proofpoint.

EBOOK

Anatomie des attaques BEC

Cadre d'identification, de classification et de neutralisation des fraudes par email du RSSI moderne

Présentation du cadre de taxonomie des fraudes par email de Proofpoint

Le piratage de la messagerie en entreprise (BEC, Business Email Compromise), également appelé fraude par email, représente l'une des menaces les plus coûteuses et les moins bien comprises du domaine de la cybersécurité. Cette catégorie de fraude par email en plein essor ne bénéficie pas toujours d'autant d'attention que d'autres types d'attaques cybercriminelles très médiatisés. Cependant, en termes de coût financier direct, elle éclipse facilement ces autres types.

Pour la seule année 2020, les attaques BEC ont coûté plus d'1,8 milliard de dollars aux entreprises et aux particuliers[1]. Cela représente une augmentation de plus de 100 millions de dollars par rapport à 2019, et 44 % des pertes totales liées à la cybercriminalité.

Les attaques BEC n'ont cessé d'évoluer au fil des ans et la nomenclature du secteur a fait son temps. Les termes utilisés pour expliquer les tactiques et techniques de piratage de la messagerie en entreprise sont devenus ambigus, ils ont été amalgamés avec d'autres concepts et sont souvent mal utilisés. En l'absence de cadre permettant de décrire les attaques BEC, et a fortiori de les conceptualiser, il est difficile, voire impossible, d'investiguer et de gérer ces menaces.

C'est pourquoi nous avons créé le cadre de taxonomie des fraudes par email de Proofpoint, dans le but d'aider les professionnels de la sécurité à mieux identifier, classer et bloquer cette menace onéreuse.

Importance de la terminologie

L'expression « attaque BEC », ou piratage de la messagerie en entreprise, est souvent utilisée à l'emporte-pièce pour décrire une sous-classification entière de menaces par email. Elle est employée de façon générique pour évoquer toute une série de tactiques et techniques liées à des fraudes par email motivées par l'appât du gain et qui ont recours à l'**ingénierie sociale** pour susciter une réponse de la part des cibles.

Voilà qui est un peu vague, preuve s'il en est que le terme « attaque BEC » est devenu beaucoup trop inclusif. La menace a dépassé les mots utilisés pour la décrire, ce qui complique les efforts des chercheurs pour étudier les attaques BEC et les tentatives des entreprises pour les gérer.

1 FBI, « Internet Crime Report 2020 » (Rapport 2020 sur la cybercriminalité), mars 2021.

Une nouvelle façon d'appréhender les attaques BEC et la fraude par email

Pour simplifier les choses et mettre en lumière les principaux aspects des attaques BEC (et, plus généralement, des fraudes par email), nous avons créé ce cadre de taxonomie. Notre objectif : aider les entreprises à mieux identifier, comprendre et gérer les nombreuses formes de fraude par email auxquelles elles sont susceptibles d'être confrontées.

Identité

Nous adoptons une approche centrée sur les personnes de la fraude par email. C'est la raison pour laquelle notre carte taxonomique commence par le niveau *Identité*. À ce niveau, l'identité fait référence à la personne ou à l'entité pour laquelle l'auteur de l'attaque (c'est-à-dire le cybercriminel) se fait passer. Nous divisons l'identité en « collaborateur », « fournisseur » et « inconnue ». Mais vous pouvez la préciser davantage encore, par exemple en subdivisant le terme « collaborateur » en « dirigeants » et « collaborateurs généraux ».

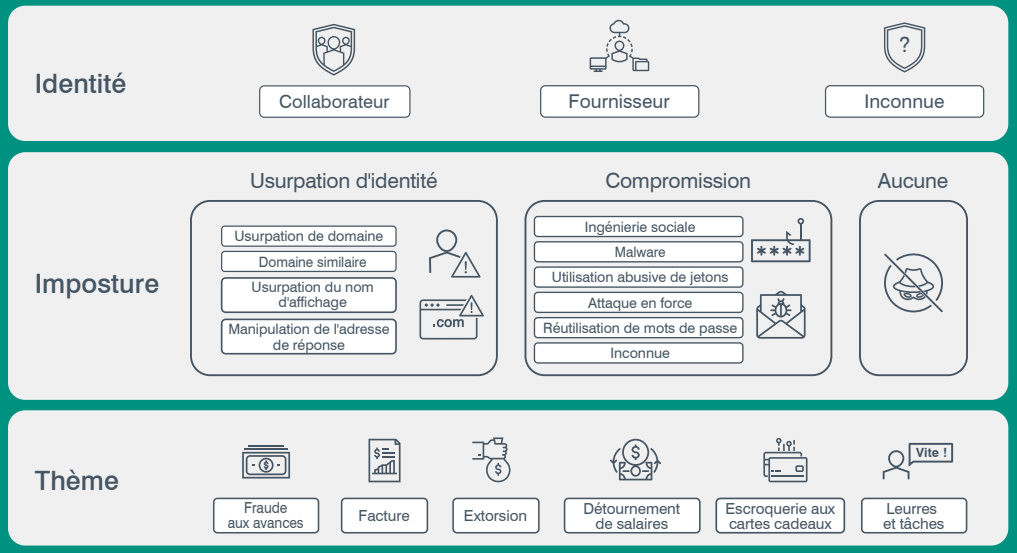


Figure 1. Taxonomie des fraudes par email de Proofpoint

Imposture

Le niveau suivant est le niveau *Imposture*, qui couvre les techniques utilisées par les auteurs de fraude par email. Ce niveau comprend trois catégories : « Usurpation d'identité », « Compromission » et « Aucune ».

L'« usurpation d'identité » fait référence aux techniques par lesquelles le cybercriminel modifie un ou plusieurs en-têtes de message afin de masquer l'origine du message. Il peut par exemple usurper des en-têtes, utiliser des domaines similaires ou avoir recours à d'autres techniques pour se faire passer pour quelqu'un d'autre.

La catégorie « Compromission » désigne les techniques utilisées par le cybercriminel pour accéder à une boîte email légitime afin d'entrer en contact avec sa cible. Le compte peut appartenir à un fournisseur de confiance, un collègue de travail ou une personne incarnant l'autorité. Le destinataire n'a aucune raison de mettre en doute la légitimité de l'email et ne dispose pas des indices habituels pour repérer l'attaque.

Lorsque la technique d'imposture est « Aucune », le cybercriminel utilise une tactique BEC qui ne repose pas sur l'usurpation d'identité. Il peut par exemple envoyer des emails à partir de comptes de messagerie gratuits, sans falsification de l'origine.

Thème

Le dernier niveau, *Thème*, contient les informations les plus pertinentes et les plus exploitables. Il s'agit de loin du niveau le plus important de cette taxonomie. Il contient les thèmes suivants :

- Fraude aux factures
- Détournement de salaires
- Extorsion
- Leurres et tâches
- Escroqueries aux cartes cadeaux
- Fraude aux avances

Ces thèmes couvrent les catégories que nous avons jugées les plus pertinentes pour le paysage des menaces BEC et les plus utiles au plus grand nombre d'entreprises. Bien qu'ils soient suffisamment larges pour tenir compte des nuances (chaque attaque étant unique), les thèmes sont également suffisamment spécifiques pour vous permettre d'identifier, de classer et de gérer rapidement l'éventail complet des menaces BEC.

Thème 1 – Fraude aux factures

La fraude aux factures consiste fondamentalement à tenter de tromper quelqu'un pour l'amener à payer des produits ou services qu'il n'a pas achetés ou à rediriger un paiement légitime vers le compte du cybercriminel. Parmi les thèmes de fraude par email de notre taxonomie, la fraude aux factures est sans doute celle qui s'avère la plus coûteuse. Les transactions interentreprises tendent à être nombreuses et à porter sur des montants élevés, ce qui donne aux fraudeurs l'occasion et l'envie d'en profiter.

L'objet des emails contenant des factures frauduleuses est généralement axé sur le paiement. Les fausses factures semblent souvent authentiques, notamment grâce à des logos d'entreprise, à un formatage professionnel, etc. L'email peut également détailler des frais spécifiques et contenir des formulations suscitant un sentiment d'urgence, telles que : « Cette facture est échue depuis plus de 90 jours et doit être payée immédiatement. » Souvent, le cybercriminel utilise un langage menaçant si le destinataire n'agit pas rapidement.

Au niveau *Identité*, une facture frauduleuse donne l'impression d'avoir été envoyée par un collègue ou une personne extérieure à l'entreprise, par exemple. Mais les attaques les plus performantes exploitent les relations existantes avec les fournisseurs. Exemples de fraude aux factures par excellence, les fraudes aux fournisseurs peuvent coûter de plusieurs milliers à plusieurs millions de dollars.

Fonctionnement

Au niveau *Imposture*, la fraude aux factures fournisseurs peut faire appel aussi bien à l'usurpation d'identité qu'à la compromission.

Usurpation d'identité

Dans le cadre de l'usurpation de l'identité d'un fournisseur, le cybercriminel utilise des techniques courantes d'usurpation de comptes de messagerie pour se faire passer pour le fournisseur. Souvent, ces emails frauduleux sont envoyés à partir de domaines de webmail gratuits ou de comptes compromis sans lien avec le fournisseur qui sont contrôlés par le cybercriminel.

Comme le montre la figure 2, l'usurpation d'identité n'est pas toujours simple et directe. Dans certains cas, un cybercriminel peut d'abord se faire passer pour l'entreprise ciblée afin d'obtenir une vraie facture du fournisseur, puis utiliser celle-ci pour se faire passer pour le fournisseur. (Comme elle implique une vraie facture d'un fournisseur réel, cette attaque à double sens peut, de prime abord, être assimilée à une compromission de compte.)

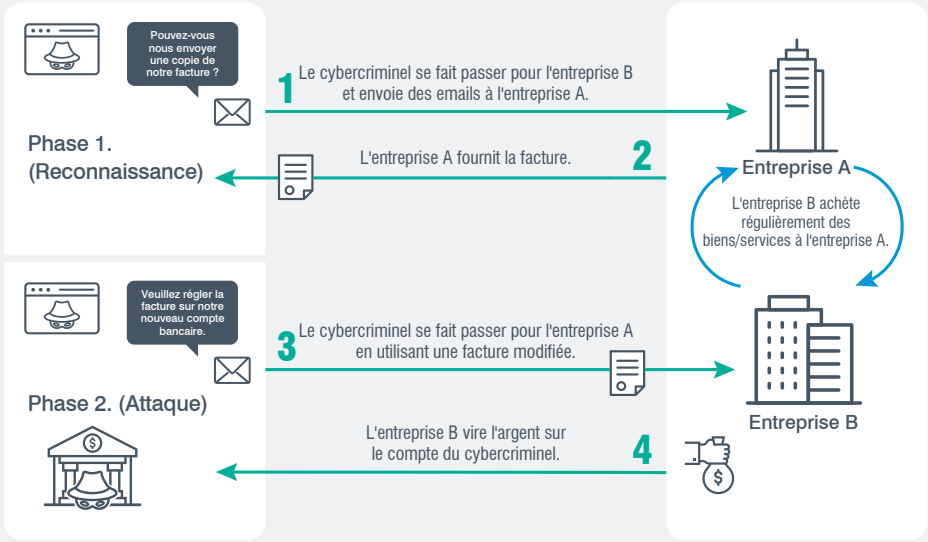


Figure 2. Anatomie d'une fraude aux factures fournisseurs dans le cadre de laquelle le cybercriminel utilise plusieurs niveaux d'usurpation d'identité

Compromission

Dans le cadre d'une compromission de fournisseur, le cybercriminel obtient un accès non autorisé au compte de messagerie d'un fournisseur de confiance, puis utilise ce compte pour mener des attaques BEC contre les clients du fournisseur. Le cybercriminel obtient généralement l'accès au compte par le biais d'une campagne de phishing antérieure ou l'achat d'identifiants de connexion.

Dans certains cas, le cybercriminel peut même détourner un fil de discussion existant d'un compte compromis (une technique connue sous le nom de « piratage de fils de discussion »). En observant, en imitant et en répondant à des conversations réelles au sein du fil de discussion, il peut rédiger des messages crédibles et créer des documents à l'appui.

C'est la tactique d'usurpation d'identité la plus efficace. Les emails de piratage de la messagerie en entreprise s'immiscent dans une conversation active. Le destinataire n'a aucune raison de soupçonner que la personne avec laquelle il communiquait a soudainement été remplacée par un imposteur. Il n'est dès lors pas étonnant que ces emails fassent partie des attaques BEC les plus convaincantes auxquelles la plupart des utilisateurs seront confrontés.

Pourquoi pas les deux ?

Souvent, les cybercriminels utilisent à la fois l'usurpation d'identité et la compromission comme tactiques d'imposture. Certaines de ces attaques sont ciblées. Mais un grand nombre d'entre elles sont opportunistes et découlent d'informations que les cybercriminels obtiennent lors de la compromission de chaînes logistiques. (Notre taxonomie tient compte de cette nuance en classant ces attaques à la fois comme compromission et comme usurpation d'identité dans le niveau *Imposture*, comme illustré à la figure 3)

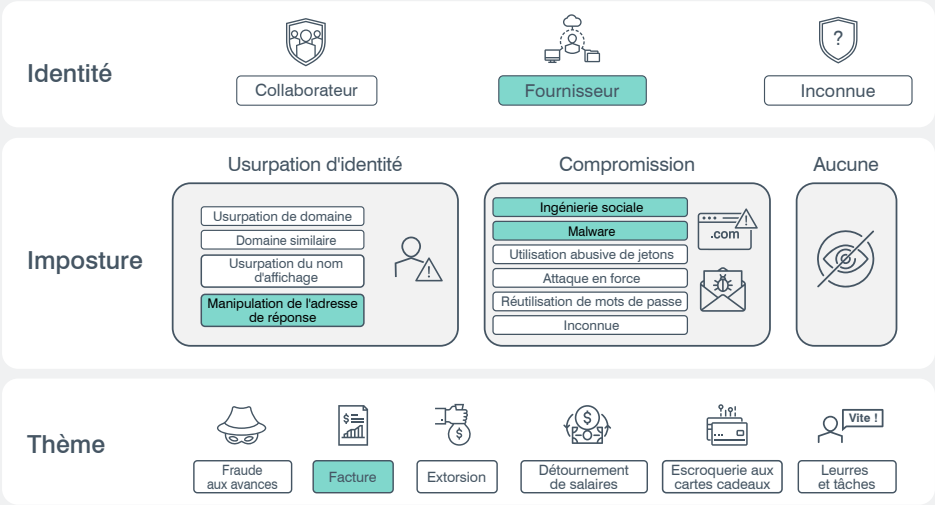


Figure 3. Exemple de fraude aux factures fournisseurs faisant appel à la fois à des tactiques d'usurpation d'identité et de compromission

Exemple concret

Lors d'une fraude aux factures fournisseurs que nous avons récemment observée, un cybercriminel a tenté de dérober plus de 100 000 dollars à une entreprise en se faisant passer pour son fournisseur de vin habituel.

Il a répondu à un fil de discussion existant entre le client et le fournisseur, demandant au client d'envoyer le paiement directement sur un compte bancaire spécifique. (Comme le montre la figure 4, le message indiquait également que toutes les communications devaient se faire par email.) Bien que le cybercriminel ait détourné un fil de discussion réel et semble avoir eu une connaissance approfondie du fournisseur, l'attaque utilisait des adresses email usurpées plutôt qu'un compte de messagerie compromis.

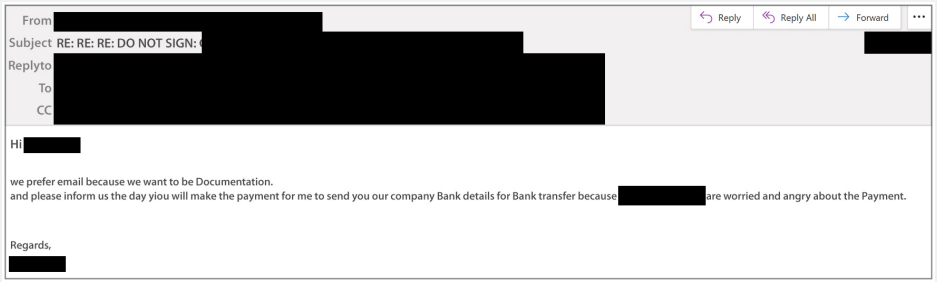


Figure 4. Tentative initiale de fraude aux factures

N'ayant pas obtenu la réponse souhaitée, le cybercriminel a relancé le client avec un email plus pressant, comme illustré à la figure 5. L'email comprenait une facture détaillée sur laquelle figuraient le logo et le cachet du véritable fournisseur pour la rendre convaincante (voir la figure 6 à la page suivante).

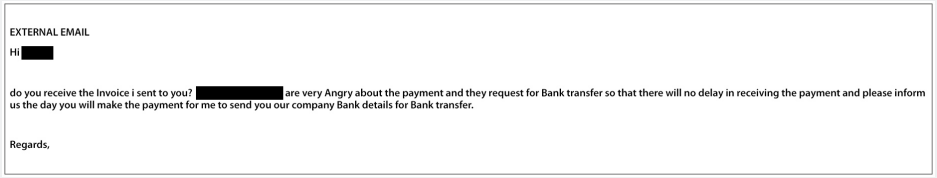
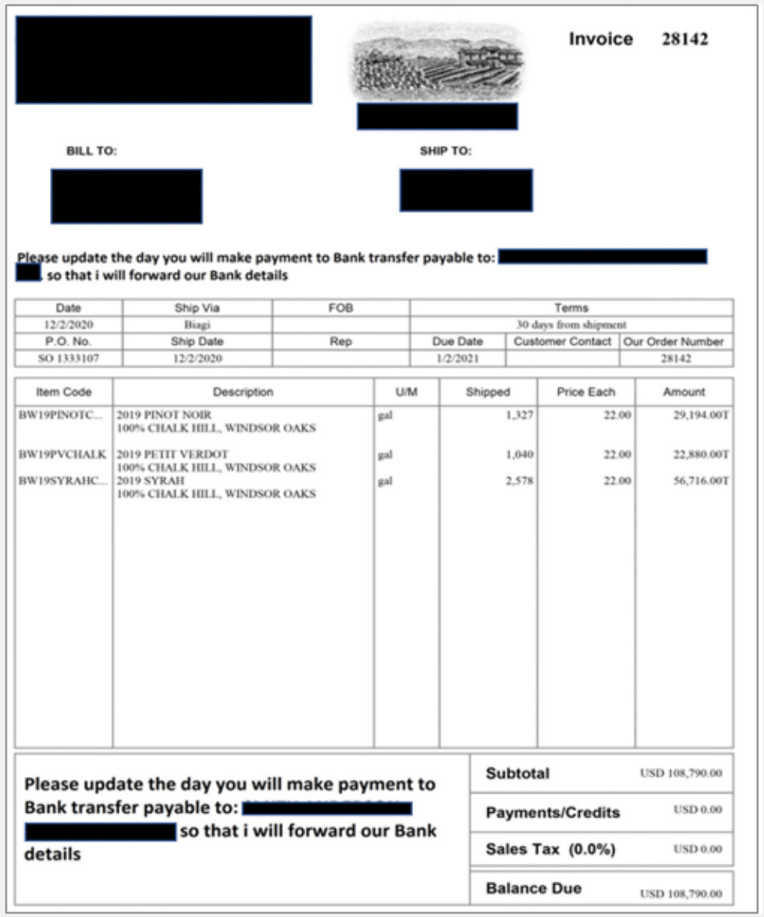


Figure 5. Tentative de relance par le même cybercriminel



[redacted]

Invoice 28142

[redacted]

BILL TO:

[redacted]

SHIP TO:

[redacted]

Please update the day you will make payment to Bank transfer payable to: [redacted]
[redacted] so that i will forward our Bank details

Date	Ship Via	FOB	Terms		
12/2/2020	Biagi		30 days from shipment		
P.O. No.	Ship Date	Rep	Due Date	Customer Contact	Our Order Number
SO 1333107	12/2/2020		1/2/2021		28142

Item Code	Description	U/M	Shipped	Price Each	Amount
BW19PINOTC...	2019 PINOT NOIR 100% CHALK HILL, WINDSOR OAKS	gal	1,327	22.00	29,194.00T
BW19PVCHALK	2019 PETIT VERDOT 100% CHALK HILL, WINDSOR OAKS	gal	1,040	22.00	22,880.00T
BW19SYRAHC...	2019 SYRAH 100% CHALK HILL, WINDSOR OAKS	gal	2,578	22.00	56,716.00T

Please update the day you will make payment to Bank transfer payable to: [redacted] so that i will forward our Bank details

Subtotal	USD 108,790.00
Payments/Credits	USD 0.00
Sales Tax (0.0%)	USD 0.00
Balance Due	USD 108,790.00

Figure 6. Facture au format PDF

Comme les emails contenaient des informations que seul le véritable fournisseur de vin pouvait connaître, nous pensons que le fournisseur avait été compromis avant la tentative d'attaque BEC. Le cybercriminel a probablement utilisé des détails glanés lors de cette compromission ainsi que des tactiques d'usurpation du nom d'affichage et de manipulation du champ d'adresse de réponse pour se faire passer pour le fournisseur. (La figure 7 illustre la façon dont nous avons cartographié cette attaque.)

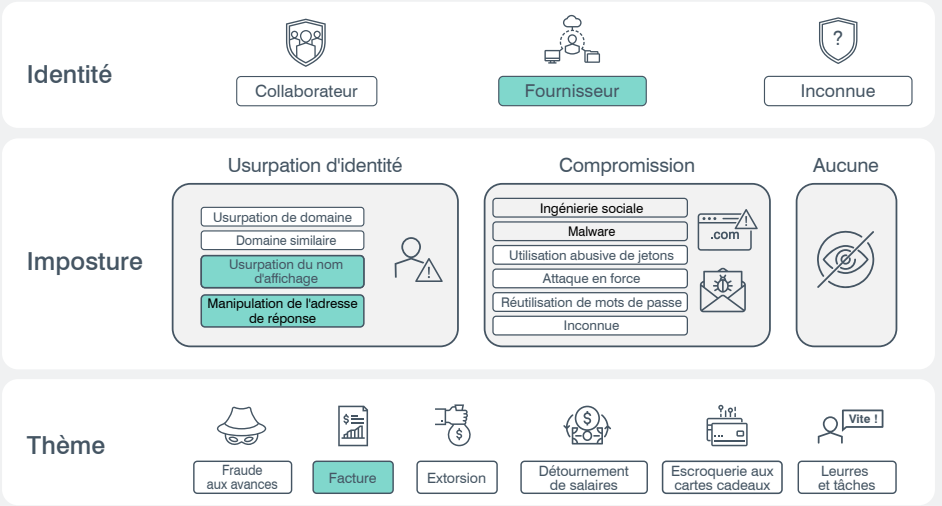


Figure 7. Exemple concret de fraude aux factures fournisseurs

Thème 2 – Détournement de salaires

Les attaques de détournement de salaires font partie des attaques BEC les plus simples que nous rencontrons. Qu'elles ciblent le service financier, fiscal, de paie ou des ressources humaines (RH), l'objectif est simple : inciter le destinataire à rediriger vers le cybercriminel les salaires durement gagnés par les collaborateurs, voire les remboursements d'impôts.

Nous détectons en moyenne quelque 2 000 tentatives de détournements de salaires par jour (voir la figure 8) et considérons que ces attaques représentent un risque moyen pour les employeurs.

Selon le FBI, les pertes moyennes liées à ces attaques s'élèvent à 7 904 dollars par incident signalé[2]. L'administration fiscale américaine a inclus les détournements de salaires dans sa liste des pires escroqueries fiscales pour 2020[3]. Selon elle, les cybercriminels utilisent des documents authentiques de l'administration fiscale dans le cadre des attaques de détournement de salaires pour convaincre les destinataires que les demandes frauduleuses de changement de banque sont légitimes.

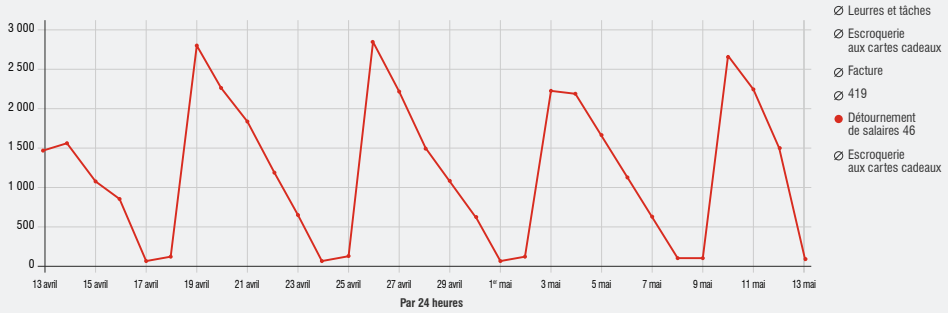


Figure 8. Tentatives de détournement de salaires (nombre total de tentatives par période de 24 heures , entre le 13 avril et le 13 mai 2021)

Fonctionnement

Les attaques de détournement de salaires peuvent utiliser la compromission comme technique d'*imposture*, mais elles impliquent généralement une usurpation d'identité. (Les cybercriminels ayant accès à un compte compromis ont tendance à concentrer leurs efforts sur des formes d'attaques BEC plus rentables, comme la fraude aux factures.)

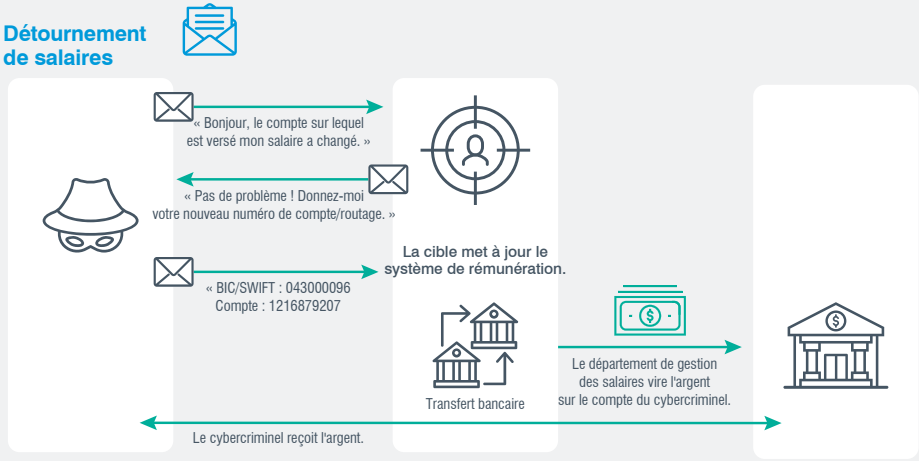


Figure 9. Anatomie d'une attaque de détournement de salaires ayant recours à l'usurpation d'identité

La plupart des attaques de détournement de salaires basées sur l'usurpation d'identité utilisent des services de messagerie gratuits tels que Gmail. En général, le cybercriminel recourt à la technique d'usurpation du nom d'affichage pour faire croire que l'email provient d'un collaborateur (voir la figure 9 ci-dessus).

1. FBI, « 2020 Internet Crime Report » (Rapport 2020 sur la cybercriminalité), mars 2021.
2. IRS, « Dirty Dozen » (Liste des pires escroqueries fiscales), septembre 2021.

Certaines attaques de détournement de salaires ciblent des cadres supérieurs et des dirigeants dans l'espoir de détourner un salaire plus élevé. Lors de ces tentatives, les cybercriminels peuvent utiliser des adresses email mentionnant un poste de direction afin de gagner en crédibilité et de susciter un sentiment d'urgence dans le chef des destinataires désireux de plaire à leur supérieur. (Voir la figure 10 ci-dessous. Parmi les exemples récents, citons également « ceo@companywebaxccs.com » et « ceo_task2@icloud.com ».)

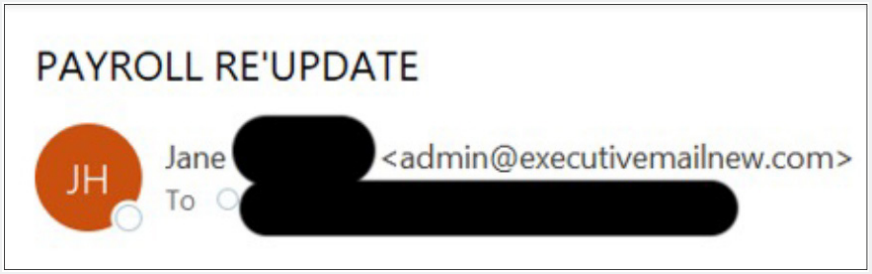


Figure 10. Domaine de messagerie conçu pour communiquer une impression d'autorité

La figure 11 illustre la façon dont notre taxonomie classerait les deux attaques décrites.

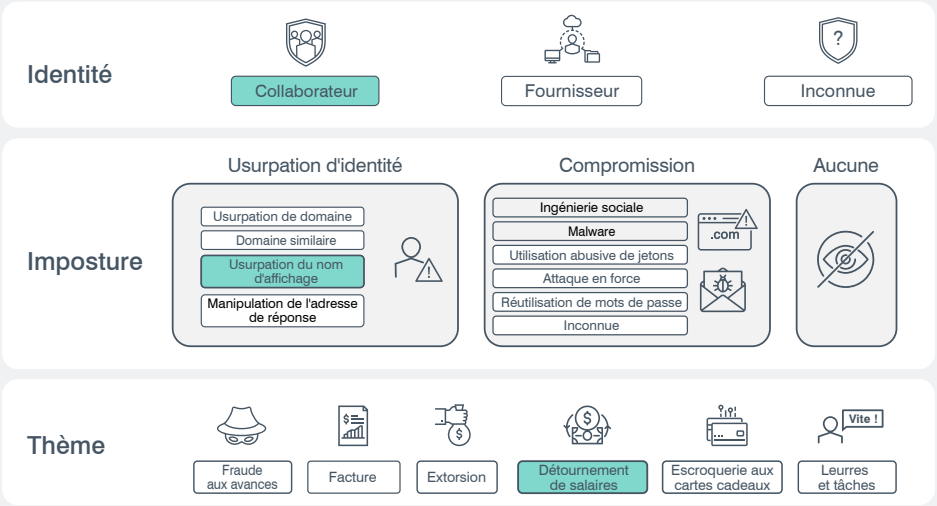


Figure 11. Attaque de détournement de salaires utilisant un nom d'affichage d'email usurpé

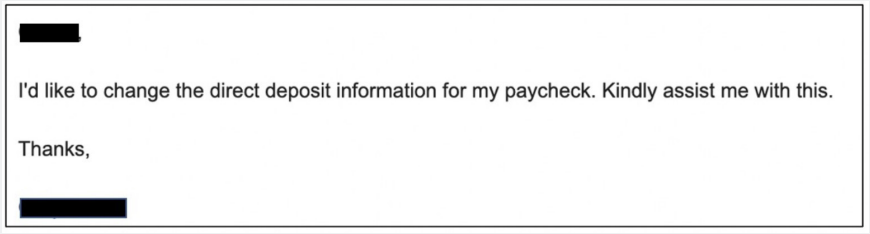
Exemples concrets

Les attaques de détournement de salaires se caractérisent par leur simplicité. Lors d'une attaque que nous avons récemment observée, un cybercriminel a usurpé l'identité de plusieurs collaborateurs dans des emails envoyés au service de paie d'une grande entreprise. Comme le montre la figure 12, tous les emails utilisaient la même approche et ne différaient qu'au niveau des éléments suivants :

- Destinataire de l'email
- Personne dont l'identité était usurpée
- Langue utilisée (anglais, allemand ou espagnol)

Figure 12. Exemples d'emails usurpant l'identité de collaborateurs lors de tentatives de détournement de salaires

Certaines tentatives sont encore plus simples et culottées. À la figure 13, le cybercriminel tente d'usurper l'identité du PDG d'une entreprise.


[redacted]

I'd like to change the direct deposit information for my paycheck. Kindly assist me with this.

Thanks,

[redacted]

Figure 13. Email de détournement de salaires usurpant l'identité d'un PDG

Malgré leur nature peu sophistiquée, ces attaques peuvent être étonnamment efficaces. Cela est dû au fait qu'elles exploitent un processus métier normal. Les collaborateurs des services financiers, fiscaux, de paie et des ressources humaines reçoivent chaque jour des demandes de ce genre par email, pour la plupart légitimes.

Thème 3 – Extorsion

La fraude par email à des fins d'extorsion fonctionne comme les autres formes d'extorsion. Le cybercriminel menace de détruire des biens, de commettre des actes de violence ou de divulguer des informations confidentielles, embarrassantes ou compromettantes, à moins que le destinataire ne fournisse un paiement (généralement au moyen d'une cryptomonnaie) ou autre chose de valeur. L'extorsion se subdivise en plusieurs sous-types, notamment :

- **Divulgation de données –** Le cybercriminel menace de divulguer des informations sensibles, embarrassantes ou compromettantes, des données clients, des secrets commerciaux ou encore des preuves d'une activité criminelle (réelle ou non).
- **Déni de service distribué (DDoS) –** Le cybercriminel menace de submerger les serveurs d'opération en ligne du destinataire de trafic non pertinent, de façon à les rendre inaccessibles aux utilisateurs légitimes.
- **Préjudice physique –** Le cybercriminel menace de porter physiquement atteinte au destinataire ou à l'entreprise. Les tactiques les plus courantes sont les alertes à la bombe, les complots d'assassinat et d'autres avertissements de violence imminente.
- **Sextorsion –** Le cybercriminel menace de divulguer des photos ou des vidéos à caractère sexuel de la victime. La sextorsion est probablement le plus courant de ces sous-types d'extorsion.

Fonctionnement

Contrairement aux autres thèmes abordés dans cet eBook, la fraude par email à des fins d'extorsion n'a recours qu'à une seule tactique d'imposture (l'usurpation d'identité), pour autant qu'elle en utilise une. Si usurpation d'identité il y a, le cybercriminel fait généralement en sorte que l'email semble provenir du compte de messagerie de la victime.

En général, le cybercriminel envoie aux victimes un email dans lequel il prétend avoir accédé à leur ordinateur et les avoir enregistrées en train de regarder des contenus réservés aux adultes. L'email contient du contenu sensible semblant provenir du compte de messagerie du destinataire. Le cybercriminel avertit les destinataires que s'ils ne paient pas, le contenu embarrassant sera envoyé à leurs collègues et aux membres de leur famille.

La figure 14 illustre la façon dont ce type d'attaque est cartographié dans notre cadre BEC.

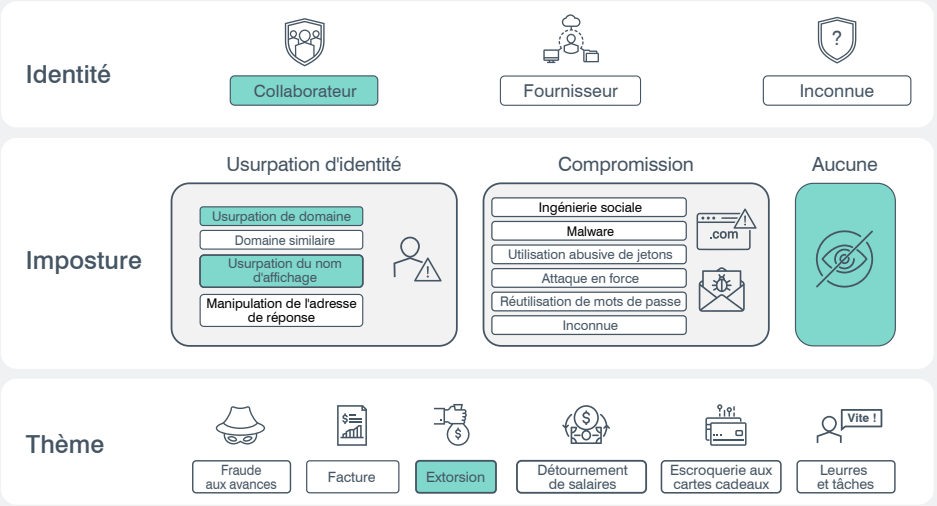


Figure 14

À moins que les cybercriminels n'essaient d'usurper l'identité de quelqu'un, ils utilisent généralement des services de messagerie gratuits et ne prennent pas la peine de falsifier l'adresse. Ce genre de scénario serait cartographié comme suit dans le cadre BEC (figure 15).

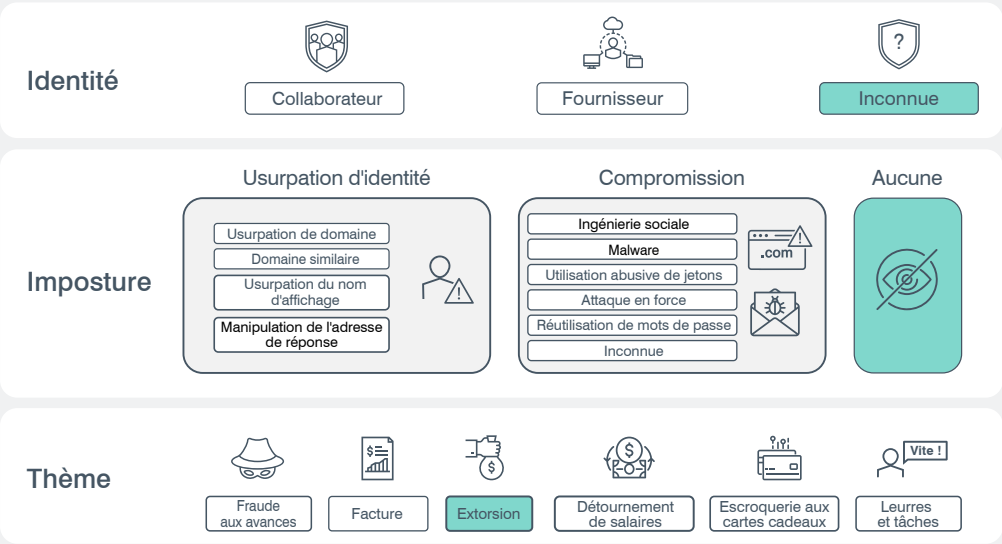
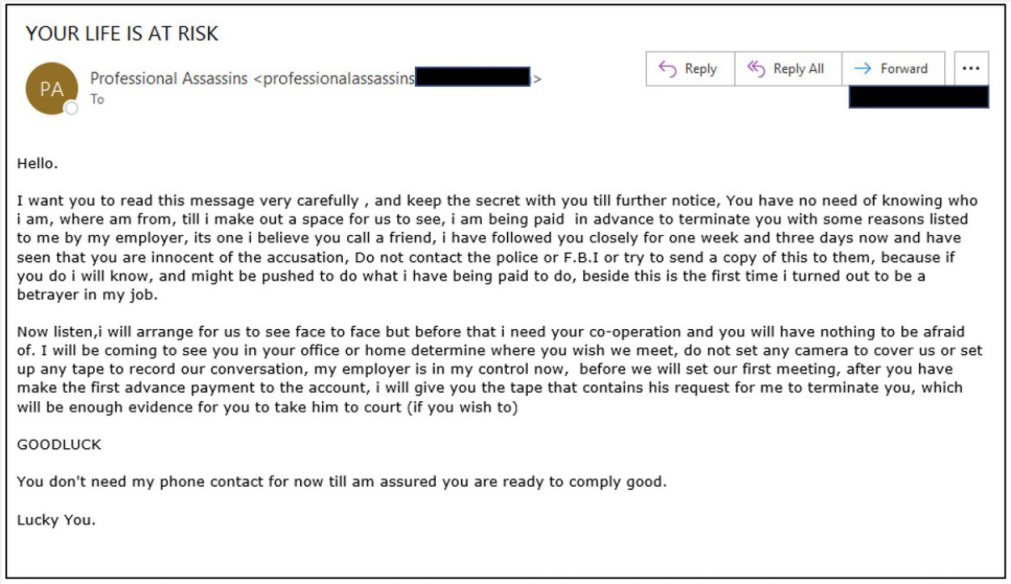


Figure 15. Certaines attaques d'extorsion n'utilisent pas de tactiques d'usurpation d'identité

Exemples concrets

La sextorsion est probablement la forme d'extorsion que nous observons le plus souvent. Les emails concernés ont tendance à être longs et détaillés. Mais l'objectif est simple et pragmatique : convaincre les victimes qu'elles sont dans une situation délicate et qu'elles doivent répondre aux exigences du cybercriminel.



YOUR LIFE IS AT RISK

PA Professional Assassins <professionalassassins[redacted]>
To

Reply | Reply All | Forward | ...

Hello.

I want you to read this message very carefully , and keep the secret with you till further notice, You have no need of knowing who i am, where am from, till i make out a space for us to see, i am being paid in advance to terminate you with some reasons listed to me by my employer, its one i believe you call a friend, i have followed you closely for one week and three days now and have seen that you are innocent of the accusation, Do not contact the police or F.B.I or try to send a copy of this to them, because if you do i will know, and might be pushed to do what i have being paid to do, beside this is the first time i turned out to be a betrayer in my job.

Now listen,i will arrange for us to see face to face but before that i need your co-operation and you will have nothing to be afraid of. I will be coming to see you in your office or home determine where you wish we meet, do not set any camera to cover us or set up any tape to record our conversation, my employer is in my control now, before we will set our first meeting, after you have make the first advance payment to the account, i will give you the tape that contains his request for me to terminate you, which will be enough evidence for you to take him to court (if you wish to)

GOODLUCK

You don't need my phone contact for now till am assured you are ready to comply good.

Lucky You.

Figure 16. Tentative d'extorsion promettant d'annuler un supposé complot d'assassinat si le destinataire paie l'expéditeur

Les menaces d'atteinte à l'intégrité physique sont moins fréquentes, mais elles inquiètent évidemment les personnes qui les reçoivent. Comme le montre la figure 16, ces tactiques musclées tentent d'effrayer les victimes en leur faisant croire que leur vie est en grand danger si elles ne paient pas.

Ces emails se caractérisent essentiellement par un sentiment d'urgence, des délais réduits pour l'exécution des instructions et des avertissements fermes interdisant de contacter la police.

Thème 4 – Leurres et tâches

Du fait de leur nature peu sophistiquée, les emails de leurres et de tâches passent facilement inaperçus. Ils commencent souvent par la demande d'un service simple, voire anodin. Si certaines attaques s'ouvrent sur une demande spécifique, bon nombre d'entre elles sont formulées en termes vagues et ferrent la victime au fil de plusieurs emails. En l'occurrence, les messages initiaux peuvent contenir une demande générale de type :

- « Es-tu disponible ? »
- « Tu peux me rendre un petit service ? »
- « Tu as un moment ? »
- « Tu es là ? J'aurais besoin que tu achètes des cartes cadeaux pour moi. »

Les leurres et tâches sont souvent un point d'entrée, la première étape d'attaques en plusieurs phases qui couvrent d'autres thèmes de fraude par email. Un email de leurre ou de tâche tente tout d'abord d'attirer l'attention du destinataire, l'objectif final du cybercriminel (par exemple, le détournement de salaires ou une fraude aux factures) se révélant au fil du temps.

Ces attaques multicatégories peuvent compliquer la classification. Souvent, pour différencier les emails de leurres ou de tâches des autres emails de notre taxonomie, nous devons observer ce que le cybercriminel fait ensuite. Si nous ne voyons qu'un seul email de leurre ou tâche, nous le classons comme tel. Mais si les emails suivants révèlent un objectif sous-jacent allant au-delà de la tâche ou du leurre initial, nous les classons à la fois sous le thème Leurres et tâches et sous un autre thème.

Fonctionnement

Dans notre taxonomie, les emails de leurres et de tâches n'utilisent qu'une forme d'*imposture* : l'usurpation d'identité. Les cybercriminels usurpent généralement l'identité d'une personne que la cible connaît ou en qui elle a confiance, notamment :

- Personnes incarnant une figure d'autorité, que ce soit au niveau personnel ou professionnel
- Amis proches
- Membres de la famille

L'usurpation de l'identité d'une personne familière désamorce les soupçons que le destinataire pourrait avoir à l'égard d'une demande inattendue ou inhabituelle et l'oblige presque à répondre.

Une réponse quelconque permet au cybercriminel d'atteindre son premier objectif : identifier un compte de messagerie actif et un public potentiellement réceptif.

La plupart de emails de leurres ou de tâches ont recours à la technique d'usurpation du nom d'affichage pour tromper le destinataire, comme illustré à la figure 17. Certains utilisent d'autres tactiques d'usurpation d'identité, comme l'usurpation du domaine ou des adresses de réponse. Après avoir reçu une réponse, le cybercriminel peut changer de tactique d'imposture si cela permet d'améliorer la crédibilité de l'attaque.

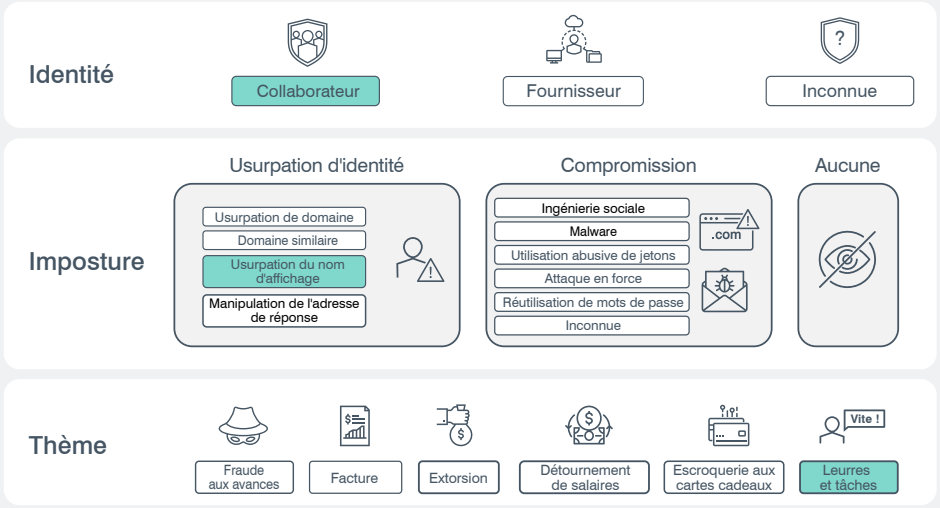


Figure 17

Exemples concrets

De nombreuses attaques BEC de type leurre ou tâche que nous observons commencent par un bref email destiné à évaluer le degré de réceptivité de la cible. Comme le montre la figure 18, ces premiers emails ne tentent même pas nécessairement de créer un sentiment d'urgence.

Figure 18. Email de leurre ou de tâche initial

La fraude par email basée sur un leurre ou une tâche est extrêmement courante et représente plus de la moitié des menaces de fraude par email que nous avons observées en 2021. (Nous bloquons la remise en boîte de réception d'environ 30 000 de ces emails par jour.)

Ces emails semblent bénins au premier abord. Mais si le destinataire tombe dans le panneau, cela peut conduire à des formes de fraude par email plus graves, avec des conséquences potentiellement coûteuses : escroquerie aux cartes cadeaux, fraude aux factures, détournement de salaires, etc.

Thème 5 – Escroquerie aux cartes cadeaux

Dans le cadre des escroqueries aux cartes cadeaux, les cybercriminels obtiennent des paiements sous la forme de cartes cadeaux de détaillants. Les destinataires sont amenés par la ruse à acheter les cartes et à envoyer les numéros d'identification et les codes PIN au cybercriminel, qui peut alors les utiliser ou les revendre.

Ces attaques fonctionnent parce que les entreprises récompensent souvent leurs collaborateurs et partenaires avec des cartes cadeaux. Pour le destinataire, cette demande peut paraître ordinaire. Si l'email semble urgent et offre une explication raisonnable, le destinataire peut agir sans se méfier.

Fonctionnement

Au niveau *Imposture*, les cybercriminels usurpent généralement l'identité d'un dirigeant ou d'une personne en position d'autorité pour conférer à la demande une apparence de légitimité. Comme c'est le cas pour d'autres formes de fraude par email, l'usurpation de l'identité d'une personne familière, notamment les amis proches et les membres de la famille, augmente la probabilité que le destinataire tombe dans le piège.

La plupart de emails d'escroquerie aux cartes cadeaux ont recours à la technique d'usurpation du nom d'affichage pour tromper le destinataire, comme illustré à la figure 19. Parfois, les cybercriminels utilisent d'autres tactiques d'usurpation d'identité, notamment l'usurpation du domaine ou la modification du champ d'adresse de réponse.

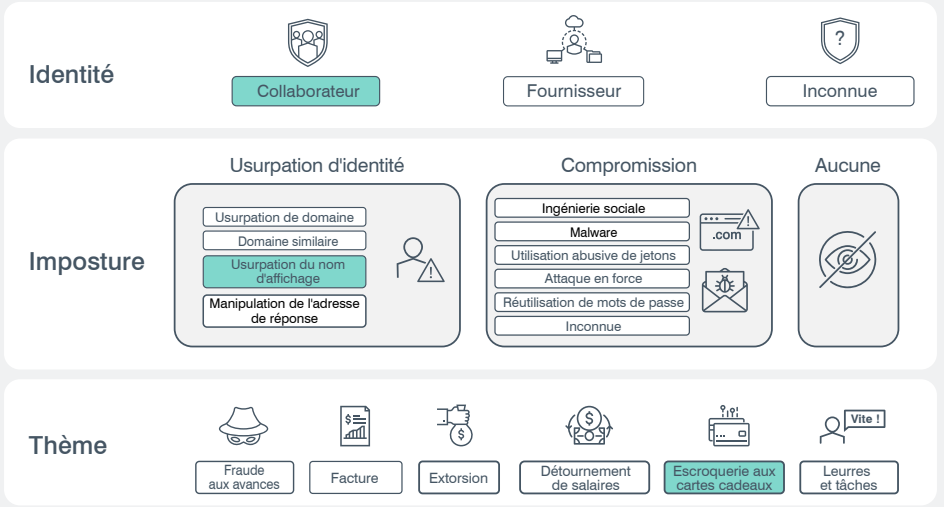


Figure 19. Taxonomie des escroqueries aux cartes cadeaux

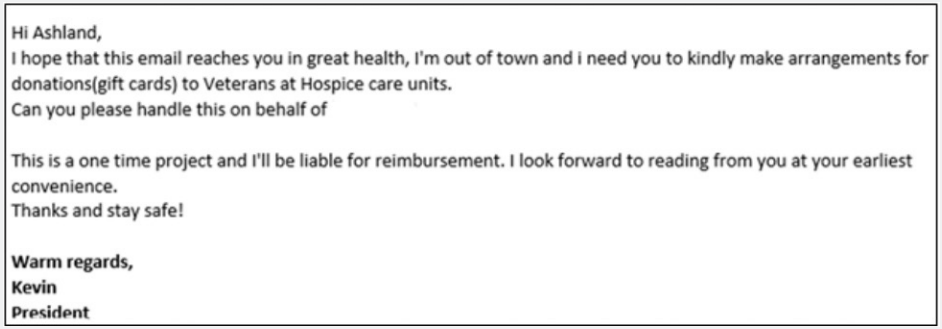
Exemples concrets

Les emails d'escroquerie aux cartes cadeaux utilisent toutes sortes de leurres pour que la demande paraisse valable au destinataire (voir les figures 20, 21 et 22 à la page suivante). Les cybercriminels peuvent faire flèche de tout bois, de l'actualité (par exemple, la pandémie) aux diverses fêtes du calendrier. Quel que soit le leurre, l'objectif est de fournir une raison plausible à la demande et de susciter la sympathie pour accroître les chances de réussite.

Sympathie pour l'escroc

Les figures 20 et 21 sont des exemples frappants de cybercriminels tentant de toucher la corde sensible du destinataire.

À la figure 20, l'expéditeur affirme que les cartes cadeaux sont destinées aux résidents d'un hospice, des anciens combattants, rien de moins. À la figure 21, l'expéditeur explique qu'il n'est pas en ville et est en isolement (probablement une allusion à la pandémie), et qu'il ne peut donc pas acheter de cadeau pour l'anniversaire de sa nièce.

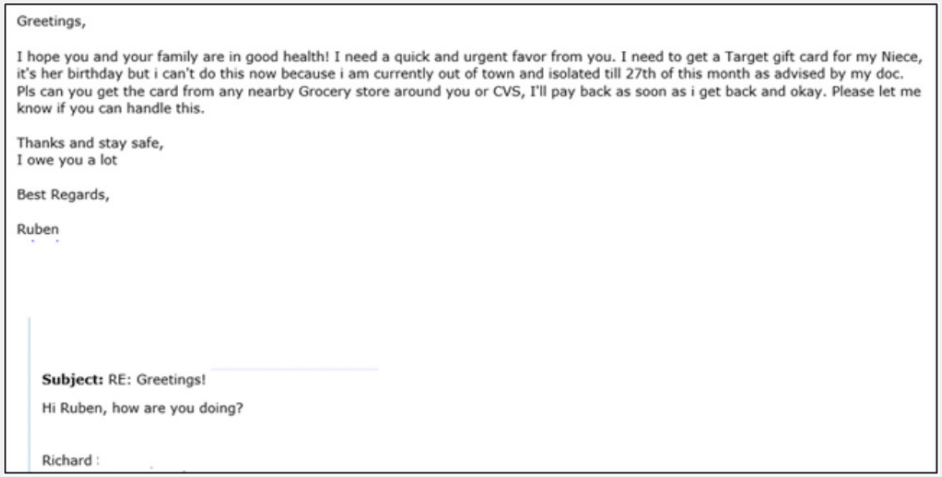


Hi Ashland,
I hope that this email reaches you in great health, I'm out of town and i need you to kindly make arrangements for donations(gift cards) to Veterans at Hospice care units.
Can you please handle this on behalf of

This is a one time project and I'll be liable for reimbursement. I look forward to reading from you at your earliest convenience.
Thanks and stay safe!

Warm regards,
Kevin
President

Figure 20. Email demandant au destinataire d'acheter des cartes cadeaux en vue d'un prétendu don à un hospice



Greetings,

I hope you and your family are in good health! I need a quick and urgent favor from you. I need to get a Target gift card for my Niece, it's her birthday but i can't do this now because i am currently out of town and isolated till 27th of this month as advised by my doc. Pls can you get the card from any nearby Grocery store around you or CVS, I'll pay back as soon as i get back and okay. Please let me know if you can handle this.

Thanks and stay safe,
I owe you a lot

Best Regards,

Ruben

Subject: RE: Greetings!

Hi Ruben, how are you doing?

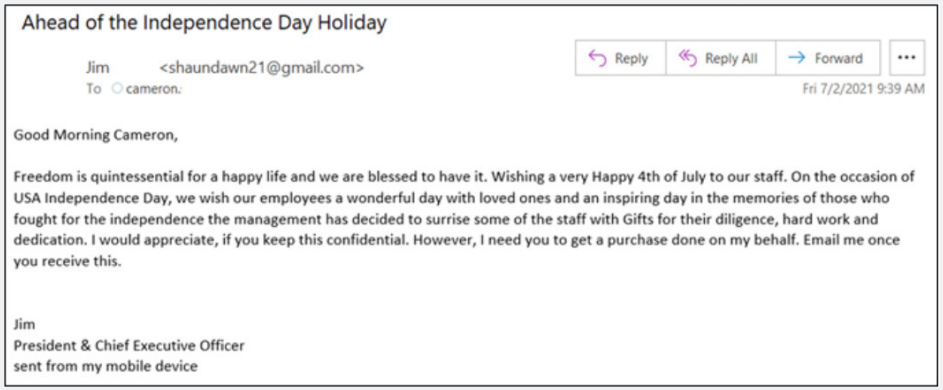
Richard :

Figure 21. Email demandant au destinataire d'acheter des cartes cadeaux au prétexte que l'expéditeur est en isolement

La figure 22 montre également que certaines escroqueries aux cartes cadeaux commencent par un bref email de leurre ou de tâche visant à tester la réceptivité de la victime potentielle. (Pour en savoir plus sur ce leurre, voir la section précédente, « **Thème 4 – Leurres et tâches** ».) En l'occurrence, le cybercriminel a d'abord cherché à savoir si la victime visée était disponible. La demande de carte cadeau n'est arrivée qu'après que la personne a répondu.

Escroqueries aux cartes cadeaux d'entreprise

Dans notre dernier exemple (figure 22), le cybercriminel explique qu'il souhaite offrir des cartes cadeaux aux collaborateurs en guise de remerciement, une pratique courante dans les entreprises. En l'occurrence, la demande s'inscrit dans le contexte de la fête nationale américaine.



Ahead of the Independence Day Holiday

Jim <shaundawn21@gmail.com>
To cameron.

Reply | Reply All | Forward | ...
Fri 7/2/2021 9:39 AM

Good Morning Cameron,

Freedom is quintessential for a happy life and we are blessed to have it. Wishing a very Happy 4th of July to our staff. On the occasion of USA Independence Day, we wish our employees a wonderful day with loved ones and an inspiring day in the memories of those who fought for the independence the management has decided to surrise some of the staff with Gifts for their diligence, hard work and dedication. I would appreciate, if you keep this confidential. However, I need you to get a purchase done on my behalf. Email me once you receive this.

Jim
President & Chief Executive Officer
sent from my mobile device

Figure 22. Email provenant d'une personne se présentant comme le PDG de l'entreprise et demandant au destinataire d'acheter des cartes cadeaux en guise de bonus pour les collaborateurs ; le cybercriminel demande au destinataire de garder la demande secrète, soi-disant pour éviter de gâcher la surprise

Cadeau empoisonné

L'escroquerie aux cartes cadeaux est une forme courante de fraude par email. Avec un coût moyen de 840 dollars par incident, cette forme de cybercriminalité a permis à ses auteurs de ponctionner près de 245 millions de dollars depuis 2018. Nous bloquons entre 7 000 et 10 000 emails de ce type chaque jour.

Thème 6 – Fraude aux avances

La fraude aux avances est une vieille escroquerie que l'on appelle parfois, de façon quelque peu trompeuse, la fraude par email « 419 », l'« arnaque nigériane » ou l'« email du prince nigérian ». Dans le cadre de cette escroquerie, le cybercriminel demande à la victime potentielle une petite somme d'argent en guise d'avance sur un paiement plus important à venir. Les fonds demandés sont généralement présentés comme un capital de départ pour débloquer ou transférer la récompense promise.

Les cybercriminels ont imaginé d'innombrables variantes de la fraude aux avances. Ils racontent souvent des histoires élaborées expliquant pourquoi une grosse somme d'argent est disponible et pourquoi ils ont besoin d'une petite avance pour la faire parvenir au destinataire de l'email. Les fraudeurs appâtent souvent les victimes avec des lignes d'objet telles que :

- Héritage
- Gains de loterie
- Récompenses
- Paiements du gouvernement
- Commerce international

Une fois que la victime a versé l'avance, le fraudeur peut lui demander de l'argent supplémentaire (en invoquant des complications imprévues) ou simplement couper tout contact et disparaître.

Fonctionnement

Au niveau *Imposture* de notre taxonomie, la fraude aux avances a recours à des techniques d'usurpation d'identité. Les cybercriminels se font généralement passer pour un fonctionnaire, un représentant légal ou une personne en situation critique. La plupart des emails de fraude aux avances ont recours à l'usurpation du nom d'affichage (voir la figure 23), mais certains utilisent d'autres tactiques d'usurpation d'identité, comme l'usurpation de domaine ou des domaines similaires.

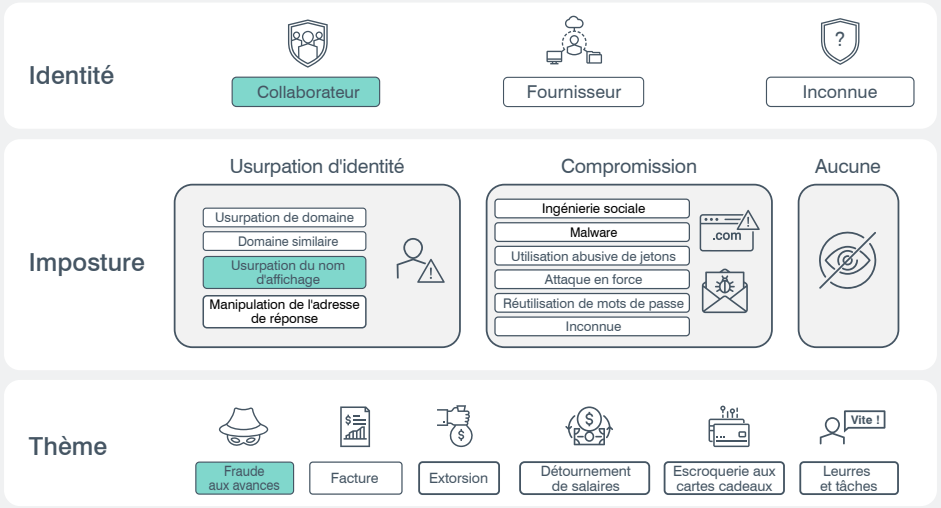


Figure 23. Taxonomie de la fraude aux avances

Exemples concrets

Les emails de fraude aux avances utilisent divers leurres pour ferrer les victimes, conserver leur confiance et les persuader d'agir. Comme le montrent les exemples suivants, les cybercriminels peuvent se servir d'un large éventail d'accroches, qu'il s'agisse d'événements d'actualité tels que la pandémie, de transactions commerciales ou de promesses de paiements.

À la figure 24 (voir page suivante), l'expéditeur tente d'exploiter la pandémie de COVID-19. À la figure 25 (également à la page suivante), l'expéditeur exhorte le destinataire à agir rapidement, ce qui laisse peu de temps à la cible pour déterminer si l'email est frauduleux.

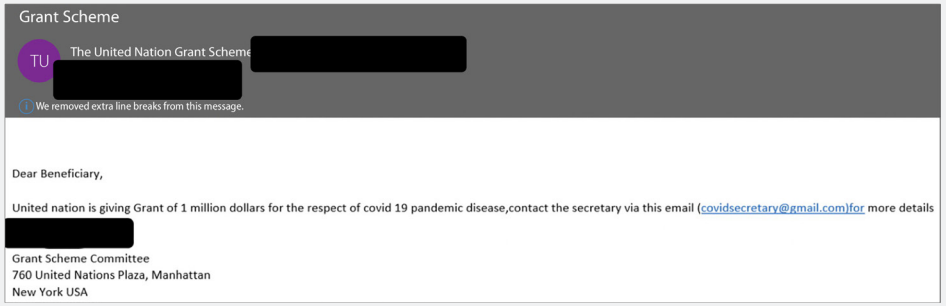


Figure 24. Email de fraude aux avances promettant une subvention d'un million de dollars

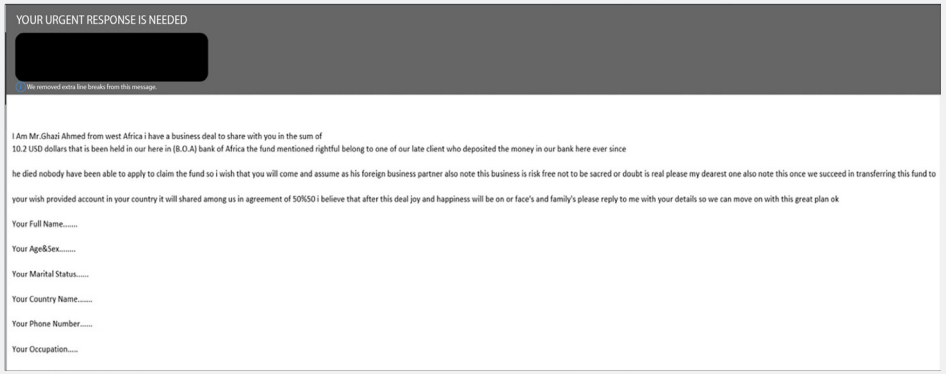


Figure 25. Email proposant de partager un héritage non réclamé avec le destinataire

À la figure 26, le cybercriminel tente d'attirer la victime en lui faisant miroiter un paiement important, une stratégie courante dans les fraudes aux avances qui exploitent la cupidité humaine. En plus d'inciter le destinataire à payer des « frais de sécurité » de 95 dollars, l'email tente d'obtenir des données personnelles.

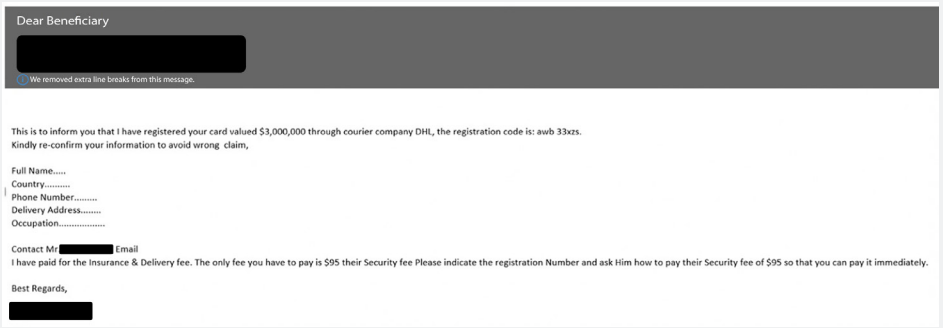


Figure 26. Email promettant un paiement de 3 millions de dollars après le versement de 95 dollars de « frais de sécurité » par le destinataire

La plupart des emails de fraude aux avances sont simples et faciles à repérer ; rares sont ceux qui sont bien rédigés ou plus complexes que les exemples fournis ici.

Les emails de fraude aux avances ne représentent qu'une petite proportion des emails frauduleux que nous rencontrons. Néanmoins, certaines personnes tombent dans le panneau et les pertes moyennes s'élèvent à environ 5 100 dollars par incident. Bien que le taux de réussite soit probablement beaucoup plus faible que pour d'autres types de fraude comme l'escroquerie aux cartes cadeaux, la fraude aux avances peut être lucrative pour les cybercriminels.

Conclusion et recommandations

Les types de fraude par email décrits dans notre taxonomie sont pernicieux, omniprésents et difficiles à gérer avec les outils et passerelles de sécurité traditionnels axés sur le périmètre. En effet, comme la plupart des cyberattaques modernes, ils ciblent les personnes, pas les technologies. La lutte contre ce type d'attaques exige donc une approche centrée sur les personnes.

Les contrôles financiers, comme l'obligation de faire approuver par au moins deux personnes les modifications apportées aux comptes de paiement ou aux détails de fiche de paie, sont un bon début. Mais la neutralisation des attaques BEC nécessite également une protection avancée de la messagerie. Pour bénéficier d'une meilleure visibilité sur la surface d'attaque constituée par vos collaborateurs et bloquer les attaques BEC sous toutes leurs formes, vous avez besoin d'une plate-forme complète offrant des contrôles intégrés sur les emails, les comptes cloud, les utilisateurs et les fournisseurs.

Optez pour une solution offrant les avantages suivants :

- Visibilité sur la surface d'attaque constituée par vos collaborateurs. Vous devez connaître vos utilisateurs les plus ciblés, les cybercriminels qui ciblent votre entreprise et les fournisseurs susceptibles d'être compromis ou victimes d'une usurpation d'identité.
- Fonctionnalités de détection avancées pour neutraliser les attaques BEC, la fraude par email et d'autres menaces dépourvues de malwares. La fraude par email utilise l'ingénierie sociale et des tactiques en constante évolution qui exploitent les faiblesses de la nature humaine. Cela signifie que les jeux de règles statiques, même régulièrement mis à jour, ne suffisent pas à les identifier et à les arrêter. Les solutions les plus performantes s'appuient également sur l'apprentissage automatique, qui analyse des éléments tels que les en-têtes d'email, la relation expéditeur/destinataire et la réputation de l'expéditeur. Cependant, l'efficacité de l'apprentissage automatique dépend des données qui l'alimentent et des modèles d'entraînement qui le façonnent. C'est pourquoi nous vous recommandons de chercher des fournisseurs disposant d'ensembles de données vastes et diversifiés et de ressources humaines spécialisées dans la gestion de menaces.
- Capacité d'empêcher les cybercriminels de prendre le contrôle des comptes des utilisateurs et de les utiliser pour des attaques de fraude par email. Dans la mesure où les entreprises sont de plus en plus nombreuses à migrer vers le cloud, la protection contre la fraude par email passe également par la protection des comptes cloud. Choisissez des outils qui empêchent la prise de contrôle des comptes de vos utilisateurs en vue de mener des attaques de fraude par email.
- Formation de sensibilisation à la sécurité informatique pour compléter les contrôles techniques. En offrant à vos utilisateurs une formation adéquate (en particulier si elle repose sur des menaces réelles), vous pouvez les transformer en véritables piliers de défense contre les cyberattaques. Faites en sorte que vos utilisateurs puissent signaler facilement les messages suspects et que vos équipes informatiques puissent les vérifier rapidement grâce à des fonctionnalités d'analyse et de correction automatisées.

EN SAVOIR PLUS

Pour en savoir plus sur la façon dont Proofpoint peut vous aider à gérer les attaques BEC et la fraude par email, consultez la page : **proofpoint.com/us/solutions/bec-and-eac-protection**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0501-010-01-01 04/22