French companies Under Attack from Clever BEC Scam

trendmicro.com/en_us/research/20/j/french-companies-under-attack-from-clever-bec-scam.html

October 6, 2020

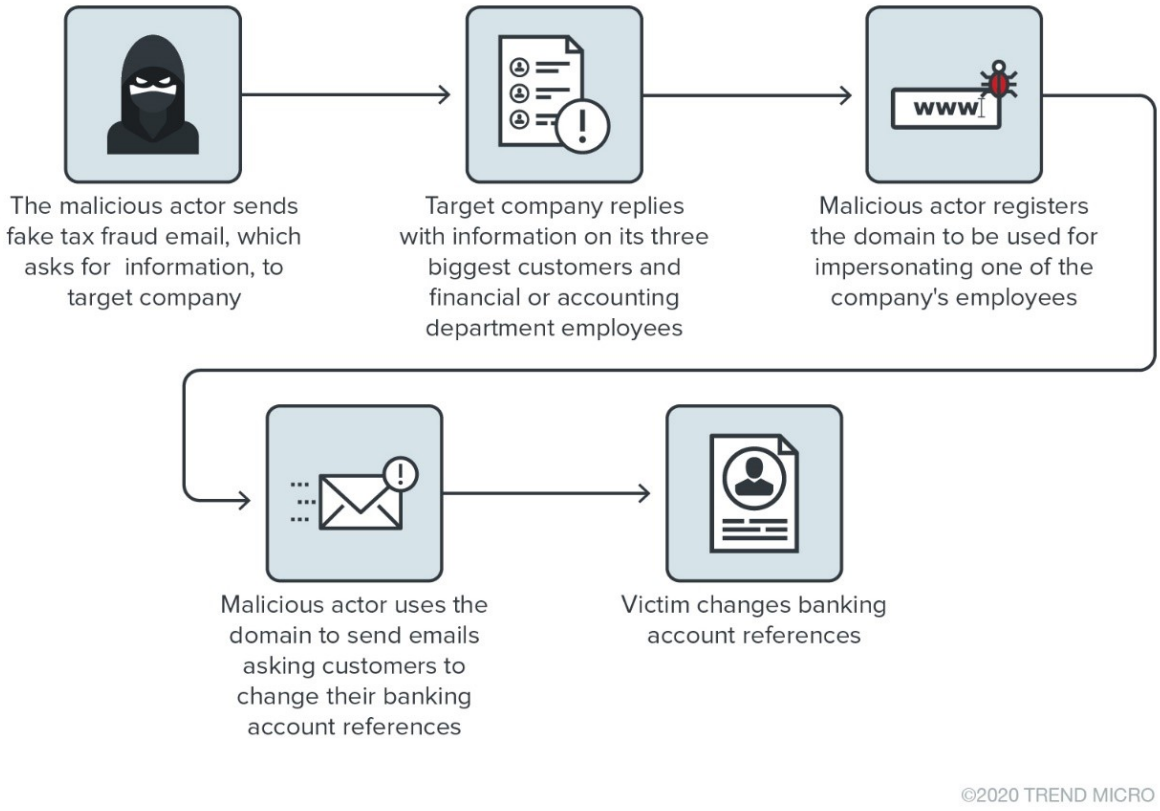

Figure 1. Diagram showing how the BEC scam is carried out

The highly anonymous and often secretive nature of the internet has led to the proliferation of scams aimed at separating people and organizations from their money. Trend Micro has been following these scams over the years and have seen many of them evolve from simplistic schemes to more sophisticated campaigns. One of the most dangerous scams today — one which cost organizations a combined US$1.7 billion in exposed losses in 2019 — is Business Email Compromise (BEC).

We have already tackled a large number of BEC-related topics. In this article, however, we would like to raise awareness about a new modus operandi involving a very clever BEC campaign that uses social engineering to target a huge number of French companies across different industries.

Background

While investigating various BEC attacks, we found an isolated incident where malicious actors impersonated a French company in the metal fabrication industry, which provides its services to a lot of different companies.

The malicious actors behind the scam registered a domain that is very similar to the legitimate one used by the business (with the fake one having a misspelled company name) and used it to send emails to their targets. The fraudulent domain was registered on July 27, 2020, and the perpetrators sent the fraudulent email on the same day.

The email, which was impersonating a real employee of the company, contained a request asking the targets to change the company's banking reference to a new account with an Italian bank.

De :
Envoyé : lundi 27 juillet 2020 16:50
À :
Objet : Nouvelles Coordonnées Bancaires
Importance : Haute

Avertissement de sécurité: Sachez que ce message vous a été envoyé par un expéditeur externe.

Security notice: Please be aware that this email was sent by an external sender.

Bonjour,

Suite à un changement de compte, veuillez trouver ci-joint nos nouvelles coordonnées bancaires (courrier et RIB) que nous vous demandons de bien vouloir mettre à jour dans vos dossiers à réception de ce courrier.

En vous remerciant pour votre bienveillante compréhension et de votre diligence, nous vous prions de bien vouloir accuser la réception de ce courriel et nous confirmer la prise en compte de notre demande (Très urgent !)

Dans cette attente,

Cordialement,

Service comptabilité

Figure 2. Screenshot of the email containing a request to change the target company's banking reference to a new account in an Italian bank. A rough translation of the email: "Following a banking account change, please find our new banking references (mail and Bank Identifier Code) attached, which we kindly ask you to update in your files. Thank you for your understanding. Please confirm the reception of this email and confirm the handling of our request (very urgent!)
The email contained two PDF file attachments. The first one was a letter to confirm the change, as seen in the screenshot below.

27 juillet 2020

Objet : **Nouvelles Coordonnées Bancaires**

Cher Client,

Nous vous informons que notre compte domicilié au CIC est actuellement soumis à un audit de routine régulier et qu'il restera inactif pendant trois (3) mois.

Durant cette période d'audit, tous les paiements (en attente et futurs) devront être effectués sur notre compte BANCO BPM dont vous trouverez ci-dessous les informations :

Nous vous prions de bien vouloir mettre à jour vos dossiers à réception de ce courrier.
Nous nous excusons pour tout inconvénient que ce changement pourrait causer et vous remercions par avance pour votre compréhension et coopération et vous prions d'agréer, Madame, Monsieur l'expression de nos salutations distinguées.

Service Comptabilité

Figure 3. Letter confirming the changes in the company's bank reference. The PDF file looks very professional and even contains the real footers and logos from the impersonated company.

Meanwhile, the second PDF file shows the banking account reference number:

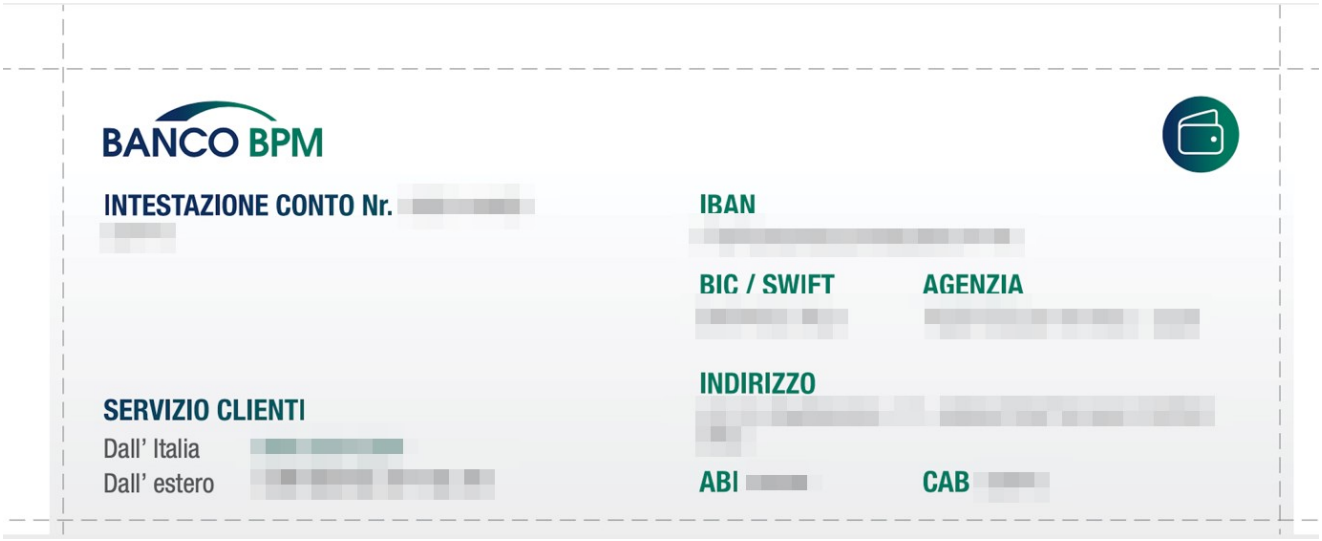

Figure 4. The PDF file showing the new banking reference account

Note that as soon as we noticed the scam, we reached out to the targeted company (who was incredibly responsive) and worked with them to prevent it from affecting their organization. In addition, they had filed a complaint and reached out to the Italian bank to stop the fraud attempt.

Initial investigation

We found references on the company website showing that the alleged sender of the fraudulent email is an actual employee of the target company. However, instead of working in the accounting department, as seen in the email, the person actually worked as a webmaster. It's possible that the fraudsters chose a random person based on the information they found prior to their scheme and decided to use it for their operation.

Interestingly enough, the fraudsters committed several mistakes:

- They forgot to change the target name in the header of the email content, therefore leaking the name of another target. A perceptive employee could potentially identify this as something unusual, which raises red flags.
- We found another version of the PDF file that revealed the account being used for the bank reference change had the name of an individual and was not registered under the name of the target company.

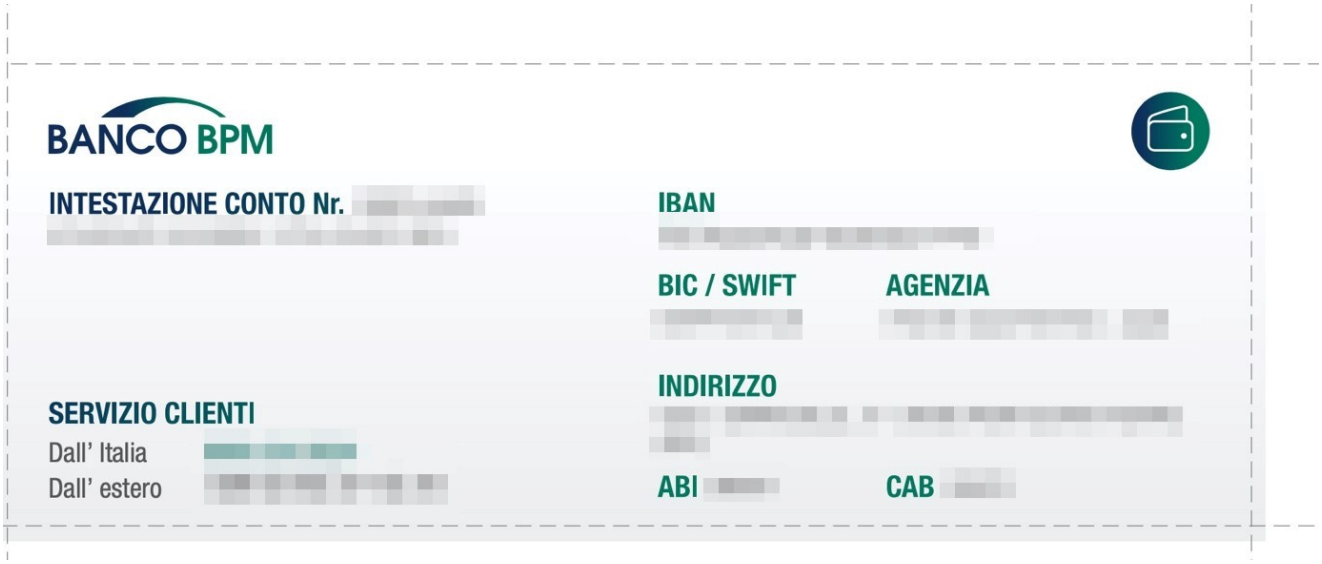

Figure 5. The PDF file showing the banking account reference. However, instead of showing the target company as the owner of the account, it shows the name of a person.
We investigated the name shown on the account but did not find any useful information other than the fact that this name is used mostly in the Ivory Coast in Africa.

Delving deeper into the scam

The email address used to register the fraudulent domain has been used to register several other domains since 2019, all of them showing similar names to legitimate French company domains, but again with slight errors here and there (for example using “techrnologies” instead of “technologies).

Domain	Creation Date
eltn[.]fr	8/23/2019
chnonopost[.]fr	9/30/2019
sfrbiz[.]fr	11/24/2019
ouflook[.]fr	12/9/2019
carre-haussrmann[.]fr	12/10/2019
4a-archifectes[.]fr	1/16/2020
harribeyconstuctions[.]fr	2/5/2020

stanvwell[.]r	5/28/2020
paretsarl[.]fr	6/17/2020
tkl-consutling[.]fr	6/29/2020
axa-etancheite[.]fr	7/1/2020
garantiesdesdepots[.]fr	7/6/2020
jacormex[.]fr	7/14/2020
harribeyconsstructions[.]fr	7/15/2020
transportcazaux[.]fr	7/17/2020
atg-techrnologies[.]fr	7/22/2020
cephii.eu	7/27/2020
efiiltec[.]fr	7/27/2020
benne-rci[.]fr	7/28/2020
soterm[.]fr	7/29/2020
phamasys[.]fr	7/31/2020
huuaume.fr	08/05/2020
larm-inox[.]fr	8/13/2020

Table 1. Domains registered using the email address

The email address used did not seem to have been compromised and was probably created by the malicious actors themselves.Table 1. Domains registered using the email address

This list also reveals that the attackers are targeting a wide swath of industries, probably in an opportunistic manner. While we could not confirm that all of these domains have been used to commit BEC fraud, we did find at least one additional case in which the fraudsters targeted an organization that was part of the healthcare industry.

Impersonating the French tax system

In many BEC schemes, the perpetrators infect the machines of their targets with malware that will allow them to read — and therefore gather information — from emails. Once the cybercriminals gain access to the mailboxes of their targets, they search for material on the people involved with the organization's finance and accounting departments. In addition, the attackers also look for information on the company's customers and partners. Using this method, BEC scammers can then impersonate an employee to entice a victim to carry out their goals via social engineering.

This is BEC as we usually know it. We found evidence that the cybercriminals involved in this case had used malware as well, but ultimately, they did not really even need it. Instead, they used an alternative — and admittedly clever — method of hunting for their target's financial data themselves.

With the help of the organization that the scam targeted, we were able to determine the initial approach the cybercriminals used: they presented their emails to appear as if it was from the French tax system to gather information on their target. A little over two weeks before the registration of the fake domain, the attackers sent the following email to the company:

De : ODAC <ODAC@dgfip.finances.gouv.fr>
Envoyé : mercredi 8 juillet 2020 08:45
À :
Objet : IMPORTANT : Enquête SEPA

Bonjour,

Le bureau 2FCE-1D - Contrôle de la qualité des comptes de la Direction générale des Finances publiques engage sa campagne 2020 pour la vérification du respect des conditions SEPA (Single Euro Payments Area) / et normes internationales.

A cette fin, je vous adresse le courrier ci-joint et vous invite à nous transmettre les documents et informations demandés sous forme dématérialisée à l'adresse suivante : odac@dgfip-finances-gouv.cloud .

Dans l'hypothèse où la taille de votre envoi dépasserait 50Mo, je vous invite à nous contacter par téléphone afin que nous vous communiquions les modalités d'accès à notre plateforme d'échanges sécurisés FTP.

Merci par avance.

Cordialement

Direction Générale des Finances Publiques
Bureau 2FCE-1D – Contrôle de la qualité des comptes
Secteur des Organismes divers d'administration centrale

Adresse mail : ODAC@dgfip-finances-gouv.cloud

Coronavirus : il existe des gestes simples pour vous protéger et protéger votre entourage

Se laver les mains très régulièrement | Tousser ou éternuer dans son coude ou dans un mouchoir | Utiliser des mouchoirs à usage unique | Saluer sans se serrer la main, éviter les embrassades

Figure 6. The initial email sent by the malicious actors, allegedly from the General Directorate of Public Finances (DGFiP) of France, concerning tax inquiries

The email contained an attached PDF file that seemed to be a letter from the French Tax service:

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES
SERVICE DE LA FONCTION FINANCIERE ET COMPTABLE DE L'ETAT

Paris, le 8 juillet 2020

Le Directeur Général des Finances Publiques

à

Référence : DGFIP BUREAU 2FCE-1D 2020/07/3964

Objet : Enquête SEPA (Single Europ Payments Area)

Comme chaque année, dans le respect du pacte de stabilité et de croissance avec la Commission européenne, la Direction générale des Finances publiques engage une enquête dans le cadre de la vérification du respect des conditions SEPA (Single Euro Payments Area) et / normes internationales.

A ce titre, conformément aux dispositions des articles L.81, L.85 et l'article L.102 B du livre des procédures fiscales, je souhaiterais disposer dès que possible et au plus tard pour le 20 juillet 2020, sous forme dématérialisée, pour **chacun** de **vos trois (3) principaux Clients** qui règlent leurs prestations par virement SEPA (Single Euro Payments Area) concernant la période du **01/04/2020 au 31/07/2020** de : La **balance âgée à ce jour**, **duplicatas des factures correspondantes** (**N'ayant pas été réglées** par le client et concernant **les échéances Juin, Juillet et Août**), **contacts du service financier ou comptable (**Emails, Téléphones et Adresse postale**)** et d'**un (1) contrat commercial** dûment **signé** et **cacheté**.

Je vous précise que cette opération ne constitue pas une vérification de votre situation fiscale et vous indique que tout refus de coopération est sanctionné par une amende fiscale prévue à l'article 1734 du code général des impôts.

Je vous invite à nous transmettre ces documents **sous forme dématérialisée** sur notre messagerie sécurisée et fonctionnelle : odac@dgfip-finances-gouv.cloud

En vous remerciant de votre collaboration, je vous prie de croire à l'assurancede mes sentiments distingués.

L'administrateur

Chef du Bureau 2FCE-1D

Signé

MINISTÈRE DE L'ACTION ET DES COMPTES PUBLICS

Figure 7. The content of the PDF attachment sent with the email

Figure 7. The content of the PDF attachment sent with the email

Essentially, the PDF file contains a request from the spoofed government organization asking the target company for information on their customers, employees, and other financial data. The text also adds to the urgency of the request by mentioning possible fines if the target organization refuses to cooperate.

The translation of the text found in the PDF file is as follows:

As happens every year, in accordance with the Stability and Growth Pact with the European Commission, the Directorate General of Public Finances is launching an investigation as part of the verification of compliance with SEPA (Single Euro Payments Area) conditions and international standards.

As such, in accordance with the provisions of articles L.81, L.85 and article L.102 B of the book of tax procedures, ***I would like to have, as soon as possible and no later than July 20, 2020, in dematerialized form, for each of your three (3) main Customers who pay their services by SEPA (Single Euro Payments Area) transfer for the period from 04/01/2020 to 07/31/2020 of: The aging balance to date, duplicate invoice correspondents (Not having been paid by the customer and concerning the June, July and August deadlines), contacts of the financial or accounting department (Emails, Telephones and Postal address) and one (1) duly signed and sealed commercial contract.***

I would point out that this operation does not constitute a verification of your tax situation and indicates to you that any refusal to cooperate is sanctioned by a tax fine provided for in article 1734 of the general tax code.

I invite you to send us these documents in dematerialized form on our secure and functional messaging: odac@dgfip-finances-gouv[.]cloud

While thanking you for your cooperation, please believe in the assurance of my distinguished feelings.

The PDF letter looks (and reads) like a real document from the French tax service. In fact, most French people would probably think this is a legitimate letter unless they look closely at the email address used (dgfip-finances-gouv[.]cloud instead of the real domain, which is dgfip.finances.gouv.fr).

As we highlighted in bold, the social engineering trick used in this email is for gathering data that could potentially be useful for the malicious actors, such as client information and commercial contracts. Once this information is in the hands of the scammers, they can then move on to the next stage of the attack, which involves reaching out to the three contacts mentioned in the PDF file.

One interesting side note: it seems the BEC scammers actually built their PDF file from a real PDF file used by the French tax system. The real name of the author of the document (as seen in the metadata) is indeed the name of a real government employee working in the department responsible for handling tax-related issues.

The use of tax-related scams is something we've seen before. This incident confirms that the information stolen using tax fraud is being used for malicious purposes, in this case, a BEC scam.

Expanding the target range

We searched our systems for similar emails and found at least 73 different French companies targeted by these cybercriminals.

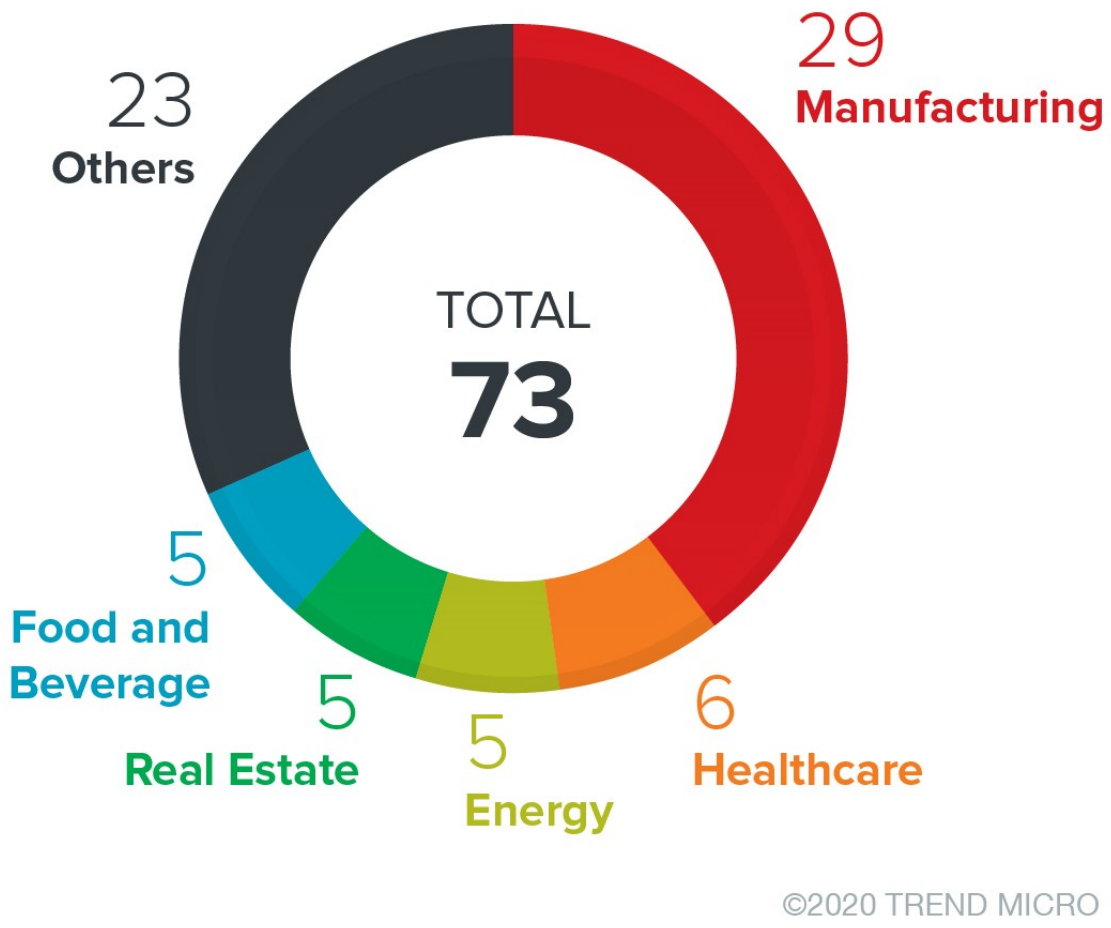

Figure 8. The industry distribution of the companies targeted in this particular BEC scam. Organizations in the manufacturing sector were by far the most targeted

The most targeted industry in this BEC campaign is manufacturing, particularly manufacturing companies that build high tech products and materials. This was followed by the healthcare, real estate, energy, and food and beverage industries. Many of the targeted companies work with many different service providers and partners, making requests for changes in banking references look less suspicious. It's highly likely that the fraud is more widespread than we have data on.

In addition to reaching out and working with the first organization we investigated, we also notified the other targets, all of whom have been very reactive to the threat. We also helped close the fraudulent domains.

Defending your organization from BEC attacks

Businesses are advised to educate employees on how BEC scams and other similar attacks work. These schemes do not require advanced technical skills: all that's needed to launch an effective BEC scam is a single compromised account and services that are widely available in the cybercriminal underground.

As such, here are some tips on how to stay safe from these online schemes:

- Carefully scrutinize all emails. Be wary of irregular emails sent by high-level executives, especially those that have an unusual sense of urgency, as they can be used to trick employees into furthering the scam. Always review emails requesting for funds to determine if the requests are out of the ordinary.
- Raise employee awareness. While employees are a company's biggest asset, they can also be its weakest link when it comes to security. Commit to training employees, reviewing company policies, and developing good security habits.
- Verify any changes in vendor payment location by using a secondary sign-off by company personnel.
- Stay updated on customer habits, including the details and reasons behind payments.
- Always verify requests. Confirm requests for fund transfers using phone verification as a part of two-factor authentication (2FA), use known familiar numbers and not the details provided in the email requests.
- Report any incident immediately to law enforcement or file a complaint with the Internet Crime Complaint Center (IC3).

Trend Micro Solutions

Email

The email security capabilities of the Trend Micro User Protection and Network Defense solutions can block email messages used in Business Email Compromise attacks.

Malware

Endpoint security capabilities in Trend Micro User Protection and Network Defense solutions can detect advanced malware and other threats used in BEC schemes.

Indicators of Compromise (IoCs)

Domains

- dgfip-finances-gouv[.]cloud
- bellingstudio@gmail.com