AGARI CYBER
INTELLIGENCE DIVISION

THREAT ACTOR DOSSIER

Silent Starling

BEC to VEC—The Emergence of Vendor Email Compromise

Executive Summary

Agari researchers have uncovered a West African cybercriminal organization that uses vendor email compromise (VEC) to surveil the communications of hundreds of companies and steal millions from their global supply chains.

Business email compromise has grown into a billion dollar industry as cybercriminals use look-alike domains and display name deception to trick employees into revealing sensitive information or depositing money into criminally-owned bank accounts. When they can compromise a legitimate account and use it to send malicious messages, the success rate becomes even greater. And cybercriminals are taking advantage, to the tune of $3.6 billion per year and counting.

The Agari Cyber Intelligence Division (ACID) has identified a West African cybergang, dubbed Silent Starling, that uses compromised email accounts to perpetrate a troubling new form of business email compromise that our researchers call vendor email compromise, or VEC. Our visibility into Silent Starling's operations offers a direct and in-depth look into how the VEC attack chain unfolds.

Unlike typical BEC scams designed to defraud a single organization, this type of attack targets entire supply chains, using legitimate employee email accounts to swindle a business's customers into paying fraudulent invoices. Due to its covert nature, the ability for companies to effectively protect themselves from VEC scams becomes much more difficult.

Operatives of Silent Starling initiate these attacks by hijacking email accounts belonging to employees within a targeted company's finance department. The fraudsters then lay low, methodically gathering information, data, and critical context from email archives and all the communications passing through these captured mailboxes. Armed with this intel, operatives can then send perfectly timed messages to multiple targets, requesting payment on fraudulent invoices or changes to vendor payment details.

Most common security controls are unable to recognize this kind of socially-engineered email message, especially when it is nearly indistinguishable from those typically sent by the impersonated vendor or supplier. Only the bank account details are different.

In the course of our research, Agari was able to document Silent Starling's successful infiltration of more than 700 employee email accounts, spanning more than 500 companies in the United States and over a dozen other countries, collecting more than 20,000 internal and sensitive emails since late 2018.

As Silent Starling and other fraud groups continue to evolve this attack modality, VEC scams will proliferate, and the financial impact will be harrowing, causing disruption throughout the global supply chain.

ACID

Table of Contents

ACID

Silent Starling

Scamming the Supply Chain

The investigation by the Agari Cyber Intelligence Division (ACID) into cybercriminal group Silent Starling offers visibility into a new attack vector we've named vendor email compromise. From our research, we have discovered that cybercriminals are infiltrating email accounts and using them in new ways to trick customers into paying fake invoices.

This attack on the supply chain represents a dangerous new phase in the evolution of business email compromise. Unlike traditional BEC attacks targeting a single company, VEC scammers use legitimate accounts to target a company's supply chain ecosystem—often scamming dozens of customers at once.

According to the US Treasury Department, businesses lose as much as $300 million per month to BEC scams overall. Payment invoice scams accounted for nearly half of those fraudulent transactions in 2018, to the tune of more than $1.5 billion in business losses. That number is likely to be even higher when cybercriminals gain access to legitimate email accounts and use them to run their scams.

Silent Starling is the first case in which Agari has documented a cybergang using VEC as its primary method for scamming businesses. Unfortunately, we do not expect it to be the last, as vendor email compromise becomes the most dangerous cyberthreat faced by businesses and their supply chains in the next year.

According to the US Treasury Department, businesses lose as much as

$300M

per month to BEC scams overall.

Payment invoice scams accounted for nearly half those fraudulent transactions in 2018, causing more than

$1.5B

in business losses.

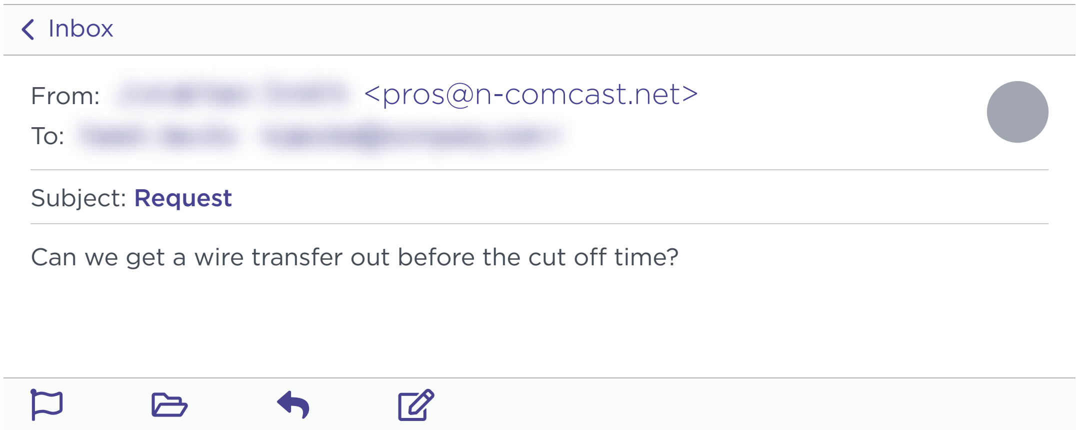
Angling for Prey

Silent Starling Takes the Stage

Every single day, researchers in the Agari Cyber Intelligence Division engage with dozens of BEC scammers who have tried (and failed) to target our customers. In doing so, we collect rich intelligence that allows us to better understand cybercriminal group operations, discover and track the evolution of their methods over time, unravel the financial infrastructure they use to launder stolen proceeds, and uncover the identities of those involved in the criminal schemes.

In July 2019, one of these active defense engagements led us to a cybercriminal organization we've dubbed Silent Starling—named after an invasive species of bird native to West Africa. The messages below detail our initial interaction with the group.

Silent Starling attempted to attack an Agari customer by impersonating the CEO in an email directed toward the CFO with a basic subject line of "Request." Like most BEC attacks, the initial email message was brief and was meant to elicit a response from the target. In this case, the attacker wanted to know if a wire transfer could be sent before the end of the day.



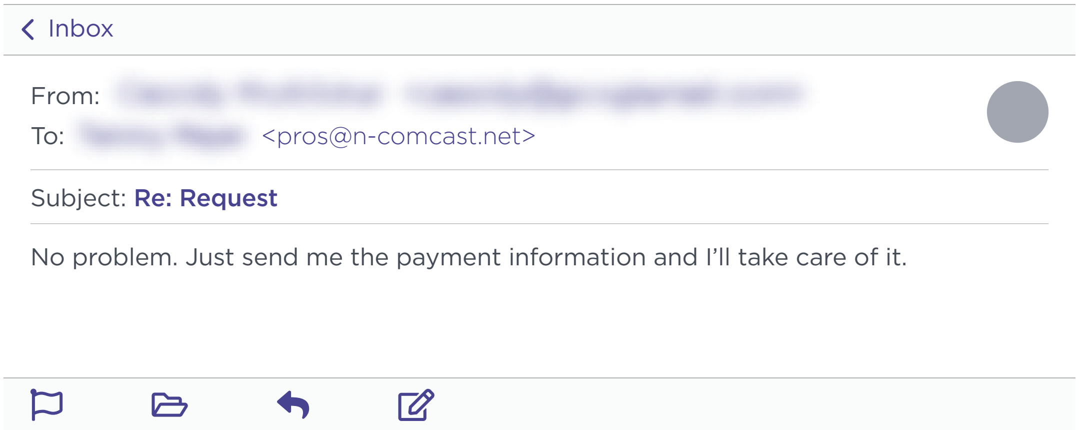
From: [redacted] <pros@n-comcast.net>
To: [redacted] [redacted]

Subject: **Request**

Can we get a wire transfer out before the cut off time?

We took action and re-crafted a new email conversation with the scammer from a separate persona account, creating new identities for a fake CEO and CFO and simply recycling the original email subject and body. This switch was done to protect the identities of those in the target email.

Under this new persona, we responded to the scammer, generously offering to help him take care of the necessary transfer.

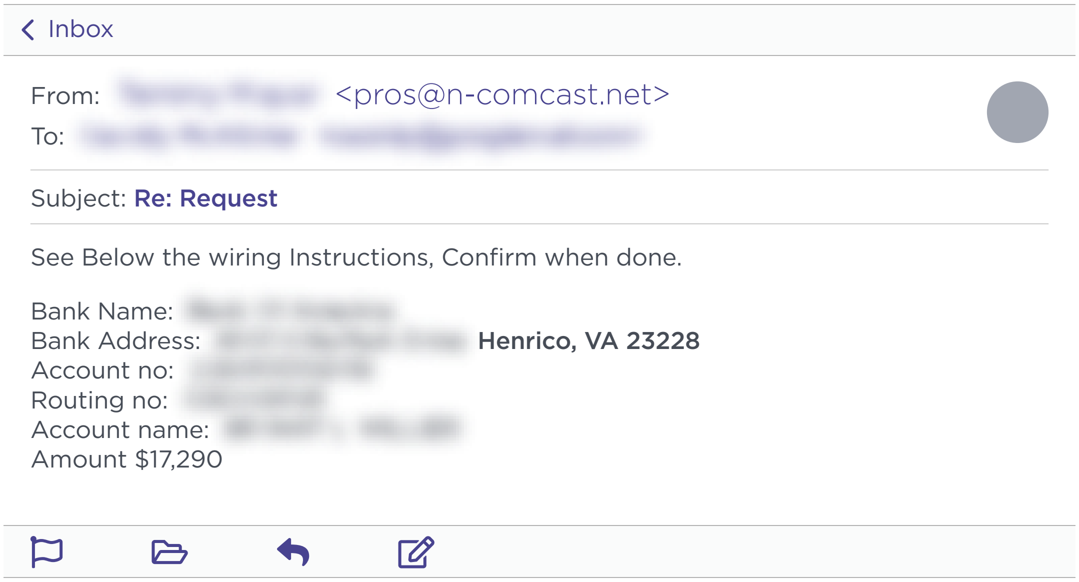


From: [redacted]
To: [redacted] <pros@n-comcast.net>

Subject: **Re: Request**

No problem. Just send me the payment information and I'll take care of it.

Fourteen minutes later, our fake CEO provided us with the first of many mule accounts where he wanted the $17,290 “transfer” to be sent.



From: [redacted] <pros@n-comcast.net>
To: [redacted]

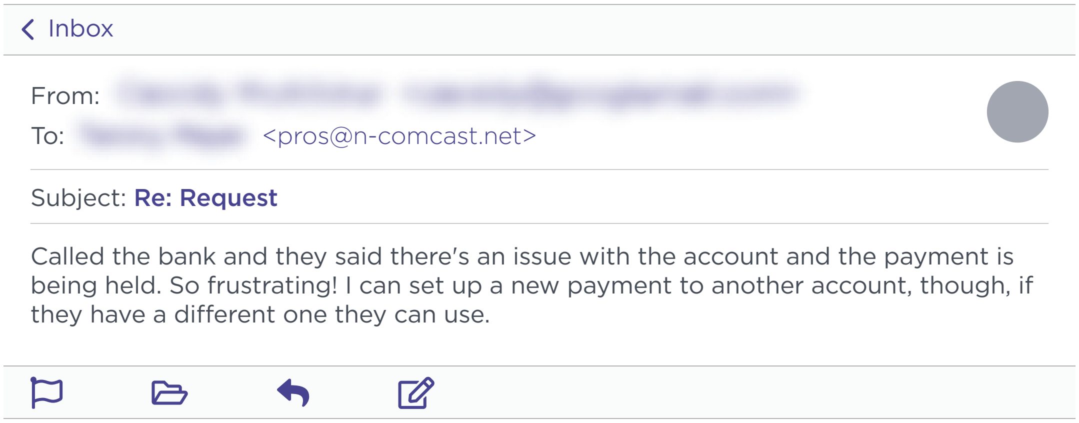
Subject: **Re: Request**

See Below the wiring Instructions, Confirm when done.

Bank Name: [redacted]
Bank Address: [redacted] **Henrico, VA 23228**
Account no: [redacted]
Routing no: [redacted]
Account name: [redacted]
Amount $17,290

When he never received confirmation that the funds had been transferred, the fake CEO contacted our persona CFO and inquired about the status of the payment. Unfortunately for the scammer, the bank found an “issue” with the account and the payment was rejected.

However, because our persona CFO is so helpful, they offer to reprocess the payment to another account if the “vendor” has one. Predictably, the scammer obliges and offers another mule account for us to try.

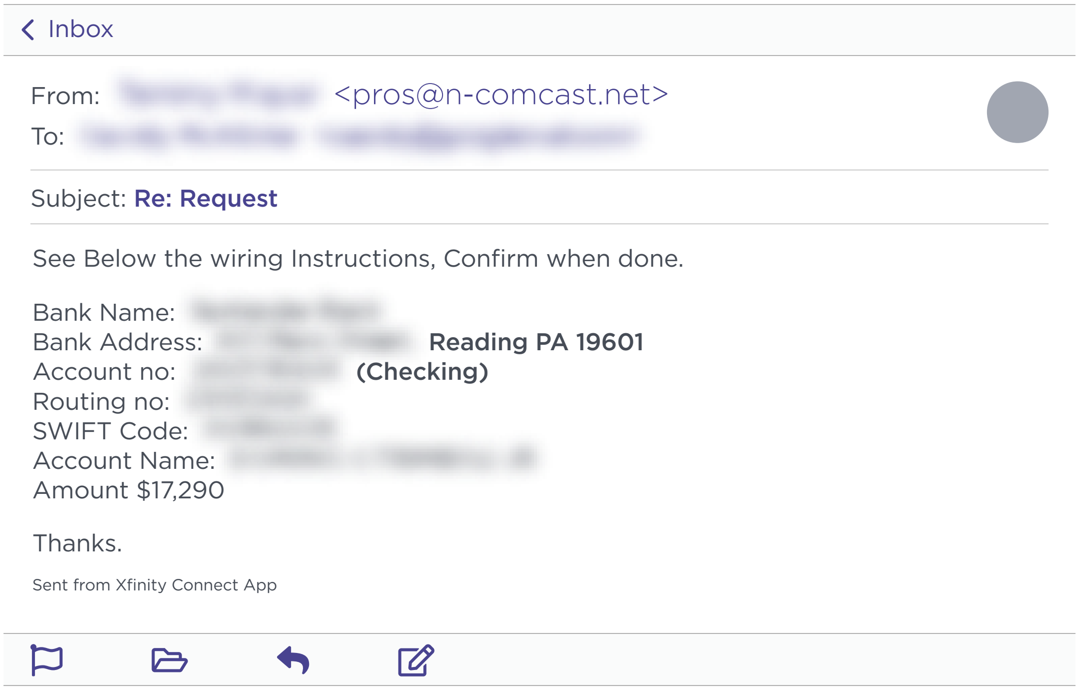


From: [redacted]
To: [redacted] <pros@n-comcast.net>

Subject: **Re: Request**

Called the bank and they said there's an issue with the account and the payment is being held. So frustrating! I can set up a new payment to another account, though, if they have a different one they can use.

The scammer quickly replied with new banking details.



From: [redacted] <pros@n-comcast.net>
To: [redacted]

Subject: **Re: Request**

See Below the wiring Instructions, Confirm when done.

Bank Name: [redacted]
Bank Address: [redacted] **Reading PA 19601**
Account no: [redacted] **(Checking)**
Routing no: [redacted]
SWIFT Code: [redacted]
Account Name: [redacted]
Amount $17,290

Thanks.

Sent from Xfinity Connect App

This cycle of the Silent Starling actor sending us mule accounts and our fake CFO running into "problems" continued for more than a month. By the time the engagement finally ended, we had collected 13 different mule accounts used by the group to launder money from BEC attacks, which we passed to financial partners and law enforcement.

In addition to actively engaging with the Silent Starling scammer, we used various tools and tactics that allowed us to gain significant insight into the group's background, methods, and primary actors. What follows is an overview of what we discovered during our investigation into Silent Starling.

Who is Silent Starling?

The Dramatic Descent into Cybercrime

Silent Starling is a cybercriminal organization with members that reside in and around Lagos, Nigeria. The group has been involved in criminal activity since 2015, starting with romance scams and check fraud before turning to BEC in mid-2016. For two years, Silent Starling scaled their BEC operations, focusing on wire transfer requests and gift card attacks, before evolving their methods to commit VEC scams in late 2018.

While we believe Silent Starling is larger than what our visibility covers, our research has identified three primary members responsible for day-to-day operations.

In addition to these three group members, we have identified information linking at least eight other individuals who have assisted the core group of actors in various ways. Similar to what we have observed with other groups, Silent Starling has a loose structure with central players and tangential actors who are responsible for specific tasks, such as collecting targeting leads, obtaining mule accounts, and monitoring compromised email accounts for relevant information.

ACTOR 1

LIVES IN IKEJA, NIGERIA

- Primary actor responsible for sending credential phishing attacks and monitoring incoming emails from compromised business email accounts
- Proficient in English, Spanish, Ukranian, and Russian
- Previously traveled to Kenya, South Africa, and the United Arab Emirates

ACTOR 2

LIVES IN LAGOS, NIGERIA

- Responsible for collecting and distributing BEC targeting leads
- Involved in romance scams, most recently posing as a 43-year-old Turkish female

ACTOR 3

LIVES IN LAGOS, NIGERIA

- Previously employed at a Nigerian mortgage lender
- Explored applying to international universities in Belgium, Canada, France, Russia, and the United States

V is for Vendor

Portrait of a VEC Scam

One of the most significant emerging threats in the cyber threat landscape is vendor email compromise. The key to these attacks is gaining access to email accounts belonging to key individuals within a company's accounts receivable or finance department. Once infiltrated, these email accounts are mined for intelligence and weaponized through the distribution of fraudulent invoices or requests to change vendor payment details.

The ultimate targets of these attacks are a vendor's or supplier's customers, who are sent realistic-looking phishing emails requesting payment for an actual service. Because the emails closely mimic the look and feel of legitimate correspondence from the compromised vendor, the success rate and financial loss caused by VEC attacks can be significantly higher than other types of email-based attacks.

Beyond Business Email Compromise

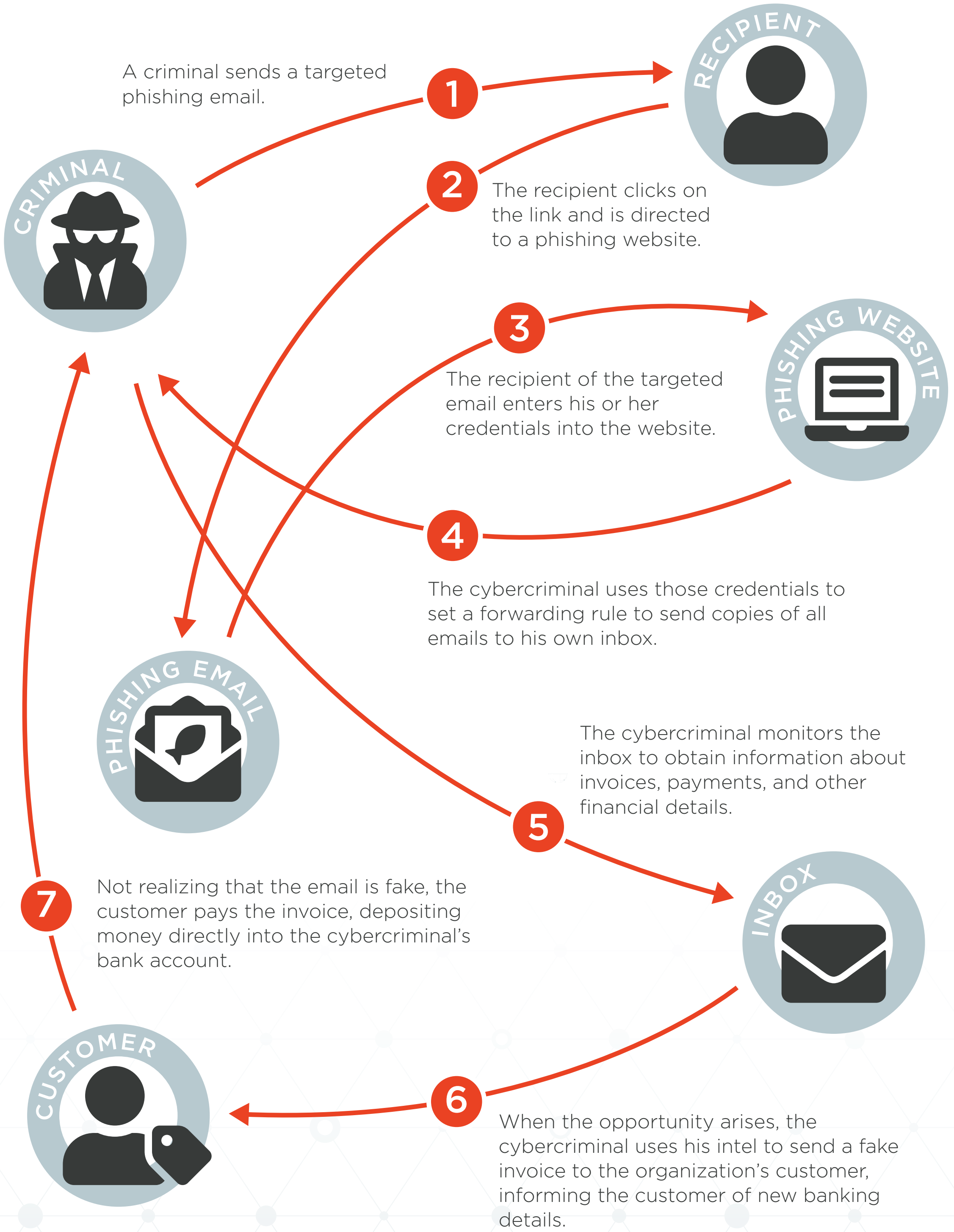
VEC scams are technically a form of business email compromise, yet they are distinctive in their required level of sophistication, sourced intelligence, and savvy customization—as well as in their superior payout potential.

BEC fraud relies on economies of scale to convert leads into financial rewards. In a typical BEC scheme, fraudsters gather information on possible targets by researching job roles and contact email addresses, as well as the name of the CEO or other high-profile executives. The fraudster then uses that intelligence to spoof the email address of a trusted executive, sending emails to lower-level employees requesting wire transfers or gift cards. A certain number of recipients will be hoodwinked into making a payment. But as the percentage of people who can be tricked into completing requests drops off, the less successful the campaign becomes.

By contrast, VEC is something far more insidious. The front-end of these attacks can be as broad as BEC campaigns, but once an email account is compromised within a target organization, threat actors must exercise extreme patience. Lurking in the background, they find opportunities to compromise additional email accounts, typically targeting those in the finance department. These are the most important accounts, as they have the appropriate authority to issue invoices to the organization's customers or authorize payments on invoices coming from suppliers.

To effectively run their scam, the ebb and flow of an organization's entire workflow needs to be observed and understood. For example, if a supplier is on payment terms of 60 days, and a scammer makes a follow-up request after only 30 days, they risk drawing unwanted attention. To prevent these errors, the fraudsters lay low, surveilling email messages to prepare and launch exquisitely personalized attacks on the business's employees, customers, or partners.

A differentiating element of VEC, as compared to a typical vendor invoice scam—is that the bad actor infiltrates an email account and then lies in wait so that he can observe transactions, conversations, and exchanges taking place within that email account. As a result, that actor gains valuable context around a vendor's invoicing cadence, processes, and customers. This intelligence enables him to create emails that are realistic to the point that they are virtually undetectable. Making matters worse, they are launched from legitimate accounts of real employees. It's no surprise that VEC is working.



1 A criminal sends a targeted phishing email.

2 The recipient clicks on the link and is directed to a phishing website.

3 The recipient of the targeted email enters his or her credentials into the website.

4 The cybercriminal uses those credentials to set a forwarding rule to send copies of all emails to his own inbox.

5 The cybercriminal monitors the inbox to obtain information about invoices, payments, and other financial details.

6 When the opportunity arises, the cybercriminal uses his intel to send a fake invoice to the organization's customer, informing the customer of new banking details.

7 Not realizing that the email is fake, the customer pays the invoice, depositing money directly into the cybercriminal's bank account.

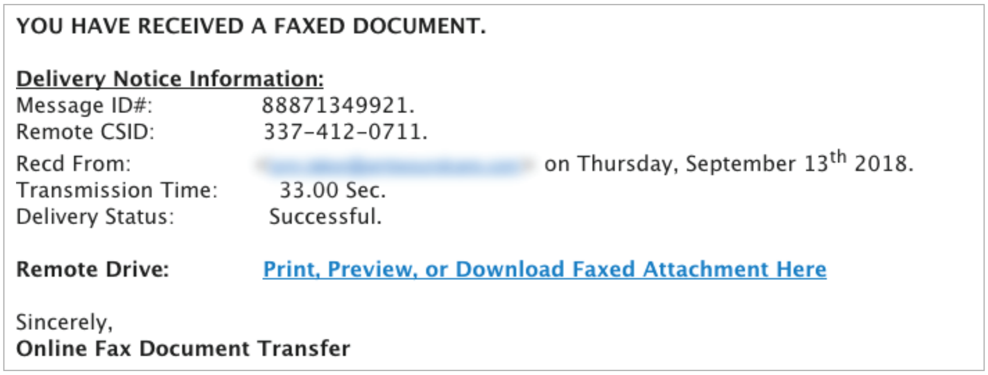
From Credentials to Cash-Out

How Silent Starling Snares Their Victims

The first step in the VEC attack chain is to compromise business email accounts that can be used to collect intelligence to exploit later in the attack process. The primary method VEC actors use to collect account credentials is credential phishing.

Using Legitimate Services for Illegitimate Activities

Like most credential phishing attacks targeting enterprise email accounts, Silent Starling's credential phishing emails posed as commonly-used business applications. While the group has used a number of different phishing lure templates since the beginning of 2018, the phishing sites these lures link to usually mimic Microsoft OneDrive or DocuSign login pages, as well as voicemail and fax notifications.

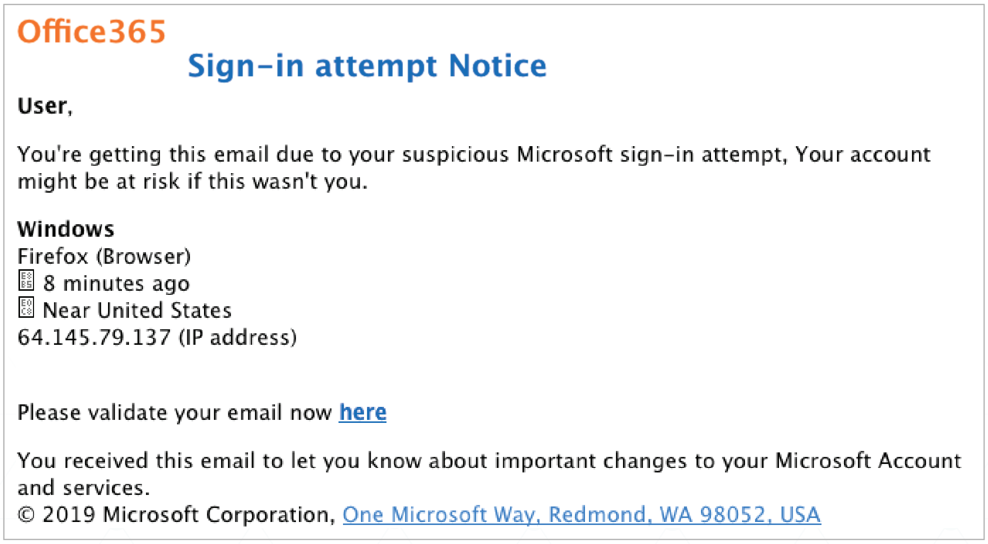


YOU HAVE RECEIVED A FAXED DOCUMENT.

Delivery Notice Information:
Message ID#: 88871349921.
Remote CSID: 337-412-0711.
Recd From: [redacted] on Thursday, September 13th 2018.
Transmission Time: 33.00 Sec.
Delivery Status: Successful.

Remote Drive: Print, Preview, or Download Faxed Attachment Here

Sincerely,
Online Fax Document Transfer



Office365

Sign-in attempt Notice

User,

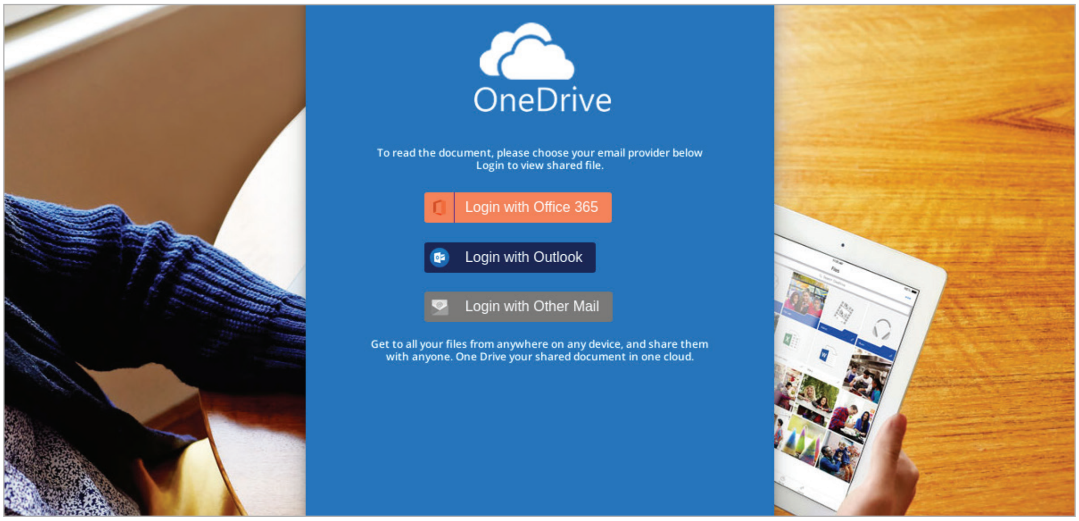
You're getting this email due to your suspicious Microsoft sign-in attempt, Your account might be at risk if this wasn't you.

Windows
Firefox (Browser)
▯ 8 minutes ago
▯ Near United States
64.145.79.137 (IP address)

Please validate your email now **here**

You received this email to let you know about important changes to your Microsoft Account and services.
© 2019 Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA

Example Phishing Lures Used by Silent Starling

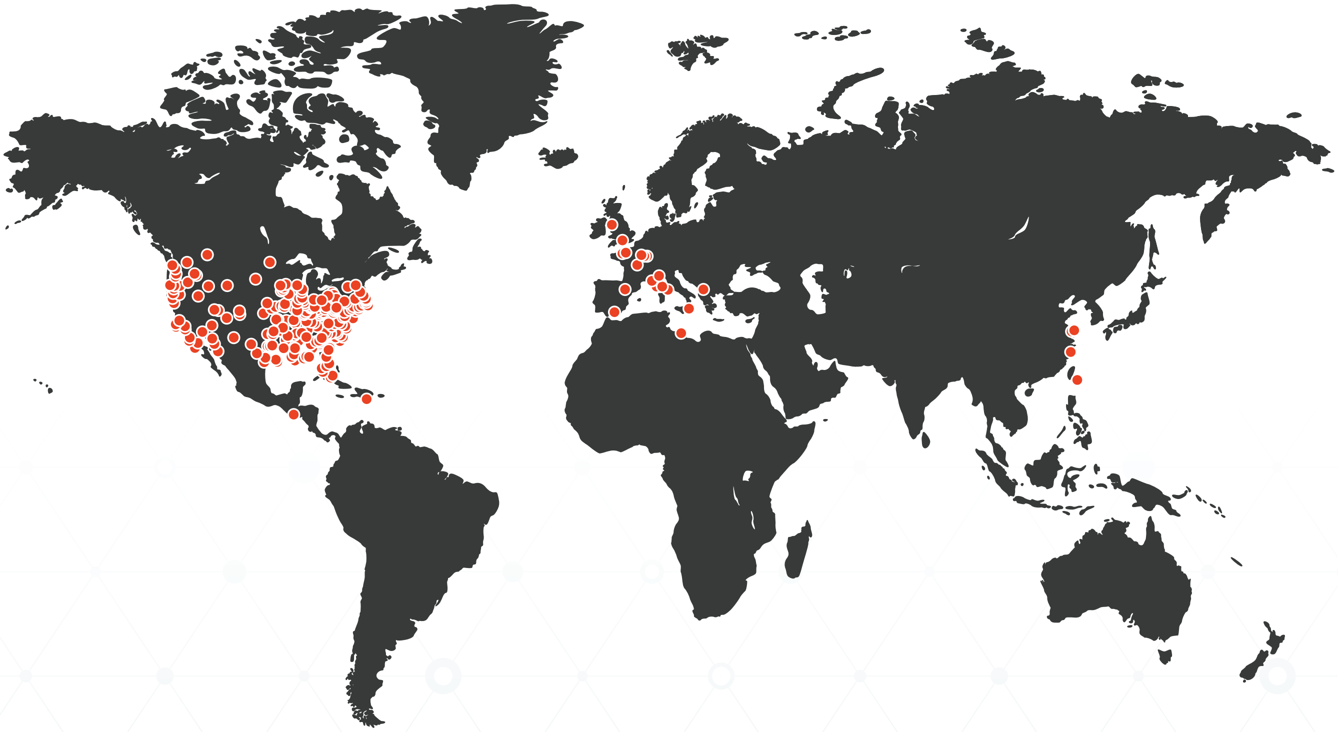


To read the document, please choose your email provider below Login to view shared file.

Get to all your files from anywhere on any device, and share them with anyone. One Drive your shared document in one cloud.

OneDrive Phishing Site Used by Silent Starling

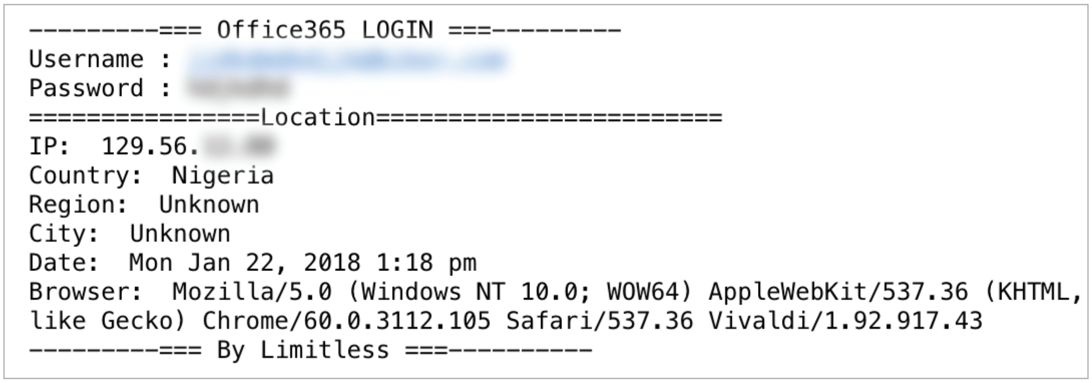
Our research identified more than 70 phishing sites used by Silent Starling to collect compromised email credentials. From these phishing sites, Silent Starling collected credentials for more than 700 employee email accounts at over 500 companies in 14 countries. While a few compromised accounts came from users in Central America, East Asia, and Europe, nearly all (97%) of the victims of Silent Starling's credential phishing attacks were located in three countries: the United States, Canada, and the United Kingdom.



Map of Silent Starling Credential Phishing Victim Locations

As their credential phishing attacks yielded successful results, Silent Starling actors regularly reviewed the incoming credentials, weeding out results that were likely fake or useless and extracting compromised accounts that they considered valuable. Members of the group starred incoming emails with notable account data and made notes to "check later" batches of compromised accounts, especially when a large number of accounts were collected from a single company.

Most scammers test the functionality of a phishing site to be used in an attack by submitting dummy credentials to the site prior to sending out phishing campaigns. Ironically, this approach can lead to attribution leakage during the intelligence collection process because most phishing kits are designed to collect additional information about a victim, such as IP address, location, and user agent string data. Our analysis of Silent Starling attacks uncovered multiple test submissions that backed up our assessment that these actors resided in Nigeria.



```
----------=== Office365 LOGIN ===---------
Username : [redacted]
Password : [redacted]
===============Location=======================
IP:  129.56.[redacted]
Country:  Nigeria
Region:  Unknown
City:  Unknown
Date:  Mon Jan 22, 2018 1:18 pm
Browser:  Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/60.0.3112.105 Safari/537.36 Vivaldi/1.92.917.43
----------=== By Limitless ===----------
```

Attribution Leakage from a Silent Starling Phishing Test Submission

Finding Success in Phishing

So how effective can these credential phishing campaigns be? In one case, Silent Starling compromised the email accounts of 39 employees at a single US-based company over the course of five distinct OneDrive phishing campaigns between September 2018 and March 2019. The credentials of billing specialists, branch managers, sales account executives, human resources employees, business consultants, and a senior executive were compromised in these campaigns.

In one February 2019 campaign targeting this company, 13 email accounts were compromised within thirty minutes from the time the campaign was initiated, highlighting how fast these attacks can produce devastating results. At least six employees also had their personal email account credentials compromised as a direct result of Silent Starling's phishing tactics. And once a company has been successfully compromised, it only gets worse, likely due to the fact that those employees are considered ripe for exploitation.

Spy Craft

Moving the Attack Forward

Once Silent Starling has collected a cache of compromised business email accounts, it is time for them to put them to use. The goal of this next phase of the VEC attack chain is to access the contents of these compromised accounts, identify accounts belonging to employees that are involved in the payment process, and set up an inbox rule that sends copies of all incoming emails to the scammer.

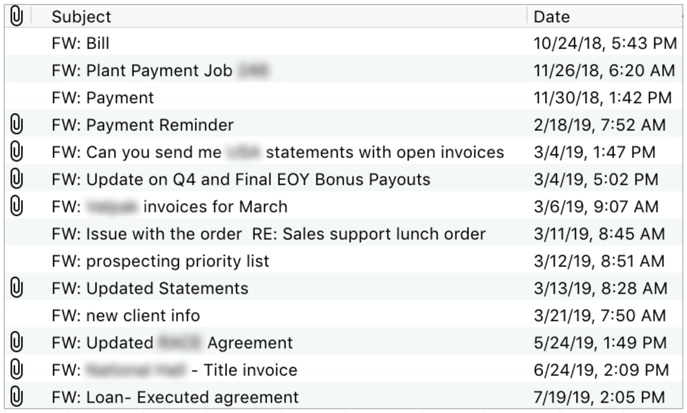
The purpose of this step is to identify high-value vendor/supplier accounts and collect intelligence from these accounts so they can be used at a later date to craft a devastatingly realistic invoice in the next phase of the attack, which targets the vendor's customers.

Inbox Rules: A Scammer's Cloak of Invisibility

Silent Starling's preferred method for collecting intelligence on compromised mailboxes is to set up a forwarding rule on the compromised email account simply delivers a copy of each incoming email message to a separate email account which controlled by the group. Another common tactic used in VEC attackers is to redirect messages, rather than forward them. The effect of these rules is the same—the scammers obtain duplicates of all incoming communication to the victim. The only difference is how the diverted emails appear in the scammer's inbox.

Because these rules do not modify or remove messages from a mailbox, a victim likely will not see any overt signs that scammers are spying on the communication flowing through his/her mailbox until it is too late. Unless a victim is alerted to potential suspicious activity, such as a customer complaining that they received a questionable invoice, a cybercriminal can sit on a compromised email account and collect intelligence for months without ever being detected.

In one example, Silent Starling had access to an employee's mailbox at a US-based real estate advisory firm for more than four months. During this time, Silent Starling received copies of more than 2,800 emails containing sensitive documents and communications, including income statements, invoices, customer agreements, rental injury reports, and other policy paperwork.



📎	Subject	Date
	FW: Bill	10/24/18, 5:43 PM
	FW: Plant Payment Job [redacted]	11/26/18, 6:20 AM
	FW: Payment	11/30/18, 1:42 PM
📎	FW: Payment Reminder	2/18/19, 7:52 AM
📎	FW: Can you send me [redacted] statements with open invoices	3/4/19, 1:47 PM
📎	FW: Update on Q4 and Final EOY Bonus Payouts	3/4/19, 5:02 PM
📎	FW: [redacted] invoices for March	3/6/19, 9:07 AM
	FW: Issue with the order RE: Sales support lunch order	3/11/19, 8:45 AM
	FW: prospecting priority list	3/12/19, 8:51 AM
📎	FW: Updated Statements	3/13/19, 8:28 AM
	FW: new client info	3/21/19, 7:50 AM
📎	FW: Updated [redacted] Agreement	5/24/19, 1:49 PM
📎	FW: [redacted] - Title invoice	6/24/19, 2:09 PM
📎	FW: Loan- Executed agreement	7/19/19, 2:05 PM

Forwarded Emails from Compromised Accounts Received by Silent Starling

The Early Bird Waits for the Worm

Patience is a virtue in the VEC attack chain. Now that the attacker has a stream of information about a vendor's inner-workings, the attacker just needs to sit back and mine this email feed for artifacts that can be used to create a new phishing email that looks and feels completely legitimate.

To do so, the attacker looks for answers to a few specific questions:

- Who are the vendor's customers?
- What does the vendor's standard invoice look like?
- When are customer payments due?
- How much money do specific customers owe?
- Which customer contacts are responsible for payments?

A VEC scammer can receive hundreds or thousands of emails from compromised mailboxes, depending on the number of accounts feeding their pipeline. Since late 2018, Silent Starling has received copies of more than 20,000 emails from infiltrated inboxes.

Silent Starling associates review incoming messages and bookmark ones that contain useful information. Based on emails that group members have flagged, it is likely that they search for emails containing the specific keywords related to payments, invoices, and payroll, rather than reviewing each message individually. This strategy makes the process more efficient and likely identifies most of the content the group needs for the final stage in the VEC attack chain.

Chain Reaction

Silent Starling Strikes

Once an attacker has collected enough intelligence from a compromised account, he is ready to launch the next stage of the VEC attack chain, which involves using this wealth of information to send ultra-realistic phishing emails to the vendor's customers. Like a typical BEC attack, the purpose of these spearphishing emails is to trick the recipient into sending money to the scammer's bank account.

Usually when a company is breached by a cyber attack, they bear the brunt of the financial impact. Ironically, the entity that is impacted the most by VEC attacks is not the original victim of the initial attack—the vendor or supplier. Rather, it is a completely separate organization that is targeted—the compromised vendor's customer. In a rather cruel twist, these customers have no control over the security of the system where the attack began.

From Exploitation to Execution

This final stage of a VEC attack takes advantage of three primary aspects of vendor/customer communication by identifying the appropriate contact, creating the right content, and ensuring that timing is consistent with previous correspondence.

Identity

The primary targets for impersonation in VEC attacks are employees that handle customer billing, rather than the company executives we see as targets in most BEC attacks. Most of Silent Starling's marks have been accounts receivable employees or office managers of very small businesses.

VEC scammers impersonate vendor identities in three primary ways.

1. The scammer can log into the compromised account of an impersonated vendor and send an email directly from the account. While this is the easiest and most direct route to the ultimate victim, it can create noise and leave a significant trail as the scammer logs in and out of the account.

2. The attacker can spoof the impersonated vendor's email address so it appears an email is coming from their actual address when, in fact, it is not. This solves the problem of having to interact with a compromised email account, but if the domain of the compromised account has established a DMARC record to reject spoofing attempts, then this option is not possible.

3. The threat actor can register a domain that looks almost exactly the same as the domain of the impersonated vendor, perhaps by inserting an additional letter or by using unicode characters that mimic English letters. They can then create an email account on this new domain that looks almost identical to the impersonated vendor's account. The downside to this tactic is that because the domain is not actually associated with the vendor, it opens the possibility for recipients to spot the difference.

The latter two strategies require no additional access to the vendor's email account. This means that once the initial compromise has occurred and an inbox rule has been set on the account, a scammer does not need to interact with the account again throughout the duration of the VEC attack chain, which highlights the stealth nature of these attacks.

Based on our observations of Silent Starling's VEC attacks, attackers have used a combination of the first and third strategies described above. It seems their initial preference is to email secondary targets using a vendor's compromised account. When they have lost the ability to log into a compromised account—likely because the account password has been changed—Silent Starling then pivots to using look-alike domains of impersonated vendors to continue their attacks.

It should be noted that even if the password is changed on an account that is forwarding emails to a VEC scammer, it does not mitigate the attack. This only prevents an attacker from regaining direct access to the account, but the flow of intelligence being sent as a result of the forwarding rule is not impacted.

Content

As actors review emails being passed from compromised vendor email accounts, they are able to quickly recognize normal patterns in communication used by the employee linked to the account, as well as every other person that communicates regularly with that employee. These communication patterns play an integral role in the success of the final VEC attacks.

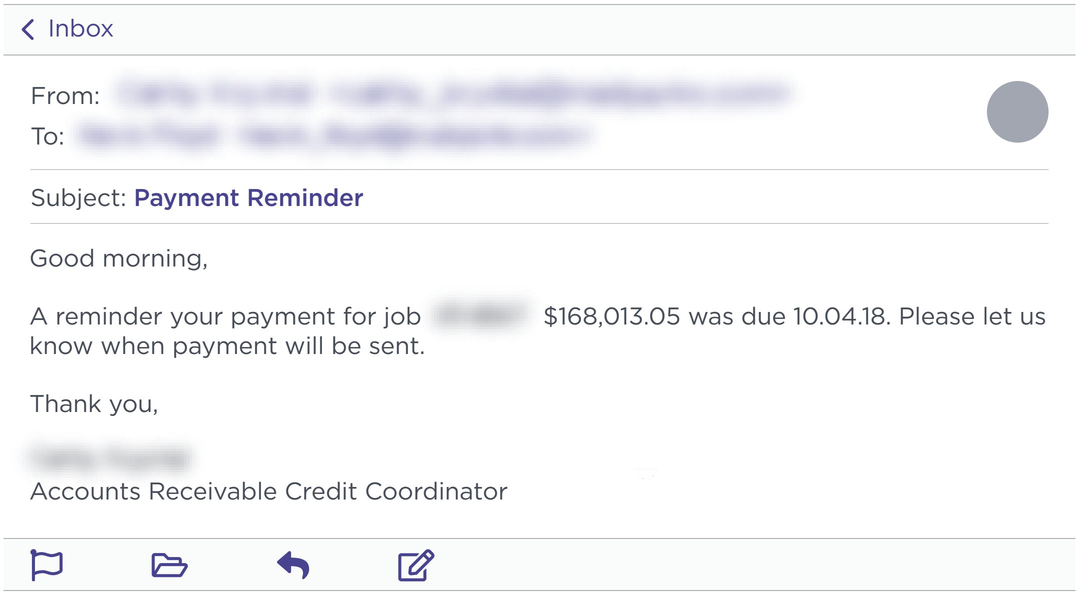
VEC scammers are careful to mirror the way an impersonated vendor typically constructs an email. How do they address a recipient? Are their emails generally brief or verbose? How do they usually close an email? All of this is essential to appear believable during an attack,

One of the more notable aspects of Silent Starling phishing emails that impersonate a vendor is how the group takes care to copy the signature of an impersonated vendor, no matter how intricate it may be. Including a vendor's actual signature in an email is a sophisticated touch because, a person's signature can often be a more recognizable identity association than a person's email address.

Timing

The third variable a scammer uses to craft contextually realistic VEC attacks is timing. While a payment due date may seem innocuous, having access to previous invoices gives Silent Starling actors the framework they need to help them understand when to strike. For example, if they send an email to an unsuspecting customer too early, it could draw unwanted attention if the payee contacts the vendor asking why someone is reaching out to them well before the due date. Alternatively, if they wait too long, the invoice will have already been paid to the legitimate company and Silent Starling has missed its opportunity. However, if a scammer times their attack correctly, they can apply the perfect amount of pressure to persuade the customer to send a payment quickly.

During our research into Silent Starling, we observed multiple instances where the group used information they collected about a customer's payment due date to their advantage. In one case, the group intercepted a message from the accounts receivable coordinator at a US-based marketing agency, intended for a franchise owner that was past due on a $168,000 payment. Within 24 hours of the email being sent, Silent Starling actors registered a look-alike domain, which they then used to impersonate the accounts receivable coordinator. Using this domain, they sent a follow-up email to the original recipient letting them know that the banking information for the payment had changed.



From: [redacted]
To: [redacted]

Subject: **Payment Reminder**

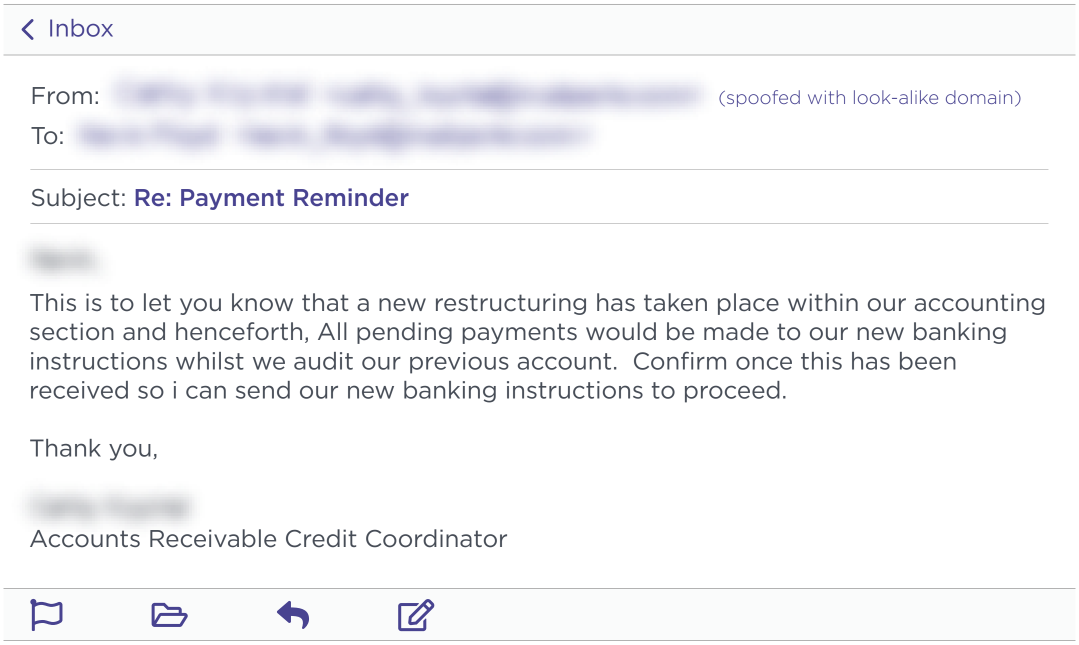
Good morning,

A reminder your payment for job [redacted] $168,013.05 was due 10.04.18. Please let us know when payment will be sent.

Thank you,

[redacted]
Accounts Receivable Credit Coordinator

Email Containing Legitimate Payment Reminder Intercepted by Silent Starling



From: [redacted] (spoofed with look-alike domain)
To: [redacted]

Subject: **Re: Payment Reminder**

[redacted]

This is to let you know that a new restructuring has taken place within our accounting section and henceforth, All pending payments would be made to our new banking instructions whilst we audit our previous account. Confirm once this has been received so i can send our new banking instructions to proceed.

Thank you,

[redacted]
Accounts Receivable Credit Coordinator

Silent Starling VEC Impersonation Email

While we cannot conclusively say whether this customer sent the money to Silent Starling, the chances this attack was successful are significant given the realistic nature of the email.

Making Easy Scams Easier

Another powerful artifact that VEC scammers may use to advantageously time their attacks is an aging report. An aging report, or schedule of accounts receivable, lists unpaid customer invoices and unused credit memos. It is an essential tool for both accounts and management to maintain an overview of their credit and collection processes, and breaks down outstanding debts into thirty day increments, culminating with payments that are more than ninety days overdue.

Armed with intelligence from these reports—customer names, their outstanding balances, and contact information—scammers can then assume the identity of an employee on the finance team, contact customers with outstanding debts, and request that they pay the balance referenced on the report. Scammers could also offer incentives to these customers for them to resolve their debts more quickly, such as reducing the amount they owe if they settle their outstanding balance immediately.

In one case, Silent Starling received multiple copies of aging reports that included details about delinquent payments of a company's customers. This company works with thousands of small and mid-sized businesses across the United States for advertising services, so the aging reports passed on to Silent Starling were sometimes quite detailed. In early 2019, one consolidated aging report forwarded to a Silent Starling account included details of more than 3,500 customers with past due payments totalling more than $6.5 million. While we do not have any direct evidence that the group used this report for subsequent attacks, the value of the data and opportunity for abuse is significant.

Conclusion

Preventing VEC in Your Supply Chain

This report demonstrates that advanced email attacks continue to evolve as cybercriminal organizations operationalize their strategies and develop inventive new schemes. Silent Starling's remarkable patience in leveraging compromised email accounts to score higher payouts through vendor email compromise scams should put every business on notice.

The supply chain is no longer safe from the email attacks that come with heavy financial costs, serious reputational damage, and lost customers and opportunities. With the vendor email compromise scams run by Silent Starling as one example, this report demonstrates that a new approach to email security—one focused on detecting true identity rather than malicious content—is needed to protect against the VEC that may materialize from within the supplier ecosystem.

Appendix A

Email Accounts Used in Silent Starling BEC Attacks

8155200270293611@comcast.net
bors@n-comcast.net
ceo@cod-pd.com
ceo_@m-verizon.net
cmd@covatt.net
cmd@mavapi.net
cmd@mofap.net
cmd1@wincmd.net
cmd2@wincmd.net
cmdwin@covatt.net
cmg@movap.net
co@c-comcast.net
co@on-comcast.net
coo@sevapp.email
cxo@covapp.net
cxo@dorapp.net
cxo@koxapp.net
ehn@mofap.net
ghsj@movap.net
homeconnection@m-verizon.net
infoceo@ceoinfo.tv
ipad@royapp.net
ipad@wincmd.net
ipadd@movap.net
jhu@mini-pad.com
kpad@dorapp.net
kpad@homapp.net
kpad@honapp.net
lpad@covatt.net
lsr@m-verizon.net
mat@mofap.net
mds@movap.net
mo@c-comcast.net
mobile@biznow.org
of@n-comcast.net
pad@ipad-mobi.com
por@m-verizon.net
por@on-comcast.net
privateemail@myicloudonline.net
pro@n-comcast.net
pros@n-comcast.net
to@n-comcast.net
win@mavapi.net
win@mavett.net
win@mofap.net

Appendix B

List of Silent Starling Credential Phishing Sites

1sthealth.net/Feladoc/

account-dominicplaisance.net/direct/

activation-confirming-mainpage.com/parkdoc/

alsonsproperties.com/voicemessage/one/

arind.net/Telefax/one/

ascententerprise.in/Scan/Newnew/docusi/

beautybuzzed.com/OneDrive/

benefitsofhoney.us/miracle/one/

blushhairmakeupbeauty.com.au/fastonedrive/

blushhairmakeupbeauty.com.au/One/

cacoinnatur.org.ve/dkny/one/

capitallaw.com.ng/mercy/one/

chamandelsur.net/kall/one/

chapapax.club/doc/Onedriv/

chisonia.com/Onedriv/

choumqnktrse.gq/micah/one/

confirmyour.stream/OneDrive/

creditwaves.com/powerdesign/one/

datamix.us/call/Aquadrive/

dhartidhorari.com/OneDrive/

dominique-services.org/Casefile/

dominique-services.org/vmail/365/

dynamanagement.net/OneDrive/

emater.com.br/data/one/

exploreitbd.net/OneDrive/

fagiot.co.vu/Med/OneDrive/

galacticbridge.com/Disk/OneOne/

groupinvestment.in/Disk/OneOne/

hearingaidexpert.co.in/YandAdoc/

hjks.in/generation/one/

host5.biz/filename/one/

hotelpuertasdecartagena.com/page/fastonedrive/

idehijau.com/OneDrive/

jimezq.com/one/

justsixpackabs.com/office/

kesho-kenya.org/OneDrive/

khaledsabry.eu/pope/one/

kuiters.co.vu/Doc/OneDrive/

lethbridgecoffee.com/YandAdoc/

libertymerchantservices.com/Max/Newnew/docusi/

limitedshelpt.online/Doc/OneOne/

lisetti.online/OneDrive/

lucioavila.com/doc/OneDrive/

lucioavila.com/OneDrive/

marcelopuente.com/Sharefile/

mundoestetic.cl/Onedriv/

oriereruer.info/que/fastdropbox/strdropbox/office365/

ot-matour.com/profile/one/

ot-matour.com/voicemail/one/

perrhijosmios.com/fuul/Aquadrive/

personalchefbyronbay.com.au/doc/one/

preemagear.com/micro/login/office/

preemagear.com/zipdoc/

radiosusanense.com/doc/one/

ramminghretire.info/jkiu/

sdinpres22menrong.sch.id/Messagefile/

service-zfairy.com/cp/oneddrive/

servisanit.cl/domain/one/

servise-eugeniasouplet.com/zipdoc/

simone-hoarau.fr/doc/zipdov/oneddrive/

simone-hoarau.fr/Filedoc/oneddrive/

soutemaire.com/betterinvesting/one/

tablo365.com/VNreports/one/

top.com.ar/Ericka/drive/

upditeies-limitednow.net/awkazip/

upditeies-limitednow.net/zipfile/oneddrive/

urbansaddleranch.com/YandAdoc/

www.host5.biz/filename/one/

zartakin.net/doc/OneDrive/

zartakin.net/OneDrive/

ACID® | AGARI CYBER INTELLIGENCE DIVISION

About Fortra's Agari Cyber Intelligence Division

Agari Cyber Intelligence Division (ACID) is the world's only counterintelligence research group dedicated to business email compromise (BEC) investigation and cybercrime abatement. ACID has conducted more than 12,000 active defense engagements with threat actors since May 2019. ACID works closely with CISOs at global enterprises, law enforcement, and other trusted partners to stop identity-based phishing and socially-engineered cybercrimes.

Learn more at acid.agari.com