Understanding BEC Scams: Supplier Invoicing Fraud

proofpoint.com/us/blog/cybersecurity-essentials/understanding-bec-scams-supplier-invoicing-fraud

December 14, 2020

December 07, 2020 Tony Paterra

About the Series:

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.

An indication of how pervasive a problem BEC/EAC is: Proofpoint blocks over 15,000 BEC/imposter messages a business day or nearly 4 million messages a year.

In this series, we cover BEC/EAC attack types that Proofpoint considers the most important for a business to be aware of. In each of these posts, we explain what the attack is and how it works so that you can better understand these BEC/EAC attacks and can better protect yourself. In this post, we focus on BEC/EAC supplier invoicing attacks.

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.

Proofpoint stopped multiple million dollar supplier invoicing scams in 2020.

BEC supplier invoicing fraud can be so successful that even prominent, well-known individuals can fall for them. In February 2020, Shark Tank's Barbara Corcoran nearly lost close to US$400,000 to a BEC supplier invoicing attack. Happily for her, they were able to recover the funds before the attackers were able to collect them. That happy ending however is rare: BEC supplier invoicing scams rarely end with funds being successfully recovered.

This example is consistent with the high payoff successful supplier invoicing scams can yield. Proofpoint has successfully stopped invoicing fraud that could have yielded attackers millions of dollars if successful.

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 below). 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.

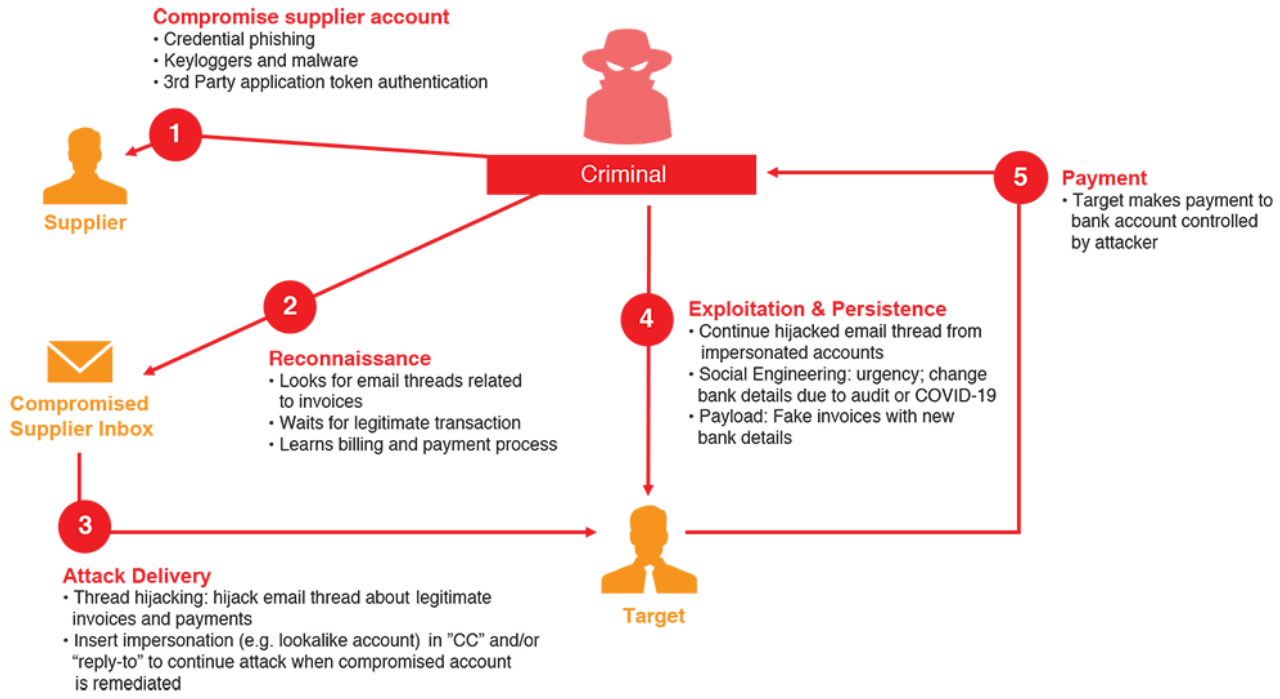


Figure 1: Anatomy of a Supplier Invoicing Fraud Attack

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 be 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 images below 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.

From: Chris@supplier (compromised supplier account)
To: Jason (target)

"External Message"
Thanks Connie~

Dear Jason,

Hope you are well.
The following invoices are due or will be due in Apr. And now we haven't received the payment from you side.
Could you please help to arrange the payment in Apr? Thank you.

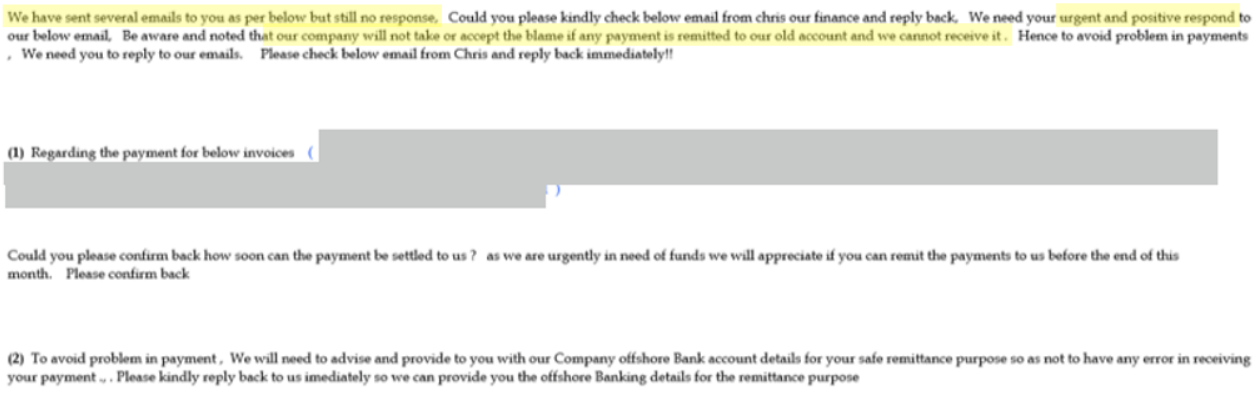
Total amount: USD 2,791,867.92

Class	Number	Amount(USD)	Days Late	Transaction Date	Due Date
Invoice		179,976.49	43	12-26-2019	03-10-2020
Invoice		15,328.07	34	01-04-2020	03-19-2020
Invoice		36,128.50	31	01-07-2020	03-22-2020
Invoice		29,744.80	31	01-07-2020	03-22-2020
Invoice		62,243.65	29	01-09-2020	03-24-2020
Invoice		9,306.72	28	01-10-2020	03-25-2020
Invoice		8,846.00	28	01-10-2020	03-25-2020
Invoice		1,873.20	28	01-10-2020	03-25-2020
Invoice		3,439.44	27	01-11-2020	03-26-2020
Invoice		54,257.82	27	01-11-2020	03-26-2020
Invoice		1,267.58	24	01-14-2020	03-29-2020
Invoice		11,290.40	22	01-16-2020	03-31-2020

Figure 2: Hijacking Email Thread from Compromised Supplier Account to Target Account 1

In Figure 3 the attackers pivot from the compromised account to an impersonated account fully under the attacker's control. This account appears to be another trusted individual from the supplier sending a follow up email to both target victims. The impersonation is carried out through use of a fake account made to seem like the trusted individual's account.

From: Sobha_supplier@fake.com (*impersonated* supplier account)
To: Jason and Carrie (targets)



We have sent several emails to you as per below but still no response. Could you please kindly check below email from chris our finance and reply back. We need your urgent and positive respond to our below email. Be aware and noted that our company will not take or accept the blame if any payment is remitted to our old account and we cannot receive it . Hence to avoid problem in payments , We need you to reply to our emails. Please check below email from Chris and reply back immediately!!

(1) Regarding the payment for below invoices (

Could you please confirm back how soon can the payment be settled to us ? as we are urgently in need of funds we will appreciate if you can remit the payments to us before the end of this month. Please confirm back

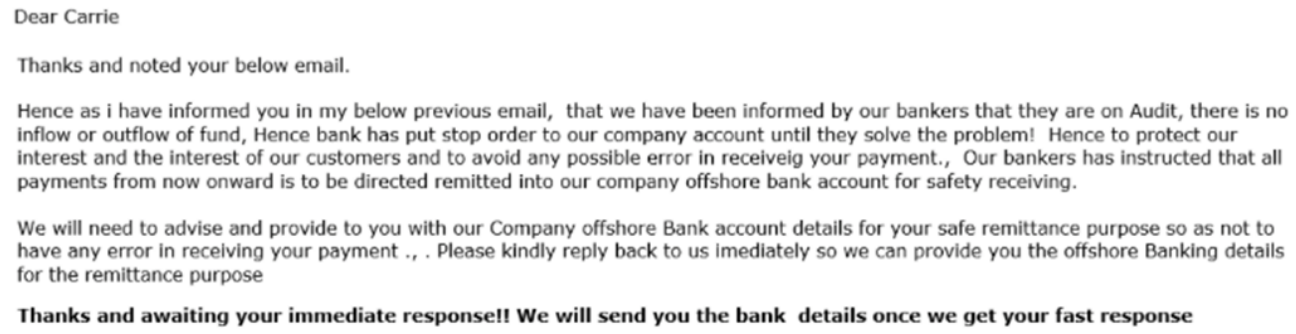
(2) To avoid problem in payment , We will need to advise and provide to you with our Company offshore Bank account details for your safe remittance purpose so as not to have any error in receiving your payment ., . Please kindly reply back to us imediately so we can provide you the offshore Banking details for the remittance purpose

Figure 3: Email from Impersonated Account to Both Target Accounts

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.

From Chris (*compromised* supplier account)
To: Carrie (target)



Dear Carrie

Thanks and noted your below email.

Hence as i have informed you in my below previous email, that we have been informed by our bankers that they are on Audit, there is no inflow or outflow of fund, Hence bank has put stop order to our company account until they solve the problem! Hence to protect our interest and the interest of our customers and to avoid any possible error in receiveig your payment., Our bankers has instructed that all payments from now onward is to be directed remitted into our company offshore bank account for safety receiving.

We will need to advise and provide to you with our Company offshore Bank account details for your safe remittance purpose so as not to have any error in receiving your payment ., . Please kindly reply back to us imediately so we can provide you the offshore Banking details for the remittance purpose

Thanks and awaiting your immediate response!! We will send you the bank details once we get your fast response

Figure 4: Email from Compromised Supplier Account requesting bank change for 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 deception, 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 to implement adaptive controls to mitigate that risk.

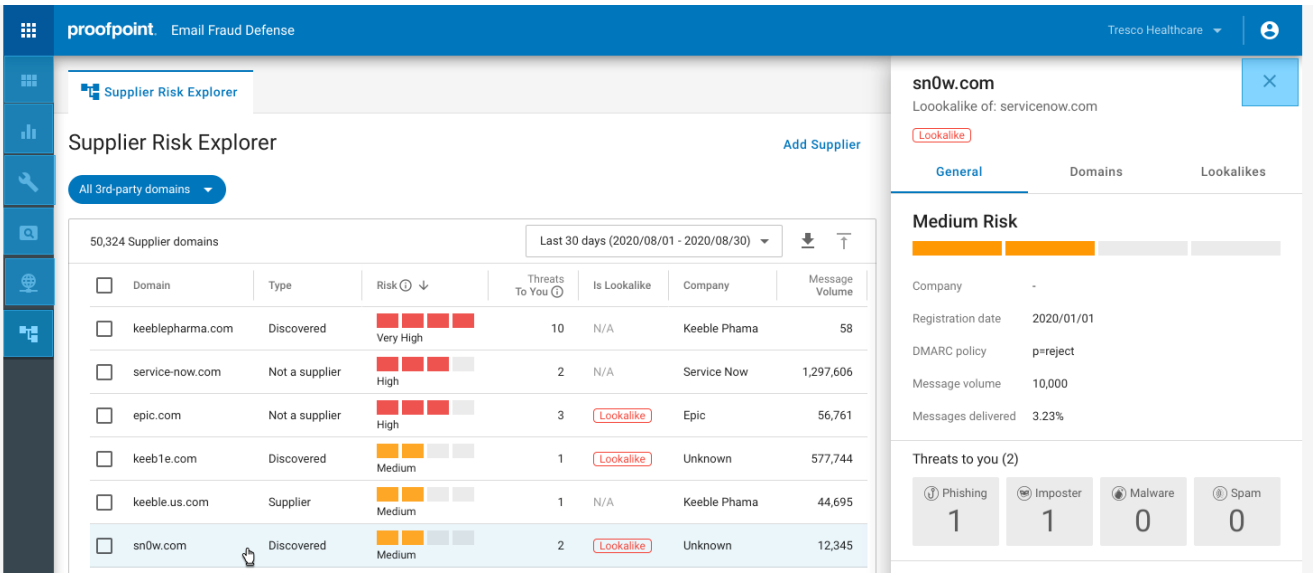


Figure 5: Nexus Supplier Risk Explorer automatically identifies your suppliers and the risks they pose

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 an 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, included forwarded mail and distribution lists.

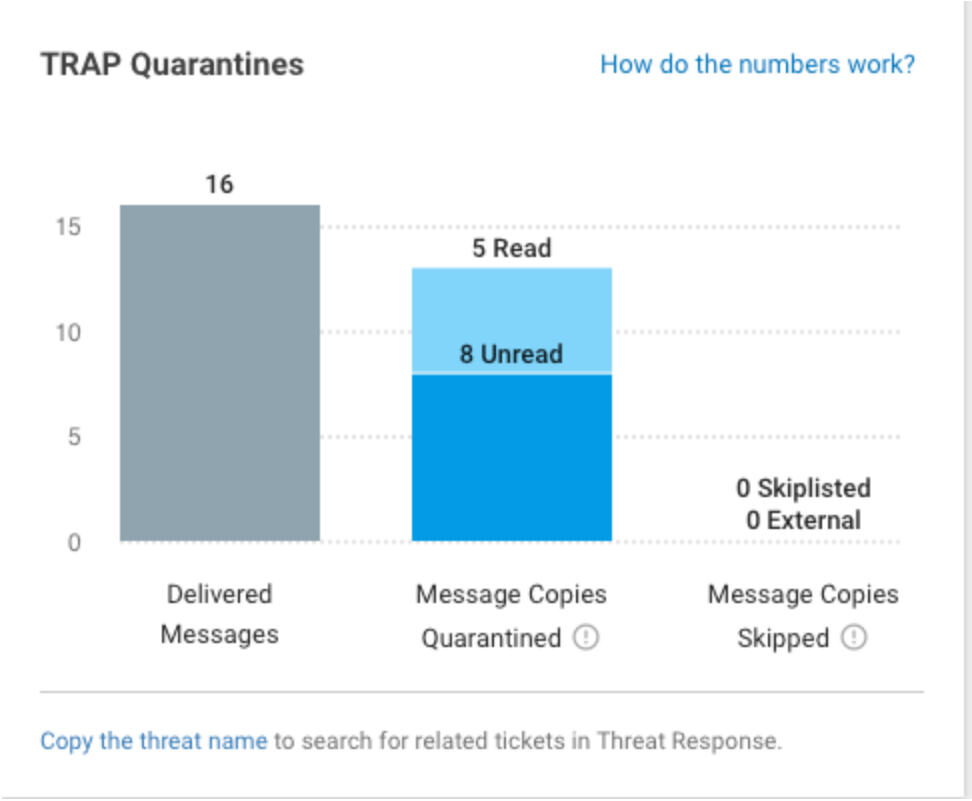


Figure 6: Detailed reporting helps incident responders understand what type of BEC attack and understand who received this attack.

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.

One of the most important things you can do to help protect against BEC/EAC gift card scams is to understand how prepared your organization is to combat them. Find out by taking our BEC/EAC readiness assessment here.

Subscribe to the Proofpoint Blog