SecureWorks®

REPORT

February 15, 2017

Offense-in-Depth: Reflective Social Engineering

Author: Joe Stewart and James Bettke, SecureWorks® Counter Threat Unit™ Threat Intelligence

Introduction

Billions of dollars have been lost due to business email compromise (BEC) and business email spoofing (BES). Much of this loss can be directly attributed to spearphishing attacks, which involve targeted emails crafted to impersonate a trusted party and trick the victim into performing a specific action. Spearphishing is easy to perform and hard to defend against, so it remains virtually unchallenged by commercial security solutions. As a result, it is the preferred method for fraudsters worldwide.

Security solutions primarily prevent or detect network or computer intrusions. They focus on countering malware threats, mass phishing, and the spam networks that deliver them. These threats are ubiquitous and can be measurably diminished through signature-based or behavioral-based automated defensive tools. Targeted social engineering is far less frequent and is difficult for an automated system to detect. A well-trained and skeptical human can be an effective countermeasure, which is why the current “best practices” defense against spearphishing is continual user awareness training. This type of training can efficiently combat most of the obvious cases of fraud, such as Nigerian “419” scams where a stranger writing in broken English promises easy riches. These examples, while comical, may lead to the false notion that all phishing scams are easy to spot and pose little risk.

Most organizations are unaware of the evolving tradecraft of advance-fee fraud (also known as 419), BES (CEO fraud), and BEC (wire-wire). SecureWorks® Counter Threat Unit™ (CTU) researchers have observed multiple campaigns where fraudsters tailored convincing and credible narratives. Whether the goal is to convince a victim to divulge their email password or send a wire transfer to a CEO impersonator, the criminals have fine-tuned their pitches and are becoming difficult for the average victim to detect. Even worse, the fraudsters are teaching each other these improved methods, creating a problem that is growing exponentially over time.

Demonetization

In the “Demonetizing Botnets" presentation at the RSA security conference in 2009, CTU™ researcher Joe Stewart called for an alternate cybercrime-fighting strategy termed “offense-in-depth.” The premise asserts that modern cybercrime is profit-driven and the strategy to combat it is to “increase the cost of doing business for our adversary through tactics that do not force technical evolution.” The offense-in-depth approach involves stealthy disruption. Simple infrastructure takedowns are discouraged, as it is easily replaced. Instead, defenders must impact the adversaries’ operation at the most vulnerable points. Increasing risk levels and effort required to achieve their objective, while reducing the corresponding reward, causes adversaries to eventually relent or face incarceration (see Figure 1).

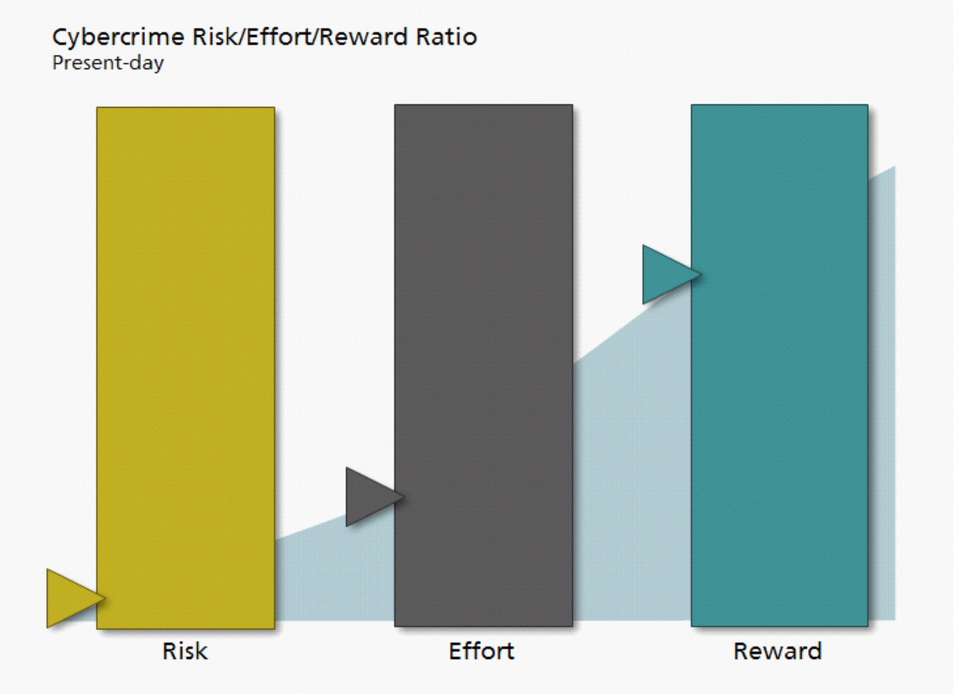


Figure 1. The risk/effort/reward ratio for most cybercrime operations. Facing relatively little risk, criminals achieve a high level of reward with a moderate amount of effort. (Source: SecureWorks)

Defenders can use the three factors of offense-in-depth to attack BEC/BES fraud:

- Risk: Work with law enforcement to identify and arrest the criminals.
- Effort: Waste the fraudster’s time by responding with stalling tactics.
- Reward: Report “mule” bank accounts so ill-gotten funds are frozen.

Increasing risk

Law enforcement organizations are highly motivated to pursue BEC/BES fraud because monetary losses tend to be substantial. Unfortunately, these cases frequently cross international borders, making efforts to arrest and extradite the fraudsters time-consuming and difficult.

Much of the BEC/BES fraud identified by CTU researchers originates from Nigeria. Since 2003, Nigeria has increased anti-fraud enforcement, forming the Economic and Financial Crimes Commission (EFCC) and arresting numerous criminals each year. However, compared to the magnitude of the problem, the EFCC is under-resourced. Law enforcement bodies and governments might be better served by training and assisting the EFCC than by placing additional burdens on investigators in their countries and jurisdictions.

Increasing effort

Setting up an email account and sending a batch of spearphishing emails is nearly effortless for criminals, so it makes little sense to report these accounts to the service providers for takedown. Instead of blocking or deleting these emails, recipients could leverage their strength-in-numbers by replying and occupying the fraudster's attention for as long as possible. Every minute the criminal spends reading and replying to bogus responses is time not spent defrauding another victim. Some organizations already use this approach on a routine basis, and the impact could be significant if others followed their lead.

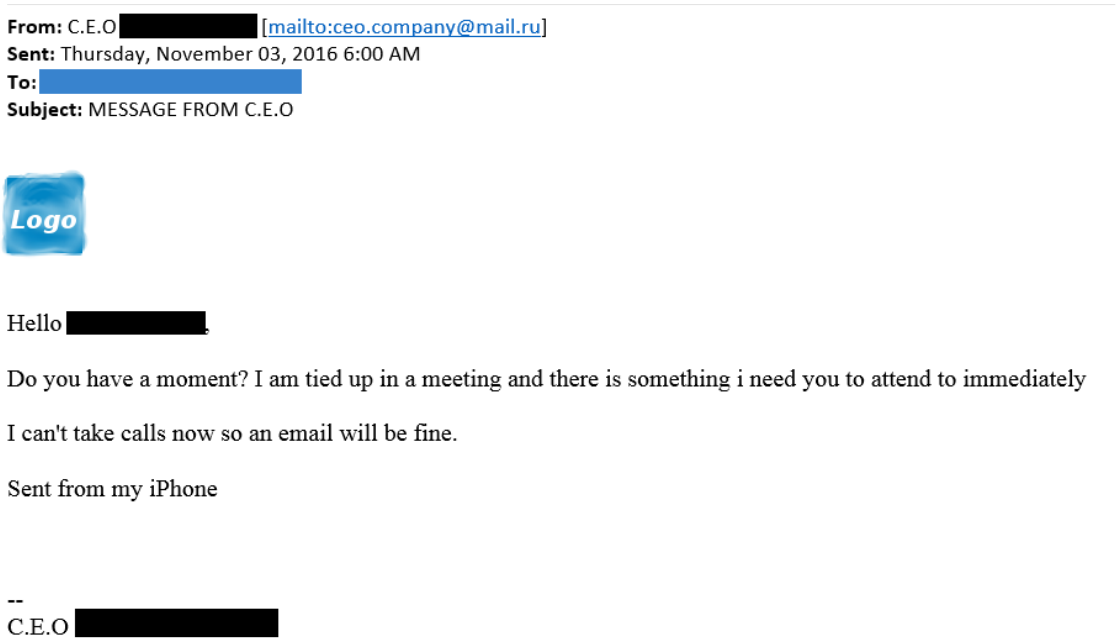
Decreasing reward

To profit from a campaign, criminals need to move stolen funds out of a victim's bank account and into theirs. They use intermediary "mule" accounts for this process, sometimes transferring the money through multiple accounts in different countries before depositing it into the final destination account. Without these mule accounts, it would be very difficult for criminals to move large sums of money without being caught by law enforcement.

Recipients of spearphishing attempts who convincingly play the role of "willing dupe" may persuade the fraudsters to send bank account details for the first-hop transfer. The intended victim should immediately report the account to the bank's fraud department, rendering it useless for transferring the money. The criminal is forced to obtain another account, which impacts their expended effort and their money flow. There is no universal mule account reporting mechanism available to the public. There are ad-hoc efforts to coordinate reporting of these accounts to participating banks, but a more effective approach would be a uniform process across all banking institutions for flagging fraudulent accounts and transfers.

BES offense-in-depth case study

In early November 2016, an attempted BES spearphishing attack against a U.S. technology company impersonated the company's CEO (see Figure 2). CTU researchers performed a deep-dive into this fraud operation to learn as much as possible, while also employing offense-in-depth tactics. Our goals were to waste the fraudster's time, flag the mule accounts, and positively identify and report the criminal.



From: C.E.O [redacted] [mailto:ceo.company@mail.ru]
Sent: Thursday, November 03, 2016 6:00 AM
To: [redacted]
Subject: MESSAGE FROM C.E.O

Hello [redacted].

Do you have a moment? I am tied up in a meeting and there is something i need you to attend to immediately

I can't take calls now so an email will be fine.

Sent from my iPhone

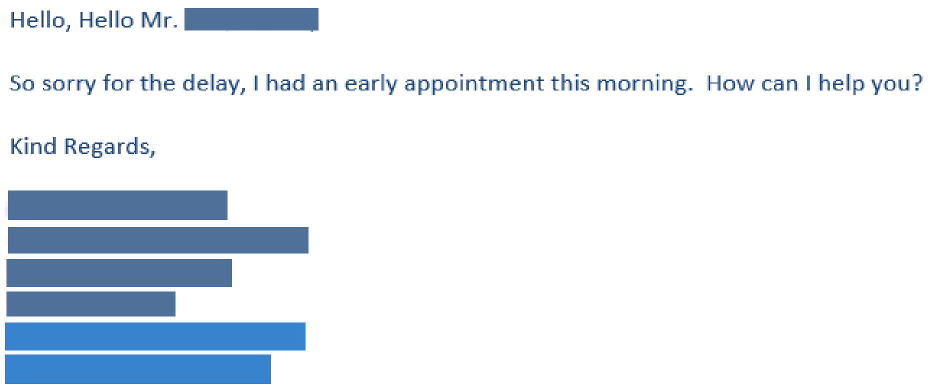
--
C.E.O [redacted]

Figure 2. First email from a CEO fraud campaign. (Source: SecureWorks)

Because this attack was simple spearphishing and not a malware campaign, there was limited infrastructure to follow. Reporting the email account to the service provider does little to deter the sender, but replying provides an opportunity to “reflect” the social engineering attack. By assuming the “victim’s” identity, an offense-in-depth practitioner can use “reflective social engineering” to leverage the fraudster’s social engineering attack against them.

Victim impersonation

CTU researchers replied to the CEO fraud email, acting as a gullible victim cooperating with the request (see Figure 3).



Hello, Hello Mr. [redacted]

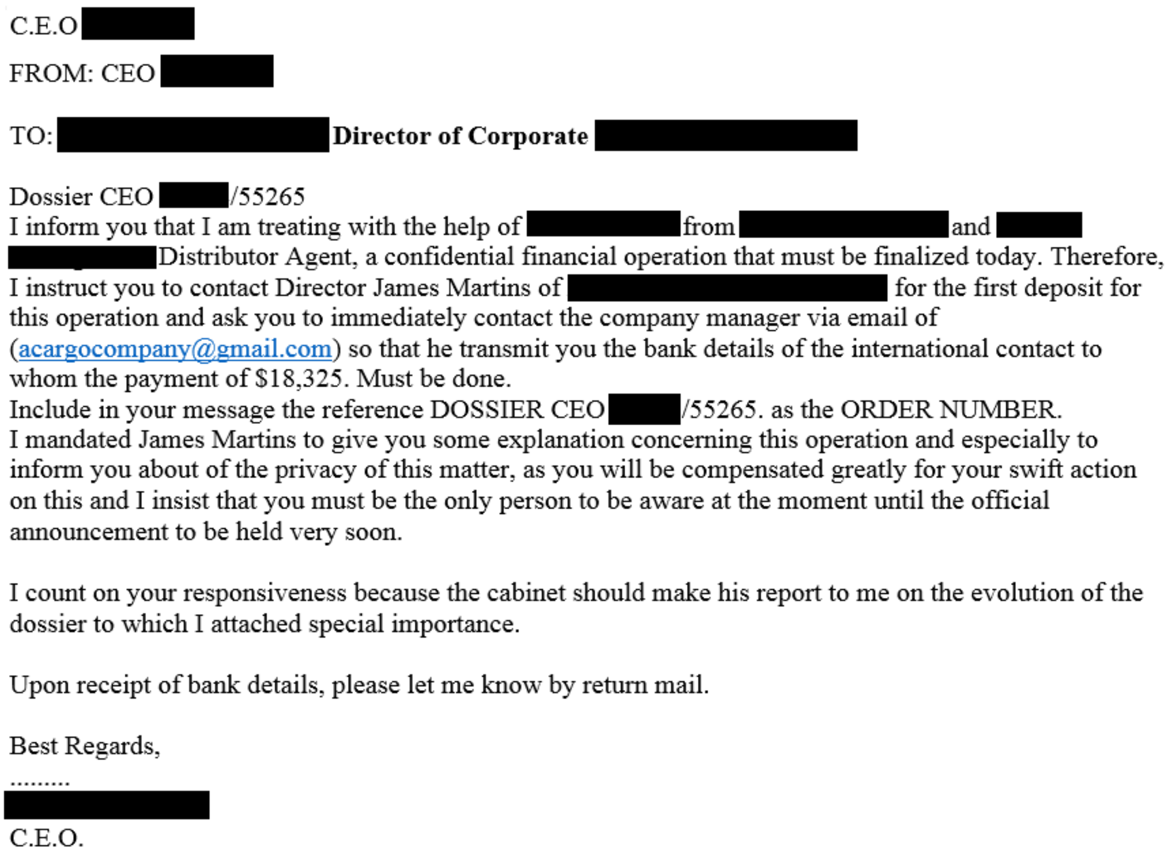
So sorry for the delay, I had an early appointment this morning. How can I help you?

Kind Regards,

[redacted]

Figure 3. Recipient replies to fraudster. (Source: SecureWorks)

The subsequent reply (see Figure 4) referenced a CEO of a U.S. private equity firm that invests in technology services, and a U.S. hedge fund management firm. The fraudster also introduced a fictitious individual named “James Martins” employed by a freight shipping company.



C.E.O [redacted]

FROM: CEO [redacted]

TO: [redacted] **Director of Corporate** [redacted]

Dossier CEO [redacted]/55265
I inform you that I am treating with the help of [redacted] from [redacted] and [redacted] [redacted] Distributor Agent, a confidential financial operation that must be finalized today. Therefore, I instruct you to contact Director James Martins of [redacted] for the first deposit for this operation and ask you to immediately contact the company manager via email of (acargocompany@gmail.com) so that he transmit you the bank details of the international contact to whom the payment of $18,325. Must be done.
Include in your message the reference DOSSIER CEO [redacted]/55265. as the ORDER NUMBER.
I mandated James Martins to give you some explanation concerning this operation and especially to inform you about of the privacy of this matter, as you will be compensated greatly for your swift action on this and I insist that you must be the only person to be aware at the moment until the official announcement to be held very soon.

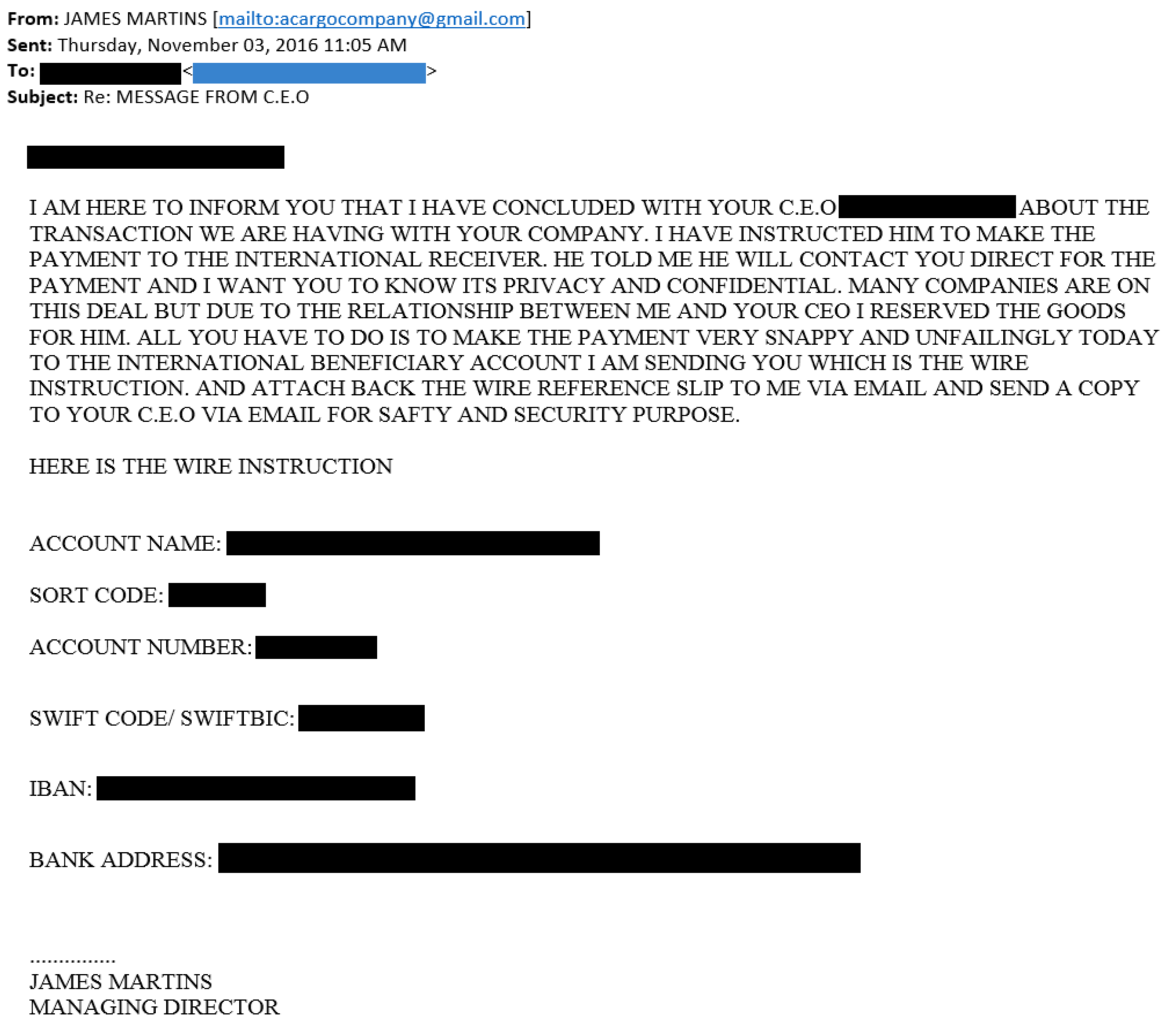
I count on your responsiveness because the cabinet should make his report to me on the evolution of the dossier to which I attached special importance.

Upon receipt of bank details, please let me know by return mail.

Best Regards,
....
[redacted]
C.E.O.

Figure 4. Fraudster pretext for payment. (Source: SecureWorks)

Following the typical BES and BEC process, the fraudster then sent instructions for the wire transfer (see Figure 5). CTU researchers immediately reported the account to the bank because the criminal would likely reuse it to steal from another victim.



From: JAMES MARTINS [mailto:acargocompany@gmail.com]
Sent: Thursday, November 03, 2016 11:05 AM
To: [redacted]<[redacted]>
Subject: Re: MESSAGE FROM C.E.O

[redacted]

I AM HERE TO INFORM YOU THAT I HAVE CONCLUDED WITH YOUR C.E.O [redacted] ABOUT THE TRANSACTION WE ARE HAVING WITH YOUR COMPANY. I HAVE INSTRUCTED HIM TO MAKE THE PAYMENT TO THE INTERNATIONAL RECEIVER. HE TOLD ME HE WILL CONTACT YOU DIRECT FOR THE PAYMENT AND I WANT YOU TO KNOW ITS PRIVACY AND CONFIDENTIAL. MANY COMPANIES ARE ON THIS DEAL BUT DUE TO THE RELATIONSHIP BETWEEN ME AND YOUR CEO I RESERVED THE GOODS FOR HIM. ALL YOU HAVE TO DO IS TO MAKE THE PAYMENT VERY SNAPPY AND UNFAILINGLY TODAY TO THE INTERNATIONAL BENEFICIARY ACCOUNT I AM SENDING YOU WHICH IS THE WIRE INSTRUCTION. AND ATTACH BACK THE WIRE REFERENCE SLIP TO ME VIA EMAIL AND SEND A COPY TO YOUR C.E.O VIA EMAIL FOR SAFTY AND SECURITY PURPOSE.

HERE IS THE WIRE INSTRUCTION

ACCOUNT NAME: [redacted]

SORT CODE: [redacted]

ACCOUNT NUMBER: [redacted]

SWIFT CODE/ SWIFTBIC: [redacted]

IBAN: [redacted]

BANK ADDRESS: [redacted]

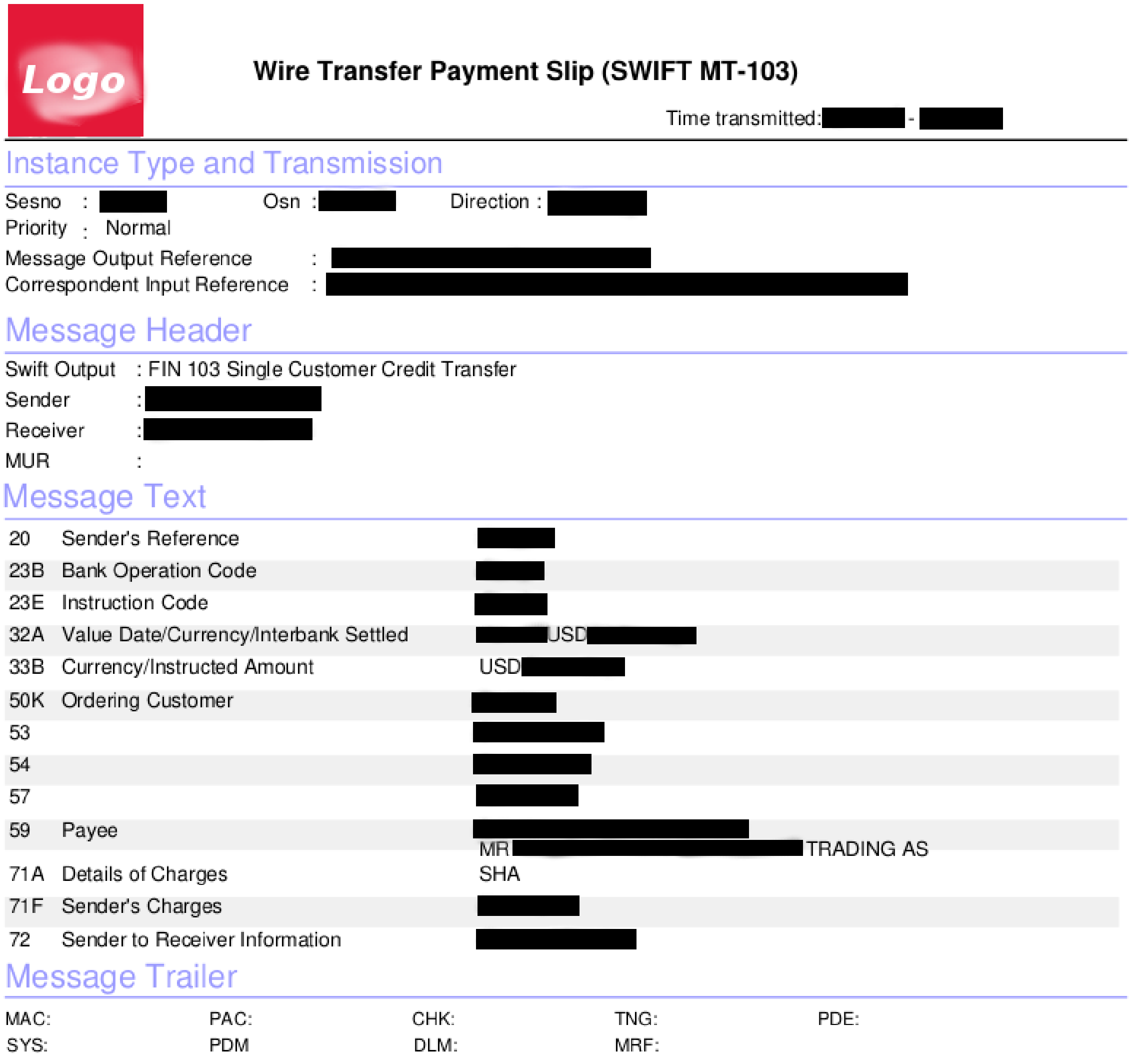
....
JAMES MARTINS
MANAGING DIRECTOR

Figure 5. Wiring instructions from CEO fraud email. (Source: SecureWorks)

The fraudster typically does not provide additional information until receiving proof that the requested payment has occurred, usually via a wire transfer receipt or payment slip. When depending on a third party to provide mule accounts and money laundering services, the payment slip is the only confirmation the criminal has that the victim has paid. Without it, the money launderer could keep the funds and claim the payment never occurred. This payment slip provides additional opportunities for the offense-in-depth practitioner because it is guaranteed to be opened by the fraudster and perhaps the money launderer. A crafted payment slip could help gather additional information and possibly lead to distrust between the fraudster and the money launderer over the confusion regarding the “proof” of transferred funds.

A law enforcement organization with a valid warrant could likely deliver a malware payload that could be used to positively identify the perpetrator. The U.S Federal Bureau of Investigation (FBI) has used this technique on several occasions. However, private companies do not have that authorization, so this approach would be ill-advised. Instead, CTU researchers used an online service to generate a fake but convincing PDF wire transfer payment receipt (see Figure

6). We then added a full-page transparent rectangle that includes a “web bug” that links to a CTU-controlled website. Recipients who click anywhere on the page activate a hyperlink that reveals their IP address and perhaps additional information about their web browser.



Logo

Wire Transfer Payment Slip (SWIFT MT-103)

Time transmitted:[redacted] - [redacted]

Instance Type and Transmission

Sesno : [redacted] Osn : [redacted] Direction : [redacted]
Priority : Normal
Message Output Reference : [redacted]
Correspondent Input Reference : [redacted]

Message Header

Swift Output : FIN 103 Single Customer Credit Transfer
Sender : [redacted]
Receiver : [redacted]
MUR :

Message Text

20	Sender's Reference	[redacted]
23B	Bank Operation Code	[redacted]
23E	Instruction Code	[redacted]
32A	Value Date/Currency/Interbank Settled	[redacted] USD [redacted]
33B	Currency/Instructed Amount	USD [redacted]
50K	Ordering Customer	[redacted]
53		[redacted]
54		[redacted]
57		[redacted]
59	Payee	[redacted] MR [redacted] TRADING AS
71A	Details of Charges	SHA
71F	Sender's Charges	[redacted]
72	Sender to Receiver Information	[redacted]

Message Trailer

MAC: PAC: CHK: TNG: PDE:
SYS: PDM DLM: MRF:

Figure 6. Decoy payment confirmation sent by CTU researchers to fraudster. (Source: SecureWorks)

The fraudster clicked the hyperlink soon after receiving the receipt document, revealing that they were using an ISP in Lagos, Nigeria, and viewing the document on an iPhone. There was another click in rapid succession from an Android device, also in Lagos, which may have been from the money launderer’s device.

CTU researchers sent the fraudster a message indicating that the bank had returned the payment, and asking for new instructions from the fake CEO. Over the next several days, the criminal provided four additional bank accounts. For each account, we sent another fake payment slip and reported it to the bank. This activity provided many IP addresses and timestamps pointing to the fraudster's location. However, an IP address is not solid evidence of the criminal's identity.

Information gathering

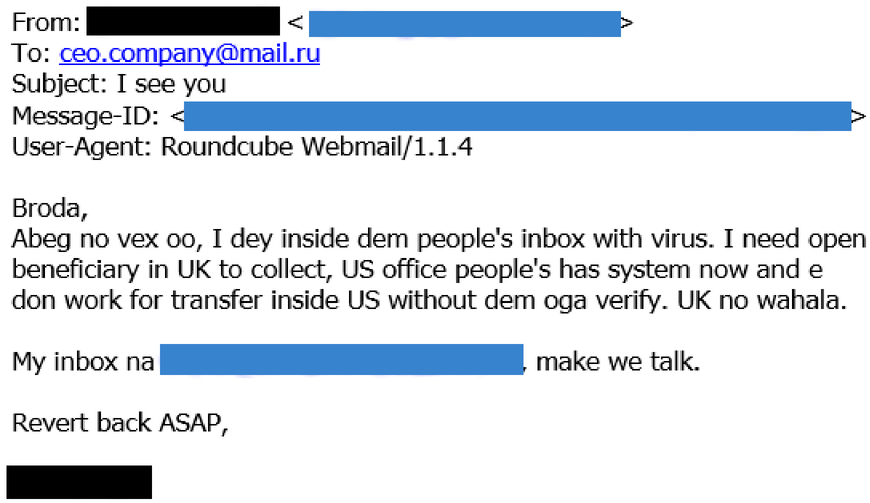
To gather additional information using reflective social engineering, CTU researchers used "Phission," a third-party attribution/penetration-testing/reconnaissance tool. Phission displays a convincing and customizable front-end that leverages the criminal's trust of conventional file-sharing services. Adding a professional logo, a working contact number, and a social media presence makes it nearly indistinguishable from a commercial website.

Fraudsters familiar with phishing may not recognize the interface as a phishing attempt. Instead of obtaining an email password or credit card information, Phission requests a second form of identification to "authenticate" the criminal for authorization to view the payment slip. The document cannot be downloaded regardless of what authentication is provided, so the fraudster provides more verifiable information in desperation to view the payment details. In this case study, the criminal provided a legitimate mobile phone number (Phission rejects VoIP numbers) in Nigeria and used the OAuth open authentication standard to verify his Google and Facebook accounts. The mobile phone number led to the same Facebook identity, nicknamed "Seun," leading CTU researchers to conclude it was his actual account. This case study refers to the fraudster by his nickname because of a pending criminal investigation.

Infiltration

There was enough information to report Seun to the FBI and the EFCC, but it is unlikely either agency would open an investigation in the absence of a real victim with actual monetary losses. CTU researchers therefore decided to continue the reflective social engineering approach to learn more about Seun's operation.

In 2016, CTU researchers observed hours of conversation among self-termed "Yahoo-Yahoo" and "Wire-Wire" Nigerian fraudsters. There is a lingo specific to the fraud culture spoken along with the Pidgin English that is commonly used throughout Nigeria. Armed with this knowledge, we infiltrated Seun's operation by posing as a Nigerian fraudster who had access to the email account of the original spearphishing email recipient. This approach seemed plausible because CTU researchers had observed unrelated fraudsters encounter one another in a victim's email account and start communicating. We sent Seun the email in Figure 7 from the original email account, claiming to be a hacker who has obtained access to the inbox via a remote access trojan (RAT). The message also claims that the would-be victim's organization has installed additional accounting controls in its U.S. payment system, and that it would be possible to steal money from the UK subsidiaries with a mule account in the UK.



From: [redacted] <[redacted]>
To: ceo.company@mail.ru
Subject: I see you
Message-ID: <[redacted]>
User-Agent: Roundcube Webmail/1.1.4

Broda,
Abeg no vex oo, I dey inside dem people's inbox with virus. I need open beneficiary in UK to collect, US office people's has system now and e don work for transfer inside US without dem oga verify. UK no wahala.

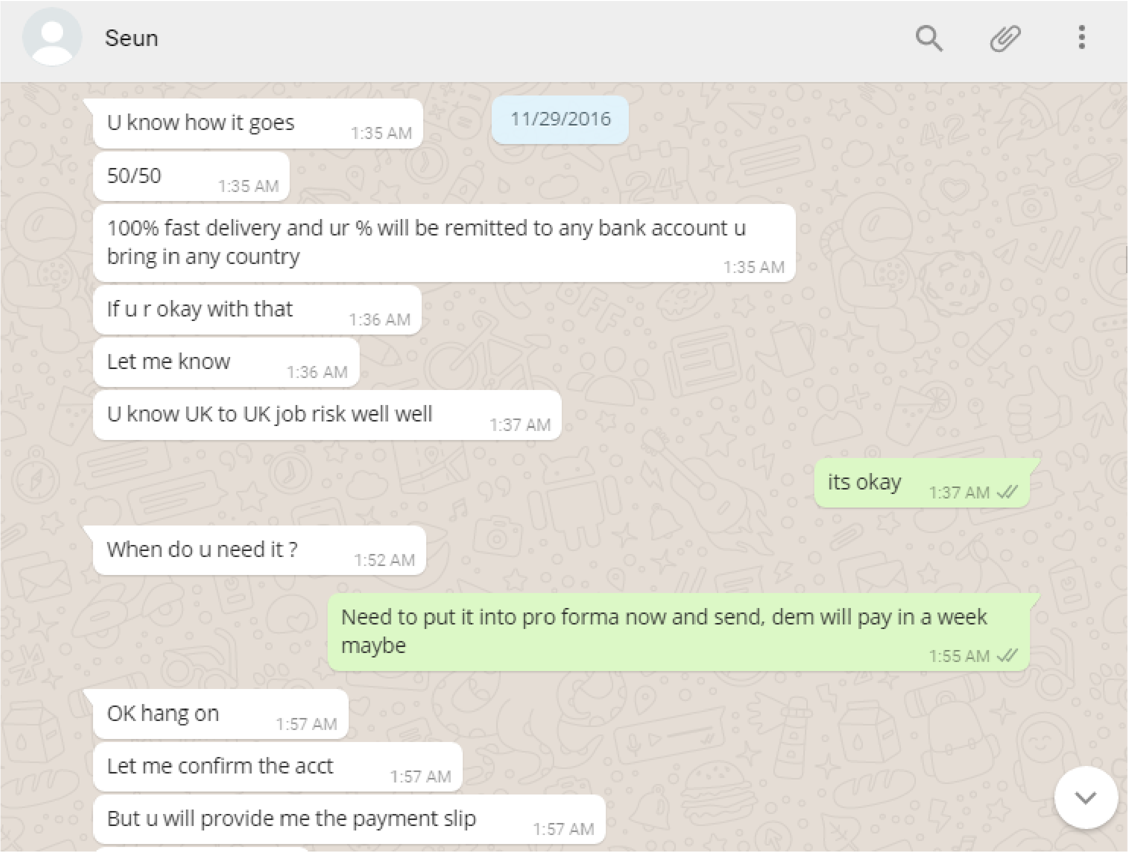
My inbox na [redacted], make we talk.

Revert back ASAP,

[redacted]

Figure 7. CTU researchers communicating Nigerian Pidgin to fraudster. (Source: SecureWorks)

CTU researchers are not masters of Nigerian Pidgin, but the message was sufficiently convincing for a response. Seun replied to a secondary email account to communicate “fraudster-to-fraudster” and disclosed additional information during the conversation (see Figure 8). He obtained bank accounts for money laundering from his “*aboki*” (friend), which is typical of wire-wire fraud. The criminals work together as needed and then share the money. CTU researchers shut down two additional mule bank accounts he provided.



Seun

11/29/2016

U know how it goes 1:35 AM

50/50 1:35 AM

100% fast delivery and ur % will be remitted to any bank account u bring in any country 1:35 AM

If u r okay with that 1:36 AM

Let me know 1:36 AM

U know UK to UK job risk well well 1:37 AM

its okay 1:37 AM

When do u need it ? 1:52 AM

Need to put it into pro forma now and send, dem will pay in a week maybe 1:55 AM

OK hang on 1:57 AM

Let me confirm the acct 1:57 AM

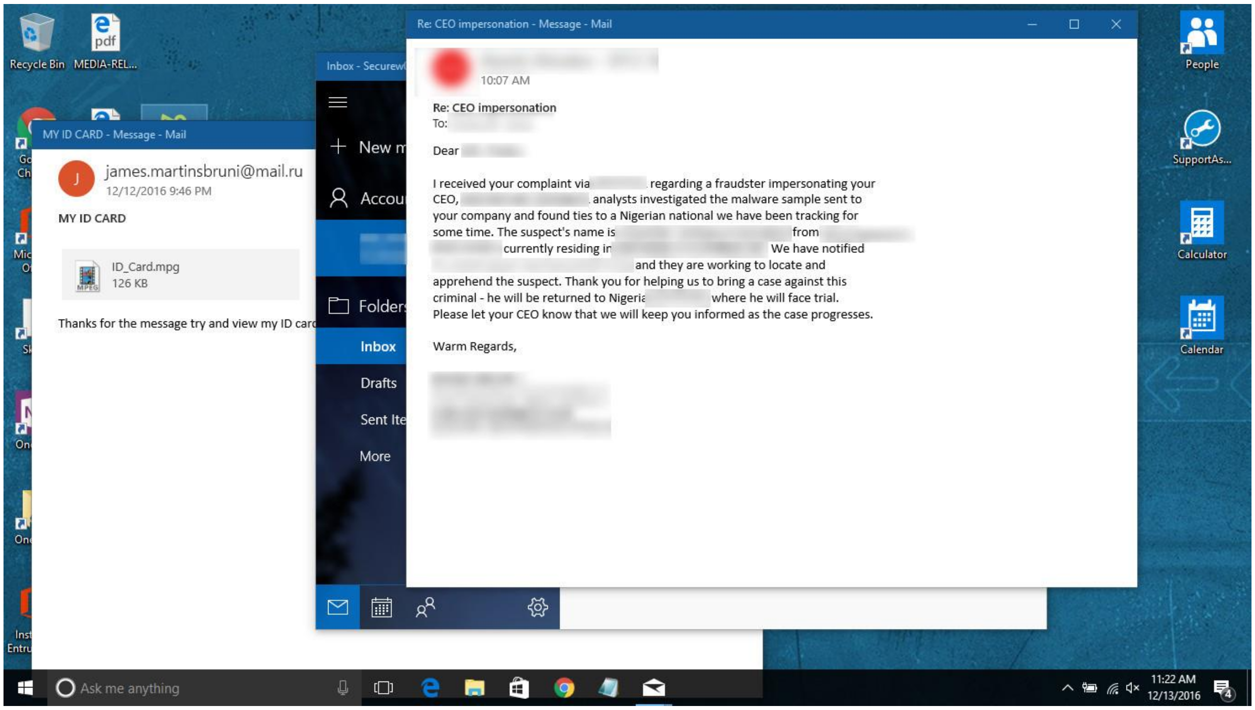
But u will provide me the payment slip 1:57 AM

Figure 8. CTU researchers converse with fraudster on WhatsApp. (Source: SecureWorks)

Seun was very interested in moving from simple spearphishing and impersonation to using malware to gain direct access to his victims' computers and email accounts. CTU researchers set up a fake website pretending to be a malware control panel and spam mailer. Seun thought he was using the website to send malware to his victims, but he was only revealing other targets, which included an international airline and a major consulting firm.

Endgame

It seemed prudent to cut off contact after learning most of the details about Seun's two-man operation. However, a final test would reveal how loyal Seun would be to another countryman in the same line of work. CTU researchers populated the fake malware control panel with results from his "victim," namely the original recipient of his email at the U.S. technology company. The screenshot of the victim's desktop (see Figure 9) showed an email client displaying a crafted message from a non-existent law enforcement agent, claiming that the arrest of the fake fraudster (in actuality, the CTU researcher) was imminent.



MY ID CARD - Message - Mail

james.martinsbruni@mail.ru
12/12/2016 9:46 PM

MY ID CARD

ID_Card.mpg
126 KB

Thanks for the message try and view my ID card

Re: CEO impersonation - Message - Mail

[redacted]
10:07 AM

Re: CEO impersonation
To: [redacted]

Dear [redacted]

I received your complaint via [redacted] regarding a fraudster impersonating your CEO, [redacted] analysts investigated the malware sample sent to your company and found ties to a Nigerian national we have been tracking for some time. The suspect's name is [redacted] from [redacted] currently residing in [redacted] We have notified [redacted] and they are working to locate and apprehend the suspect. Thank you for helping us to bring a case against this criminal - he will be returned to Nigeria [redacted] where he will face trial. Please let your CEO know that we will keep you informed as the case progresses.

Warm Regards,

[redacted]

Figure 9. CTU researchers crafted a screenshot to convince Seun that law enforcement identified the fraudster persona. (Source: SecureWorks)

Seun never alerted his fellow "fraudster" about the imminent arrest. He attempted to send a few more malware payloads to victims, knowing he would not be blamed. Finally, we replaced the fake malware control panel with a "takedown" message to make the impending arrest convincing (see Figure 10).

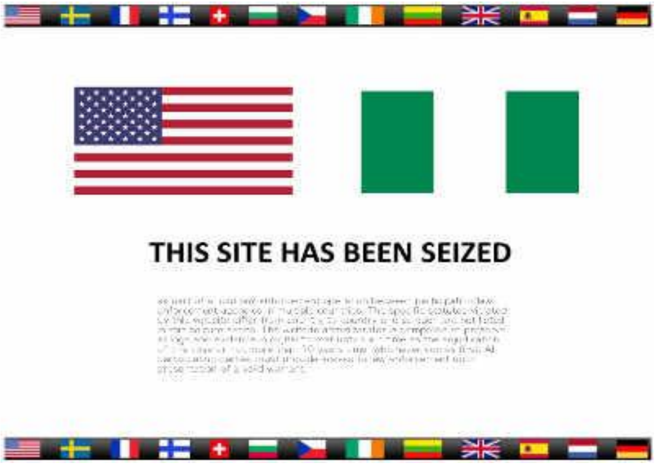


Figure 10. Fictitious seized website banner to deceive fraudster. (Source: SecureWorks)

After a few days, CTU researchers ceased contact with Seun. During this case study, we observed him using the following email addresses:

- acargocompany@gmail.com
- ceoaconnor@zoho.com

- ceo.company@mail.ru
- company.ceopresident@mail.ru
- davidrobbertbruni@gmail.com
- davidybentdickson@gmail.com
- james.martinsbruni@mail.ru

Will this activity convince him that crime does not pay and that he should turn his life to good deeds? Probably not.

Organizations that lost money in one of Seun's scams should alert their country's law enforcement and report the incident to the EFCC. Reporting the incidents to law enforcement increases the likelihood of an arrest. Impacted organizations can also inform law enforcement that CTU researchers know Seun's real identity.

References

U.S. Federal Bureau of Investigation. "Business E-Mail Compromise: The 3.1 Billion Dollar Scam." June 14, 2016. https://www.ic3.gov/media/2016/160614.aspx