PHISHLABS

R.A.I.D. INTELLIGENCE REPORT

Scammers up Their Game with New BEC Attacks

Introduction

BEC is an acronym for "business email compromise." BEC refers to social engineering attacks used to convince those in charge of finances at an organization to send large payments to the scammers. These attacks are carried out over email conversations initiated by the scammer who spoofs the identity of an executive at the organization.

BEC attacks have become more prevalent since PhishLabs' first report in May 2014 (http://blog.phishlabs.com/targeted-wire-transfer-scam-aims-at-corporate-execs) and there appear to be a greater number of copycat attacks. More importantly, tactics have evolved as scammers experiment and benchmark their successes, resulting in better targeting, more convincing scams, and greater losses. PhishLabs' recent research has produced findings than can help fight back against this type of targeted attack.

Then and now

PhishLabs' original BEC report described the general flow of the attacker's playbook and gave some specific indicators for what was one of the most successful BEC campaigns ever. Over the last year or more, almost every tactic has changed. Only the basic premise and ultimate goal remain the same. The following chart compares key tactics between those first attacks and two current campaigns:

	Then	Now
Email services used	Sent from free services or use compromised organizational account	Uses paid webmail service from GoDaddy
Spoofed senders	Executives at targeted organizations or an executive or finance personnel at vendors/suppliers	The top executive at the targeted organization
Domain names	Used look-alike domain names	Spoofs the targeted organization's domain name
Conversation	Single message	Multiple messages exchanged
Call to action	Instructions in attached PDF	Instructions sent in body of follow-up message
Destinations	Accounts in China, Hong Kong, Taiwan	Domestic accounts

There are a few differences among the two current campaigns, but they are more similar to each other than both are to past attacks. It seems more likely that someone looking for emails from impersonated domains with PDFs containing overseas bank account details -- key indicators of past attacks -- might miss and be more likely to fall for these new attacks, so it's important to look at indicators for these new campaigns.

New BEC example #1

This first example arrived in the inbox of a controller for an Atlanta-based equity firm. The email system assigned a "spam score" of zero and was configured so that a message would have to generate a threshold score of 95 before automatically blocking delivery to users' inboxes. In other words, it was treated as a completely legitimate message despite the following warning signs:

- The message was sent from the webmail account at an organization whose domain, although it was legitimate and well-established, had never been seen by the mail server before.
- The message had a reply-to address at a free email service
- The message used an address in the "from" header that indicated it was from someone inside the targeted organization

There are legitimate reasons for all of these things to happen with email systems, but all of them together seems very suspicious -- certainly not a zero on the spam meter.

Spoofing

Many new BEC campaigns use compromised email accounts on GoDaddy's Workspace Webmail service. Typically, these are configured for simple authentication with credentials that are easily phished and replayed. The interface makes it easy to configure a separate "reply-to" address. However, the primary reason these are targeted is the "Identities" feature, which allows sending as an arbitrary email address. These 'from" identities allow any arbitrary address. Used together, emails have an unusual combination of sender and recipient information

```
Received: ... (envelope-from <compromised@somewebmail.com>) ← hidden from user
From: Barry Boss <executive@example.com> ← spoofed using "Identities" feature
To: Aaron Accountant <accounting@example.com> ← actual target
Reply-To: "Barry Boss" <ceo.email@execs.com> ← monitored by scammer
```

Other addresses have been changed, but the "ceo.email@execs.com" is the actual reply-to address used in this scam. The execs.com domain is a vanity email domain provided by the free Mail.com email service.

Confirmation required to obtain mule account info

The message itself reads (the names have been changed):

```
Martha,

How soon can you process a domestic wire transfer? I need a transaction
taken care of.




Thanks,

Aubrey J. Moore
```

This plain-text message is short and to the point. Unlike in past campaigns, no bank details are included or attached. Instead it asks a question, prompting a response. This lets the scammer know when he has a mark on the hook. The destination account details are not disclosed unless a positive response is sent back to the scammer. This prevents a valuable resource (the money mule bank account details) from being spammed out broadly where it can be intercepted and acted upon. Instead, these limited cybercriminal resources are only divulged as needed.

Targeting and recon

In the past, the more successful BEC campaigns often targeted larger organizations with large vendor/supplier networks. Typically, BEC scammers behind the current campaigns are targeting smaller, faster-growing, more nimble organizations who are more likely to make exceptions to payment processes based on personal requests. It appears a lot of effort is being put into target selection and reconnaissance.

In this particular case, the email was addressed to the correct username at the target's domain. That's not always the case, as is illustrated in the following example; however, in this case, the targeted organization made it fairly easy for the scammers to figure out the addressing scheme. On the targeted organization's

website, all partners in the firm had detailed contact information on an "Our Team" page. Beyond just full names, photos, and email addresses that demonstrated a consistent email address scheme, firm partners also offered links to download complete vCard (.vcf) contact information files. This gave the scammers the identities they needed to spoof. The administrative assistant and the company's controller (in charge of finances) had listings, too, but no email addresses or vCards published on the website, although it was easy to guess the correct email addresses for their target recipient.

New BEC example #2

This case was similar to the above case, but there were a few differences. This one appears to be part of a larger-scale campaign.

As in the previous case, the GoDaddy Workspace Webmail service's Identities feature was used to send the initial email using a spoofed identity. In this case, however, the domains do not appear to be compromised, but rather registered by the scammers or someone setting these accounts up and selling them to scammers. Also in this case, all of the actual servers behind the Workspace Webmail are part of GoDaddy's infrastructure in Europe.

As in the previous case, a response is requested. Only if a positive response is received are mule bank account details disclosed. The emails in this campaign are HTML format, not plain text, but are still formatted to appear plain and simple. The initial contact email, received by the targeted organization's CFO, is also brief and a direct request for assistance with financial matters. It looks like:

> Hi,
>
> Are you busy ? let me know if you are not, ill need you to help me process a payment.
>
> Thanks
> Sent from my iPhone

In this case, the message is sent with the High Importance flag set so that it appears urgent. The "Sent from my iPhone" may also be included to indicate that it is an urgent request, something that must be taken care of and cannot wait until the CEO returns to the office.

In this specific case, the CEO does use an iPhone and was, in fact, out of the office on business when the CFO received the message. However, it appears that the tagline/signature is the same in all known cases. It may also be a distractor, used to convince the recipient that the CEO is indeed out of the office and discouraging the recipient from trying to walk over in person to discuss the matter. In other cases, the spoofed executive was present in the same room or immediate area when the message arrived. There is no sign that the scammers are actually performing recon on a level that would let them determine the executive's mobile device type or their travel schedule. That, at least, is somewhat comforting.

Despite the facts that the CEO did use an iPhone and was on the road, the recipient CFO, was alert to these types of scams and spotted what was happening immediately. However, the recipient was instructed to "play along" in order to get mule bank account details. The recipient replied, saying they were happy to help and asking for details. The scammer's response was also sent back with High Importance, looking similar to the following:

> The details are below. Let me know once you receive it and when you are done processing the wire.
>
> Name : Dana Kendrick
> Bank Name : BigSouth bank
> Account Number : 80001737715
> Routing Number : 04400064
> Bank Address : 20115 united Ave Jackson Ms 43909
> Home Address : 3811 Wagon creek rd. Jackson Ms 43911
> Amount : $29,000
>
> Thanks
> Sent from my iPhone

The account details have been changed here, but in a way that preserves the case, whitespace, and other formatting that could provide visual cues and indications of a potential scam in progress. The amount remains unchanged here, and the actual details were turned over to the fraud team at the bank and to federal law enforcement.

Most email clients show only the names and hide the actual addresses, including the spoofed from and reply-to addresses, behind an extra click or two. At this point, no names have been used in the message body. However, when the scammer was left hanging and wanted to follow up, things became a little more personal, addressing the recipient by their first name (changed in the following illustration):

> Chris,
> Have your processed the wire ?
>
> Thanks
> Sent from my iPhone

It appears the scammer will continue to send follow-up messages of this sort about once per day for an additional two or three days until they give up. In some cases, they will attempt to reinitiate the scam, but it's unclear if the scammers are aware that they have previously engaged the target, or if they are attempting (again) solely because the organization has been identified as a potential target and was never crossed of that list.

The initial contact message and follow-up messages were sent from separate domains. The first email was sent from "bai@arekarakim.com," but it turns out that the domain had been suspended by GoDaddy after reports of fraud and abuse. Although the spoofed from address made it appear all message came from the same sender, the reply with the bank details and follow-up messages were actually sent from "admin@langrange04.com." With help from PhishLabs, that domain has now also been suspended.

Tricky addressing

In this case, the company published only names of the executive team, no email addresses and, in fact, used an inconsistent naming scheme for recipient mailbox names, so how did they guess or figure out the correct email address? The scammers made use of an addressing technique that leverages the tendency of mail servers to try their best to deliver (non-spam) messages to the correct mailbox. In cases like this, the technically correct email addresses may have been something like:

Target recipient: ccash@example.com ← "Chris Cash," the CFO
Spoofed executive: jamiemc@example.com ← "Jamie McIntyre," the CEO

Microsoft Exchange, for example, will attempt delivery based on Active Directory information like first and last name. That is what the scammers did in this case, addressing the initial email this way:

```
From: Jamie Mcintyre <jamie.mcintyre@example.com>
To: <chrish.cash@example.com>
```

Once the scammer received a reply, they automatically picked up the correct email address and used it to address follow-up messages such as those with the bank account details.

Note that the 'i' in "Mcintyre" is not capitalized. This mistake could be an unintentional tip off. In this case, however, Microsoft Exchange looks up the name in Active Directory and displays it correctly on Outlook instead, showing the user the corrected "Jamie McIntyre".

Because the scam requires interaction, the reply-to address is always the one actively monitored by the scammers. Most email clients will show the spoofed name if provided as part of the "Reply-To" email header, and this is where minor misspellings, in this case "Jamie Mcintyre" with the lower-case "i", will show up, but those types of mistakes are relatively rare when the scammers are scraping the name off public sources. Unless the name is not supplied, and the address is shown instead, and the user notices, there are no other indicators that the reply is going to an email address different than the one from which it was sent.

In this case, the actual reply-to address is interesting:

```
Reply-To: Jamie Mcintyre <executiacc@gmail.com>
```

PhishLabs was among other cybercrime fighting companies targeted by this campaign. Several other companies that offer anti-phishing products and services have also been targets. Although the email bodies are similar, including the "sent from my iPhone" tagline, they could be copycats. However, the reply-to address is the same among all of these cases and is directly associated with the scammer who seems to be picking some very dangerous (for him) targets.

The cases involving PhishLabs and similar targets all used different GoDaddy domains to send the mail, but the same Gmail reply-to address. While GoDaddy continues to promptly respond to abuse reports and suspend the domains within a day or two of the first known spam emails, the Gmail address has been active for weeks and receiving responses from individuals at targeted organizations. One can hope it remains active only for the sake of monitoring by the good guys.

New information

Another anti-phishing company has already traced the scammer's IP address to the UK. However, this is almost certainly not the criminal's base of operations. PhishLabs has discovered other addresses in related IP address ranges. These all belong to EDIS, an Austria-based hosting provider who has network infrastructure in London. The cluster of IP addresses geolocated to the UK appear to be exit nodes for a VPN type of anonymization service; they don't appear TOR exit nodes. EDIS doesn't provide such services, but services like these have been set up by other hosting companies' partners and resellers who buy service infrastructure from the hoster.

It may be difficult to obtain access logs and similar evidence from EDIS, an EDIS customer/reseller, or any anonymization service provider. Some of this has to do with jurisdiction, data protection laws, and other regulations. However, the most likely roadblock to obtaining those types of records is that they simply do not exist. It is common practice among anonymization service providers operating in Europe to not generate or store these types of logs at all.

A couple of interesting correlations may provide additional clues for attributing this campaign to a specific threat actor by eliminating the confidence that the criminal is operating from within the UK. The domain registrations and the hosting service all use payment systems configured for conducting transactions in Euros (€), not the British Pound (£). Currency conversion, either by the crook or the payment service, is likely an inconvenience and represents additional overhead which might be seen by the crook as unnecessary and eating into his or her profit. Additionally, there are clues in the content of the email messages themselves. The formatting and use of whitespace, especially indentation and around punctuation, as well as some phrasing and usage errors are indicators that the person composing the emails is actually a native French speaker. And France does use the Euro.

The only way to know for sure is to watch where the money goes until we have eyes on those who eventually pocket whatever is left after the mules get their cut.

Fighting back

There are two complementary approaches to threat disruption:

1. Lower the reward to the criminal.
2. Raise the cost to the criminal.

Stop making it easy

The first can be established through raising awareness. BEC scams rely ultimately on human social engineering. That's part of what this article hopes to accomplish. PhishLabs' previous blogs posts, contributions to press and other media reports, and features in webinars are also part of this strategy. Other elements include more closed channels and close-knit information sharing partnerships among security professionals, businesses that could become targets, providers who services are being abused, and the financial institutions that host the accounts used to move money.

There are also technological controls that reduce the criminal's success by preventing the lure from ever reaching their intended target. Tuning spam filters to look for the specific constellation of indicators mentioned will help:

- Message is sent from an external system using a webmail or free email service client
- The "From" header value is spoofed and does not match the username or domain name of the sending account
- The spoofed email address matches the domain name of the local/internal organization
- The "Reply-To" header value includes a spoofed name and the email address is different than the sender and the "From" value

To prevent becoming targets as easily, organizations should consider limiting the amount of information about employees on their website. This includes detailed information on their roles, especially if that role involves control over financial functions. Generic email addresses, public aliases, or a contact form can be used to reach key team members in ways that can be filtered and prevent full disclosure of actual email addresses. Technologically, disabling "helpful" email server features such as "Firstname.Lastname" matching can prevent the delivery of an email based on an educated guess by the criminal when actual email addresses are not readily available. Implementing DMARC and SPF are powerful prevention tools for all email-borne scams affecting an organization, although a proper implementation can be outside the budget of some smaller organizations with limited IT resources.

Hit them where it hurts

The second approach incudes using the intelligence collected about these scams and the criminals behind them to deduce operational choke-points and threat actor attribution.

Email is free, and domain registration is very inexpensive. The one part of the operation that requires the most investment from the criminal are the money mules and their access to the bank accounts used to receive funds. If you are able to obtain mule account details, you can send it directly to fraud contacts at the financial institution named in the response; however, many might not know what to do with than information, especially without context. Reporting it to law enforcement is another good choice. If your organization employs a security or anti-fraud service provider, report it to them. Some manage relationships with both law enforcement and financial institutions.

Alternatively, especially if you have no existing provider, BEC samples of spear phishing emails and any bank account information can be sent directly to PhishLabs at BEC@phishlabs.com. PhishLabs maintains working relationships with contacts at financial institutions and law enforcement specifically for security, fraud, and other cybercrime purposes. We can provide the context and a timely response. Simply reference "BEC spear phishing," and we'll be sure it quickly gets into the right hands.

Mule accounts are key because money mules must, at some point, cash out. This affords law enforcement an opportunity to identify, question, and track their financial activities, leading to the real masterminds behind these operations. For those in the United States, like most are in these BEC cases, being a money mule is absolutely illegal, and their activity is deterred through arrest, vigorous prosecution, and stiff sentencing.

Summary

PhishLabs has seen the tactics of BEC spear phishers change over time. The examples above illustrate two of the most successful recent variations. This report deconstructs each one to extract key indicators, artifacts, and characteristics, and it offers advice for threat mitigation. This information should be applied with the following goals:

1. Prevent losses, "stop the bleeding"
2. Exhaust the criminals essential resources
3. Identify those behind these criminal actions and bring them to justice

The ultimate goal is total threat eradication.

About PhishLabs

PhishLabs is the leading provider of 24/7 cybersecurity services that protect against threats that exploit people. The company is trusted by top organizations worldwide, including 4 of the 5 largest U.S. financial institutions. PhishLabs combines proprietary technology, intelligence, and human expertise to rapidly detect, analyze, and stop targeted cyberattacks before they impact organizations. Additionally, the company provides robust threat intelligence that strengthens existing cyber defenses and optimizes threat prevention. Leading organizations partner with PhishLabs to more effectively disrupt targeted cyberattacks, prevent data breaches, and reduce online fraud.

To learn more about PhishLabs, visit www.phishlabs.com or email info@phishlabs.com

Follow PhishLabs

@PhishLabs

www.linkedin.com/company/phishlabs

google.com/+PhishLabsTeam