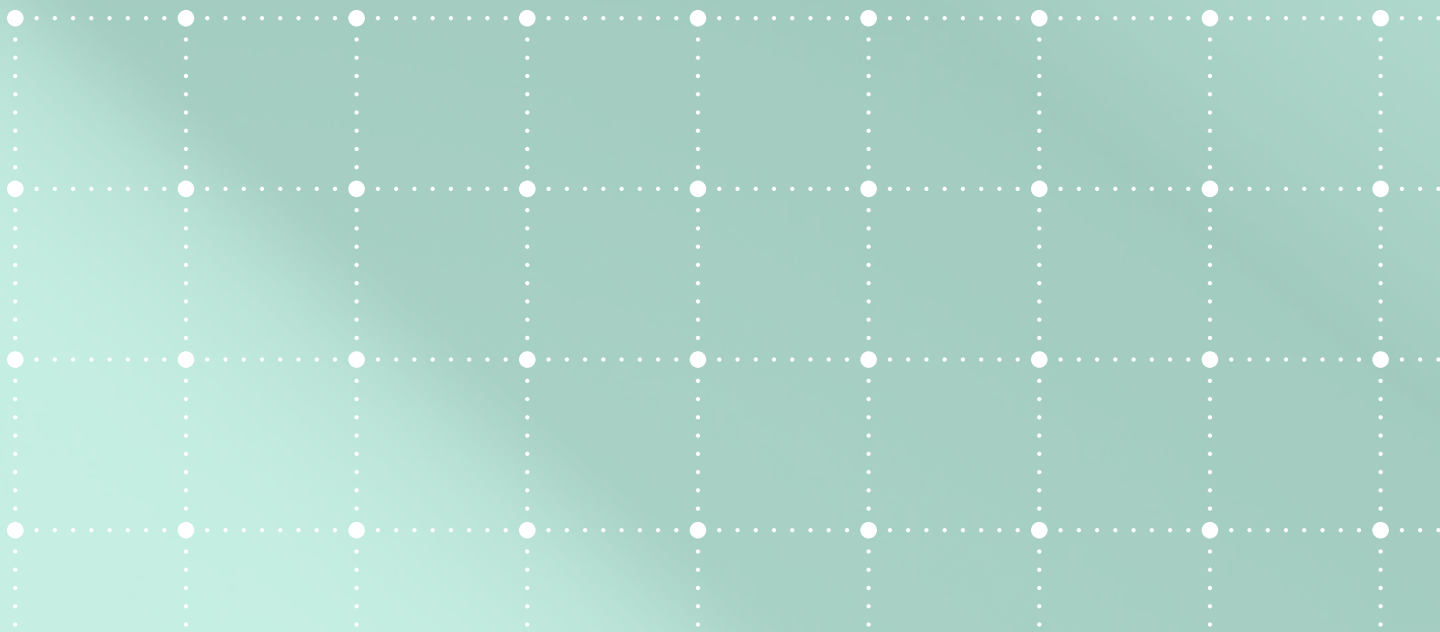


Abnormal



From CEO Fraud to Vendor Fraud:

The Shift to Financial Supply Chain Compromise



Executive Summary

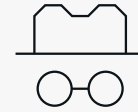
Since its initial identification in 2013, business email compromise (BEC) has been dominated by executive impersonation. But over the past few years, attackers have adjusted their strategies—opting to impersonate third party vendors and suppliers instead. In January 2022, the number of attacks impersonating third parties surpassed those impersonating internal employees for the first time. This trend has continued each month since, with third-party impersonations making up 52% of all BEC attacks in May 2022.

We've seen this shift to what we've termed financial supply chain compromise for a number of reasons, most notably because it gives threat actors a plethora of additional trusted identities to exploit. Even the smallest businesses likely work with at least one vendor, and larger companies have supplier numbers in the hundreds or thousands. And while the average employee has some level of familiarity with the company's executive team, they may not have that same awareness of the organization's entire vendor ecosystem—particularly in larger enterprises. Further, the vendor-customer dynamic has an intrinsic financial aspect to it, which means emails requesting payments or referencing bank account changes are less likely to raise red flags.

All of these factors combine to make a perfect environment for exploiting end user trust, typically in one of four ways.

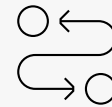
Vendor email compromise, the most impactful form of financial supply chain attacks, utilizes the compromise of a supplier's mailbox to target their customers and divert funds from a legitimate business transaction.

Aging report theft starts with the impersonation of a vendor's executive, then uses outstanding payment information to target the supplier's customers and request that outstanding balances be paid to a new account.



52%

Percentage of BEC attacks impersonating third parties in 2022.



\$2.1 million

Largest financial supply chain compromise blocked by Abnormal to date.

Third-party reconnaissance attacks leverage open source intelligence to understand the relationship between vendors and their customers, then use that information to attempt to redirect payments without actually having visibility into those transactions.

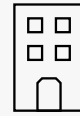
Blind third-party impersonation attacks have no direct insight into vendor-customer relationships or financial transactions and instead rely on the effectiveness of pure social engineering to be successful.

No matter which tactic threat actors use, the fact remains that this shift to financial supply chain compromise is an important milestone in the evolution from low-value, low-impact attacks like spam to high-value, high-impact attacks that can cost thousands of dollars. Abnormal research found that the average vendor email compromise attack costs \$183,000, and the highest amount requested thus far was \$2.1 million. All this goes to show us that advanced security measures are needed to protect against these evolving threats. Without them, it's no longer a matter of *if* there will be a successful attack but instead *when* one will occur.



\$183,000

Average cost of a vendor email compromise attack seen by Abnormal.



17%

Year over year decrease in attacks impersonating internal employees.



Table of Contents

The Recent Expansion in Business Email Compromise	5
An Introduction to Financial Supply Chain Compromise	8
How Attackers Impersonate Vendors	10
Four Types of Financial Supply Chain Compromise	15
Conclusion	32
About Abnormal	33

The Recent Expansion in Business Email Compromise



The impact of business email compromise, or BEC, is undeniable, with the total exposed losses tallying [\\$43 billion](#) over the past five years. And despite best efforts to prevent these attacks, they've continued at an astonishing volume, with more than [\\$2.4 billion](#) in actual losses in 2021—a 28% increase over the previous year.

A Brief History of Business Email Compromise

When BEC first entered the cybercrime scene, it was dominated by CEO impersonations. In these attacks, threat actors would access or spoof the email accounts of chief executive officers to convince unsuspecting employees to send wire transfers to unauthorized locations. Unlike phishing campaigns and legacy attacks that relied on sending millions of emails with little targeting and no personalization, BEC attacks are successful because they do the opposite.

Because they are highly targeted and personalized emails without malicious links or attachments, these attacks are difficult for secure email gateways to detect, and once delivered, they can easily dupe the target themselves. Combining a sense of urgency with the authority that a CEO commands, a well-crafted email can convince even the most security-conscious employee to complete the request. And while the attacks started almost entirely as wire transfer requests, they have evolved in recent years, where threat actors now request gift cards, or access to sensitive information like PII through W-2 forms.

In recent years, however, particularly as employees became aware of the fact that their CEO is unlikely to email them with these requests, threat actors have had to change their tactics.

2021 Business Email Compromise Statistics

\$43+

billion lost since 2016

\$180,000+

lost per attack

35%

of all cyber attacks

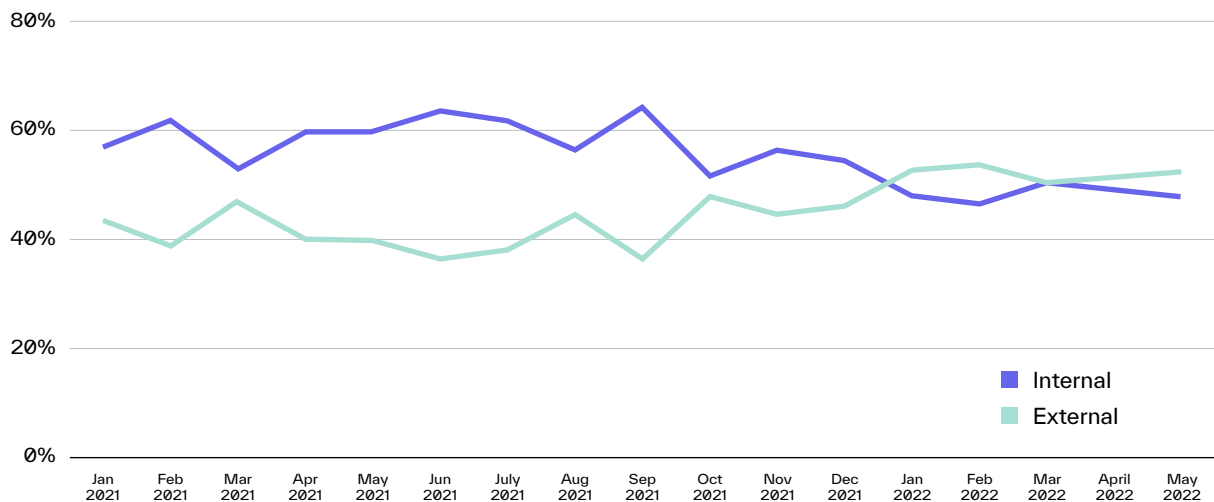
*Source: 2021 FBI Internet Crime Report

The Rise of Financial Supply Chain Compromise

Enter the rise of financial supply chain compromise, where cybercriminals are no longer reliant on impersonating top executives to run their scams. Instead, they are impersonating known (and even unknown) vendors to request that invoices be paid, billing account details be updated, or wire transfers be completed. And because the number of vendors working with a company is much, much higher than the number of CEOs within that same organization, the results are astounding.

Starting in January 2022, third-party impersonations overtook internal impersonations for the first time—and this trend continued each month since. Year over year, we've seen a 17% decrease in internal impersonations, and as of May 2022, threat actors are using the names and accounts of external vendors in 52% of all attacks.

Trend of Internal vs. External BEC Impersonation Attacks



This shift has had a profound impact on the entire cybercrime ecosystem, helping to keep BEC as the top cybercrime for the seventh year in a row. With benign attachments like invoices or purchase orders and without known malicious signatures to flag, financial supply chain compromise attacks are more likely to bypass legacy infrastructure and trick end users—causing organizations to lose millions.

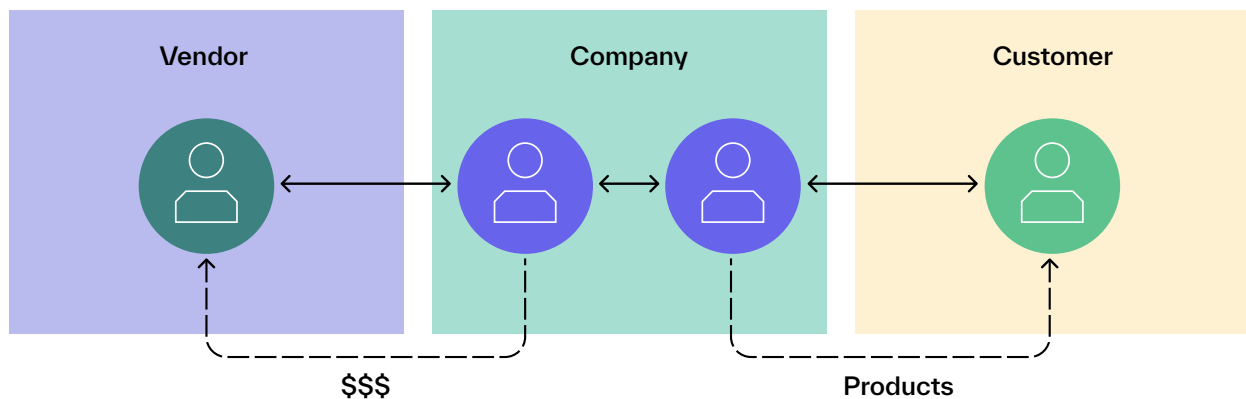
An Introduction to Financial Supply Chain Compromise

A subset of business email compromise, financial supply chain compromise uses external third-party impersonation to redirect the flow of funds exposed during the normal course of business. By exploiting the trust in the impersonated identity and the implicit authenticity of business email, these kinds of attacks can result in heavy losses for victims.

Nearly every business has at least a few vendors, and large enterprises may have hundreds or even thousands—making virtually any organization a potential target. Vendor payments can be some of the largest financial transactions made by a business, so when payments are stolen, it can be a heavy burden. In fact, the largest supply chain compromise attack stopped by Abnormal included a fake invoice for over \$2.1 million.

And on the other end, no vendor wants to be impersonated in these schemes, as they can cause compliance and reputation problems. Client trust is difficult to earn back once lost, particularly if the vendor name was used extensively in the scheme or if multiple customers lost money.

Much like pirates once plundered the new world's riches at their most vulnerable, in transit across the Atlantic Ocean, attackers target email as the easiest method to access financial transactions. The below figure illustrates the basic financial supply chain relationship, wherein a company purchases services from vendors and provides goods or services to customers while communicating via email. The illustration also shows that funds are most vulnerable when they are exposed externally.



Information about invoices, billing accounts, and upcoming payments is often discussed via email on both sides of this equation, even if the payments themselves are made through secure software. For example, here at Abnormal, we communicate with vendors like Salesforce, Marketo, Zoom, Microsoft, and dozens of others to run our business. On the other side, we provide our email security solution to hundreds of customers, many of whom we communicate with almost exclusively through email. Most businesses adhere to this general pattern, with the number of vendors changing based on the business model. For example, [retail giant Walmart has over 100,000 suppliers](#) across the globe, giving threat actors over 100,000 chances to infiltrate a vendor account and target the company.

How Attackers Impersonate Vendors

Much like traditional BEC attacks, a supply chain compromise attack requires the use of a trusted identity to run the scam. In these attacks, however, the person being impersonated is an external third-party rather than an internal executive or other employee. This impersonation can be accomplished in two main ways.

01 Account Compromise

The most dangerous type of supply chain compromise occurs when an external email account is truly compromised, as it provides opportunity for long-term surveillance and the hijacking of ongoing conversations. Upon gaining credentials to an external mailbox, most attackers will quickly determine which customers are active and identify ongoing payment cycles or outstanding invoices. Fraudsters then exploit that knowledge to impersonate a vendor and insert themselves into an email conversation about a financial transaction—sometimes using an email sent from the compromised account itself.


An essential component of this tactic is the ability to compromise the account, typically through the use of a credential phishing attack. In these attacks, an email is sent to the target that appears to come from a trusted source, typically a brand name like Microsoft, or an internal department like IT or HR. These emails are meant to inspire action, prompting the unsuspecting employee to enter their email address and password. Once those credentials are entered on the fake website, they become fair game for the next stage of the attack.

After the threat actor has access, they manipulate mailbox rules to prevent its owner from becoming aware of both the intrusion and the correspondence with his or her regular contacts. Diligent surveillance of the compromised mailbox could represent the difference between successful payment and discovery, so attackers exploit email rules, such as folder rules and message forwarding, to control message exposure. By doing so, they can keep access to the account, sometimes for months.



Examples of Phishing Emails Used to Compromise Mailbox Credentials

From: SharePoint@ [redacted] 05/06/2022, 5:59PM
Subject: Updated Financial Reports
To: [redacted]


 **SharePoint** Open Files

[Financial Reports and Cash Flow Sta....pdf](#)
453 KB • This document will expire in 3 days.


Your Organization has shared a secured document with you through Microsoft SharePoint.
Sign in with your Microsoft account to access the shared files via [Sharepoint](#)

Sign in with your Microsoft account to access the shared files via [Sharepoint](#)

The Attached SharePoint document only works for the direct recipients of this message in your organisation


 **Microsoft 365** Privacy statement
Microsoft Corporation, One Microsoft Way, Redmond WA 98052 USA


From: HR@ [redacted] 05/19/2022, 5:59PM
Subject: Folder " [redacted] /Bonus Payments 2022" Has Been Shared With You.
To: [redacted]




HR@ [redacted] shared a folder with you.

Please upload your documents in the bonus folder for 2022.

 **Bonus Payments 2022**

 This link will work for [redacted]

Open

 **Microsoft 365** Privacy statement

02 Account Mimicking

Aside from gaining direct access to an account, there are a few other ways an attacker can mimic a third party: email spoofing and lookalike domains.

In an email that uses a spoofed address, the attacker sets the from email address to look like it's coming directly from a trusted source. The trick is that the attacker creates a separate reply-to address, so when a recipient replies to the email, it gets sent to the attacker's account rather than the spoofed account. Email spoofing takes advantage of the lack of built-in authentication within the email protocol and it requires shockingly little technical knowledge to perform. To combat email spoofing attacks, many organizations have implemented DMARC policies that help verify an email's authenticity.

Example of an Attack Using a Spoofed Email Address

From: **John Smith** <accounting@████████.com> 05/16/2022
Subject: **Invoice's Due/Open "Update"**
Reply to: accounting@yandex.com
To: undisclosed-recipients

Dear Partner,

We kindly ask that you re-confirm to us the status of our outstanding or any due payments if there are any, as we currently have to give you an updated information.

Please get back to us immediately with the total amount that is outstanding with corresponding due dates and invoices respectively.

If you need any further information, please do not hesitate to contact me for further assistance.

Thank you for your compliance.

Kinds Regards

John Smith
Accounting Department
████████████████████

The next best thing to a spoofed email address is a carefully selected lookalike domain. With a lookalike domain, the goal is to register a new domain containing a subtle or common misspelling so that the target overlooks the error. These domains then host email address(es) used to further the impersonation scheme, and because they look so similar to real email addresses, targets often do not realize that they are speaking with a scammer.

Bad actors intentionally register subtly misspelled versions of a domain they are impersonating, employing tactics such as the following:



Changing characters to other similar-looking characters, like:

- [twlttter.com](#)
- [go0gle.com](#)



Adding additional characters after two repeated characters, such as:

- [faceboook.com](#)
- [apple.com](#)



Adding additional location-related or company-related characters, including:

- [amazonsellerservices.com](#)
- [microsoft-usa.com](#)



Using a different top-level domain or embedded hostname, like:

- [instagram.online](#)
- [walmart.com.shopping.com](#)

While account mimicking doesn't provide an attacker with the same breadth of internal visibility as a compromised account, it still allows the actor to convincingly imitate a third party and increases the likelihood for success.

The Four Types of Financial Supply Chain Compromise

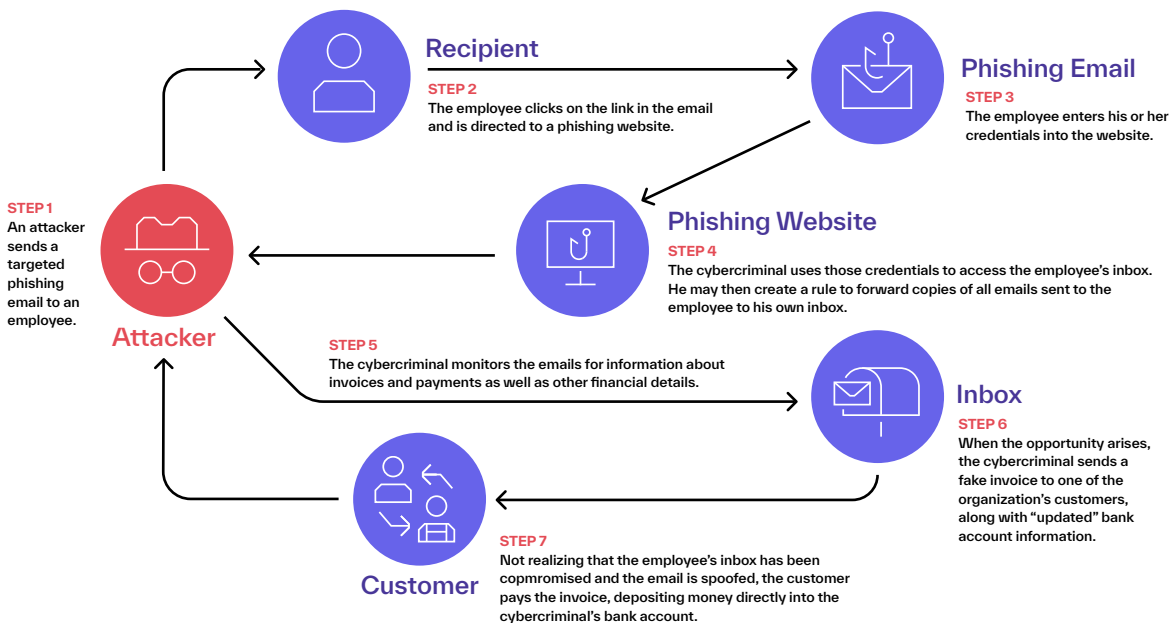


The category of financial supply chain compromise is comprised of four main subsets: vendor email compromise, aging report theft, third-party reconnaissance attacks, and blind third-party impersonation attacks. Each of these attack types leverages a different level of insight into vendor-customer relationships and has differing levels of visibility into legitimate financial transactions.

01 Vendor Email Compromise

The most impactful form of financial supply chain compromise is vendor email compromise, or VEC. In a VEC attack, an actor first compromises the mailbox of a vendor or supplier, then impersonates that vendor to target the vendor’s customers and divert funds from a legitimate business transaction. Attackers behind VEC attacks have direct access to a rich source of intelligence about vendor-customer relationships, including the exact details of financial transactions between the two parties.

How a Vendor Email Compromise Attack Works



The first stage of a VEC attack involves the attacker compromising the mailbox of a high-value target at a vendor or supplier company. These high-value targets are generally accounts payable specialists or other employees that handle customer payments. In most cases, this initial compromise is the result of a credential phishing attack that impersonates an enterprise application, such as Microsoft OneDrive, SharePoint, Adobe, or DocuSign. The initial credential phishing email often asks the recipient to “validate” their identity by providing their email credentials.

Once a vendor employee's mailbox has been compromised, an attacker begins collecting information that will help them in the next phase of the attack. In many cases, this involves adding a forwarding or redirect rule to the mailbox that sends copies of all incoming mail containing certain keywords to another external account—one that is under the control of the attacker. An attacker may sit on a compromised mailbox for days, weeks, and sometimes even months to gain in-depth visibility into vendor-customer communication patterns, payment dates and amounts, and primary customer contacts.

After an actor has collected all the information they need, they're ready to move into the second phase of their attack. This second phase involves the attacker inserting themselves into a legitimate financial transaction by impersonating the vendor and requesting a customer to redirect funds to a new bank account. While an attacker may leverage their access to a vendor employee's mailbox to send second-stage emails directly from that account, most actors will set up separate accounts from where they'll communicate with the victim. Usually, this will involve an attacker registering a lookalike domain that resembles the vendor's legitimate domain.



One of the tactics actors use at the beginning of the second stage of a VEC attack is called **thread hijacking**. With this tactic, an attacker includes the content of previous vendor-customer communications in their outreach to a victim to establish credibility and make it look like the attacker is simply responding to an existing email thread. Even if an attacker communicates with a customer using a separate account, all they need to do is copy and paste the content from a pre-existing thread into a new email and it looks as though the attacker's email is just a continuation of an ongoing conversation.

Example of a VEC Attack Using Thread Hijacking

The image shows two overlapping email screenshots. The top-left screenshot is a legitimate email from a vendor. The bottom-right screenshot is an attacker's email that hijacks the thread by using the same subject line and content as the legitimate email.

Legitimate Vendor Email (Top-Left):

From: [redacted] .com> 03/29/2022, 6:38AM
Subject: **RE: Invoices 42236 & 42231**
Reply to: [redacted] @email.com
To: [redacted]

Find attached invoices due on 3/30.
Please send payment by wire transfer, our wire details is updated on the attach invoices.
Could you confirm in reply when you will arrange wire payment?

Await your early reply,
Thank you!

On Tuesday, 03/08/2022 at 11:38
Thanks!!

Attacker's Email (Bottom-Right):

From: [redacted] <accounting@[redacted].com>
Sent: Tuesday, March 8, 2022 10:07 AM
To: [redacted]
Subject: **Invoices 42236 & 42231**

[redacted] just sent me the PO's for these.
Thank you!

2 Attachments

- Invoice_42231.pdf 173 KB
- Invoice_42236.pdf 171 KB

To add another layer of legitimacy to these attacks, threat actors sometimes use actual copies of a vendor's own invoices or other financial documents that have been stolen from the compromised mailbox. Because these invoices are exact replicas of the same invoices a customer is accustomed to receiving from the vendor, there's nothing to really differentiate the fake document from a real one. Typically, the only difference between the two is that the attacker's invoice will have modified payment account information, but everything else on the document would look exactly like the original.

Example VEC Email Containing Modified Vendor Financial Document

From: Operations <operationsm@ [REDACTED]> 05/23/2022, 3:22PM
Subject: RE: RE: Remittance
To: [REDACTED]


Hello [REDACTED],


Find attached our updated ACH detail with our W9, Please acknowledge you are in receipt of this email and notify me once payment is processed


Thanks for your business!

[REDACTED]

[REDACTED]

 2 Attachements

 EFT Vendor Direct Deposit Payables Form-.pdf 173 KB

 [REDACTED] W9.pdf 171 KB

Example of a Modified Vendor Financial Document

VENDOR AUTHORIZATION FOR AUTOMATIC DEPOSIT EFT FOR PAYABLES

COMPANY NAME [Redacted]	DATE 05/23/2022
----------------------------	--------------------

I authorize the above named company (hereafter called COMPANY) to deposit payment into the account indicated below; and I authorize the depository named below to accept my deposit and credit the amount to my account. I am responsible for notifying Accounts Payable of any bank changes.

DEPOSITORY (BANK) NAME First Financial Bank	BANK BRANCH Main
--	---------------------

CITY Weatherford	STATE TX	ZIP 76086	PHONE (IF POSSIBLE)
---------------------	-------------	--------------	---------------------

BANK ROUTING NUMBER [Redacted]	ACCOUNT NUMBER [Redacted]
-----------------------------------	------------------------------

ACCOUNT TYPE (CHECKING / SAVINGS) Checking

This authority is to remain in full force and effect until COMPANY has received written notification from me of its termination in such time and such manner as to afford COMPANY a reasonable opportunity to act on it.

NAME ON VENDOR'S ACCOUNT:
[Redacted]

EMAIL ADDRESS TO SEND REMITTANCE TO:
operationsm@[Redacted].com

ADDRESS 1 [Redacted]

ADDRESS 2 _____

STREET _____

CITY, STATE ZIP [Redacted]

PRINT NAME _____

TITLE **President**

DocuSigned by:

SIGNATURE _____

DATE **05/23/2022**

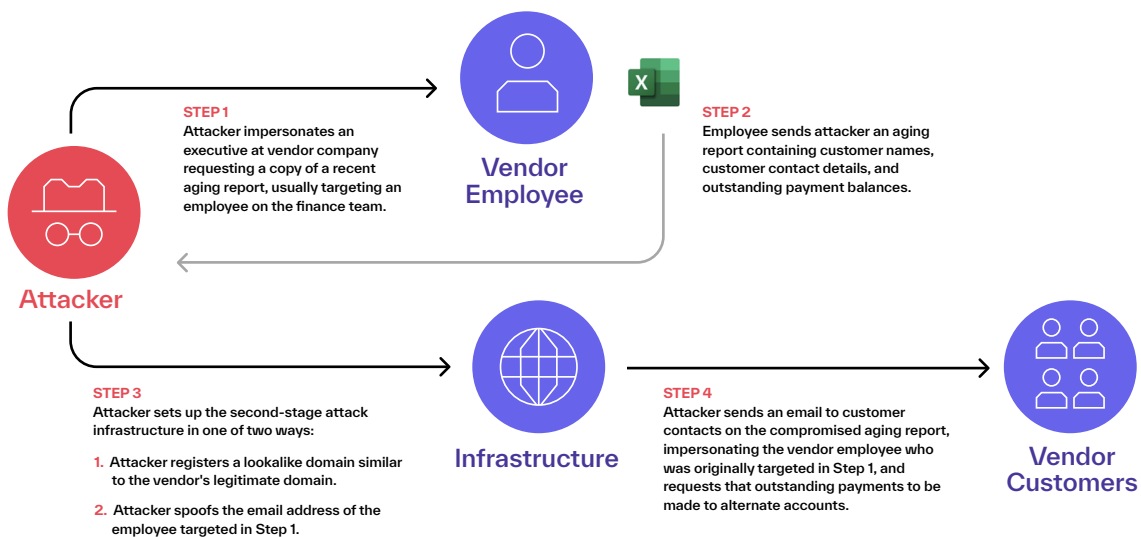
COMPANY NAME _____

Most classic business email compromise attacks contain the typical red flags we teach employees to look out for, so the average email user might look at one and ask who could possibly fall for it. But because an attacker has access to a rich source of intelligence in vendor email compromise attacks and is able to craft a very realistic-looking malicious email, the issue instead becomes *who wouldn't* fall for one of these attacks.

02 Aging Report Theft

Aging report theft is a subset of financial supply chain compromise that has become increasingly common over the last few years. While these attacks are similar to vendor email compromise in that they use insider information to craft contextually accurate attacks, they don't necessarily rely on the compromise of an email account to gather information. Instead, attackers steal a copy of a single document—an internal aging report—to collect the intelligence needed to facilitate their attacks.

How Aging Report Theft Works



Also known as a schedule of accounts receivable, an aging report lists all unpaid customer invoices and unused credit memos. In essence, an aging report is a succinct encapsulation of all outstanding payments owed to an organization and details about who to contact to inquire about those payments. As a result, these reports contain all the information a cybercriminal needs to know exactly who to target, when to target them, and how much to ask for.

Example Aging Report

Customer Name	Current	1-30 days	31-60 days	61-90 days	> 90 days	Total	Customer Contact	Customer Email Address
ABC Corp	\$113,101.40	-	-	-	-	\$113,101.40	ABC Corp	ABC Corp
DEF Inc	\$45,186.70	\$127,881.20	-	-	-	\$173,067.90	DEF Inc	DEF Inc
GHI LLC	\$68,365.75	\$118,846.40	-	-	-	\$187,212.15	GHI LLC	GHI LLC
JKL Corp	\$127,348.65	-	-	-	\$48,640.35	\$175,989.00	JKL Corp	JKL Corp
MNO Inc	\$38,324.90	-	-	-	-	\$3,324.90	MNO Inc	MNO Inc
PQR LLC	-	\$31,131.75	\$132,812.55	\$155,918.72	-	\$319,863.02	PQR LLC	PQR LLC
STU Corp	\$138,350.25	\$31,906.45	\$106,626.65	\$15,918.90	\$39,526.50	\$332,328.75	STU Corp	STU Corp
VWX Inc	-	-	-	-	\$22,002.35	\$22,002.35	VWX Inc	VWX Inc
YZA LLC	-	\$54,979.65	-	-	-	\$54,979.65	YZA LLC	YZA LLC
TOTAL OUTSTANDING	\$530,677.65	\$364,745.45	\$239,439.20	\$171,837.62	\$110,169.20	\$1,416,869.12		

An aging report attack starts off much like other types of traditional BEC attacks. The attacker usually impersonates the CEO or CFO but instead of asking an employee to make a financial transaction, the attacker simply requests a copy of a current aging report. Most of these initial emails are careful to specify that the reports also need to contain all customer contact information in addition to outstanding balances. This is an important step to knowing who to contact to request the payment be made.

From: John Smith <john.smith@company.com> 04/22/2022, 8:45AM
 Subject: Re: AR Report
 To: Lauren Rogers <lrogers@company.com>

Lauren,

I need you to email me the aging report from A/R (Due within the next 30 days and a month overdue), and also include customer payable contact email on this report

Regards,
 John

Once the employee has handed over a copy of the report, the attacker can initiate the second stage of their attack. In the next phase, the attacker uses the information in the aging report to target that company's customers, requesting they pay the outstanding balances, while also notifying them that the payments should be redirected to a new account.

In many cases, an attacker will register a lookalike domain that looks similar to the vendor's actual domain and will impersonate the same individual who was targeted in the first stage of the attack. Using these tactics, it makes this second-stage email difficult to distinguish from a legitimate email from this vendor.

Example of the Second Stage of an Aging Report Theft Attack

From: Lauren Rogers [redacted] 04/22/2022, 9:22PM
Subject: Follow up - Acme Corporation USD \$86,801.80
To: James White<james.white@[redacted]>

Hi James,
Liz, our CFO asked me to follow up with you on our payment status. Please let us know of you have any payment to remit to us.

Kindly note that our office has recently made changes to our remittance information and we advise all our payments to be remitted to our banking information via ACH, direct deposit or wire transfer only moving forward, We would provide you with our revised remittance information for proper update and payment processing.

I await your soonest response.

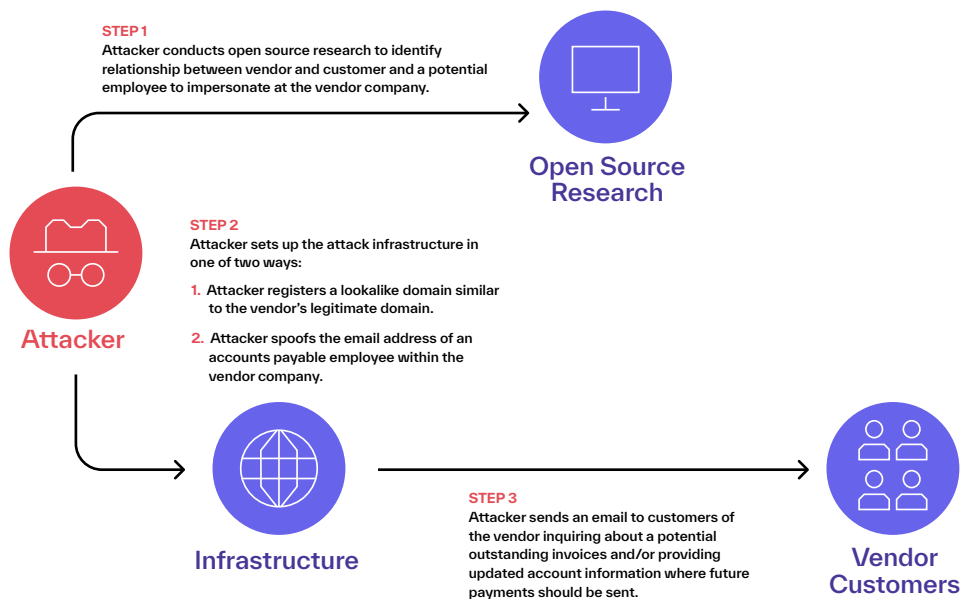
Thanks,
Lauren

The attackers behind aging report theft don't have access to the same type of in-depth intelligence gleaned from a compromised mailbox used in a VEC attack. That said, the information available in an aging report, combined with sophisticated impersonation tactics, increases the overall effectiveness of these attacks—making it one of the more impactful financial supply chain compromise attacks seen today.

03 Third-Party Reconnaissance Attacks

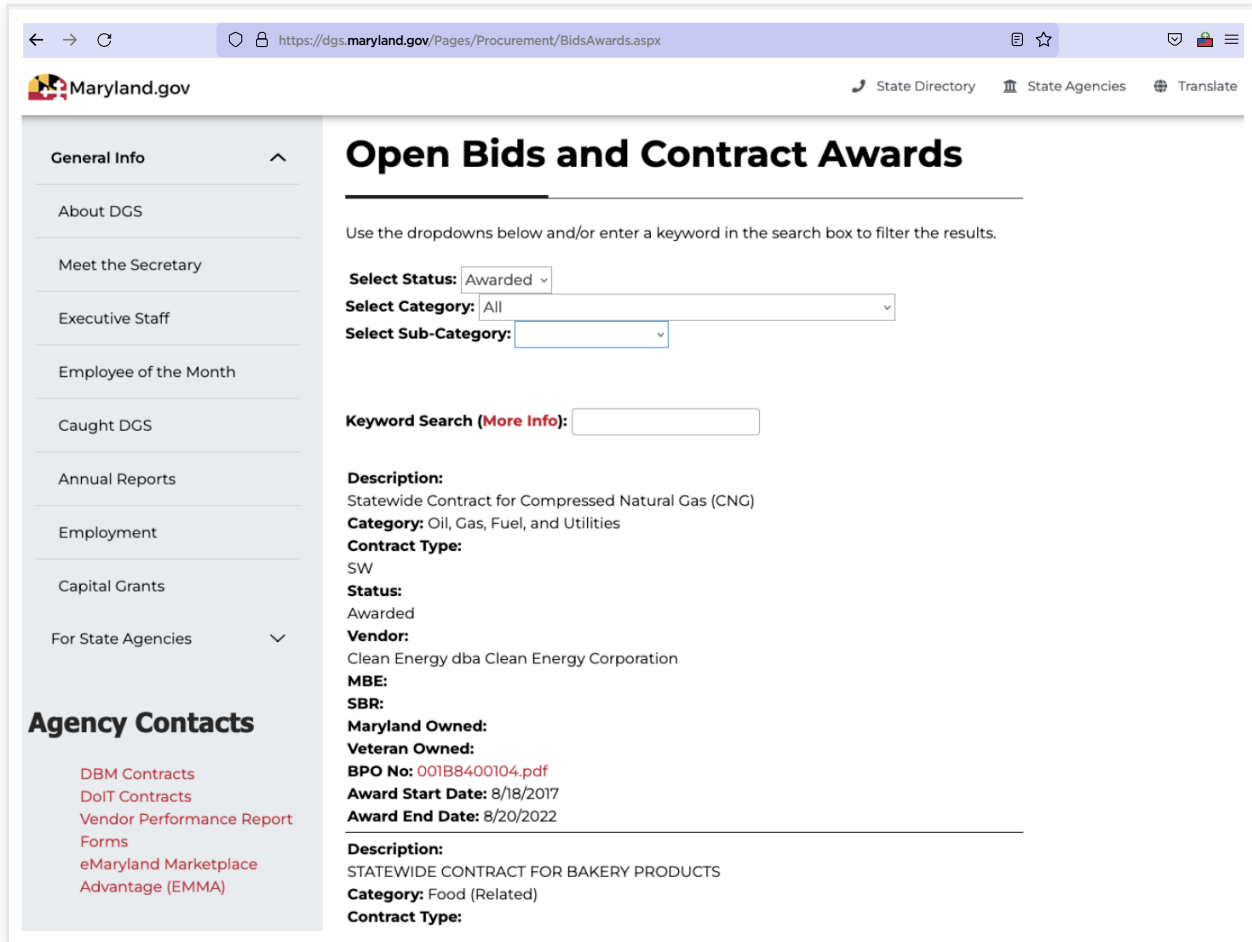
In contrast to other forms of financial supply chain compromise, third-party reconnaissance occurs when an attacker knows that there is a relationship between two organizations, but has limited or no knowledge about actual outstanding payments. In essence, an attacker in these cases has the necessary context to impersonate a vendor, but not enough information to be specific in their payment request.

How Third-Party Reconnaissance Works



These attacks typically depend on open source research in lieu of using information gained from an account compromise or document theft. It's surprising how much information is available on the internet about vendor-customer relationships. For example, many state and local governments offer detailed information about existing and previous contracts on their websites. These records provide key insights into the services a vendor has provided, contact information for both the vendor and customer, and the total contract amounts.

Example Information Available on a Government Website



Another data source that can be used to reveal business relationship information are court records. These records can provide a trove of information about business activities, names of key stakeholders and executives, or financial details from legal proceedings. They are often accessible online through various public records sources for free or a small fee.

A final place an attacker could go to identify a vendor's customers is the vendor's own website. Many times, a company will provide the names or logos of their customers to help market their products or services via customer proof. While this information is usually limited, it at least gives an adversary a small piece of information they can exploit in an attack.

Once an attacker has collected this information, they will then initiate their attack by impersonating the vendor and emailing a customer, inquiring about a potential outstanding payment. Because an attacker doesn't have specific knowledge about an actual overdue invoice, however, these initial emails tend to be a little more generic. Instead of referencing actual amounts, an attacker may simply ask if there are any payments in process, request a copy of the invoice, and mention that their payment account details have recently changed.

Example of a Third-Party Reconnaissance Attack Requesting an Outstanding Payment

From: [Susan Downs <sdowns@abnormal.com>](#) 05/12/2022, 9:53PM
Subject: **Outstanding Payments**
Reply-To: [Susan Downs <mimbills@outlook.com>](#)

Hello,
Our payment record file shows that there is an outstanding payment that is overdue with you. Can you confirm to us the status of our outstanding and due payments?
Please get back to us at the earliest with the total amount outstanding with corresponding due dates and invoices respectively.

We would appreciate it if you could check this out on your end and If the payment has already been sent, please kindly notify us but put an hold on any due payments because of recent changes in our company details.

Kind regards,
Susan Downs
Accounting Manager

[Susan Downs](#)
[sdowns@abnormal.com](#)
[\(800\) 456-1234](#)

Rather than requesting payment for a current invoice, another tactic that a threat actor might use is to simply request that a vendor's payment account be updated so any future payments get redirected to the new account. This tactic is a little more stealthy, as the attacker isn't requesting an immediate payment—the red flag accounts payable specialists are taught to notice. Instead, actors using this tactic are playing a longer game, hoping that a simple request now will result in a payment to their redirected account with next month's payment.

Example of a Third-Party Reconnaissance Attack Requesting an Account Update

From: [REDACTED] @tohowaters.com> 05/25/2022, 1:45PM
Subject: **Please Advise on Payment Status**
Cc: [REDACTED] @tohowaters.com> [REDACTED] @tohowaters.com>
Bcc: [REDACTED]

Attn: Accounts Payable Manager:

The [REDACTED] greatly appreciates you as a valued customer and we want to thank you for your continued business.

Our office will like to update our Bank Account information details you have on file.

Please note, Mailing of check payments has been temporarily put on hold for now until further notice, All payments has to go through Direct Deposit ACH payment and Wire transfer.

Could you please check if you have any open invoice payable to us as accounting is still not able to get onto the server or into Oracle to review accounts or post payments that may have been received.

Thank you

While these attacks are not quite as effective as those that have real information, they can still result in payments being made to the new bank—often for months before the error is discovered and the banking details are changed back to the correct vendor account.

04 Blind Third-Party Impersonation Attacks

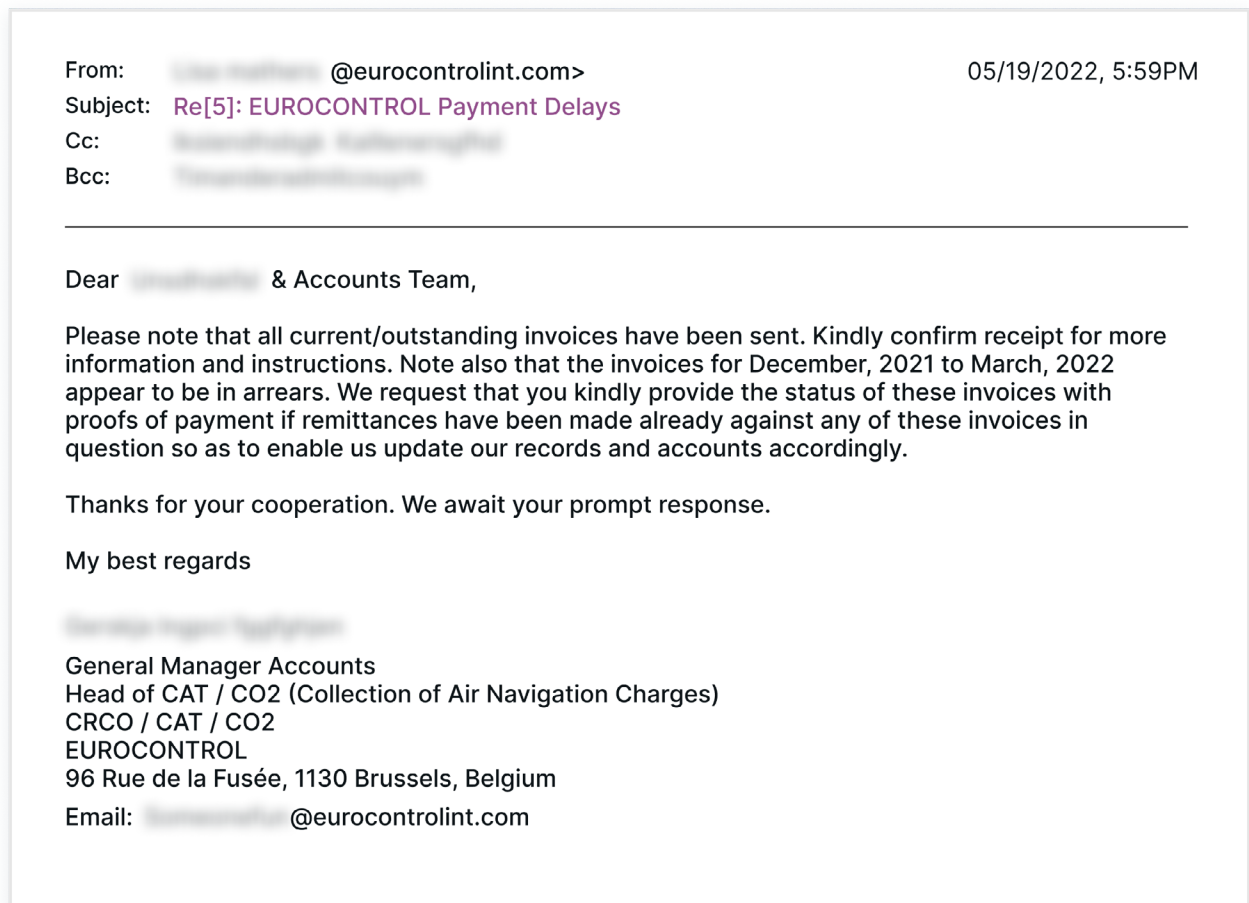
The final subset of financial supply chain compromise is a category we call blind third-party impersonation attacks. In each of the three previous categories, an attacker has at least basic knowledge about the relationship between a vendor and customer. In a blind third-party impersonation attack, however, an attacker has absolutely no knowledge about whether there is a relationship between two companies or whether a payment is actually outstanding.

Instead, scammers behind blind impersonation attacks are relying on the hope that, like so many other types of unsophisticated social engineering attacks, a target isn't paying close attention to the email and simply complies with the request.

Interestingly, we've noticed that many blind attacks impersonate some of the same third parties over and over again, sometimes for years. One of the organizations whose brand has been used in these attacks for at least the last two years is EUROCONTROL, an international organization that supports aviation across Europe. Like other blind impersonation attacks, there's no clear relationship between EUROCONTROL and the target organizations. In fact, in many cases, the target companies aren't located in Europe or even part of the aviation industry, and the emails don't reference specific payments. Instead, these attacks generally mention that a number of monthly invoices are past due.



Example of a EUROCONTROL Blind Impersonation Attack



Other organizations we've seen repeatedly used in blind third-party impersonation attacks include the International Air Transport Association (IATA) and PricewaterhouseCoopers (PwC), a multinational professional services organization. In some of the PwC impersonation campaigns we've observed recently, attackers have taken an additional step of manufacturing a fake email chain that includes an executive at the target company to add a component of authority to the payment request.

Example PwC Blind Impersonation Attack Email with a Manufactured Fake Email Chain

From: [redacted]@accounts-pwc.com> 05/20/2022, 11:48AM
Subject: Re: Fw: Re: PWC LLC: #1691134
To: [redacted] <send-via@mail-net-suites.com>
Cc: [redacted]

Please advise once payment has been made so I can confirm with my AR department that it has been received. Once we have received payment, we will be able to update our records.

Thank you,

[redacted], CPA
Chief Financial Officer
PWC network.

PricewaterhouseCoopers LLP
411 Hamilton Boulevard
Peoria, Illinois 61602
United States

On Fri, May 20, 2022 at 6:51 AM [redacted] <send-via@mail-net-suites.com> Wrote:

[redacted]

Could you please arrange ACH payment for this PC LP invoice today. See below and attached.

-----Forwarded message-----

From: [redacted]@accounts-pwc.com>
Sent: Thursday, May 12, 2022 10:14 AM
To: [redacted]
Cc: [redacted]@accounts-pwc.com>
Subject: PWC LP: Invoice# 001691134 Payment Due

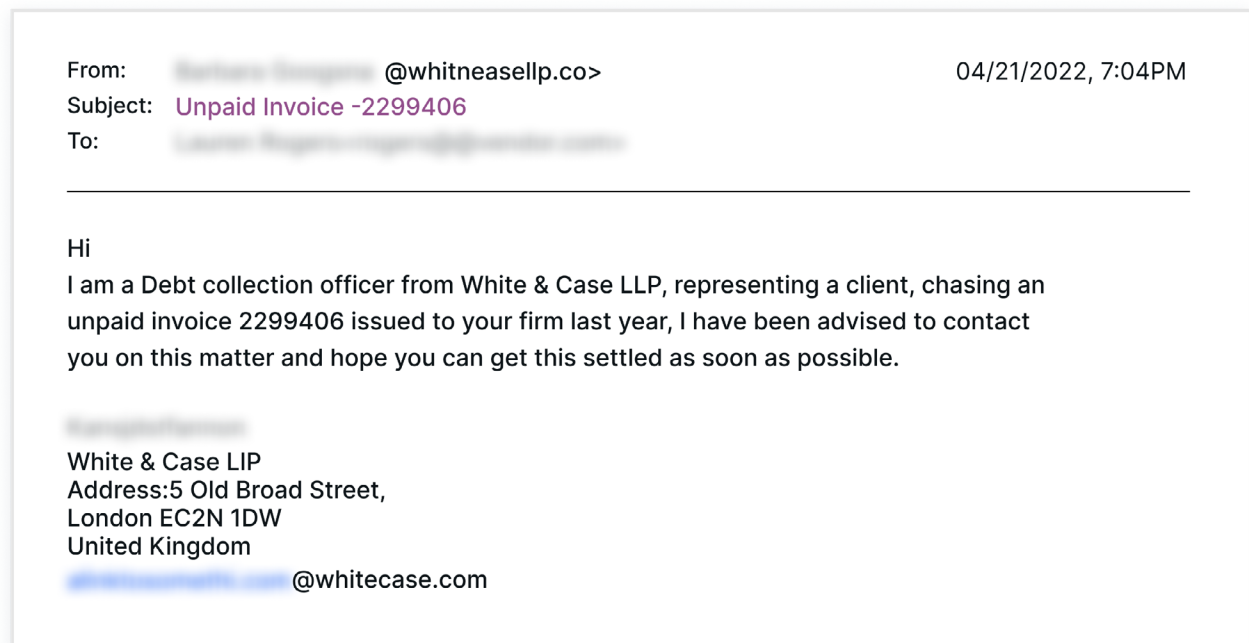
A new invoice 001691134 has been generated and is attached for your review and payment. Please make payment via ACH (Automated clearing house). Bank information is on the invoice. If you are experiencing issues viewing the attached pdf via a mobile device, please use your standard mail client or webmail.

Thank you,

[redacted], CPA
Chief Financial Officer
PWC network.

In addition to directly impersonating third parties to request payments, we've also observed an increasing trend of actors impersonating intermediaries to request payments on behalf of third parties. The most common pretext used in these attacks is the impersonation of an attorney or debt collection officer requesting to settle an outstanding invoice. Interestingly, in most of these attacks, the threat actor impersonates a real person that works at an actual law firm. That said, if an employee ran a quick Google search on the supposed sender's identity, they would find actual results to add legitimacy to the attack.

Example of a Blind Impersonation Attack Using a Debt Collection Pretext



Like traditional BEC attacks impersonating company executives or other internal employees, blind third-party impersonation attacks rely on the effectiveness of pure social engineering to be successful. Even though they don't use the breadth of intelligence we see in other types of financial supply chain compromise attacks, the fact that we continue to see them consistently increase in volume indicates that the ROI for blind impersonation attacks is worth it.

Conclusion

Whether threat actors compromise a vendor email account or simply impersonate a vendor, the fact remains that financial supply chain compromise works. Using a vendor identity provides a cover for them to run invoice fraud and aging report theft, and because their targets are often less familiar with their vendors, these attacks are much harder to identify than traditional CEO fraud.

Due to their success, these attacks from our “vendors” are only going to increase, unless we stop them at their source. Preventing vendor email compromise requires an email security solution that understands vendor behavior and can evaluate risk to determine if and when a vendor account may be compromised. And to prevent aging report theft and other forms of financial supply chain compromise, organizations should have a solution that understands identity, context, and content to block attacks before they reach inboxes.

With the rapid increase in business email compromise and this shift to vendor-focused cybercrime, now is the time to secure your environment—before the next financial supply chain compromise attack targets your organization.

Interested in Stopping Financial Supply Chain Compromise?

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

[@AbnormalSec](https://twitter.com/AbnormalSec) 

Abnormal

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

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

More information is available at abnormalsecurity.com