Attackers in Executive Clothing - BEC continues to separate orgs from their money

blog.talosintelligence.com/2021/06/business-email-compromise.html

By Nick Biasini.

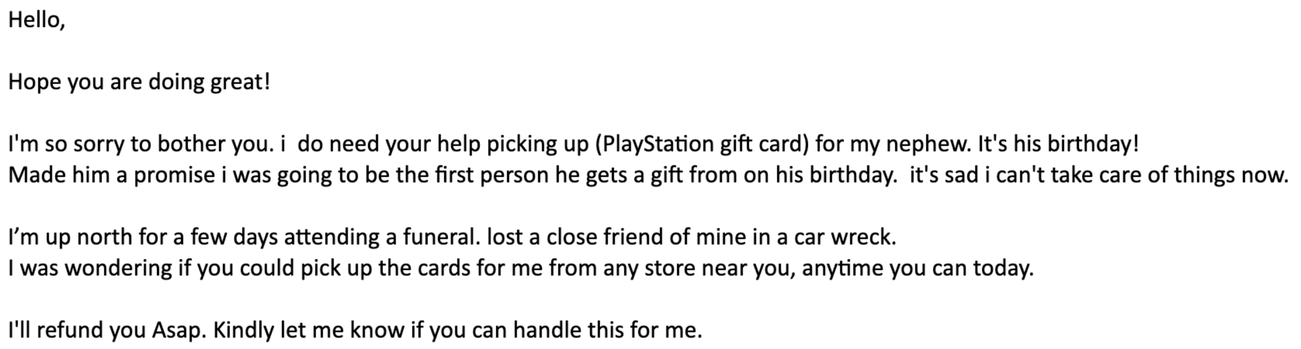
In today's world of threat research, the focus tends to be on the overtly malicious practice of distributing and installing malware on end systems. But this is far from the complete picture of what threats organizations face. One of the most, if not the most, costly is something far less sophisticated: Business Email Compromise (BEC). BEC can take a wide array of different forms, but its goal is relatively simple — trick an unsuspecting user into giving them something. Lately, we've seen a recent rise in these types of attacks, with adversaries still using COVID-19 as a major topic of lures to draw unsuspecting victims into turning over important personal and financial information.

Looking at conservative estimates, business email compromise losses are in the billions, with the FBI stating in 2020 alone the loses approached $1.8 Billion. This is an extremely lucrative enterprise with a low barrier to entry. Other forms of cybercrime are tougher to enter because the actor needs to source the malware they are going to distribute and have enough knowledge to set up and run the associated infrastructure — or at the very least, pay someone who does. At the very least, this takes a significant amount of time and effort, where BEC removes the majority of those barriers.

Business Email Compromise starts as a lot of cybercrime does, with an email. These emails can vary widely in content or in design, but they are almost always spoofed to look like they are coming from someone important. The other common thing is they will almost always ask for some type of assistance. The type of request varies widely, as we'll demonstrate throughout this blog, but the resulting ask is always financial in nature and will require the recipient to purchase something or wire funds somewhere. So let's walk through some examples of what we've seen over the past year.

Gift card requests

The overwhelming majority of the BEC emails we've encountered over the last year revolve around some sort of gift card purchase. The opening lines to these emails are typically something like, "I need you help with a quick task," or "Do you have an amazon account ?" These requests are also likely tied to some extraordinary event. Much of the time, it's a surprise for employees or tied to some specific event, as the example below shows.



Hello,

Hope you are doing great!

I'm so sorry to bother you. i do need your help picking up (PlayStation gift card) for my nephew. It's his birthday!
Made him a promise i was going to be the first person he gets a gift from on his birthday. it's sad i can't take care of things now.

I'm up north for a few days attending a funeral. lost a close friend of mine in a car wreck.
I was wondering if you could pick up the cards for me from any store near you, anytime you can today.

I'll refund you Asap. Kindly let me know if you can handle this for me.

This is by far one of the most common ways we see BEC. These emails typically come from a free email service (i.e. Gmail, Yahoo, or Outlook) but spoofed to appear to be someone important in the organization. The supposed position of the person within an organization and the amount of detail can vary widely depending on the sophistication level of the attacker. In this case, it's a relatively innocuous request to get a PlayStation gift card for an executive's nephew. Also, it's commonly tied to something that will encourage you to have sympathy for the challenges they are facing. In this case, it's due to a funeral for a close friend of the alleged executive. The reasons for this are twofold: First, it creates some sympathy from the victim to hopefully encourage them to help out. It also creates a narrative where pushing back or questioning the request appears insensitive because of the sender's current circumstances. This type of tactic is incredibly common and can get pretty despicable, as we'll demonstrate later.

The types of gift cards these actors request fall into a few different categories. The most common are iTunes or Google Play gift cards. This is a logical choice for adversaries, since there is a huge market for these types of gift cards, as most people have smartphones today, and monetization can occur quickly. Actors have a wide array of ways to re-sell these gift cards on legitimate and illegitimate marketplaces.

However, we have seen a few other types of cards, one of which can be found in the example above — PlayStation gift cards. Those, along with Amazon gift cards, make up the overwhelming majority of the requests we've seen over the past year, but should not be considered an exhaustive list.

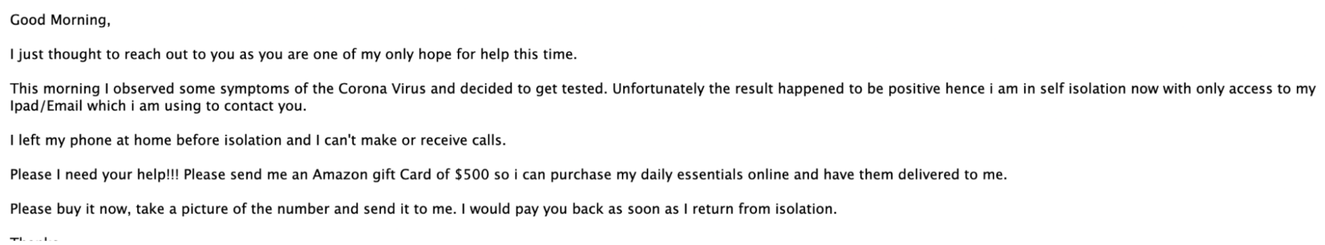
The emails themselves are usually constructed in a very simple manner, with subjects requesting help. Common examples include things like "Task," "Quick Favor" and "Hi," among many others. The subject and content are typically kept short and to the point, even including indicators the email was sent from a mobile device like a tablet or smartphone. This is done purposefully, as most individuals asking for this type of help aren't going to write several paragraphs explaining their intentions and can be used as an explanation of why they aren't using their corporate email.

The biggest difference between these types of emails and something like 419 scams — the classic "Nigerian prince asking for money" scam — is that they are at least somewhat targeted. The type and amount of targeting varies depending on the scenario. The most common examples we see are directed at email addresses that are publicly available, typically from a company webpage or directory, and they appear to originate from someone else who also works at that company. The type of person can change from owners, to executives, to directors. Regardless, it's someone with a management or ownership stake in the company. The names of these individuals and their title is usually available on the company website or elsewhere on the internet. Sometimes, the email can be spoofed to look like it actually originates from that user, but more often than not, it's just a generic email account that looks something like 'executivedirector155878@gmail[.]com' or 'lawfirm3053@outlook[.]com.'

The amount of and types of businesses that get targeted with these attacks is truly staggering, ranging from huge multinational corporations down to small mom-and-pop restaurants in U.S. cities. We found examples of small restaurants that are being targeted by impersonating the owners, since the information was available on their website. These actors are prolific and thorough with accurate impersonations for the large majority of the campaigns we saw. We did notice that there were repeated attempts at some of the larger targets, potentially demonstrating their value to criminals. These attempts typically attack different users at the same organization with similar themes and the same director/executive as the other messages.

COVID-19 impact

The themes for these campaigns were largely innocuous for a time. But just like every other aspect of life, COVID-19 has had its effects. Beginning early in 2020, we started seeing COVID being more actively integrated into these campaigns. The most common example was a request for gift cards after the person in question was infected with COVID-19, an example of which is below.



Good Morning,

I just thought to reach out to you as you are one of my only hope for help this time.

This morning I observed some symptoms of the Corona Virus and decided to get tested. Unfortunately the result happened to be positive hence i am in self isolation now with only access to my Ipad/Email which i am using to contact you.

I left my phone at home before isolation and I can't make or receive calls.

Please I need your help!!! Please send me an Amazon gift Card of $500 so i can purchase my daily essentials online and have them delivered to me.

Please buy it now, take a picture of the number and send it to me. I would pay you back as soon as I return from isolation.

In this example, we can see the criminal is claiming to have been infected with COVID-19 and it's preventing them from being able to buy things. This is obviously a ridiculous claim, but could work nonetheless.

These were not the only types of themes we saw associated with COVID. As time went on, the ways bad actors tried to profit off the pandemic shifted to helping with those dealing with losses.

One particular exchange started as most did with a simple request for help as many of these campaigns do:

`"How are you ? Hope you are keeping safe?. Are you available via email? I need your help." [Sic]`

This particular victim responded to the initial request with some information about vaccination status and some projects they've been working on. Within hours, the criminal responded with their plea for gift cards, but this time, pulling at heartstrings by discussing children losing parents to COVID and adding sympathy for the elderly and ailing, as well:

Thanks for responding, Actually, I need to get GOOGLE PLAY GIFT CARDS for my Niece who had Heart operation some days ago she had lost both parents to the disease (COVID-19). It's her Birthday gift, but I can't do this right now because I have arthritis in the knees and ankles. They are giving me problems. I am going up and down one step at a time. This method is neither graceful! Or fast!, and I tried purchasing online but unfortunately no luck with that. Can you get it from any store around you? I will reimburse you with the money spent. kindly let me know if you can handle this. [Sic].

The criminal pulls out all the stops to get their payoff. Luckily, in this particular example, the target realized the user was impersonating someone and no money was lost. Unfortunately, that is not always the case. Amazingly, this wasn't the most heinous example of business email compromise we found during our analysis. Below, there's an example of one of the worst campaigns we observed.

```
Hi <Name>,
Are you available? I need your help, I'm giving out gift cards to the
hospice care unit for donation. Can you help me with some? You will be
reimbursed.

Thank you,
```

In this campaign, an executive is requesting the employee buy gift cards to hand out to a hospice care unit. This truly shows there are no lows these actors won't sink to to try and convince people to give in to their monetary demands. This is further illustrated by the successful campaigns we've analyzed and the ways these actors typically operate.

Process

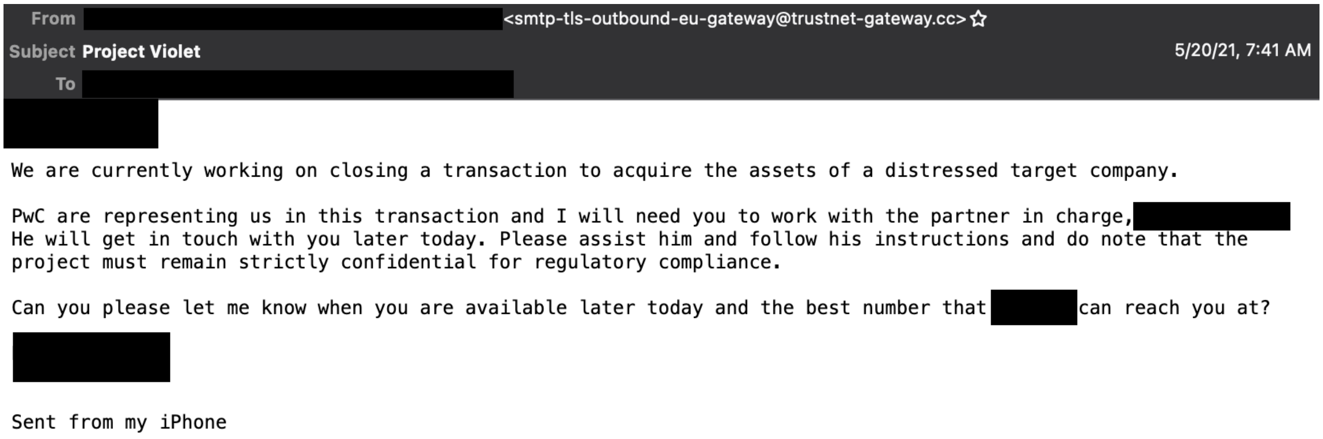
The way this works is incredibly simple and requires nothing more than some social engineering skills and persistence to reach enough potential victims. We've walked through several examples of how this works and you can see the basic, high level, overview. It starts with an innocuous, simple email asking for help, most times related to a gift card or other quickly monetizable purchase, but that request often doesn't show up until you initially respond. Once the victim responds, the actor goes into action, requesting very specific amounts of gift cards typically in the $300 - $500 range. Additionally, they will always request that the victim open the cards, expose the gift card numbers, take a picture of it, and send it to them via email. This allows them to start the monetization process and with gift cards, there's no additional cost to flip these to other individuals. This is not the end of the process though, at this point the actors pivot and come at you harder. Typical responses to the first delivery of gift cards is:

```
Thanks, did you see my other message? I'm going to need more.
```

At this point, the actor has realized they have an active victim that is willing to give them money and they begin to push even harder, going back again and again until the unfortunate victim realizes they are being scammed. However, the damage is already done. Those gift cards are already sold and used. Despite being fairly simple and low-cost, these campaigns are surprisingly effective and their popularity is only increasing. However, these are not the only types of business email compromise examples we see, some examples are a lot more sophisticated.

Acquisition-themed campaign

One of the more organized and large campaigns centered around acquisitions. This is a tactic this particular group used before and they are still at it with almost continuous rounds of emails. This group uses several different tactics to help ensure success with these campaigns. First and foremost they work to actually spoof their initial email address in the "FROM" field. In most cases, these emails will have a subject that starts with "Project," followed by either an acronym or code word of sorts. Examples include "Violet," "DKM," "HLA" and "Cactus". There was a variety in the terms used since this campaign has been going pretty steadily since late 2019. An example of some of the most recent emails are shown below.



From [redacted] <smtp-tls-outbound-eu-gateway@trustnet-gateway.cc> ☆

Subject Project Violet 5/20/21, 7:41 AM

To [redacted]

[redacted]

```
We are currently working on closing a transaction to acquire the assets of a distressed target company.

PwC are representing us in this transaction and I will need you to work with the partner in charge, [redacted]
He will get in touch with you later today. Please assist him and follow his instructions and do note that the
project must remain strictly confidential for regulatory compliance.

Can you please let me know when you are available later today and the best number that [redacted] can reach you at?
```

[redacted]

```
Sent from my iPhone
```

These campaigns rely heavily on phone-based social engineering since they are asking the target to provide a phone number for someone to call. Additionally, the email addresses of both the sender and receiver appear to be coming from the same company, but if you look closer, that is not the case. In the image above, the company in question has been redacted, however, you can still see the reply-to address in the email (smtp-tls-outbound-eu-gateway@trustnet-gateway[.]cc).

This is the first obvious indicator that this email is not legitimate. If the target were to reply, the email will be sent to that obviously illegitimate email. This is a typical behaviour for this group and the domains being used all try and leverage a sense of trust (i.e. trustnet-gateway[.]cc, trustnet-server[.]cc) or network activity (gateway-resolver[.]cc, intranetgateway[.]net).

However, if the user did work in acquisitions for a company and this email hit their inbox, the likelihood of success seems higher. This is also demonstrated in the targeting of these campaigns, since they appeared to hit a more curated list of victims. We didn't find a wide array of companies — small, medium and large — receiving emails. Instead, these tended to hit larger companies, Cisco included. They also tended to be a bit more descriptive than what we typically see, but in some cases, it was rather short and direct.

```
 I hope you are doing well.
We are currently working on a sensitive acquisition and I will need your
help to resolve certain matters by the close of the week.
Can you please let me know when you are available and the best number to
reach you at?
```

Regardless, they all used spoofed from addresses and leveraged the reply-to functionality to direct traffic to an email address leveraging the four domains they controlled: trustnet-gateway[.]cc, trustnet-server[.]cc, gateway-resolver[.]cc, intranetgateway[.]net. Some of the examples were made to appear to come from mobile sources, others were typical signature blocks. These campaigns have continued steadily for quite some time with Cisco Talos finding examples dating back to late 2019 in some cases. Despite their persistence, these campaigns are typically not high volume, with a small number of emails coming out every few weeks to a month.

Support contract theme

A second campaign provided a slightly more sophisticated approach to these campaigns and could result in a higher overall payout. These particular emails were related to something that anyone who works in an enterprise is familiar with: support contracts. In an enterprise environment when a large purchase is made for hardware, software, or other technology, a support contract is likely part of the purchase — this allows the purchaser to do things like open support tickets or get replacement parts when things break. Business Email Compromise (BEC) actors have realized that this is a common task organizations have to deal with, incurring substantial cost, and they've tried to capitalize. We started seeing a series of emails in mid-2020 with similar subject lines, all ending in "Logistics Support Request," with some acronym or company name at the beginning. For example, "IDA Logistics Support Request:"

```
Subject: IDA Logistics Support Request

Dear
Hope you are in good health?
I need your help with a logistics support payment on behalf of IDA, for
<company>.
Look forward to your reply for more details.

Best wishes, [Sic].
```

This group also made use of the COVID pandemic, with references laced through some of the emails. This serves two purposes in this context: It humanizes the criminal and provides an easy way to strike up a conversation with the victim, hopefully leading to a payout. After analyzing several of these campaigns, we have a better understanding of how the attack occurs and the type of payout the attackers seek.

Once a victim responds to the initial email, the criminal begins asking for payment associated with the support contract. In the examples we analyzed, the primary ask was for several thousand Euros or GBP specifically, indicating potential targeting of European companies for this campaign.

```
 Apologies for the inconveniences, I need your assistance with a transfer of
2'867 Euros, for a <company> Support payment. Our treasurer is indisposed
and will not be able to make the transfer at the moment. I am away on a
work-related assignment and I do not have my internet banking access card
reader to make the transfer and it is needed urgently. [Sic].
```

In most of the examples we analyzed, the victim realized they were being scammed before they sent any money, but again, this is not always the case. These actors typically just leveraged free email platforms, mostly Gmail accounts, to conduct these campaigns.

These actors try a variety of lures and means to achieve their financial goals. As with most threats, there are different tiers of sophistication, with some extremely basic actors conducting what amounts to a modified 419 scam to organized groups that are targeting large organizations with intentions to achieve payouts in the thousands of dollars, at the very least.

Language diversity

One aspect of Business Email Compromise that isn't commonly addressed is the languages these attacks leverage. The majority of the emails are in English, but that is largely true for malicious email. However, it was not the only language we observed being used in campaigns. During our research, we identified several European languages and some Asian dialects, as well, although their volume was much lower than the English language examples of BEC. There were also strange examples where people attempted to use multiple languages, as in this example that asks for help in both German and French.

```
Hallo

Ich brauche deine Hilfe, bitte.

S'il vous plaît j'ai besoin de votre aide.
```

It's important to realize that, especially if you are a multinational company or an organization that does business in multiple different languages, you need to account for BEC attacks using any of them. This may require additional filtering and terms that you are flagging based on that information, but it is likely to catch more attempts than just focusing on English.

Protecting against BEC

One of the biggest challenges of addressing BEC is that these emails rely heavily on common language and leverage human nature to steal from their victims. As such, detection can be a challenge. There are solutions in place, but always be aware that it can be difficult to ensure that only BEC emails are caught up in the net, which is one of the reasons many organizations rely on tagging of emails vs blocking them outright. The other part of this that makes it challenging is the lack of URLs or attachments. These are common aspects of most malicious emails that can be leveraged to help in detection.

The most common solutions involve identifying suspect emails that are originating from outside the organization. The challenge is determining what level of sensitivity to apply. If you make detection and blocking too strong, it's likely you will block legitimate emails, which could affect business. If you make detection too weak, you are adding risk that BEC emails will reach users' inbox. There are a variety of ways BEC can be addressed in Cisco Secure

Email, up to and including add-ons such as the advanced phishing protection, which adds sender authentication and some additional BEC detection capabilities. However, there is a second layer to protecting against BEC: Educating users on how to spot it and what to do.

One simple step that some organizations can take is adding a tag to the subject line of the email. This can be extremely useful to help users realize the request came from an external source outside the organization and maybe question the incoming request with a little additional scrutiny. This doesn't block the email outright, just adds a little context by changing the subject and adding a tag like "[External]".

There are also a few key questions to ask yourself when seeking out BEC attempts. First, why is an executive emailing you from a Gmail/Yahoo/Outlook email address? Is this typical behaviour? Would you typically respond to these requests? And are they using a generic sounding email (i.e. executivedirector9383489@gmail[.]com or lawfirm283@outlook[.]com)?

Looking for a different reply-to address is another important way to identify them. This is something you will commonly see in marketing emails but typically shouldn't be found in one-to-one communications. If you hit reply, does the address you are replying to change? Is it to an unfamiliar domain? These are the first indicators that something isn't quite right. However, it isn't always easy to make that determination.

Let's assume you're already in the process of being scammed, how would you determine something is off? Having read through thousands of these email campaigns and a fair amount of potential victims, we have gleaned a couple of key things to ask during these exchanges. First and foremost is out-of-band verification. Before you commit to buying anything, try to communicate to the supposed sender directly through other means, such as an email to their official address or a DM on a social media platform. This could also be as simple as a text message or phone call. We've come across countless examples of users starting down the path to compromise, but by asking key questions, realize they are being scammed before any serious damage has been done.

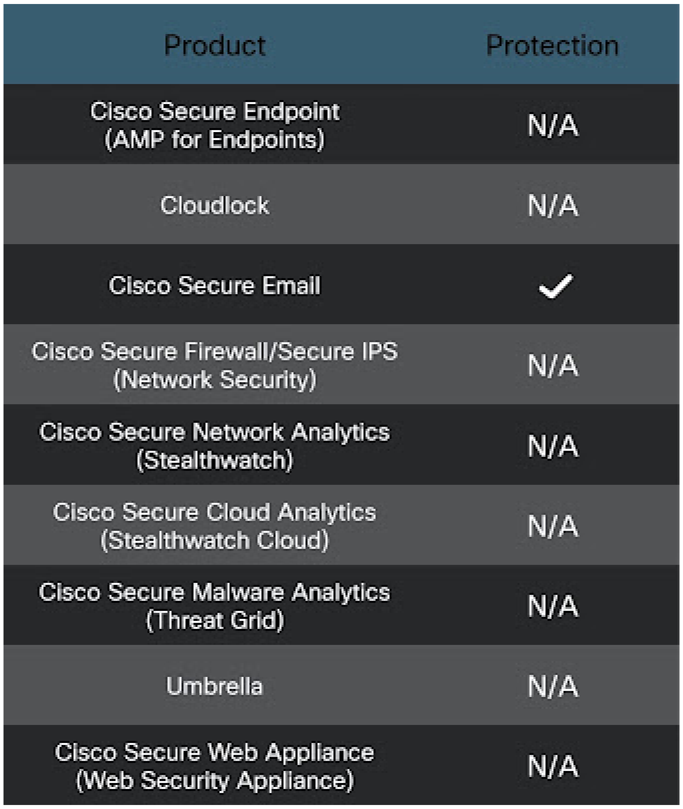
Conclusion

There is no silver bullet or one-size-fits-all solution for BEC. It's going to take a combination of technology and human capital to defeat this threat. One final note on that — if you do have a user that stops these types of campaigns, reward them. They have saved your company a lot of potential loss, and by reinforcing the behavior, hopefully more employees will be willing to step up and stop these types of attacks from occurring. The problem of Business Email Compromise isn't going away and as we get better and better at stopping malware from running and exploitation from being successful, it's only going to get significantly worse.

This post contains basic and sophisticated examples of BEC and shows that they can be extremely effective. Most estimates have the revenue generated from BEC in the billions, and although a lot of attention gets paid to more destructive and aggressive threats like big game hunting, it's BEC that generates astronomical revenue without much of the law enforcement attention these other groups have to contend with. If anything, the likelihood of this has only increased in the pandemic, with people relying more and more on digital communication. The reality is these types of emails and requests happen legitimately all over the world everyday, which is what makes this such a challenge to stop.

Coverage

Ways our customers can detect and block this threat are listed below.



Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	N/A
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	N/A
Cisco Secure Network Analytics (Stealthwatch)	N/A
Cisco Secure Cloud Analytics (Stealthwatch Cloud)	N/A
Cisco Secure Malware Analytics (Threat Grid)	N/A
Umbrella	N/A
Cisco Secure Web Appliance (Web Security Appliance)	N/A

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.