is just looking to verify if the email address works, you might be helping the attacker confirm that it has reached a recipient
- Don’t send passwords or sensitive information over email: Most legitimate organizations won’t request this over email, so be cautious when you do get an email asking for this
- Don’t share the passwords: You will be compromising the security of your account, and you will not know what they are doing with your access
Display name spoofing and using lookalike domains are both common BEC attack tactics. In this example, you can see that the sender’s address is private instead of public. The attacker also leverages parents’ emotions about their children’s wellbeing in order to increase the attacker’s success rate. Down below the message, there’s a URL that links to a compressed Microsoft Word document with macros. Clicking on this link could install a malware that can potentially lead to email account compromise.
Enabling your users to recognise and avoid BEC Attacks

BEC attacks cannot happen if you don’t take the bait! Share these tips with your employees — to identify and avoid these types of attacks, and protect your organisation’s funds, data and reputation.
Be careful about your social media posts and connections. Consider all information that you share to be public and permanent.

Be on guard with all unsolicited emails and phone calls. Even seemingly small pieces of information-like vendor names can be spoofed by attackers to make them look legitimate. In some cases, cybercriminals are able to steal email login credentials and send messages from a trusted account, making it extremely difficult to spot a fraudulent request.

Verify originating email addresses and phone numbers when sensitive requests are made. These details can be spoofed by attackers to make them look legitimate. In some cases, cybercriminals are able to steal email login credentials and send messages from a trusted account, making it extremely difficult to spot a fraudulent request.

Implement a form of two-factor authentication before initiating wire transfers, or providing sensitive data. Call a known, verified phone number and have a voice-to-voice conversation to confirm the request is legitimate.

IF YOU BELIEVE YOU HAVE BEEN A VICTIM OF A BEC ATTACK, ALERT YOUR SUPERVISOR, FINANCIAL INSTITUTION, IT DEPARTMENT AND AUTHORITIES AS SOON AS POSSIBLE. QUICK ACTION CAN HELP TO MINIMISE THE DAMAGE.
DMARC (Domain-based Message Authentication Reporting and Conformance) is an open email authentication protocol that provides domain-level protection of the email channel. DMARC authentication detects and prevents email spoofing techniques used in phishing, business email compromise (BEC) and other email-based attacks.

Building on existing standards—SPF and DKIM—DMARC is the first and only widely deployed technology that can make the header “from” domain trustworthy. The domain owner can publish a DMARC record in the Domain Name System (DNS) and create a policy to tell receivers what to do with emails that fail authentication.

Examples

According to Gartner’s ‘Top 10 Security Projects for 2020-2021’ blog: “Organisations use email as the single source of verification, and users struggle to determine real messages from fakes. DMARC is an email authentication policy. DMARC is not a total solution for email security, and should be one piece of a holistic security approach. However, it can offer an additional layer of trust and verification with the sender’s domain. DMARC can help domain spoofing but will not address all email security issues.”

- **Domain spoofing** — An attacker spoofs the domain of a company to make an email seem legitimate.
- **Email spoofing** — A term for spoofing activities involving email.
- **Business email compromise (BEC)** — An email that appears to come from a senior employee within an organization requesting that money or sensitive information be sent.
- **Impostor email** — A spoofed email sent by an impostor who claims to be someone they are not.
- **Email phishing** — An email that tries to get victims to install malware or offer their credentials. A phishing email often looks like a familiar brand to appear legitimate.
- **Consumer phishing** — Spoofed email sent to a consumer of a company claiming to be from that company with the intention of stealing credentials.
- **Partner spoofing** — Business-based spoofed email between supply chain partners, which attempts to change payment details in order to siphon money.
- **Whaling email scam** — Fraudulent email sent to a senior employee within an organization aiming to get a large financial gain.
Domain-based Message Authentication Reporting and Conformance (DMARC) — An email validation system that detects and prevents email spoofing. It helps combat certain techniques often used in phishing and email spam, such as emails with forged sender addresses that appear to come from legitimate organizations.

Sender Policy Framework (SPF) — An email validation protocol designed to detect and block email. It allows receiving mail exchangers to verify that incoming mail from a domain comes from an IP address authorized by that domain’s administrators.

DomainKeys Identified Mail (DKIM) — An email authentication method that detects email spoofing. It allows the receiver to check that an email that claims to come from a specific domain was authorized by the owner of that domain.

Binding Operational Directive 18-01 — The Department of Homeland Security has issued Binding Operational Directive 18-01 for agencies to upgrade their email and web security. Agencies will need to implement SPF, DMARC, and STARTTLS efficiently.

Sender Policy Framework (SPF) is an email validation protocol that allows an organization to specify who can send email from their domains. Organizations can authorize senders within an SPF record published in the Domain Name System (DNS). This record includes the approved IP addresses of email senders, including the IP addresses of service providers that are authorized to send email on the organization’s behalf. Publishing and checking SPF records is a reliable way to stop phishing and other email-based threats that forge “from” addresses and domains.

Domain Keys Identified Mail (DKIM) is an email authentication protocol that allows the receiver to check that an email from a specific domain was really authorized by the owner of that domain. It allows an organization to take responsibility for transmitting a message by attaching a digital signature to it. Verification is done through cryptographic authentication using the signer’s public key published in the DNS. The signature ensures that parts of the email have not been modified since the time the digital signature was attached.
How DMARC works

For a message to pass DMARC authentication, it must pass SPF authentication and SPF alignment and/or pass DKIM authentication and DKIM alignment. If a message fails DMARC, senders can instruct receivers on what to do with that message via a DMARC policy. There are three policies the domain owner can enforce: none (the message is delivered to the recipient and the DMARC report is sent to the domain owner), quarantine (the message is moved to a quarantine folder) and reject (the message is not delivered at all).

The DMARC policy of “none” is a good first step. This way, the domain owner can ensure that all legitimate email is authenticating properly. The domain owner receives DMARC reports to help them make sure that all legitimate email is identified and passes authentication. Once the domain owner is confident they have identified all legitimate senders and have fixed authentication issues, they can move to a policy of “reject” and block phishing, business email compromise, and other email fraud attacks. As an email receiver, an organization can ensure that its secure email gateway enforces the DMARC policy implemented to the domain owner. This will protect employees against inbound email threats.

SPF authentication starts by identifying all legitimate IP addresses that should send email from a given domain and then publishes this list in the DNS. Before delivering a message, email providers will verify the SPF record by looking up the domain included in the “envelope from” address within the hidden technical header of the email. If the IP address sending an email on behalf of this domain is not listed in the domain’s SPF record, the message fails SPF authentication.

For DKIM authentication, the sender first identifies what fields they want to include in their DKIM signature. These fields can include the “from” address, the body of the email, the subject and more. These fields must remain unchanged in transit, or the message will fail DKIM authentication. Second, the sender’s email platform will create a hash of the text fields included in the DKIM signature. Once the hash string is generated, it is encrypted with a private key, which only the sender can access. After the email is sent, it’s up to the email gateway or consumer mailbox provider to validate the DKIM signature. This is done by locating a public key that is an exact match of the private key. Then the DKIM signature is decrypted back to its original hash string.
DMARC Best Practices and Tools

- Due to the volume of DMARC reports that an email sender can receive and the lack of clarity provided within DMARC reports, fully implementing DMARC authentication can be difficult.
- DMARC parsing tools can help organizations make sense of the information included within DMARC reports.
- Additional data and insights beyond what’s included within DMARC reports help organizations to identify email senders faster and more accurately. This helps speed up the process of implementing DMARC authentication and reduces the risk of blocking legitimate email.
- Professional services consultants with DMARC expertise can help organizations with DMARC implementation. Consultants can help identify all legitimate senders, fix authentication issues and can even work with email service providers to make sure they are authenticating properly.
- Organizations can create a DMARC record in minutes and start gaining visibility through DMARC reports by enforcing a DMARC policy of “none.”
- By properly identifying all legitimate email senders — including third-party email service providers — and fixing any authentication issues, organizations should reach a high confidence level before enforcing a DMARC policy of “reject.”
The Modern CISO’s Guide to Stopping BEC and EAC

BUSINESS EMAIL COMPROMISE (BEC) AND EMAIL ACCOUNT COMPROMISE (EAC) ARE COMPLEX PROBLEMS THAT REQUIRE MULTI LAYERED DEFENSES. CYBER ATTACKERS HAVE COUNTLESS WAYS OF TRICKING YOUR USERS, PREYING ON THEIR TRUST AND EXPLOITING ACCESS TO KEY DATA, SYSTEMS AND RESOURCES.

Air Travel as an Analogy

Consider how airports manage a vast and changing mix of potential security issues. Most take a multipronged approach, each element featuring multiple checks and procedures.

- **Passport control.** Checks traveler’s passport (or driver’s license) and boarding pass to ensure they are 1) who they claim to be and 2) authorized to fly.
- **Screening.** Scans the luggage and passengers to ensure that nothing bad is getting on the plane - and that nothing’s leaving that shouldn’t be.
- **TSA agents.** Trained to spot and report suspicious traits and behavior.
- **Airport security.** Armed with the authority and means of physically stopping bad actors and separating them from anyone they might harm.
- **Law enforcement.** Aware of outside activity that may put travelers at risk, including identity theft, forged passports and coordinated criminal activity. Helps create no-fly lists, alerts airport security about potential threats and catches many criminals before they enter the airport.
Here’s a closer look at how Proofpoint Email Security can safeguard your people from BEC and EAC attacks at each stage of the air travel analogy...

**Passport control = Authentication**

We help you:
- View all inbound impostor threats — such as display name spoofing and lookalike domain spoofing attacks - and block them at the Proofpoint gateway
- Enforce DMARC authentication quickly and confidently to block fraudulent emails that spoof trusted domains
- Automatically identify and flag lookalike domains that are registered by third parties and are outside of your control

**Screening = Email Gateway**

Our email security solution identifies malicious URLs and attachments that could lead to compromised accounts. We also scan incoming email to look for signs of social engineering and fraud. Our dynamic classification engine analyzes and manages email based on several factors, including:
- The email’s content
- The sender’s reputation (based on the IP address in the email header)

We typically look at several factors. Does the email come from a trusted sender - and does that sender have a good reputation? Does the email include a suspicious subject? Do the sender and the receiver have an existing email relationship?

Does the body of the email look suspicious? We score each email based on its level of riskiness. Then you can decide what to do with it according to that score — let it through, block it or route it to a quarantine folder.

**TSA Agents = Security Awareness Training**

With security-awareness training, we help turn your users into a strong last line of defense by:
- Teaching users to recognize, reject and report suspicious emails
- Revealing user vulnerabilities, showing which users are most vulnerable and the BEC/EAC tactics they’re most likely to fall for
- Targeting training to those who need it based on where they’re most vulnerable, how they are being targeted in attacks, and their access privileges to key data, systems and resources

Our security awareness training modules are informed by rich, timely threat intelligence, so they reflect the latest real-world attack tactics and techniques. And reporting BEC/EAC attempts is easy with our PhishAlarm button for Microsoft Outlook users and PhishAlarm analyzer for security teams. Both tools are part of suspicious email reporting system that helps streamline both BEC/EAC reporting and remediation.
Airport Security = Threat Response

Our threat-response automation capabilities combat BEC and EAC by orchestrating and automating key parts of the incident response process. Here just a few of the actions you can set to happen automatically when a BEC or EAC attempt reaches a user’s inbox:

- Pull phishing emails that contain URLs that become unsafe after being delivered — along with any copies that have been forwarded to other users
- Remove unwanted email from internal accounts that have been compromised
- Quarantine potential impostor emails reported by users
- Force password resets
- Suspend compromised accounts
- Revoke any active user’s session
- Enforce risk-based authentication

We help you quickly contain and remediate BEC and EAC threats to avoid the worst effects of a successful attack.

Law Enforcement = Cloud Account Defence

Our cloud security is a police force for EAC attacks. It detects when a cloud-based email account has been compromised. It alerts your security team. And it takes steps to remediate the account before the attacker has a chance to misuse it.

We use the latest threat intelligence and powerful forensics to correlate outside threats, account behavior and user context. It connects the dots between:

- Account activity — unusual actions such as suddenly BCCing emails in bulk or setting up calendar-forwarding rules
- Context — out-of-character logins from locations too far apart to be from a single user, on new devices, through unknown networks and at unusual times
- Threat intelligence — attack campaigns targeting specific roles or groups or using methods consistent with activity observed in a user account.

If something looks amiss, it applies risk-based controls such as suspending the account, asking the user to log in again or requiring multifactor authentication.
Proofpoint Email Security addresses all attackers’ tactics and secures all threat vectors, including corporate email, personal webmail, cloud apps to end-users. Our integrated, end-to-end solution:

- Reduces the risk of BEC and EAC by protecting across broad range of attacker tactics.
- Provides visibility into all the email sent using your domain, including trusted third-party senders, as well as compromised account risks from cloud apps.
- Stops impostor email and fraudulent use of trusted domains and detects compromised cloud accounts and phishing.
- Identifies who your most attacked people are, who’s being attacked with credential phishing and impostor emails, and who’s vulnerable to credential theft.
- Enables you to apply adaptive controls, such as browser isolation and security awareness training, to your Very Attacked People™.
- Trains your end users to become more resilient to BEC and EAC attacks.

With deep visibility into all these areas, you can better understand the threat, communicate risks to the board and business peers and prioritize mitigation. We remove the complexity of managing different point solutions from different vendors. With this comprehensive approach, you can optimize resources to improve security and operational effectiveness.
Making the most of your Proofpoint Partnership

There are various ways to maximize your investment with Proofpoint. Take advantage of these services that are available to you — visit https://go.proofpoint.com/New_Perimeters_2021 and read ‘Continue your Journey with Proofpoint’ to learn more.

Nexus People Risk Explorer

Our new Nexus People Risk Explorer gives our customers a people-centric way to identify risky users, including the most attacked, most vulnerable, and most privileged users in an organization — into a single view.

The tool provides actionable recommended risk mitigations. The underlying risk model leverages machine learning and combines real-time Proofpoint Nexus threat telemetry across cloud (CASB), email, and security awareness training. This multi-trillion data point threat graph includes more than two billion daily emails, 13 million active cloud accounts, 86,000+ social media accounts, and 400,000-600,000 daily malware samples.

To request a free trial, visit https://go.proofpoint.com/Nexus_People_Risk_Explorer

Key Benefits:

- Understand your people-centric security risk across threat vectors and risk factors.
- Optimize risk mitigation, and lower the cost of deploying new security controls.
- Monitor your progress, and benchmark your people-centric security risk against other companies.
Virtual Executive Briefing Centre

As a Proofpoint customer, you have the opportunity to access our virtual Executive Briefing Centre.

During a virtual EBC, you’ll meet with our Executive Team for strategic discussions on topics of your choice and get the chance to learn about our new products and services. If you’d like to understand more about how a virtual EBC could benefit you — visit https://go.proofpoint.com/Virtual_EBC to request a call from your account manager.

‘Very Attacked People’ and Threat reports

As a Proofpoint customer, you can request these reports and analysis, specifically tailored to your company and industry vertical.

Very Attacked People (VAP) reports show our customers the most highly attacked end users within their organizations, and the types of attacks they have been receiving. This specific data and analysis helps you to optimize your security strategy, ensuring your VAPs are identified, protected and educated on the risks they are exposed to as part of their role.

VAP reports are a self-service feature that can be accessed via the TAP (Targeted Attack Protection) dashboard.

You can also request a Threat Report that is specific to your industry vertical, giving you the latest insight into the threat landscape that your company is exposed to. Visit https://go.proofpoint.com/VAP_Threat_Reports for more details.

Meet with a Proofpoint resident CISO

We have a team of resident CISO’s, here to support and represent our customers. They act as internal champions on behalf of customers within Proofpoint, supporting with insight and advice on any topic.

Our resident CISO’s are available to meet with customers 1-2-1, and are focused on building Proofpoint CISO communities. If you would like to arrange a meeting with one of our CISO’s — visit https://go.proofpoint.com/meet_with_a_CISO to request a call from your account manager who can help to set this up.

Customer Business Reviews

As part of your Proofpoint investment, you have the opportunity to join regular Customer Business Review (CBR) meetings.

A Proofpoint Customer Business Review (CBR) isn’t just a health check, it’s an opportunity for your key Security leaders to hear vital, board-relevant information about how your organization is being attacked, which individuals are being targeted (and by whom), and how you compare with similar organizations in your sector. A regular CBR ensures you are getting the most out of your Proofpoint investment and can be arranged to include the following and more:

- Proofpoint Health Check
- People-Centric Threat Review
- Proofpoint Corporate and Product Updates with Road Map
- Customized Threat Landscape Report
- Review of key support cases

To organize your next CBR, visit https://go.proofpoint.com/customer_business_reviews to request a call from your account manager.
USEFUL CONTACT DETAILS

If you would like to contribute to a future issue of New Perimeters, or to give feedback, contact Rebecca Cleveland: rcleveland@proofpoint.com

To view the digital version of New Perimeters, visit: https://go.proofpoint.com/New_Perimeters_2021

Technical Training:
www.proofpoint.com/us/support/technical-training
training@proofpoint.com

Proofpoint University:
www.proofpointlevelup.com/

Proofpoint Community Support:
www.proofpoint.com/community

Professional Services:
services@proofpoint.com

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.

More information is available at www.proofpoint.com