Analyzing Email Services Abused for Business Email Compromise

trendmicro.com/zh_hk/research/21/j/analyzing-email-services-abused-for-business-email-compromise.html

2021年10月14日

Cyber Threats

We analyzed five major types of email channels, and the techniques in keywords and domain names BEC actors use to appear legitimate to potential victims.

By: Marshall Chen, Loseway Lu, Paul Pajares, Fyodor Yarochkin October 14, 2021 Read time: 9 min (2668 words)

Like a number of online attacks and threats that took advantage of the changing work dynamics, business email compromise (BEC) remains one of the cybercrimes that causes the most financial losses for businesses despite the decrease in number of victims. Our continued monitoring of BEC activities showed a consistent increase in numbers during the year.

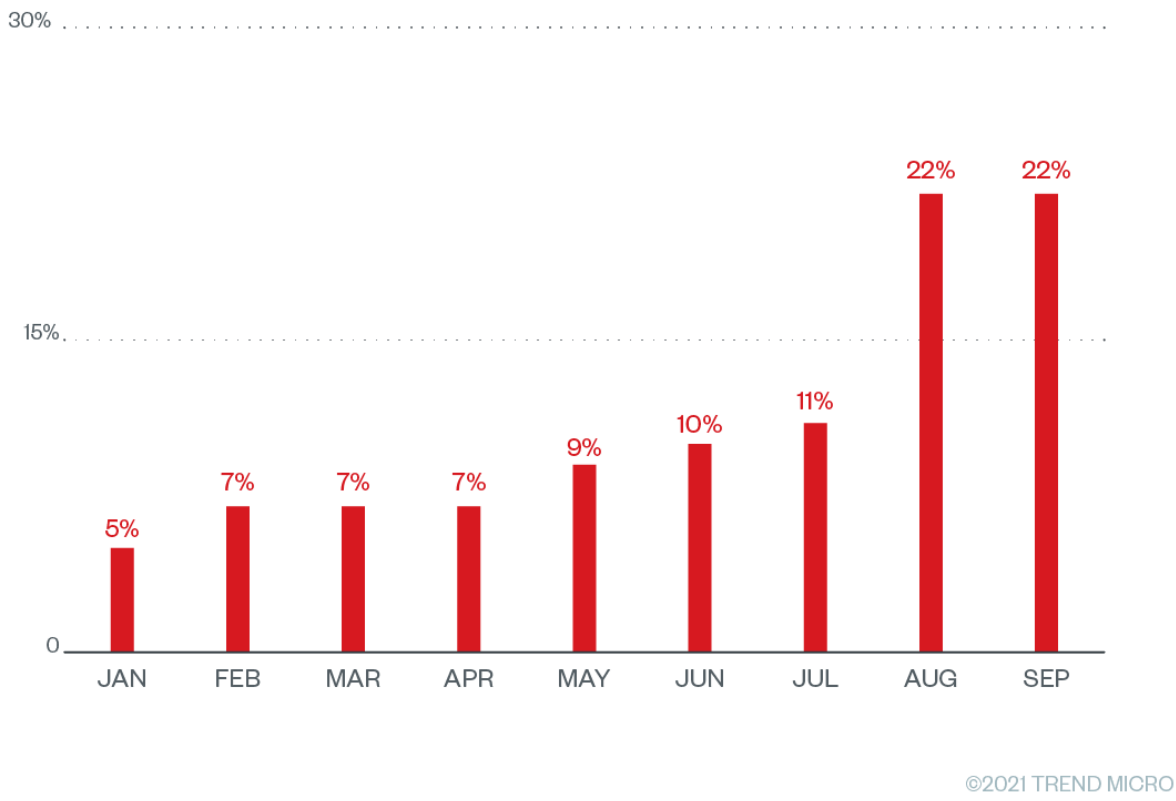


Figure 1. Percentage of BEC detections from January to September 2021. Data from Trend Micro™ Smart Protection Network™ (SPN).

The gradual increase throughout the year prompted us to pay attention to the campaigns being deployed, but the sudden increase in August caught our interest. Compared to campaigns from previous years in which BEC actors mostly impersonated executives or ranking management personnel, we observed a specific BEC campaign type spoofing general employees' display names. We noticed a sudden upshot of dangerous emails impersonating and targeting ordinary employees for money transfers, bank payroll account changes, or various company-related information. We launched the "BEC Display Name Spoofing" detection solution for Trend Micro™ Cloud App Security in Q1 to address this issue. Following this, we also observed the highest volume of BEC detections in the Americas.

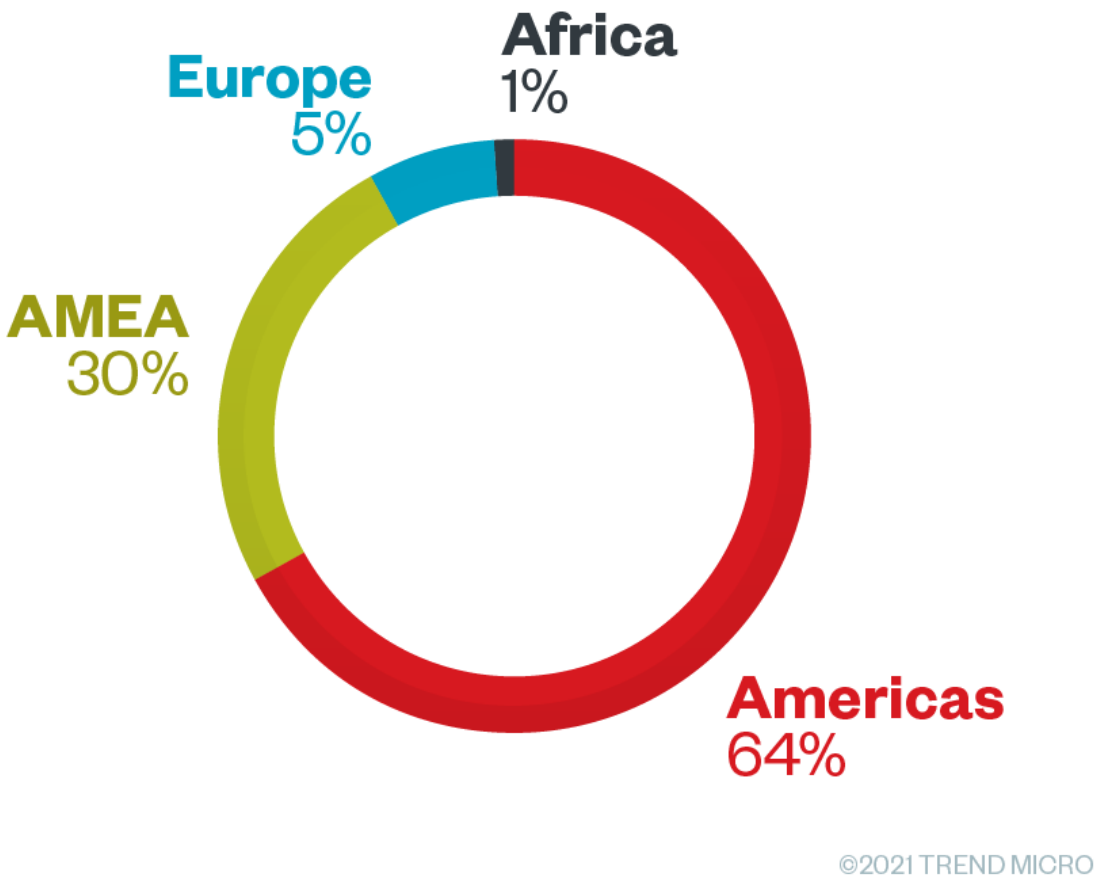
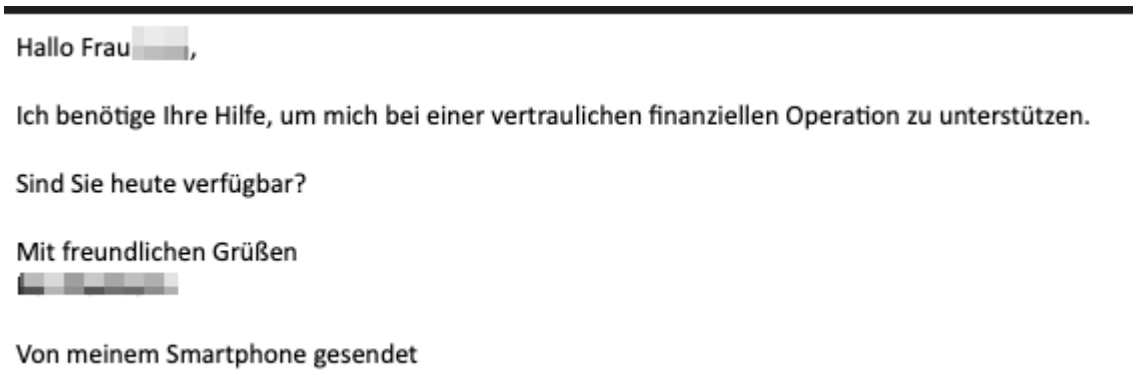


Figure 2. BEC display name spoofing detections by region from January to September 2021


Hallo Frau [redacted],

Ich benötige Ihre Hilfe, um mich bei einer vertraulichen finanziellen Operation zu unterstützen.

Sind Sie heute verfügbar?

Mit freundlichen Grüßen
[redacted]

Von meinem Smartphone gesendet

Figure 3. A BEC email sample spoofing the display name of an employee. The content of the email translates as the sender asking help for a confidential financial operation and inquiring if the recipient is available for the day.

BEC is an online scheme dependent on leveraging email and its features of convenience for legitimate users, and we noted five major types of email channels that BEC actors use. As we continue monitoring BEC operations, we also learned that BEC actors can use the same channels and techniques for a longer period than for just one deployment campaign, tracking complaints from different spoofed and scammed victims online. We also took note of the patterns in keywords and domain names that they use to appear legitimate to their potential victims, and what BEC email recipients can watch for when encountering these scams.

Types of email services used for BECWe analyzed the email services abused and the techniques that BEC actors have adopted in their campaigns.

Figure 4. Email services abused for BEC deployments

1. **Free email services**

We observed BEC groups favoring the abuse of known free email services for the low-cost entry. There is also the trusted marketing quality and service promise of confidentiality in terms of protecting legitimate users, while bulk account creation tools can be used to

facilitate numerous accounts. We observed services offered by Gmail, Hotmail, and Outlook as the top choices for BEC campaigns.

These services allow BEC actors to spoof enterprise employees' names or personal emails to use. In a typical case of this type of abuse, malicious actors spoof an employee email address and request changes to payroll deposit bank accounts.

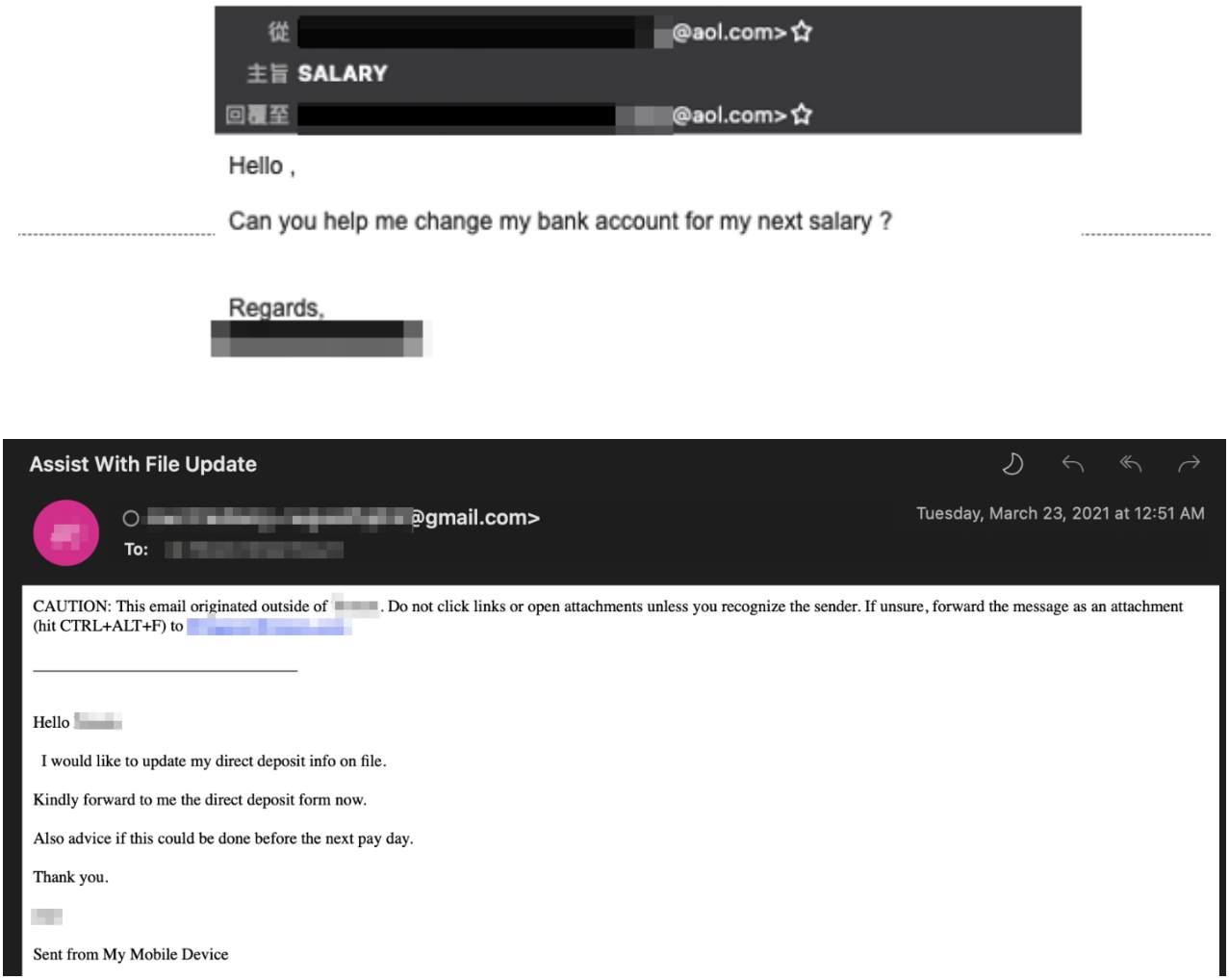


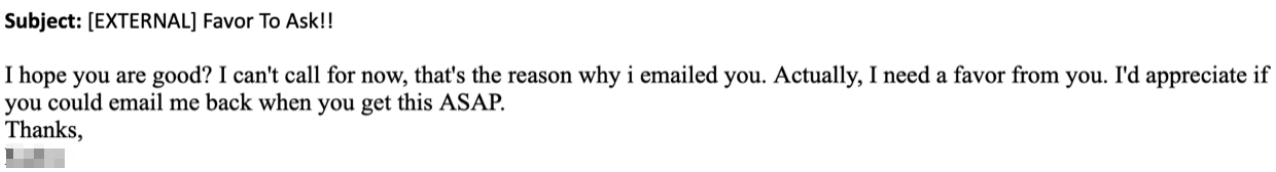
Figure 5. BEC mail from AOL (top) and Gmail (bottom)

We observed a part of the BEC chief executive officer (CEO) email fraud scheme includes having a common account naming convention, such as "office", "president", "chief", and "director", among company leadership positions. Among all these free email services, Gmail appears to be the most commonly abused service for BEC during our investigation timeframe. We identified 10 commonly used examples:

1. chiefexecutiveoffice <BLOCKED> [@]gmail.com
2. chiefexecutiveofficer <BLOCKED> [@]gmail.com
3. directorexecutiveofficer <BLOCKED> [@]gmail.com
4. officepresident <BLOCKED> [@]gmail.com
5. officepro <BLOCKED> [@]gmail.com

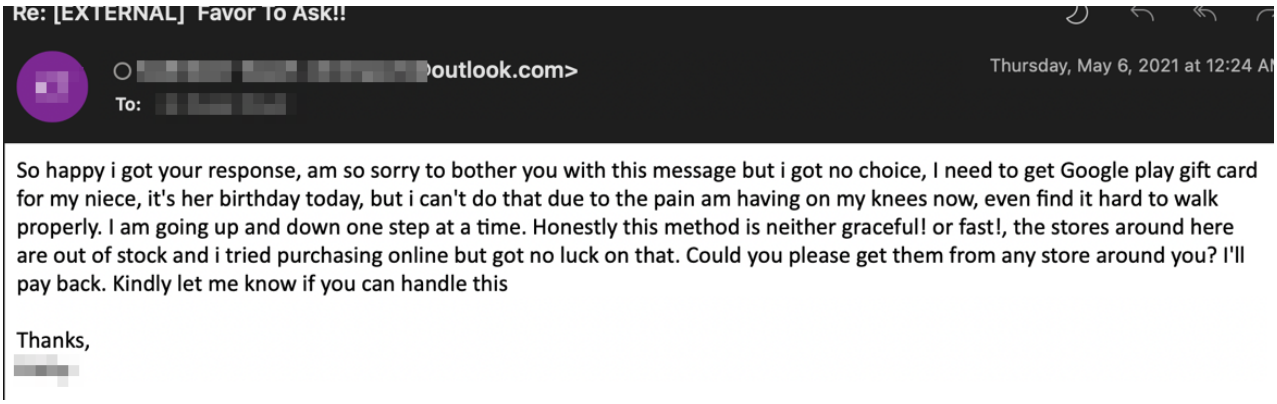
6. officeproject <BLOCKED> [@]gmail.com
7. officework <BLOCKED> [@]gmail.com
8. offshoreoffice <BLOCKED> [@]gmail.com
9. presidentoffice <BLOCKED> [@]gmail.com
10. rev.office <BLOCKED> [@]gmail.com

More often, BEC email content usually includes direct financial requests or transfers from the intended victim. However, there are also indirect approaches wherein they first ask for specific favors from the recipient. If the recipient replies, it indicates that the potential victim believes that the sender is legitimate.


Subject: [EXTERNAL] Favor To Ask!!

I hope you are good? I can't call for now, that's the reason why i emailed you. Actually, I need a favor from you. I'd appreciate if you could email me back when you get this ASAP.
Thanks,

Figure 6. BEC actor first asking for help


Re: [EXTERNAL] Favor To Ask!!

outlook.com>

Thursday, May 6, 2021 at 12:24 A

To:

So happy i got your response, am so sorry to bother you with this message but i got no choice, I need to get Google play gift card for my niece, it's her birthday today, but i can't do that due to the pain am having on my knees now, even find it hard to walk properly. I am going up and down one step at a time. Honestly this method is neither graceful! or fast!, the stores around here are out of stock and i tried purchasing online but got no luck on that. Could you please get them from any store around you? I'll pay back. Kindly let me know if you can handle this

Thanks,

Figure 7. BEC actor requesting the victim to buy a gift card after the user replies to their first email for a favor

We also observed some of these BEC email addresses being active from just a couple of days to years. For example, email account cexecutive9<BLOCKED>[@]gmail.com has been active for more than three years. We detected the address sending BEC emails in 1H 2018, and continued to see the same email account actively sending BEC more than three years later. We also noticed some users in social media complaining about an email scam received from the same address.

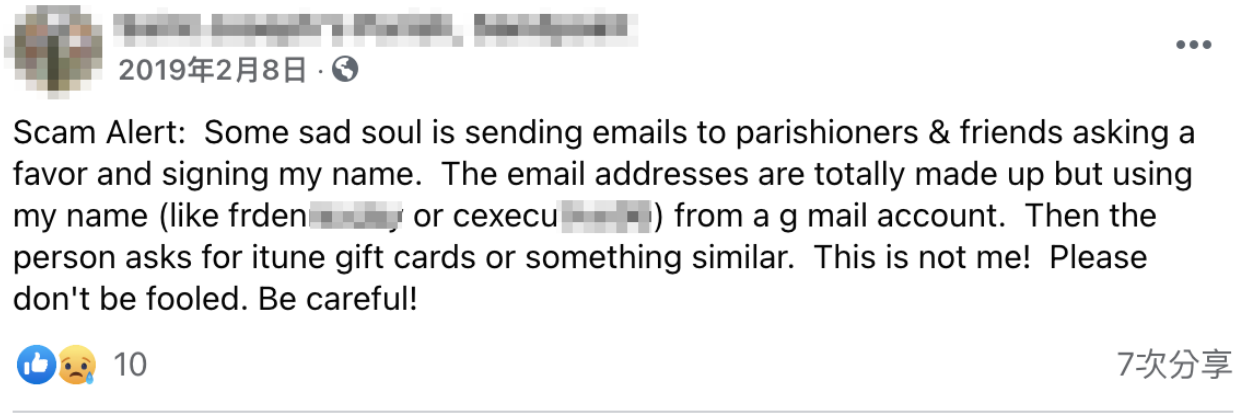


Figure 8. A user posting about a scam email account on social media in 2019. We have been following the said account since 2018, and observed it still being used to deploy campaigns in 2021.

2. Local email services

Some services provide local email services for end users. BEC actors also frequently use these services (using either compromised credentials or making new ones) to launch BEC attacks. We observed more than 15 countries' local email services with BEC email footprints, such as the United States, United Kingdom, Germany, the Czech Republic, Poland, New Zealand, South Korea, Ukraine, Russia, Portugal, Australia, Norway, Italy, France, and Canada. Table 1 lists five of the email services and the BEC email sender account that we detected:

Country	Email service	BEC email address
United Kingdom	virginmedia.com	officelink <BLOCKED> [@]virginmedia.com
United States	optimum.net	ceo <BLOCKED> [@]optimum.net
Czech Republic	seznam.cz	officeport <BLOCKED> [@]seznam.cz
Germany	mail.com	officeonlyme <BLOCKED> [@]mail.com
South Korea	naver.com	mail_ceoofficial <BLOCKED> [@]naver.com

Table 1. Sample free email services and BEC email addresses used for campaigns

We observed BEC email actors also being interested in victim's contact information or data from companies such as aging reports. They also try to get information from their victims for other attacks that use social engineering.

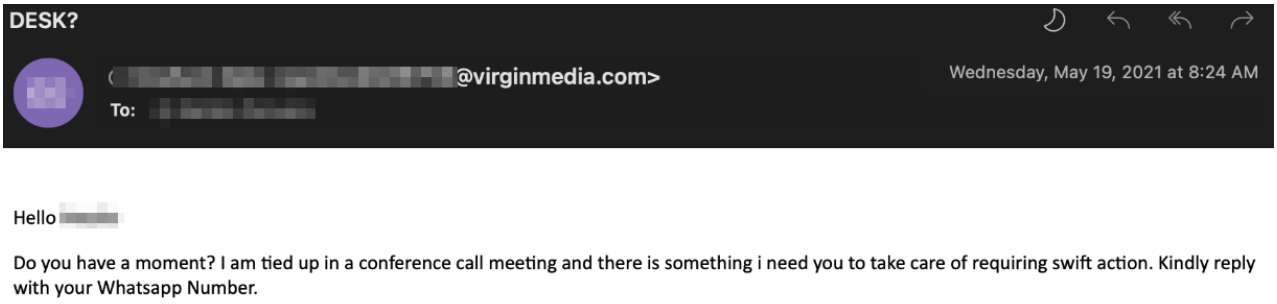


Figure 9. BEC email asking for a user's WhatsApp number

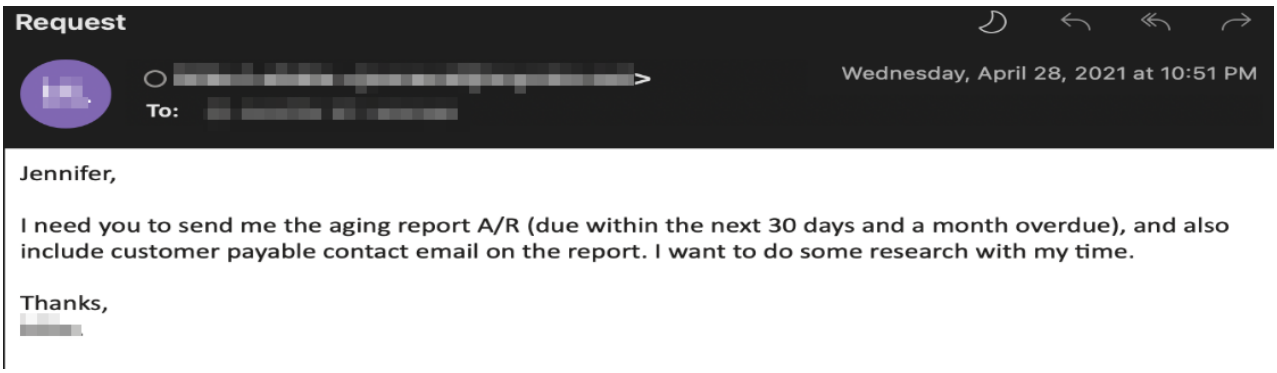


Figure 10. BEC email asking for copies of a report and contact information

3. Encrypted email services

Like other cybercriminals, BEC actors also want to hide their footprints and prevent systems from tracking them. Encrypted email services provide users with a higher level of privacy and confidentiality (that is, the inclusion of other security features compared to other email services). We observed BEC actors using some encrypted email services and list some examples below:

Encrypted email service	Sample BEC email address
Protonmail	officeiccon <BLOCKED> [@]protonmail.com
Tutanota	eye.adimn <BLOCKED> [@]tutanota.com
Criptext.com	iphone <BLOCKED> [@]criptext.com

Table 2. Sample encrypted email services used for BEC

These emails are not only found in the *From* email header, but at times also hidden in the *Reply-to* section. A common trick in email scams like BECs involves forging the From header into something legitimate-looking and hide the actors' actual email in a hidden Reply-to. When users directly reply just by clicking the in-mail Reply button, the Reply-to header will automatically be the recipient email address. This is unknown to the victim

and it allows the BEC actor to communicate with the victim thereafter. The example in Figure 11 shows how a BEC actor hides the actual email address ceoof<BLOCKED>[@]protonmail.com in the Reply-to section.

Figure 11. BEC email hiding their inbox at Reply-to headers

4. Self-registered domains and direct-to featured email service

Aside from using globally known email services, BEC actors also register domains themselves. This can bring two benefits when they conduct attacks:

1. They can create look-alike domains to deceive victims. The actors register domains with different characters but appear similar to a legitimate domain. Some commonly seen tricks include the interchange between specific letters and numbers:

- I (small letter L) – l (capital letter i) – 1 (for example, example.com vs. exampIe.com vs. examp1e.com)
- o – 0 (for example, trendmicro.com vs. trendmicr0.com)
- d – cl (for example, trendmicro.com vs. trenclmicro.com)
- m – rn (for example, example.com vs. exarnple.com)
- i – j (for example, trendmicro.com vs. trendmjcro.com)
- g – q
- u– v
- w– vv

Or the use of dashes (-) and periods (.) to separate a word or add a general postfix such as country codes (for example, example.com vs. example-tw.com). This trick is also widely used in other phishing schemes and other email-based scams, and will likely never get old.

2. Control positive email authentication results such as sender policy framework (SPF) or even DomainKeys Identified Mail (DKIM) while sending email to victims.

Figure 12. Abusing email authentication results

While a SPF or DKIM pass does not indicate that an email is threat-free, it does provide an image that the sender is somehow legitimate, gaining the recipient's trust or even fool some anti-scam solutions.

5. Stolen email credentials and email conversations

BEC actors also launch attacks from compromised email accounts. In most instances using this technique, the malicious actors deploy a spam campaign with malicious attachments dropping keyloggers or trojan stealers like Lokibot, Fareit, backdoor Remcos, and Negasteal (Agent Tesla). These can steal credentials in applications like browsers, simple mail transfer protocol (SMTP), file transfer protocol (FTP), VPNs, and from computer and system information. The operators then harvest the credentials and try to log in to the mailbox or webmail. If successful, they can manipulate the hacked accounts to perform BEC deployments.

From the compromised email account, BEC actors can also find email conversations related to finance- or purchase-themed threads such as purchase orders or invoices. Using these, they can create other spoofed email accounts, draft a reply with the stolen conversation, and start intercepting the conversation by replying to the recipients (usually suppliers). These are also called man-in-the-middle (MiTM) attacks. In this case, BEC operators carefully study the targeted victims, potentially compromising the companies' email services. They will also look for unsuspecting suppliers or other involved recipients in the original email thread.

Moreover, BEC operators use the username in the email resembling the victim's name or company name simultaneous to the email spoofing. In a few cases we observed, the malicious actors use customized usernames bearing the code "god" in their email, marking the account as a carbon copy.

- <BLOCKED>mygod@mail.com
- godpls<BLOCKED>@mail.com
- <BLOCKED>foods@post.com
- <BLOCKED>elco@dr.com
- <BLOCKED>pala@dr.com
- <BLOCKED>zado@dr.com
- nicola<BLOCKED>@dr.com
- <BLOCKED>com-int@dr.com
- ire<BLOCKED>@asia.com
- julien<BLOCKED>@mail.com

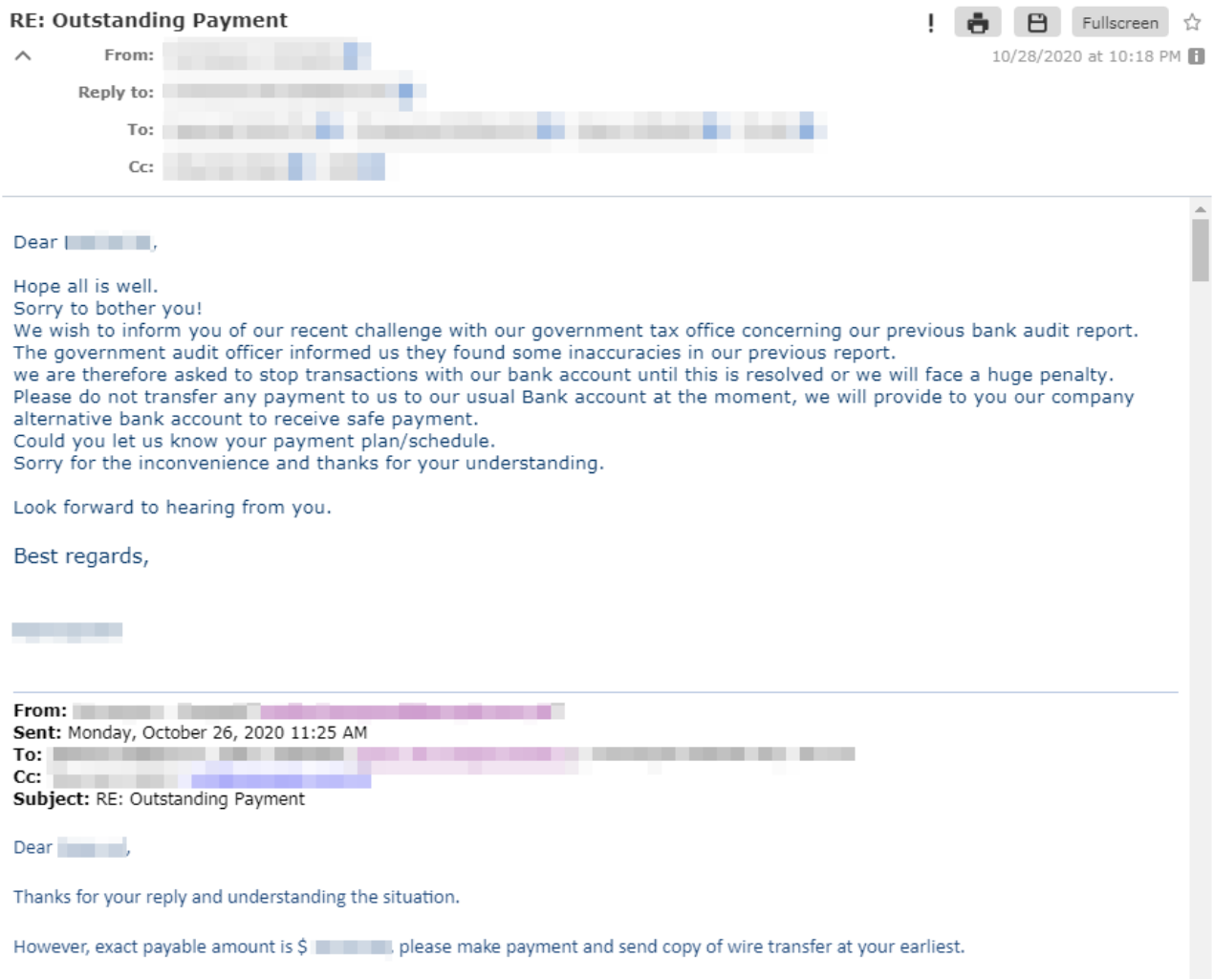


Figure 13. Sample BEC email with a stolen conversation used to deploy a BEC attack.

The BEC actors can rent virtual private servers (VPS) with SMTP and remote desktop protocol (RDP) services. They can use email marketing software like Gammadyne Mailer to craft spam mails and send it to thousands of email addresses. These email addresses are harvested via tools such as Email Extractor Lite, while some come from spam activities. The actors can then review the stealer logs and identify mail servers of interest, which can contain conversations about purchasing orders. They can then hijack the email conversation, create spoofed emails, and use the conversation to deploy a BEC attack. Another method employed involves the tampering of the invoice document to reflect the BEC actors' bank account details. Thus, if there is a request for a wire transfer the money will go directly into their account.

Keyword use and naming patterns

We also observed some keywords or naming patterns that BEC actors generally use. We identified some of them and provide examples for each.

1. Lengthy domain names with dashes (-)

A group of BEC domains operating from Africa was observed to favor lengthy names, using new generic top-level domain (TLD) words such as “[.]management”, “[.]work”, or “[.]one”. Some domains also contain “-“ and with common keywords such as “management”, “mail”, “office”, “reply”, and “secure”. We list examples that we observed here:

- admin-office-mail-server-ssl0.management
- reply-netsuite-mails.management
- system-mail-protection-outlook.management
- replys-mail-netsuite-com.management
- systerm-proctection-outlook.management
- mails-officesslappssecure-serversportal-execs.management
- reply-workplace-secure-protection-management-office.one
- servermail-reply-office-works-secure-protecty-inbound-netsuite.one
- office-xlsx-appspts-management-worksmailxls-cs.rest
- office-mails-appsslz-workmail-management.work

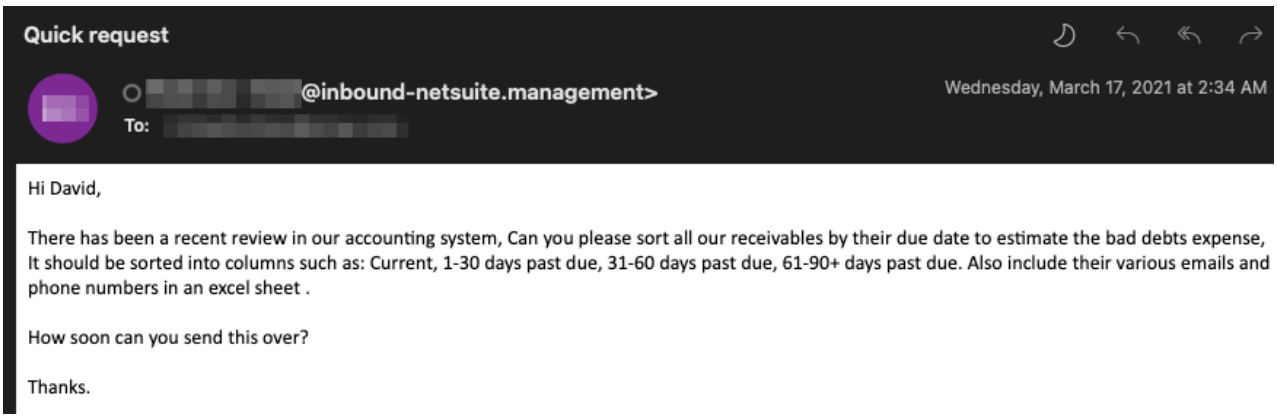


Figure 14. A BEC email using lengthy keywords and dashes

2. The use of telecom keywords

We also noticed BEC actors registering domain names with telecommunications industry-related keywords such as “5g”, “4g”, “mobile”, “network”, and “wireless”. They occasionally include names of service providers such as “Verizon” and “T-Mobile.” It’s also common to see dashes in domain names to increase the diversity of choices while registering:

- 5g-verizou.com
- network-sprint.biz
- sprint-mobile.net
- mobile-celldata.online.
- verizon-private-wireless.com
- reply-tmobile.com
- tmobilecellular.space
- 5g-tmobile.com
- t-mobile4g-us.com

- verizone4g-device.com

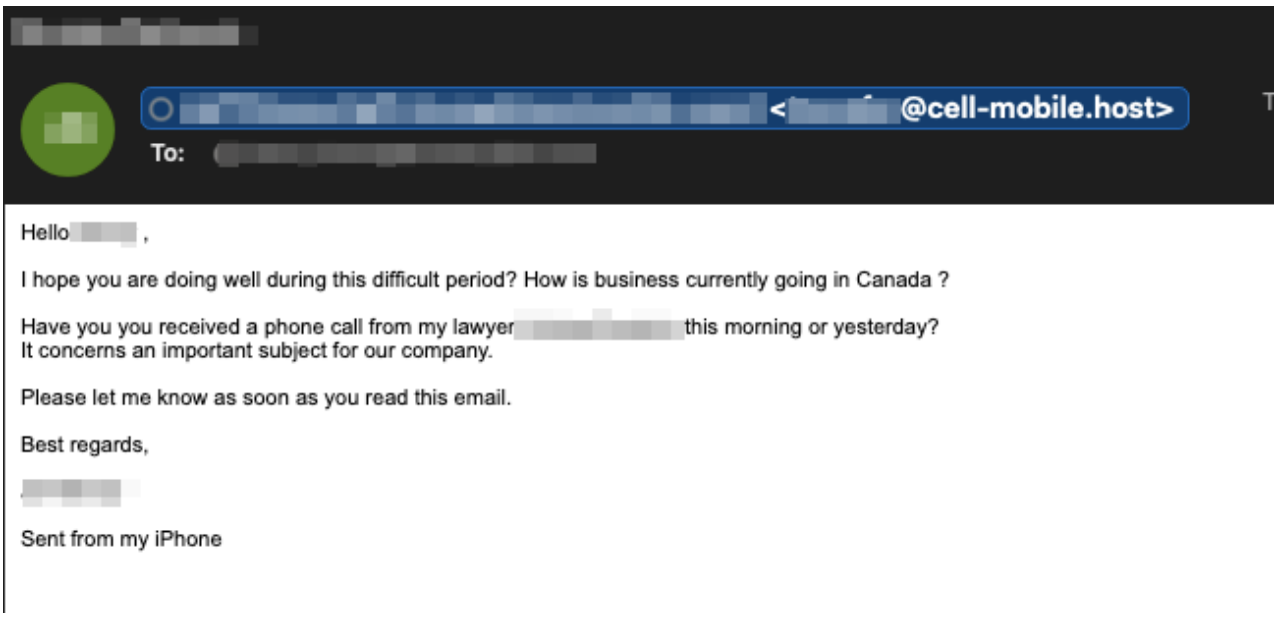


Figure 15. A BEC email using telecom-related domains

When we tracked "TELE-COMM" naming BEC domains' email infrastructure (observed from the domain name system mail exchanger or DNS MX records), we checked several commercial email services such as Google Workspace (aspmx.l.google.com) and Titan[.]email. These commercial email services provide advanced features like email tracking, scheduled sending, and follow-up reminders, and it is highly likely that BEC operators also optimize their operations' flow in leveraging these services.

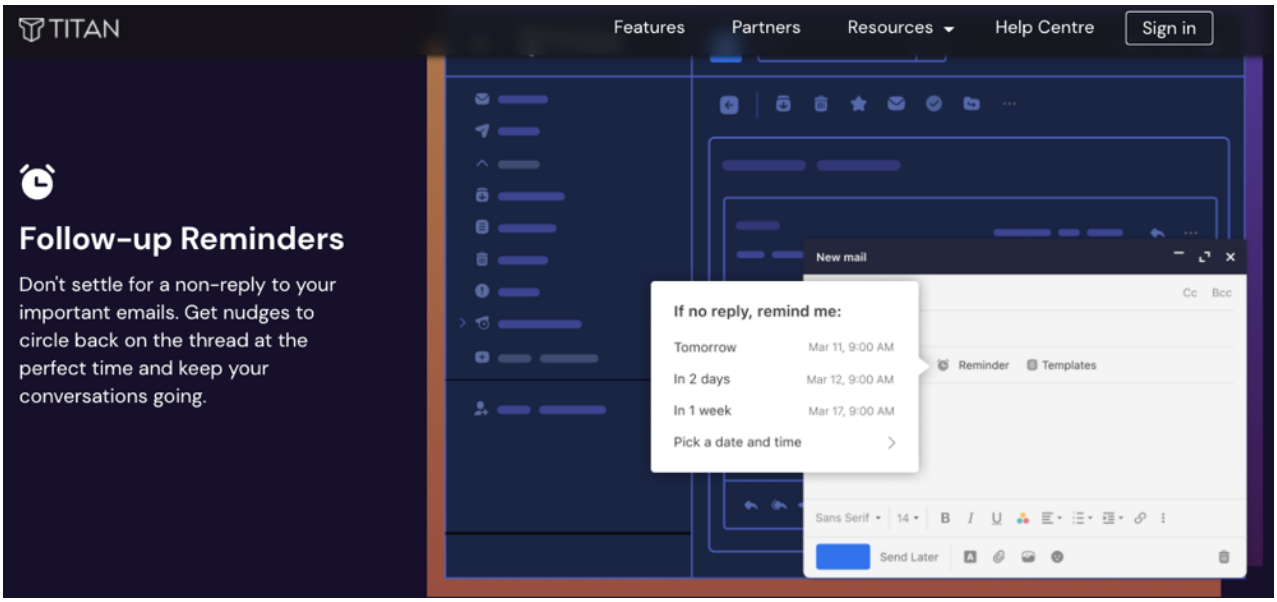


Figure 16. Email services like Titan provide advanced features for tracking the progress of emails sent

Below is an example of a BEC email initiating a conversation, wherein spaces are inserted in between words in the subject line. The word "INVOICE" is replaced with "I NVOICE" to evade anti-scam email solutions that rely on keywords or regular expressions. Similar tricks have been observed in sextortion and phishing email schemes.

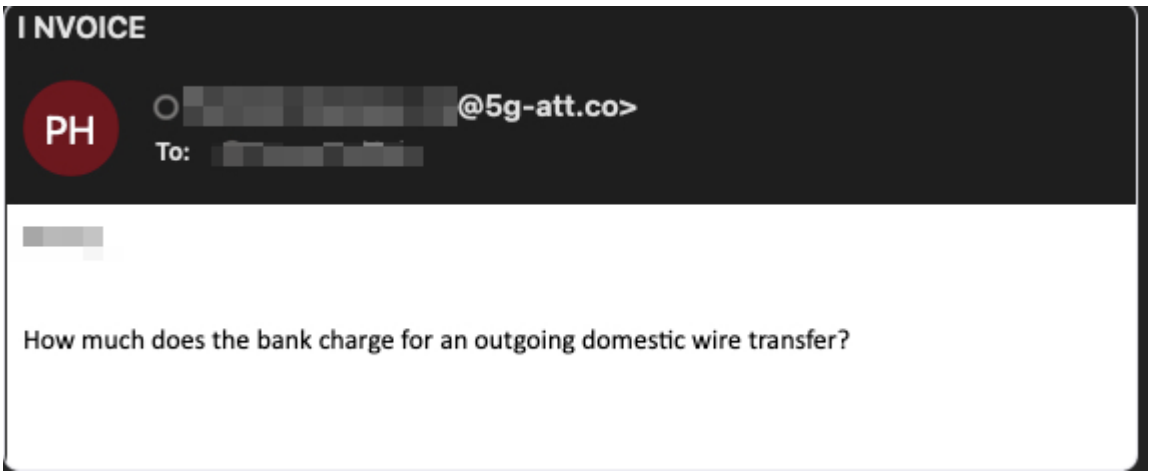


Figure 17. A BEC email sender using separate words or letters in the subject line. Screenshot sourced from VirusTotal

Conclusion

Unlike other cybercriminal schemes, phishing and BEC scams can be tricky to detect as they are targeted toward specific recipients. Attackers seek to compromise email accounts to gain access to financial and other sensitive information related to business operations, and BEC actors can easily use such access and information for other illicit activities. In the sample routines discussed here, the attackers' emails themselves do not include the typical malware payload of malicious attachments. As a result, traditional security solutions will not be able to protect accounts and systems from such attacks.

From our observations, BEC attacks don't only target high-profile users but also any employee that can be found on social media networks with significant personal information published (such as LinkedIn). These pieces of information can be used to spoof employees and partners, and cause significant financial damage to businesses.

As we observed professional email services being used for BEC attacks, we believe BEC actors will keep adopting new services and tools to optimize their operations flow as email services try to optimize services for their legitimate users. Targets in the Americas and Europe will continue to be targeted as sources of profit for these scams and will likely continue as companies see remote work becoming more mainstream, whether it be for their own operations or their managed service providers' (MSPs). Companies and employees will have to keep their guard up to mitigate the risks from BEC and other email-based scams:

- Educate and train employees. Deflect company intrusions through continuous InfoSec education. All company personnel — from the CEO to rank-and-file employees — must be aware of the various techniques and kinds of scams, and the procedure to follow when they encounter an attack attempt.

- Confirm requests using other channels. Avoid clicking on embedded links or directly replying to the email addresses used in the email. Exercise caution by following a verification system among employees who handle sensitive information, such as multiple personnel sign-off or additional verification protocols.
- **Scrutinize all emails.** Be wary of irregular emails with suspicious content such as unknown and dubious sender emails, domain names, writing styles, and urgent requests. Report suspicious emails to the respective security and InfoSec teams for analysis, tracking, and blocking.

Trend Micro solutions

Trend Micro protects both small- to medium-sized businesses and enterprises against phishing- and BEC-related emails. Using enhanced machine learning combined with expert rules, Trend Micro™ Email Security solution analyzes both the header and the content of an email to stop BEC and other email threats. For source verification and authentication, it uses Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting and Conformance (DMARC).

The Trend Micro™ Cloud App Security solution enhances the security of Microsoft Office 365 and other cloud services through sandbox malware analysis for BEC and other advanced threats. It uses Writing Style DNA, Display Name Spoofing, and High-Profile domain to detect BEC impersonations and computer vision to find credential-stealing phishing sites with Advanced Spam Protection enabled. It also protects cloud file sharing from threats and data loss by controlling sensitive data usage.

Indicators of Compromise (IOCs)

For the full list of IOCs, you may download the text file here.