proofpoint.

EBOOK

Guide du piratage de la messagerie en entreprise (BEC)

Plan en six étapes pour bloquer le détournement de paiements, la fraude aux factures fournisseurs et les escroqueries aux cartes-cadeaux

Une menace de cybersécurité extrêmement coûteuse, sans solution simple

D'après le rapport 2020 sur la cybercriminalité de l'Internet Crime Complaint Center (CI3) du FBI, l'année dernière, la « vague cybercriminelle » a fait perdre environ 1,8 milliard de dollars aux victimes de campagnes de fraude par email.

Un email réclamant un virement de 37 millions de dollars est envoyé au service financier d'un fournisseur de pièces détachées détenu par l'un des constructeurs automobiles les plus importants au monde. Bien qu'il puisse sembler a priori élevé, le montant du virement n'a rien d'exceptionnel pour une entreprise d'envergure mondiale. En revanche, la demande n'émanait ni d'un fournisseur, ni d'un partenaire commercial, ni d'un cadre de l'entreprise. Elle provenait d'un cybercriminel se faisant passer pour quelqu'un d'autre, un des exemples de piratage de la messagerie en entreprise (BEC, Business Email Compromise) les plus largement documentés[1].

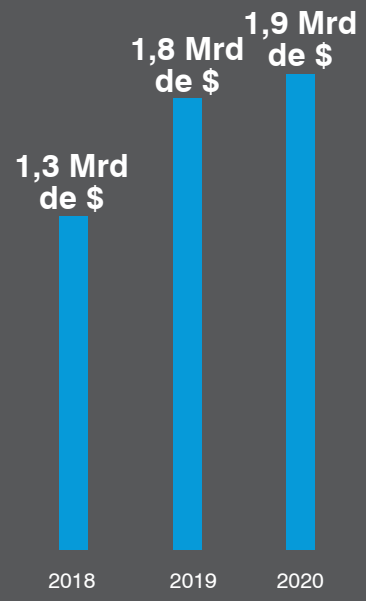
En Arizona, un homme d'affaires envoie un email à son collègue pour l'informer que la société compte un nouveau fournisseur, RS Entreprise. Étant en déplacement, il ne peut effectuer le virement de 157 000 dollars qu'il a promis au fournisseur, et transmet toutes les informations nécessaires à son collègue pour qu'il transfère l'argent. Plus de 350 personnes en Arizona ont reçu des emails contenant des instructions similaires et qui semblaient émaner d'un fournisseur ou d'un autre collaborateur habituel de l'entreprise. Les auteurs de ces messages ? Des cybercriminels qui ont extorqué plus de 30 millions de dollars, selon le FBI (Federal Bureau of Investigation)[2].

Dans un email plaintif, un homme explique au destinataire qu'il a dû se mettre en quarantaine en raison de symptômes de la COVID-19. Dans sa hâte, il a oublié de prendre son téléphone mobile et d'autres objets essentiels. Il demande donc au destinataire de bien vouloir lui acheter des cartes-cadeaux iTunes ou Walmart d'une valeur de 250 dollars. Il lui demande également de prendre en photo les cartes et leurs codes pour qu'il puisse

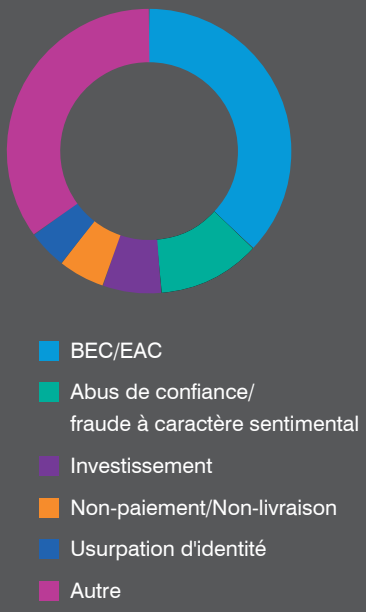
1 Nicole Lindsey (*CPO Magazine*), « Toyota Subsidiary Loses $37 Million Due to BEC » (Une filiale de Toyota perd 37 millions de dollars à la suite d'une attaque BEC), septembre 2019.

2 Susan Campbell (*azfamily.com*), « Arizona workers lost $30 million to work email scams, FBI says. » (Selon le FBI, des employés d'Arizona ont perdu 30 millions de dollars à la suite d'arnaques ciblant la messagerie d'entreprise), avril 2021.

Pertes liées aux attaques BEC signalées



Pourcentage des pertes totales signalées dues à la cybercriminalité



Source : FBI

les utiliser pour acheter les produits de première nécessité pendant sa quarantaine[3].

Une tendance coûteuse

Tous ces récits sont des exemples récents d'attaque BEC, qui ne représentent qu'un infime échantillon des milliers d'attaques qui ciblent des entreprises et utilisateurs américains depuis le début de l'année 2020. L'année 2020 a été particulièrement productive pour les cybercriminels, qui ont profité des perturbations engendrées par la pandémie, ainsi que de la dépendance accrue à l'égard des technologies pendant cette crise.

Parmi toutes ces activités malveillantes, les attaques BEC se sont révélées les plus coûteuses pour les victimes. D'après le rapport 2020 sur la cybercriminalité de l'Internet Crime Complaint Center (CI3) du FBI, l'année dernière, la « vague cybercriminelle » a fait perdre environ 1,8 milliard de dollars aux victimes de campagnes de fraude par email[4]. Cela représente près de la moitié (44 %) de l'ensemble des pertes dues à la cybercriminalité subies par les entreprises et les particuliers l'année dernière.

Ce chiffre est en outre 64 fois supérieur aux pertes financières résultant de la vague de campagnes de ransomwares lancées en 2020[5]. Le montant des pertes financières est encore plus impressionnant si l'on considère le fait que seules 19 369 du nombre record de 791 790 plaintes enregistrées par les victimes de cybercriminels auprès de l'IC3 en 2020 étaient liées à des fraudes par email, soit seulement 2,4 % de l'ensemble des plaintes.

La bonne nouvelle est qu'il est possible de lutter contre ces menaces pour peu que l'on dispose des informations, de l'approche et des mesures appropriées. Cet eBook explique le fonctionnement des attaques BEC, les formes qu'elles peuvent prendre et les mesures à prendre pour éviter de figurer au nombre des prochaines victimes.

3 Lance Whitney (*TechRepublic*), « Scammers exploit coronavirus for Business Email Compromise campaigns » (Des cyberescrocs utilisent le coronavirus pour des campagnes de piratage de la messagerie en entreprise), avril 2020.

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

5 Sara Pan (*Proofpoint*), « FBI Internet Crime Report Shows that Email Fraud Represents the Largest Financial Losses in 2020 » (Le rapport « Internet Crime Report » du FBI révèle que la fraude par email est la menace qui a occasionné le plus de pertes financières en 2020), mars 2021.

Sommaire

Pourquoi les attaques BEC sont-elles aussi efficaces ?

Pour faire court, parce que ces attaques sont difficiles à détecter et utilisent des stratagèmes très convaincants.

Les attaques BEC s'appuient principalement sur des techniques d'ingénierie sociale pour piéger les victimes et abuser de leur confiance. Les messages envoyés ne contiennent généralement pas de malware ou d'URL malveillantes, deux techniques que les dispositifs de cybersécurité traditionnels, notamment les outils d'ancienne génération, les produits isolés et les défenses des plates-formes cloud natives, peuvent bloquer ou intercepter et analyser.

De plus, les attaques BEC sont généralement très ciblées. Il est fréquent que les cybercriminels n'envoient que quelques messages à un petit nombre d'utilisateurs. Ce faible volume de messages permet au cybercriminel d'échapper à la détection de la plupart des outils de sécurité.

L'usurpation d'identité pour tromper les victimes

Les cybercriminels recourent à différentes techniques pour élaborer et lancer des attaques BEC. Les tactiques d'usurpation d'identité jouent un rôle essentiel dans les attaques BEC, notamment parce que le cybercriminel doit convaincre le destinataire que les instructions contenues dans l'email sont légitimes.

Les fraudeurs effectuent souvent des recherches dans les entreprises pour identifier leurs cibles. Ce processus consiste à déterminer, généralement au moyen de ressources publiques telles que LinkedIn, les collaborateurs qui ont accès aux données, systèmes et ressources stratégiques, ainsi que les personnes avec qui ils travaillent et en qui ils ont confiance. Ils utilisent ensuite une ou plusieurs des stratégies suivantes pour lancer leur attaque BEC (dans la plupart des cas, plusieurs tactiques d'usurpation d'identité sont utilisées).

Usurpation du nom d'affichage

Les cybercriminels utilisent le nom de cadres, d'avocats, de partenaires commerciaux et de fournisseurs de l'entreprise ou de toute autre personne ou entité qui n'éveillera pas les soupçons s'il figure dans le champ « De » d'un email. Ce champ est l'identifiant le plus facile à manipuler par les fraudeurs. La plupart des attaques BEC recourent à l'usurpation du nom d'affichage en plus d'autres méthodes comme l'usurpation de domaines (voir ci-dessous).

Usurpation de domaines

Dans le cadre de cette escroquerie par phishing, les cybercriminels piratent la marque d'une entreprise pour dérober de l'argent ou des données par le biais d'une attaque BEC. Ils copient des domaines de confiance d'une entreprise pour envoyer leurs emails frauduleux. Ils peuvent même créer un site Web factice avec une adresse Web piratée et imiter la marque d'une entreprise pour convaincre les utilisateurs qu'ils se trouvent sur le site légitime.

Domaines similaires

L'enregistrement d'un domaine très similaire au domaine de confiance de l'entreprise ciblée est une autre technique d'usurpation d'identité.
Par exemple, un cybercriminel dont l'objectif est de piéger des collaborateurs ou des partenaires commerciaux de « grandeentreprise.com » peut enregistrer un domaine tel que « grande-entreprise.com » ou « grandentreprise.com » et envoyer des emails frauduleux depuis ce domaine similaire.
Le domaine factice est tellement proche du domaine véritable qu'il est très difficile de les différencier et de ne pas se laisser piéger.

Compromission et prise de contrôle de comptes

C'est la technique d'usurpation d'identité la plus efficace. Lorsqu'un cybercriminel compromet le compte d'un utilisateur de confiance, il a accès à l'historique des emails de ce dernier, à ses contacts et à son agenda. Autrement dit, il dispose de l'ensemble des informations et des accès dont il a besoin pour usurper l'identité du titulaire du compte. Il ne se contente pas de se faire passer par l'utilisateur, il *est* l'utilisateur.

Techniques de compromission de comptes

Phishing d'identifiants de connexion

Utilisée depuis plusieurs dizaines d'années, cette stratégie de compromission est conçue pour inciter les utilisateurs à divulguer des identifiants de compte confidentiels. Un utilisateur ciblé peut, par exemple, recevoir un email qui semble provenir du service informatique de son entreprise (affichant même « Centre d'assistance » dans le champ « De ») et lui demande de cliquer sur un lien pour valider ses identifiants de connexion à une application.

Attaque par force brute

Cette technique de prise de contrôle d'un compte d'utilisateur est utilisée depuis un certain temps déjà. Elle consiste pour le cybercriminel à essayer de deviner les identifiants de connexion d'un utilisateur jusqu'à ce qu'il arrive à infiltrer son compte. Cette technique agressive est souvent efficace et rapide car de nombreux utilisateurs créent des paires identifiant/mot de passe faciles à pirater. Cette méthode reste donc prisée par de nombreux cybercriminels.

Jetons OAuth d'applications cloud

Une application OAuth (Open Authentification) s'intègre avec un service cloud et peut être fournie par un fournisseur autre que le fournisseur de services cloud. Ces applications enrichissent les services cloud, tels que Microsoft 365 et Google Workspace, de fonctionnalités d'entreprise et d'une interface utilisateur plus performante. Avec la plupart des applications OAuth, une autorisation est nécessaire pour accéder aux informations et aux données utilisateur et les gérer, ainsi que pour se connecter à d'autres applications cloud au nom de l'utilisateur.

Compte tenu du large éventail d'autorisations qu'elles nécessitent, les application OAuth constituent une surface et un vecteur d'attaque de plus en plus utilisés. Les cybercriminels utilisent des modules complémentaires tiers et des tactiques d'ingénierie sociale pour inciter les utilisateurs à leur donner accès aux applications cloud de leur entreprise par le biais d'une authentification par jeton. Lorsqu'un jeton OAuth est autorisé, l'accès est maintenu jusqu'à sa révocation.

Malwares

Certains cybercriminels recourent à des malwares pour obtenir les informations dont ils ont besoin pour accéder au compte d'un utilisateur et en prendre le contrôle. Différents types de malwares sont utilisés pour prendre le contrôle de comptes :

- Enregistreurs de frappe, qui capturent les frappes au clavier pour obtenir des identifiants de connexion
- Malwares voleurs d'informations qui, comme leur nom l'indique, dérobent des données telles que des coordonnées et des mots de passe de navigateur

Les pertes en dollars consécutives à des détournements de salaires ont connu une hausse vertigineuse de 815 % entre le 1er janvier 2018 et le 30 juin 2019[6].

— FBI

Les trois types d'attaques BEC

Dès lors que le cybercriminel dispose de toutes les informations nécessaires pour mener à bien une attaque BEC, il lance généralement un des types d'attaque suivants :

Détournement de salaires ou de paiements

Cette technique d'attaque consiste à demander directement de l'argent.

Dans le cas d'une campagne de **détournement de salaires**, le cybercriminel usurpe l'identité de collaborateurs ou utilise des compte compromis pour tenter de faire virer les salaires sur son propre compte bancaire.

Dans une attaque de **détournement de paiements**, le cybercriminel se fait par exemple passer pour un expéditeur externe, tel qu'un fournisseur, et demande aux responsables de l'entreprise de régler une facture sur un compte bancaire différent du compte habituel (à savoir, sur son propre compte).

6 FBI, « Business Email Compromise: The $26 Billion Scam » (Piratage de la messagerie en entreprise : des arnaques chiffrées à 26 milliards de dollars), septembre 2019.

Si les attaques de détournement de salaires et de paiements ont un objectif simple, elles sont en revanche relativement complexes à mettre en œuvre. Tout d'abord, elles nécessitent de collecter de nombreux renseignements. Le cybercriminel doit identifier précisément un collaborateur du département des ressources humaines (RH) ou de gestion de salaires, et les ressources publiques, telles que LinkedIn, le site Web de l'entreprise et les bases de données commerciales constituent de précieuses sources à cette fin.

Reste encore une étape délicate pour les fraudeurs : faire montre d'une familiarité crédible avec le processus de gestion des salaires ou de règlement des factures de l'entreprise pour ne pas éveiller les soupçons de la cible.

Déroulement d'une attaque de détournement de salaires et de paiements

1. Le cybercriminel contacte le département RH ou de gestion des salaires.

Un cybercriminel contacte le département RH ou de gestion des salaires par email en se faisant passer pour un collaborateur de l'entreprise et lui demande de mettre à jour les informations du compte sur lequel est versé le salaire. (Le numéro de routage et le numéro du nouveau compte appartiennent au cybercriminel et pas au collaborateur dont l'identité a été usurpée.)

2. Le département RH ou de gestion des salaires modifie le compte.

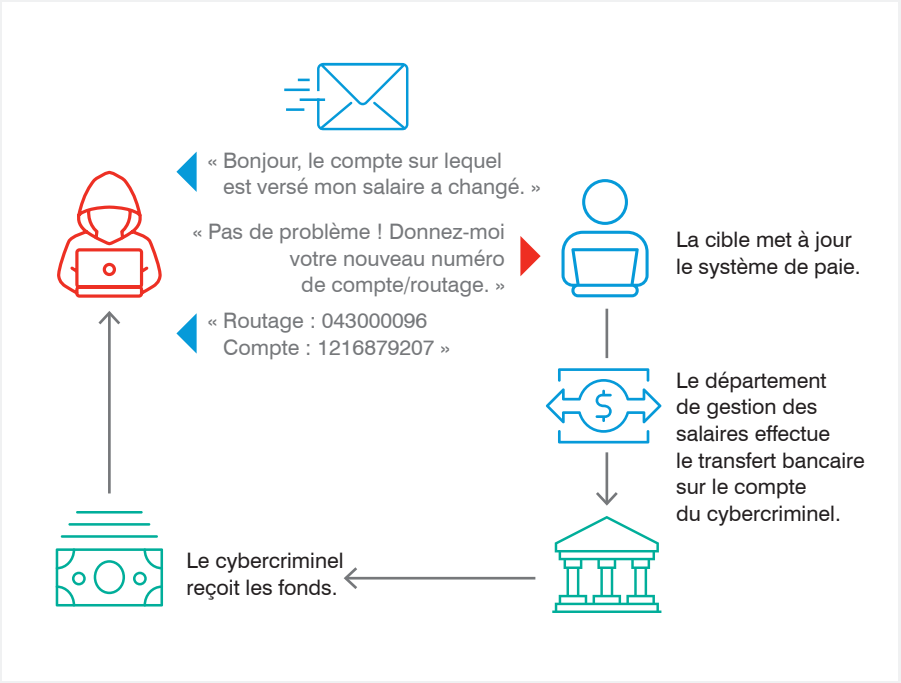
Pensant que la demande est légitime, le département RH ou de gestion des salaires modifie les informations bancaires.

3. Le salaire est envoyé.

Le salaire suivant du collaborateur est versé sur le compte du cybercriminel.

4. Le cybercriminel retire l'argent.

Le cybercriminel retire l'argent et clôture le compte avant que le collaborateur ne s'aperçoive qu'il n'a pas été payé.



Escroqueries aux cartes-cadeaux

Imaginons que vous receviez un email de votre supérieur vous demandant d'acheter quelques cartes-cadeaux auprès d'un détaillant connu. Il vous explique qu'il a l'intention de les offrir aux membres de l'équipe afin de les récompenser pour leur travail sur un projet récent. Comme vous êtes en télétravail, il vous demande également de lui envoyer les codes de ces cartes pour simplifier leur utilisation par les destinataires.

Quelle sera votre attitude : mettre en doute cette demande ou y répondre sans réfléchir ? Dans le dernier cas, sachez que vous n'êtes pas le seul et que vous serez malheureusement tombé dans le panneau

Selon la Federal Trade Commission (FTC), depuis 2018, les consommateurs ont déclaré avoir dépensé près de 245 millions de dollars en achats de cartes-cadeaux qu'ils ont utilisées pour payer des cybercriminels dans le cadre d'un large éventail d'escroqueries[7]. En outre, d'après le Better Business Bureau (BBB), dans plus d'un tiers (35 %) des escroqueries ciblant les entreprises, qui incluent les attaques BEC, les fraudeurs demandent aux victimes d'acheter des cartes-cadeaux[8].

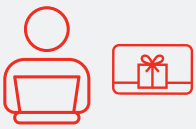
Pourquoi les cybercriminels demandent-ils à leurs victimes de leur envoyer des cartes-cadeaux ? Parce qu'il s'agit d'une source de revenus rapide et simple. Cette technique ne nécessite aucun transfert bancaire complexe, ce qui évite d'éveiller les soupçons de la victime et permet de contourner les contrôles financiers habituels de l'entreprise.

De plus, les cartes-cadeaux sont un outil idéal pour le blanchiment d'argent. Les fraudeurs peuvent les utiliser pour acheter et revendre des marchandises ou simplement vendre les codes au rabais en ligne. Et une fois les cartes-cadeaux utilisées, il est impossible de récupérer l'argent.

Déroulement des attaques aux cartes-cadeaux

1. Le cybercriminel usurpe l'identité d'un collaborateur/ami/PDG.

Un cybercriminel usurpe l'identité d'une personne de confiance de l'entreprise, telle que le PDG, et envoie un email à une cible (un assistant de direction, par exemple) pour lui demander d'acheter des cartes-cadeaux. Le cybercriminel explique que ces cartes-cadeaux sont destinées à des collaborateurs, des clients ou des fournisseurs. Il demande également à la victime de lui envoyer les numéros des cartes et les codes nécessaires pour les utiliser.



2. L'utilisateur ciblé achète les cartes-cadeaux et envoie les informations demandées.

La victime exécute la demande.

3. Le cybercriminel reçoit les fonds.

Le cybercriminel encaisse les cartes ou les échange contre des marchandises, qu'il revend ensuite. Il peut également vendre les codes directement au marché noir.

7 FTC, « FTC Data Show Gift Cards Remain Scammers' Favorite Payment Method » (Les données de la FTC montrent que les cartes-cadeaux demeurent le mode de paiement privilégié des cyberescrocs), décembre 2010.

8 Better Business Bureau, « BBB Investigation on gift card payment scams: Why do scammers love gift cards? » (Enquête du BBB sur les arnaques aux cartes-cadeaux : pourquoi les cyberescrocs apprécient autant les cartes-cadeaux), mars 2021.

Fraude aux factures fournisseurs

Sur une période de sept jours début 2021, 98 % des entreprises ont été ciblées par des attaques reposant sur un compte fournisseur usurpé ou compromis.

Ce type de fraude, comme son nom l'indique, consiste pour un cybercriminel à se faire passer pour un revendeur, un fournisseur ou un autre partenaire commercial de l'entreprise pour obtenir le paiement d'une facture factice. Parmi les tactiques utilisées par les fraudeurs, citons l'usurpation de l'adresse email d'un fournisseur légitime ou la prise de contrôle du compte de messagerie d'un des collaborateurs du fournisseur.

La fraude aux factures fournisseurs connaît un succès croissant. En effet, de plus en plus de cybercriminels utilisent la chaîne logistique et l'écosystème de partenaires comme vecteur de menaces pour lancer des attaques indirectes à l'encontre des entreprises ciblées. Les données suivantes donnent à réfléchir :

- Sur une période de sept jours début 2021, 98 % des entreprises ont été ciblées par des attaques reposant sur un compte fournisseur usurpé ou compromis[9].
- Les usurpations d'identité et les compromissions de compte de fournisseurs représentent un quart des emails de phishing[10].

Les cybercriminels usurpent l'identité de revendeurs de matériel de bureau, d'agences de conception de sites Web, d'entreprises de marketing, de services de nettoyage, de traiteurs, de services de lutte contre les parasites, etc. Et comme de nombreuses entreprises, en particulier les plus grandes, manquent de visibilité sur leur chaîne logistique, l'usurpation d'identité peut perdurer un certain temps. De fait, la plupart des entreprises ignorent combien elles ont de fournisseurs, et si l'un d'eux peut poser un risque.

Des perspectives de gains élevés

La fraude aux factures fournisseurs est souvent responsable des principales pertes financières imputables aux attaques BEC en raison des montants élevés des paiements B2B en jeu[11]. L'efficacité de ces escroqueries s'explique par le fait qu'elles exploitent des processus métier courants et utilisent généralement les comptes de messagerie légitimes de fournisseurs ou d'autres partenaires commerciaux en qui les victimes ont confiance. Ces comptes légitimes compromis échappent à la plupart des contrôles de sécurité.

Certains cybercriminels particulièrement audacieux et habiles se font même passer pour des fournisseurs qui n'existent pas et arrivent quand même à leurs fins. Ainsi, un fraudeur et quelques complices ont réussi à soutirer plus de 100 millions de dollars à Google et Facebook entre 2013 et 2015 grâce à une fraude complexe aux factures fournisseurs. Ils ont créé une fausse société en Lettonie utilisant le nom d'une vraie société basée à Taïwan avec laquelle ces entreprises technologiques entretenaient des relations commerciales. Google et Facebook ont toutefois eu de la chance : les cybercriminels ont été arrêtés et les deux sociétés ont pu récupérer tout ou partie de leur argent[12].

9 Sara Pan (*Proofpoint*), « 98% of Organizations Received Email Threats from Suppliers: What You Should Know » (98 % des entreprises ont reçu des menaces transitant par des emails de fournisseurs : ce qu'il faut savoir), février 2021.

10 Ibid.

11 Sara Pan (*Proofpoint*), « FBI Internet Crime Report Shows that Email Fraud Represents the Largest Financial Losses in 2020 » (Le rapport « Internet Crime Report » du FBI révèle que la fraude par email est la menace qui a occasionné le plus de pertes financières en 2020), mars 2021.

12 Vanessa Roma (*NPR*), « Man Pleads Guilty to Phishing Scheme That Fleeced Facebook, Google of $100 Million » (Un homme plaide coupable pour une attaque de phishing qui a réussi à soutirer 100 millions de dollars à Facebook et Google), mars 2019.

De : Chris@fournisseur (compte fournisseur compromis)
À : Jason (cible)

External Message
Thanks Connie~

Dear Jason,

Hope you are well.
The following invoices are due or will be due in Apr. And now we haven't received the payment from you side.
Could you please help to arrange the payment in Apr? Thank you.

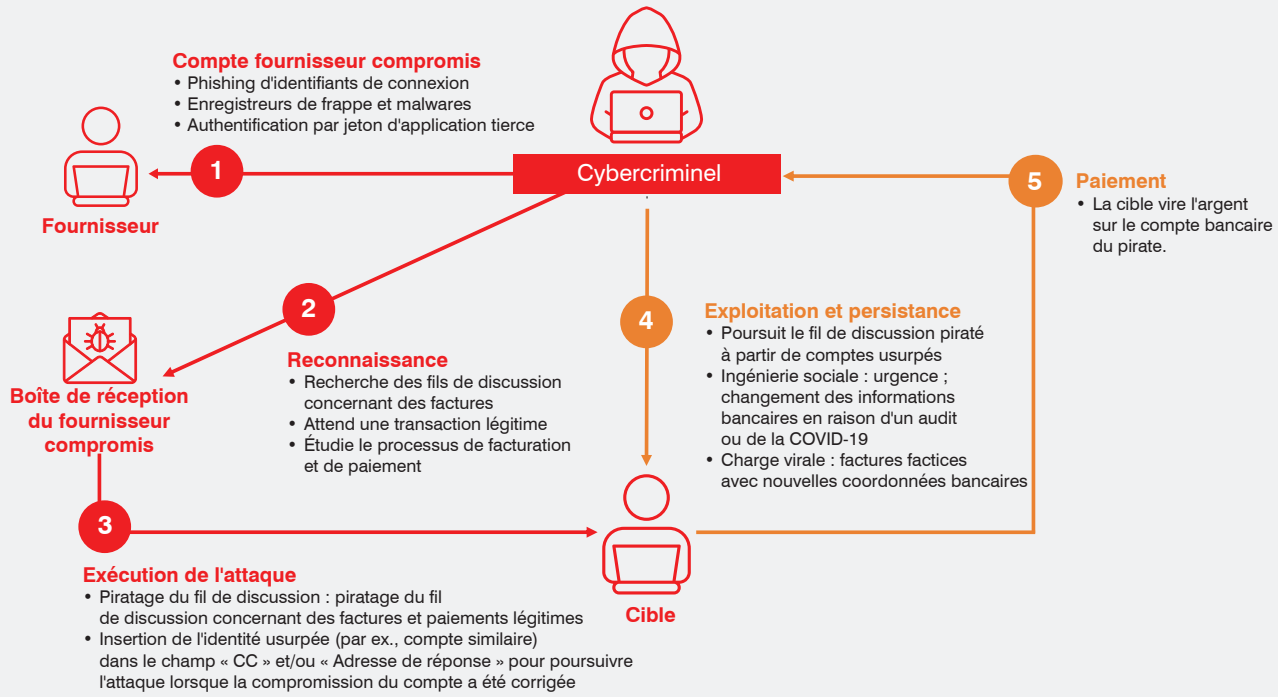
Total amount: USD 2,791,867.92

Class	Number	Amount(USD)	Days Late	Transaction Date	Due Date
Invoice		179,976.49	43	12-26-2019	03-10-2020
Invoice		15,328.07	34	01-04-2020	03-19-2020
Invoice		36,128.50	31	01-07-2020	03-22-2020
Invoice		29,744.80	31	01-07-2020	03-22-2020
Invoice		62,243.65	29	01-09-2020	03-24-2020
Invoice		9,306.72	28	01-10-2020	03-25-2020
Invoice		8,846.00	28	01-10-2020	03-25-2020
Invoice		1,873.20	28	01-10-2020	03-25-2020
Invoice		3,439.44	27	01-11-2020	03-26-2020
Invoice		54,257.82	27	01-11-2020	03-26-2020
Invoice		1,267.58	24	01-14-2020	03-29-2020
Invoice		11,290.40	22	01-16-2020	03-31-2020

Exemple d'email envoyé dans le cadre d'une tentative de fraude aux factures fournisseurs

Les cybercriminels qui recourent à la fraude aux factures fournisseurs n'hésitent pas à utiliser à la fois l'usurpation d'identité et la compromission de comptes pour voler des identifiants de connexion, distribuer des malwares et, bien sûr, envoyer de fausses factures. Si leur intention première est de soutirer de l'argent à leurs victimes, ils préparent également le terrain pour d'autres attaques dès que l'occasion se présente.

Déroulement des fraudes aux factures fournisseurs



1. Le pirate prend le contrôle d'un compte de messagerie.

Lors d'une fraude aux factures fournisseurs, le cybercriminel prend d'abord le contrôle d'un compte de messagerie d'un collaborateur d'un fournisseur de confiance ou crée un compte très similaire.

2. Le pirate recherche des emails concernant des factures.

Le cybercriminel analyse ensuite la liste des contacts du compte fournisseur compromis et recherche dans la boîte de réception de l'utilisateur les emails concernant des factures.

3. Le pirate exploite une transaction légitime.

Après avoir récupéré les informations sur les processus de facturation et de paiement de l'entreprise, le pirate attend l'occasion d'exploiter une transaction légitime.

4. Le pirate répond dans un fil de discussion existant.

À ce stade, le pirate opte pour un compte de domaine similaire et répond dans un fil de discussion existant pour conserver un accès à la conversation légitime, même si l'entreprise ciblée reprend le contrôle du compte.

5. Le pirate envoie une fausse facture.

Lorsque le fournisseur envoie une facture à l'entreprise ciblée, le pirate intervient et envoie une fausse facture à la place. Cette facture renseigne les coordonnées bancaires d'un compte appartenant au pirate et demande même parfois le changement des informations bancaires dont dispose actuellement l'entreprise cible pour ce fournisseur.

6. L'entreprise transfère l'argent sur le compte du pirate.

L'entreprise ciblée règle la facture et le versement arrive sur le compte du pirate. Avant que le vrai fournisseur ne se rende compte qu'il n'a pas été payé, le pirate aura retiré les fonds et clôturé le compte.

Six étapes pour protéger votre entreprise contre les attaques BEC

Les cybercriminels utilisent diverses tactiques et combinaisons d'usurpation d'identité et de compromission de comptes dans leurs attaques par email. Si chaque attaque est différente, toutes ont néanmoins un point en commun : elles doivent réussir à abuser la confiance de la victime pour parvenir à leurs fins.

Aucune ligne de défense ne permet à elle seule de prévenir ces attaques complexes, sophistiquées et furtives. Il est donc nécessaire d'adopter une approche multicouche totalement intégrée et centrée sur les personnes.

Voici les six principales stratégies nécessaires à la mise en place de ce type de système de défense :

1. Obtenir une visibilité sur les risques d'attaques BEC de vos utilisateurs

Une approche centrée sur les personnes commence inévitablement par les individus. Chaque personne est unique, tout comme sa valeur aux yeux des cybercriminels et le risque qu'elle représente pour votre entreprise. Le profil de risque global d'un utilisateur est formé d'une combinaison infinie de trois facteurs (vulnérabilité, attaques et privilèges).

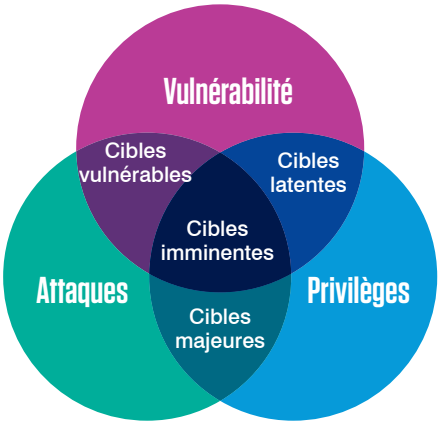
Pour déterminer le profil de risque de vos collaborateurs, vous devez évaluer les éléments suivants :

- **Habitudes numériques et points faibles (vulnérabilité).** Posez-vous les questions suivantes : Quel est le rôle de l'utilisateur ? De quelles autorisations dispose-t-il ? Quel est son mode de fonctionnement ? Sur quoi clique-t-il ? Comment accède-t-il aux ressources de l'entreprise ? À quels types d'applications et de données a-t-il accès ?
- **Types de menaces potentielles (attaques).** L'utilisateur est-il susceptible d'être confronté à une attaque très ciblée, de type BEC, et a-t-il dès lors besoin d'une protection renforcée et d'une formation de sensibilisation à la sécurité informatique ? Ou risque-t-il plutôt d'être victime de cybermenaces plus classiques pour lesquelles les défenses traditionnelles et une formation de base à la cybersécurité sont suffisantes ?
- **Niveau d'accès (privilèges).** Les privilèges désignent tous les éléments potentiellement de valeur auxquels un utilisateur a accès (données, autorité financière, relations clés, etc.). La position de l'utilisateur dans l'organigramme de l'entreprise (service financier ou direction, par exemple) est bien entendu un facteur à prendre en considération lors de l'évaluation des privilèges. Ce n'est cependant pas le seul facteur et, bien souvent, il est loin d'être le plus important.

Un niveau de risque élevé dans l'une de ces catégories est préoccupant et demande, dans la plupart des cas, l'implémentation de mesures de sécurité supplémentaires. Deux facteurs élevés ou plus sont le signe d'un problème de sécurité plus urgent.

Les quatre catégories d'utilisateurs suivantes montrent comment le cumul des vulnérabilités, des attaques et des privilèges peut affecter votre niveau de risque global :

- **Cibles latentes :** ces utilisateurs à haut niveau de privilèges sont également plus vulnérables aux leurres de phishing.
- **Cibles vulnérables :** ces utilisateurs sont très attaqués et exposés aux menaces.



ÉVALUATION DES RISQUES LIÉS AUX UTILISATEURS

Chaque collaborateur est unique. Sa valeur aux yeux des cybercriminels et les risques qu'il représente pour l'employeur le sont également.

Les collaborateurs ont tous leurs propres **vulnérabilités**, habitudes numériques et points faibles. Ils sont **attaqués** de diverses manières et avec une intensité variable. Ils disposent en outre de différents niveaux de **privilèges** d'accès aux données, systèmes et ressources.

Ces facteurs se conjuguent pour déterminer le risque global posé par chacun d'eux.

- **Cibles majeures :** ces utilisateurs à haut niveau de privilèges et particulièrement ciblés doivent faire face à une vague ininterrompue d'attaques qui, si elles aboutissent, peuvent être très dommageables pour l'entreprise.
- **Cibles imminentes :** cette quatrième catégorie regroupe les utilisateurs à considérer par l'entreprise comme une priorité de sécurité majeure. Ces utilisateurs présentent des niveaux élevés des trois facteurs de risque que sont la vulnérabilité, les attaques et les privilèges. Autrement dit, ils sont exposés aux outils et tactiques des cybercriminels. Ils sont dans leur ligne de mire et ont accès à des données, systèmes et autres ressources dont la compromission pourrait entraîner des dégâts à long terme.

2. Renforcer la visibilité au niveau des fournisseurs

L'identification des collaborateurs les plus vulnérables, attaqués et à privilèges de votre entreprise est une étape indispensable pour prévenir les attaques BEC. Il ne faut cependant pas négliger l'importance de la chaîne logistique et de l'écosystème de partenaires comme vecteur de menaces utilisé par les cybercriminels pour lancer des attaques indirectes à l'encontre des entreprises ciblées. C'est pourquoi vous devez bénéficier d'une bonne visibilité sur la chaîne logistique de votre entreprise et comprendre les risques que peuvent poser certains tiers.

Vous devez identifier les fournisseurs à risque, les domaines qu'ils utilisent pour envoyer des emails à vos collaborateurs, ainsi que les utilisateurs généralement en contact avec ces fournisseurs.

Vous devez identifier les fournisseurs à risque, les domaines qu'ils utilisent pour envoyer des emails à vos collaborateurs, ainsi que les utilisateurs généralement en contact avec ces fournisseurs. Vous devez également connaître, dans la mesure du possible, les fournisseurs de vos fournisseurs. Prenez le temps de créer un catalogue de fournisseurs aussi détaillé que possible pour disposer d'une visibilité sur les risques associés.

Pour faciliter ce processus, vous pouvez choisir une solution qui se chargera automatiquement des tâches suivantes :

- Identifier vos fournisseurs et les domaines qu'ils utilisent pour envoyer des emails à vos collaborateurs
- Identifier les domaines similaires aux domaines de vos fournisseurs
- Identifier les menaces émanant des domaines de vos fournisseurs, notamment les imposteurs, les malwares, le phishing et le spam
- Valider les enregistrements DMARC de vos fournisseurs et bloquer les attaques d'usurpation des domaines de vos fournisseurs

3. Détecter et bloquer les attaques BEC avant qu'elles n'infiltrent l'entreprise

Cette troisième recommandation peut sembler évidente, mais n'oubliez pas que toutes les cyberdéfenses ne parviennent pas à détecter et à bloquer efficacement les tactiques d'usurpation d'identité.

Les attaques BEC ne sont pas des cybermenaces classiques. Pour les neutraliser, vous avez besoin de solutions et de stratégies avancées pour procéder à des analyses dynamiques et surveiller de près l'apparition de menaces potentielles. Une fonctionnalité de détection statique basée sur des règles ne suffit pas à identifier et à bloquer les attaques BEC compte tenu de l'évolution constante des techniques et des tactiques.

Où rechercher des signes d'attaques BEC ?

- Données d'en-tête de message
- Adresse IP de l'expéditeur
- Relation entre l'expéditeur et le destinataire
- Réputation de l'expéditeur
- Ressenti, ton et langage utilisés

La fraude aux factures fournisseurs, qui recourt à des comptes fournisseur légitimes mais compromis, est encore plus difficile à détecter. Votre système de défense doit être en mesure de bloquer toutes les attaques, même les fraudes aux factures fournisseurs les plus sophistiquées. Pour ce faire, vous avez besoin d'une solution qui analyse de façon dynamique les messages pour identifier les nombreuses tactiques associées aux fraude aux factures fournisseurs.

Tactiques de fraude aux factures fournisseurs

- Détournement d'adresses de réponse
- Utilisation d'adresses IP malveillantes
- Utilisation de domaines de fournisseurs dont l'identité a été usurpée
- Mots ou expressions couramment employés dans les fraudes aux fournisseurs

Apprentissage automatique

Contrairement aux outils d'ancienne génération, les outils basés sur l'apprentissage automatique peuvent s'adapter aux menaces BEC les plus récentes sans nécessiter d'ajustements manuels continus.

Contrairement aux outils d'ancienne génération, les outils basés sur l'apprentissage automatique peuvent s'adapter aux menaces BEC les plus récentes sans nécessiter d'ajustements manuels continus. Le système d'apprentissage automatique le plus efficace peut réagir rapidement à l'évolution des tactiques d'attaque et bloquer les messages dangereux tout en autorisant la remise des emails inoffensifs.

Mais ne vous y trompez pas, l'apprentissage automatique seul n'est pas une solution miracle. L'efficacité des modèles d'apprentissage automatique dépend de l'étendue et de l'exhaustivité des données avec lesquelles ils sont entraînés, ainsi que des ressources humaines spécialisées dans la gestion de menaces qui permettent de les affiner. Les modèles entraînés à l'aide de données incorrectes ou incomplètes et dépourvues de contexte sur les menaces génèrent un taux élevé de faux positifs, qui alourdissent la charge de travail des équipes responsables de la sécurité et de la messagerie et nuisent à l'expérience utilisateur.

4. Renforcer la résilience des utilisateurs

Les attaques BEC s'appuient sur l'ingénierie sociale, pas sur des exploits techniques. Elles ne fonctionnent que si les utilisateurs tombent dans le piège. C'est pourquoi des collaborateurs correctement formés constituent votre dernière et meilleure ligne de défense.

Tous vos collaborateurs doivent être sensibilisés aux menaces d'imposteurs. Cependant, comme ces attaques visent des personnes spécifiques, votre formation de sensibilisation à la sécurité informatique doit cibler en priorité les collaborateurs des services comptabilité, financier, ressources humaines et approvisionnement, par exemple, afin qu'ils puissent détecter les tactiques d'usurpation courantes. Veillez également aux points suivants :

- Former de manière appropriée les collaborateurs des échelons supérieurs de l'entreprise (par ex., le PDG et le directeur financier).
- Inclure les collaborateurs qui présentent un risque plus élevé parce que plus vulnérables, attaqués ou à privilèges.
- Proposer une formation de sensibilisation à la sécurité informatique aux sous-traitants et aux travailleurs indépendants qui ont accès aux systèmes de l'entreprise. Ces collaborateurs sont souvent présents dans l'environnement du travail actuel, en particulier compte tenu de la dispersion croissante des effectifs et du recours au télétravail, mais sont fréquemment ignorés par les stratégies de sécurité.
- Aborder le risque de fraude aux factures fournisseurs avec les utilisateurs les plus susceptibles d'être confrontés à ce type d'attaque BEC

Les formations de sensibilisation à la sécurité informatique, de même que toute autre formation aux attaques BEC, ne doivent pas se faire de façon ponctuelle ou occasionnelle. Ces menaces, comme toutes les cybermenaces, ne cessent d'évoluer.

Faites appel à des prestataires externes spécialisés dans la formation de sensibilisation à la sécurité informatique pour offrir la formation adéquate aux personnes concernées. Vous pouvez, par exemple, procéder à des simulations de phishing nourries par des informations concernant des attaques BEC réelles afin d'aider vos collaborateurs à détecter les menaces auxquelles ils sont exposés.

Nous vous conseillons également d'encourager vos collaborateurs à signaler tout email suspect et de faciliter ce signalement. Les équipes de sécurité doivent également réagir rapidement lorsqu'un utilisateur signale un message et déterminer instantanément si cet email constitue ou non une menace. En l'absence de réponse rapide, les utilisateurs risquent d'hésiter à signaler les messages suspects par la suite et d'être moins vigilants avant d'ouvrir un email dangereux ou d'y répondre.

5. Automatiser la réponse aux incidents et la mise en quarantaine

L'automatisation des principaux aspects de l'analyse et de la correction des emails permet aux équipes de sécurité de prioriser leurs tâches et de traiter plus rapidement les menaces et les emails signalés par les utilisateurs.

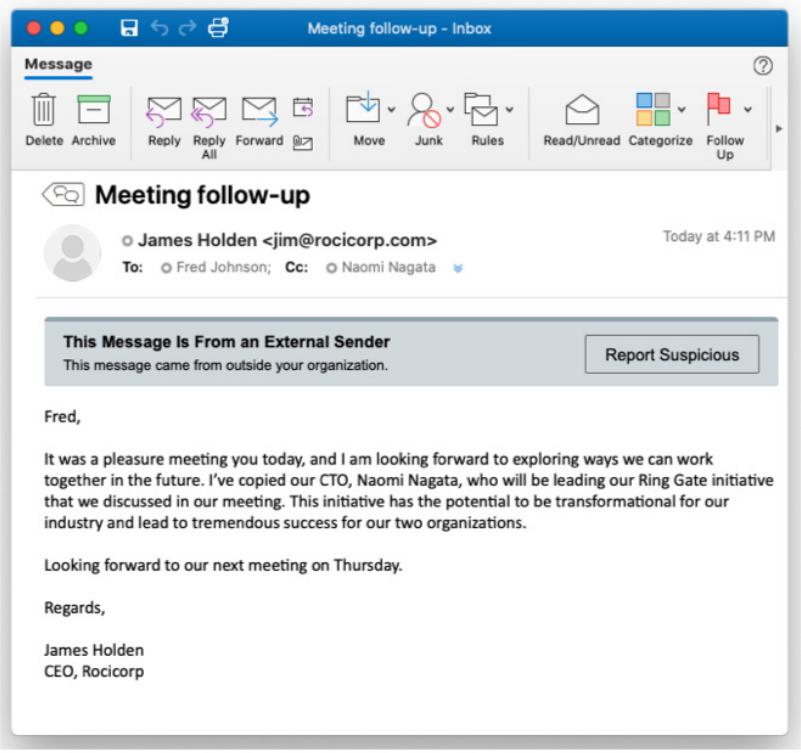
La plupart des entreprises souffrent de la pénurie de talents en matière de sécurité informatique. Les équipes de sécurité ont bien des difficultés à gérer les multiples fournisseurs et produits de sécurité, de surcroît rarement compatibles. Par conséquent, la détection, l'investigation et la neutralisation rapides des attaques BEC à l'échelle de l'entreprise s'avèrent compliquées. Et plus ces opérations prennent du temps, plus longtemps votre entreprise est exposée.

L'automatisation des principaux aspects de l'analyse et de la correction des emails permet aux équipes de sécurité de prioriser leurs tâches et de traiter plus rapidement les menaces et les emails signalés par les utilisateurs. Les équipes de sécurité doivent également permettre aux utilisateurs inquiets qui reçoivent un email suspect d'accéder, si nécessaire, aux informations qu'il contient pendant l'analyse du message.

Le marquage automatique des emails externes pour informer les destinataires de l'origine de l'email permet également aux utilisateurs de surveiller de plus près la légitimité de ces messages.

S'il s'avère que le message signalé est malveillant, ce dernier et toutes ses copies (y compris celles transférées à d'autres utilisateurs) sont automatiquement mis en quarantaine. Il n'est pas nécessaire de gérer ou d'analyser manuellement chaque incident, ce qui permet à votre équipe d'économiser du temps et de l'énergie.

Les utilisateurs reçoivent, quant à eux, un email personnalisé les informant qu'il s'agissait d'un message malveillant, ce qui a pour effet de renforcer les comportements positifs et encouragera les utilisateurs à signaler des messages similaires à l'avenir.



6. Protéger votre entreprise contre les attaques ciblant vos clients et votre marque

Vous devez donc opter pour une solution qui protège votre marque et la réputation de votre entreprise en empêchant l'envoi d'emails frauduleux via vos domaines de confiance.

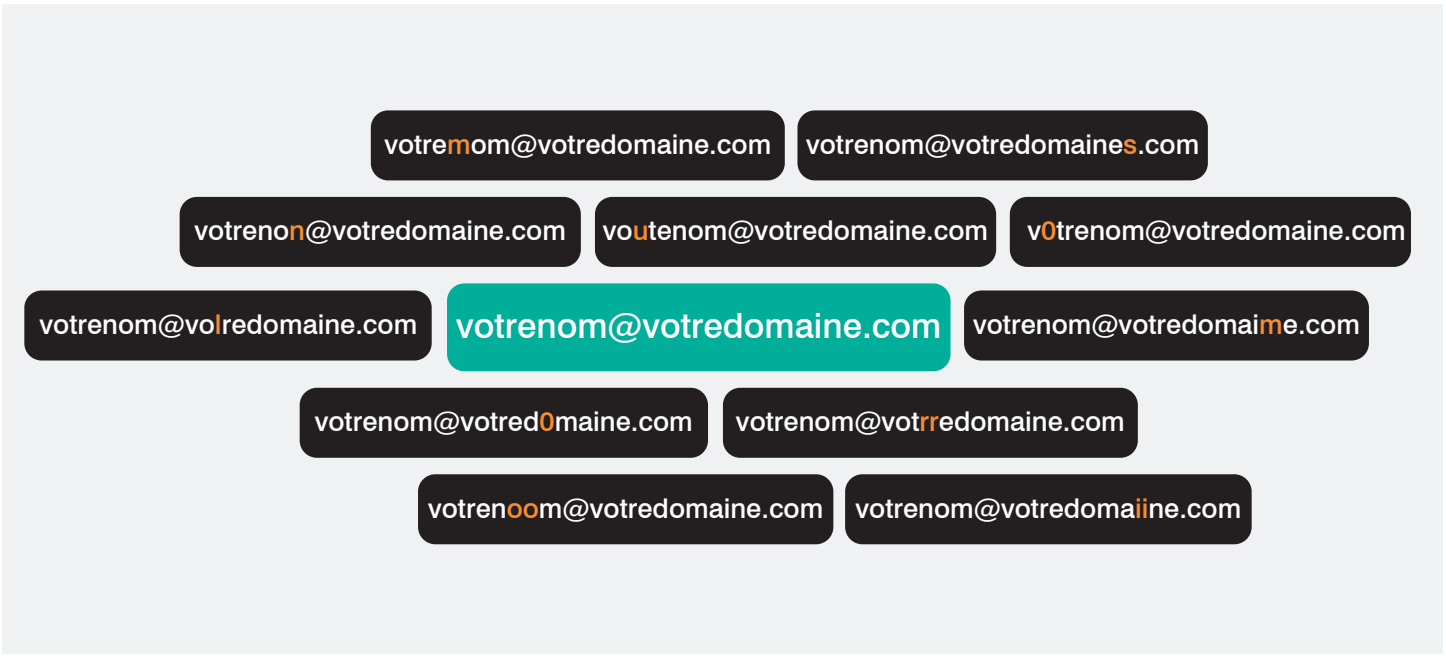
Dans le cas de l'usurpation de marque, les cybercriminels utilisent le nom et la marque de votre entreprise pour piéger vos clients et vos partenaires commerciaux et leur voler de l'argent.

L'usurpation de marque n'a pas forcément de répercussions financières directes pour votre entreprise. En revanche, elle peut entacher sa réputation, ébranler la confiance des clients et avoir des conséquences négatives à long terme.

Vous devez donc opter pour une solution qui protège votre marque et la réputation de votre entreprise en empêchant l'envoi d'emails frauduleux via vos domaines de confiance. Cette solution doit pouvoir vérifier l'ensemble des emails reçus et envoyés par votre entreprise grâce à des contrôles DMARC (Domain-based Message Authentication, Reporting and Conformance).

Elle doit également repérer tous les emails envoyés via votre domaine, y compris par des expéditeurs tiers de confiance.

Même si vous avez verrouillé votre domaine, des domaines similaires peuvent être créés. Ces domaines similaires malveillants peuvent amener vos collaborateurs à tomber dans le piège d'emails BEC semblant provenir de votre entreprise. Recherchez les domaines récemment enregistrés usurpant l'identité de votre marque dans des attaques par email ou sur des sites Web de phishing avant qu'ils ne soient activés et ne piègent vos collaborateurs. Cela vaut aussi pour les cybercriminels qui usurpent votre marque sur d'autres canaux numériques, comme les domaines Web, les réseaux sociaux et les Darknets non approuvés.



Conclusion : la puissance d'une défense unifiée centrée sur les personnes

Pour mettre en place une approche multicouche, totalement intégrée et centrée sur les personnes capable de protéger votre entreprise contre les attaques BEC, vous devez abandonner les produits de sécurité isolés traditionnels. Même si vous disposez de produits isolés qui couvrent les différents aspects d'une attaque, il est essentiel que ces éléments collaborent étroitement et se renforcent mutuellement.

Avec une solution de protection de la messagerie unifiée ou intégrée, vous pouvez rationnaliser vos opérations de sécurité et optimiser l'utilisation de vos ressources informatiques. Vous réduirez également les coûts et les tâches manuelles. Et surtout, vous protégerez plus efficacement votre entreprise contre les attaques BEC en constante évolution.

Pour en savoir plus sur les solutions Proofpoint conçues pour protéger votre entreprise contre les attaques BEC, consultez la page :

proofpoint.com/us/solutions/bec-and-eac-protection.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) 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.

0503-004-01-01 06/21