proofpoint.

EBOOK

Cinq cyberattaques réelles et comment les neutraliser

Vol. 1 : attaques d'ingénierie sociale

proofpoint.com/fr

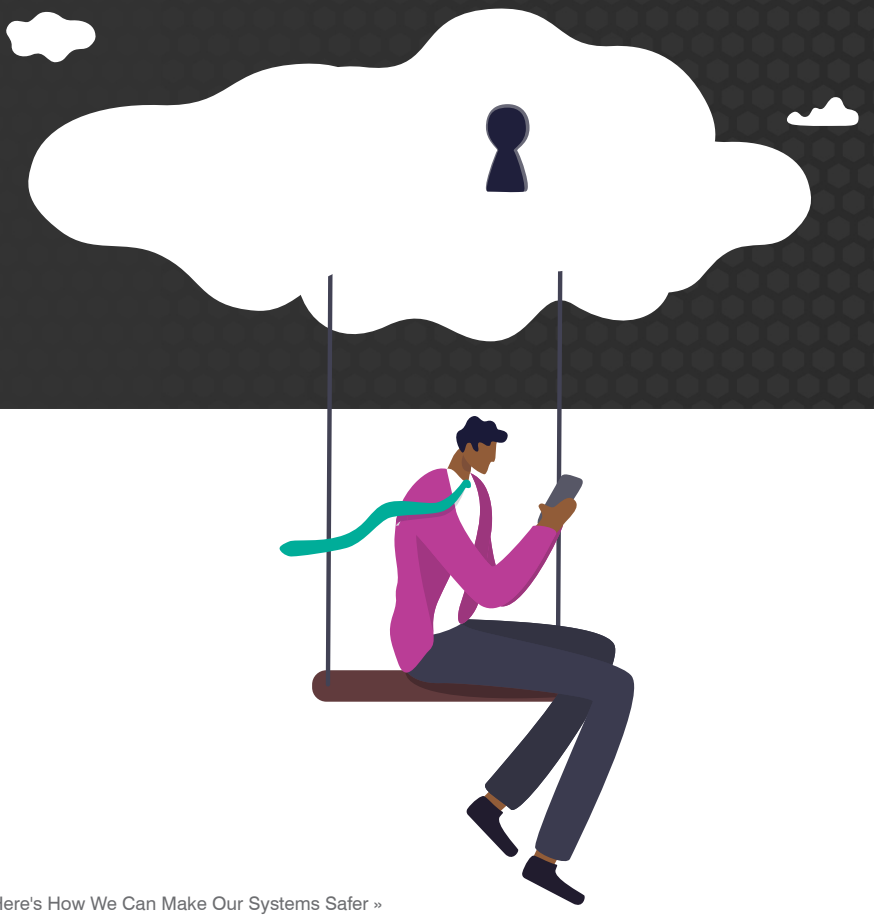
Introduction

Les cybercriminels sont habiles et extrêmement motivés. Pourquoi ne le seraient-ils pas ? Ils évoluent dans un secteur à forte croissance où les risques sont faibles et les bénéfices si importants que la cybercriminalité devrait coûter au monde 23,8 billions de dollars par an d'ici 2027[1].

Face à de telles perspectives de profits, la créativité dont font preuve les cyberpirates semble infinie. De nouvelles campagnes de malwares, attaques de phishing et tactiques d'ingénierie sociale ingénieuses voient quotidiennement le jour, les équipes de sécurité jouant au chat et à la souris avec les cybercriminels. Bien que ces nouvelles menaces puissent sembler infiniment variées, elles présentent un certain nombre de points communs : elles sont véhiculées par la messagerie et ciblent des personnes.

Dans cette série d'eBooks, nous nous pencherons sur certaines des attaques par email les plus insidieuses actuellement en circulation. Bon nombre d'entre elles ont franchi les défenses de plusieurs outils de sécurité avant d'être détectées. Pour vous aider à comprendre pourquoi, nous analyserons chaque attaque pas à pas afin de vous montrer comment elles se sont déroulées et comment les cybercriminels ont essayé d'exploiter les vulnérabilités humaines. Nous vous expliquerons ensuite comment elles ont été neutralisées.

Ce volume se penche sur les attaques ayant recours à l'ingénierie sociale. Dans le volume 2, nous nous intéresserons à des attaques plus techniques.



1 Forum économique mondial, « 2023 Was a Big Year for Cybercrime – Here's How We Can Make Our Systems Safer » (2023 a été une excellente année pour les cybercriminels – voici comment renforcer la sécurité de nos systèmes), janvier 2024.

Sommaire

SECTION 1

Attaques BEC et de la chaîne logistique

Lors des attaques par piratage de la messagerie en entreprise (BEC, Business Email Compromise), un cybercriminel se fait passer pour une personne ou une entité en laquelle un destinataire a confiance, comme un collègue, un fournisseur ou un partenaire. Bon nombre des attaques BEC actuelles sont très sophistiquées, bien financées et soutenues par une planification et des recherches minutieuses.

Depuis quelques années, ces attaques sont source de bénéfices faramineux pour les cybercriminels. D'après le *rapport 2023 Internet Crime Report du FBI*, elles ont coûté 17 milliards de dollars aux entreprises américaines. À l'échelle mondiale, les attaques BEC ont coûté aux entreprises la bagatelle de 50 milliards de dollars[2], tandis que les victimes de ransomwares ont perdu 1,1 milliard de dollars[3].

2 FBI, « Business Email Compromise: The $50 Billion Scam » (Piratage de la messagerie en entreprise : des arnaques chiffrées à 50 milliards de dollars), juin 2023.

3 Wired, « Ransomware Payments Hit a Record $1.1 Billion in 2023 » (Les paiements de rançon atteignent la somme record de 1,1 milliard de dollars en 2023), février 2024.

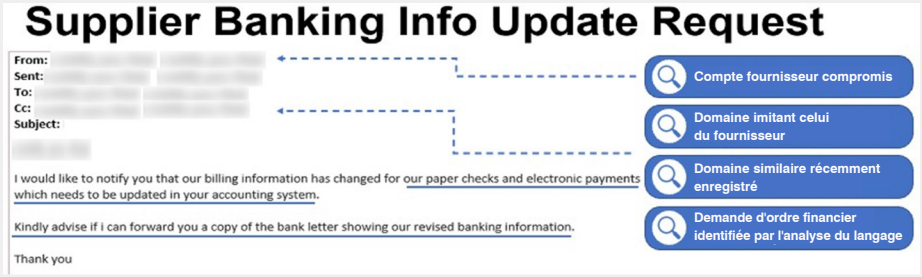
Le scénario

Proofpoint a détecté cet incident BEC chez un groupe mondial de la grande distribution comptant plus de 40 000 utilisateurs. La menace émanait de la chaîne logistique du groupe et a échappé à la détection de son outil de sécurité. Cet exemple est intéressant, car il met en avant le rythme effréné auquel le paysage de la cybersécurité évolue.

Le déroulement de l'attaque

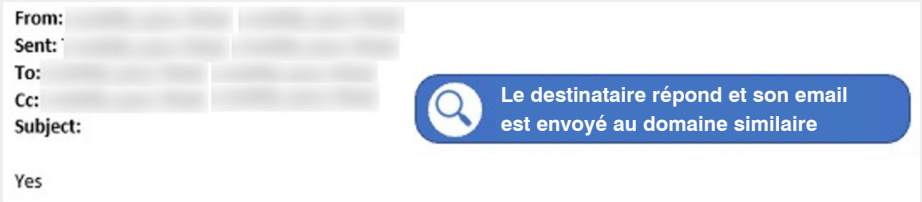
Examinons plus en détail le déroulement de l'attaque.

1. **Le message de leurre.** Le groupe mondial de la grande distribution a reçu un email d'un expéditeur de sa chaîne logistique qui demandait la mise à jour de ses informations de paiement. Cette demande en apparence inoffensive était en réalité malveillante, car le compte de l'expéditeur avait été compromis.



Email initial du cybercriminel, accompagné des observations de l'équipe d'investigation numérique de Proofpoint

2. **Le domaine similaire malveillant.** Le cybercriminel souhaitait rediriger les emails de réponse vers un domaine similaire récemment enregistré. Son objectif était d'intercepter des données sensibles et de détourner des fonds.



Réponse du client, envoyée à un domaine similaire

Pourquoi ces menaces sont difficiles à détecter

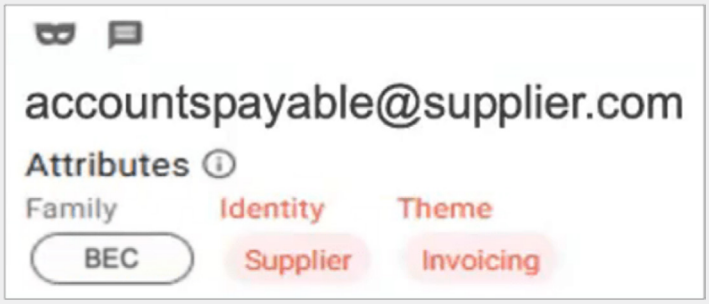
Les attaques BEC sont très difficiles à détecter, car elles ne contiennent pas les charges virales que nous avons l'habitude d'analyser, à savoir des URL ou des pièces jointes malveillantes. Les cybercriminels s'appuient plutôt sur l'usurpation d'identité et d'autres techniques d'ingénierie sociale pour piéger les utilisateurs.

L'outil de sécurité du groupe est passé à côté de cette menace pour diverses raisons. Pour commencer, il accordait une trop grande importance à l'âge du domaine comme facteur de détection. Par ailleurs, il n'était pas capable d'identifier les domaines similaires. Enfin, il n'analysait pas l'adresse de réponse, ce qui lui aurait permis de détecter la redirection vers un nouveau domaine.

Comment Proofpoint a détecté l'attaque

Pour identifier de nombreux types de menaces, telles que les attaques BEC et le phishing d'identifiants de connexion, il est essentiel de combiner l'âge du domaine avec d'autres indicateurs d'intention malveillante. C'est la raison pour laquelle Proofpoint utilise une approche multicouche. Notre moteur de détection s'appuie sur l'intelligence artificielle (IA), l'apprentissage automatique et l'analyse comportementale pour identifier les principaux indicateurs de compromission. Il identifie notamment les modèles d'emails suspects.

Dans cet exemple, Proofpoint a identifié des termes indiquant que l'email contenait une demande de nature financière. Si la demande ne paraissait pas inhabituelle en soi, associée au changement d'adresse de réponse, elle était suspecte. En outre, le domaine avait été enregistré le jour même de l'envoi de l'email.



Le tableau de bord Proofpoint Targeted Attack Protection (TAP) catégorise chaque menace. Dans cet exemple, il montre que nous avons identifié la menace comme une attaque BEC, que celle-ci émanait d'un fournisseur et qu'il était question de facturation.

SECTION 2

Phishing par signature électronique

Le phishing par signature électronique est une menace qui incite un destinataire à divulguer ses identifiants de connexion ou d'autres informations personnelles au moyen d'un message qui demande sa signature. Le message peut inclure un contrat ou une facture à signer en pièce jointe.

En 2023, au cours d'un seul mois, Proofpoint a détecté plus de 75 000 menaces différentes comme celle ci-dessous.

Le scénario

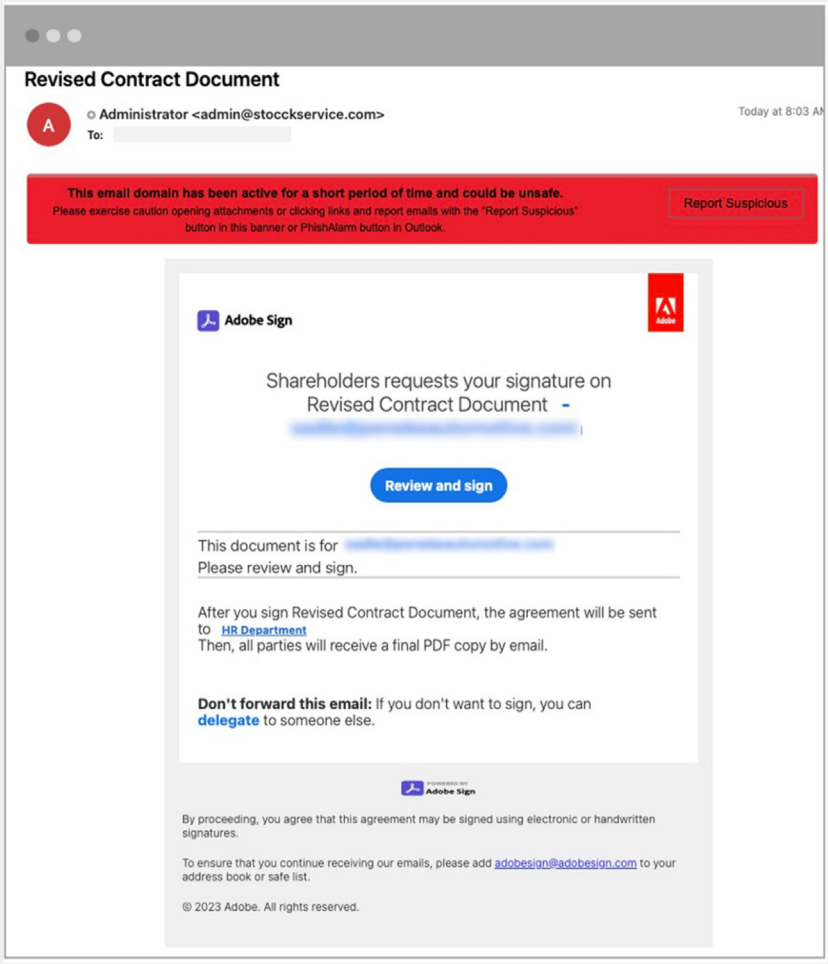
Proofpoint a détecté une menace de collecte d'identifiants de connexion qui était hébergée sur l'application SaaS Amazon Web Services (AWS) Amplify. L'application était utilisée par notre client, une entreprise automobile comptant 2 000 collaborateurs.

Un cybercriminel avait créé un leurre de phishing qui ressemblait à un lien vers un document sensible, à savoir un contrat mis à jour qui devait être consulté et contresigné. La cible était un collaborateur travaillant avec des contrats et ayant d'autres responsabilités fiduciaires, qui communique souvent avec des membres du conseil d'administration, des clients et des fournisseurs dans le cadre de son travail. Il n'était donc pas inhabituel qu'il reçoive ce type de demande.

Le déroulement de l'attaque

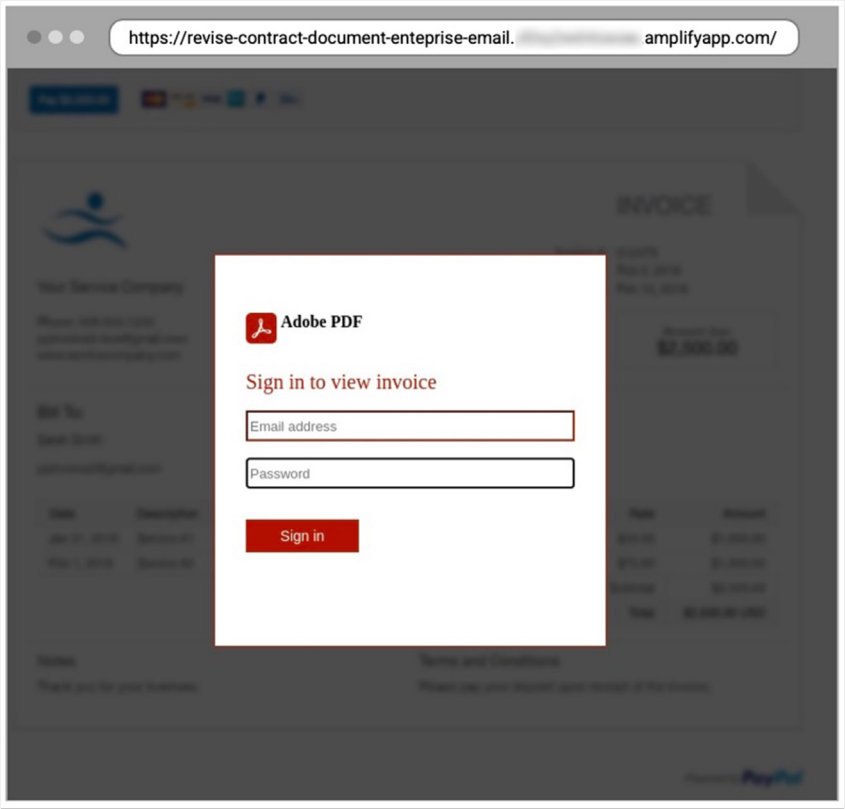
Examinons plus en détail le déroulement de l'attaque.

1. **Le message de leurre.** Notre client a reçu un email invitant le collaborateur à consulter et à signer un contrat mis à jour.



L'email malveillant

2. **L'URL malveillante.** Si le collaborateur avait cliqué sur l'URL malveillante, il aurait vu s'afficher un écran de connexion conçu pour ressembler à d'autres écrans de connexion légitimes. L'objectif du cybercriminel était d'inciter le collaborateur à divulguer ses identifiants de connexion.



Fausse page de connexion hébergée sur amplifyapp.com

Pourquoi ces menaces sont difficiles à détecter

Des applications telles qu'AWS Amplify et d'autres services SaaS comme DocuSign, Adobe Sign et OpenSpan Sign sont souvent utilisés dans ces attaques. Ils offrent aux cybercriminels un moyen simple de distribuer du contenu malveillant en apparence légitime.

Dans ce scénario, le domaine de l'URL avait plus de cinq ans. L'adresse IP appartenait à Amazon, ce qui aboutirait probablement à un verdict de légitimité. La plupart des éditeurs de solutions de protection de la messagerie sont capables de détecter une attaque de phishing d'identifiants de connexion standard. Toutefois, le domaine de confiance du fournisseur SaaS complique la tâche de la plupart des moteurs de détection. Preuve en est, 19 autres éditeurs de solutions de protection de la messagerie, dont un grand nombre prétendent avoir recours à des technologies d'IA et d'apprentissage automatique avancées pour bloquer ces attaques, n'ont pas intercepté cette menace.

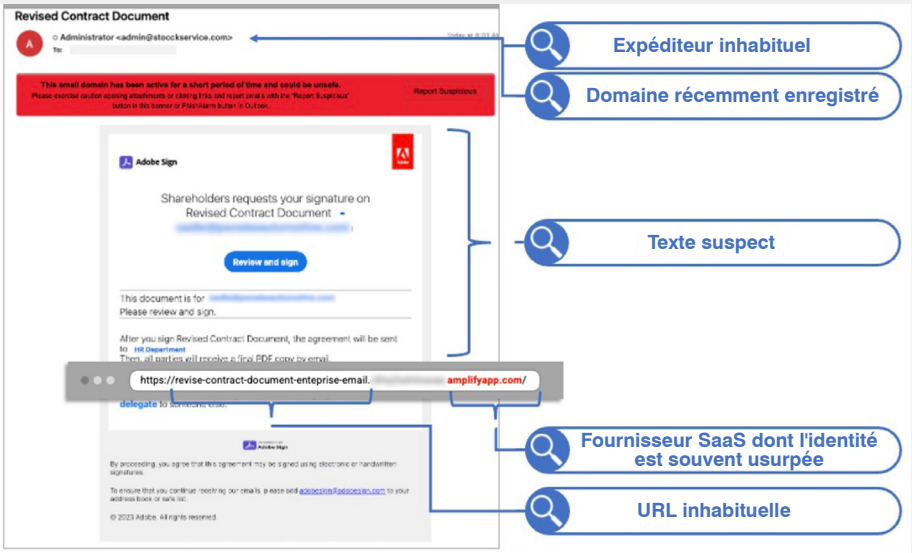
Comment Proofpoint a détecté l'attaque

Le moteur d'IA comportementale de Proofpoint s'appuie sur plusieurs signaux au niveau des messages pour détecter et bloquer un éventail de menaces. Nous pouvons donc détecter les menaces de phishing encore inconnues à un stade plus précoce de la chaîne d'attaque afin de les bloquer avant leur remise.

Proofpoint a procédé à une analyse multicouche approfondie du profil de l'utilisateur et a identifié une combinaison expéditeur/destinataire inhabituelle sur la base des schémas de communication antérieurs. Nous avons découvert que l'expéditeur communiquait rarement avec le destinataire ou tout autre collaborateur de l'entreprise automobile.

Grâce à l'IA comportementale et à l'apprentissage automatique, Proofpoint a procédé à une analyse approfondie de l'URL, afin d'évaluer la pertinence de l'URL en fonction des points de données historiques et d'autres activités inhabituelles. Après examen des comportements d'envoi de toute l'entreprise, il a été établi que l'URL n'avait jamais été utilisée par le destinataire ni par aucun autre collaborateur de l'entreprise.

Proofpoint a également détecté l'utilisation du domaine d'un fournisseur SaaS légitime et réputé. Dans d'autres entreprises dont nous assurons la protection, nous avons constaté que des cybercriminels exploitaient ce même domaine pour distribuer du contenu malveillant.



Résumé des observations de Proofpoint concernant l'email de signature électronique ayant conduit à son signalement

SECTION 3

Menaces TOAD

Les tactiques d'ingénierie sociale continuent d'évoluer à mesure que les cybercriminels cherchent de nouveaux moyens créatifs d'obtenir un accès initial à des systèmes sensibles. Les attaques par téléphone (TOAD, Telephone-Oriented Attack Delivery) en sont la preuve. Les cyberpirates envoient des emails aux destinataires et tentent de les convaincre d'appeler un faux centre d'appels.

Les utilisateurs ne sont généralement pas protégés contre les appels téléphoniques malveillants. C'est la raison pour laquelle il est primordial de bloquer ces emails. Ces attaques sont très difficiles à détecter, car, souvent, elles ne contiennent pas d'URL ou de pièces jointes.

En 2023, au cours d'un seul mois, Proofpoint a détecté plus de 19 000 menaces TOAD ayant échappé à 14 outils de protection de la messagerie différents.

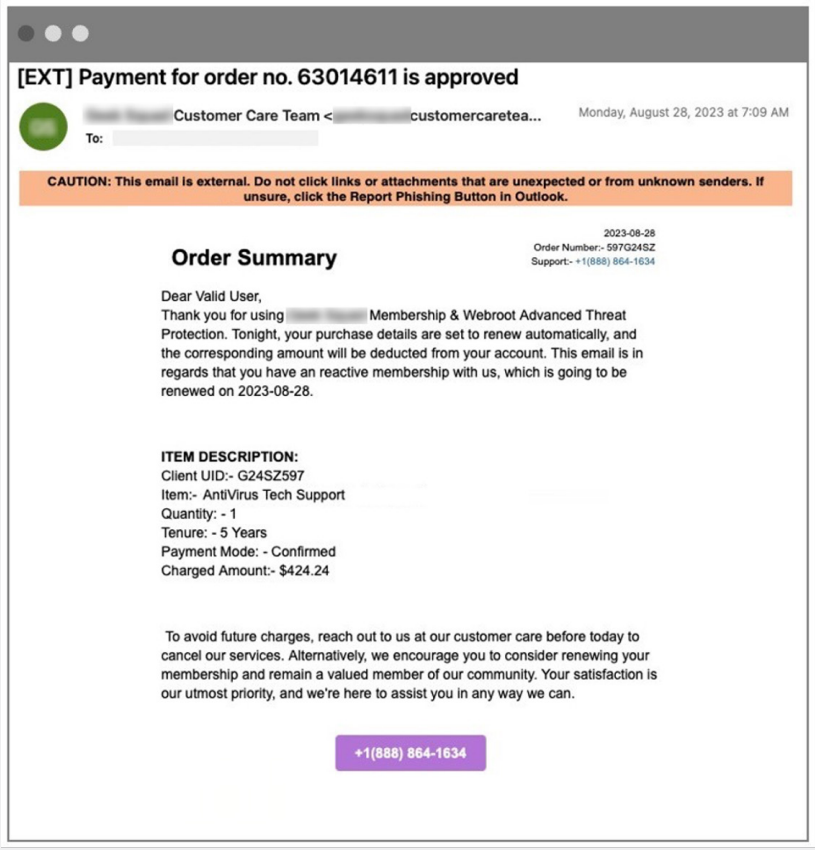
Le scénario

Proofpoint a détecté une menace TOAD dans une entreprise de fabrication comptant plus de 45 000 collaborateurs. Un cyberpirate qui prétendait travailler pour un éditeur de logiciels antivirus renommé a envoyé un message frauduleux à l'un de ses collaborateurs. Plutôt que d'ajouter des URL ou des pièces jointes à son message, le cybercriminel y a inclus un numéro de téléphone.

Le déroulement de l'attaque

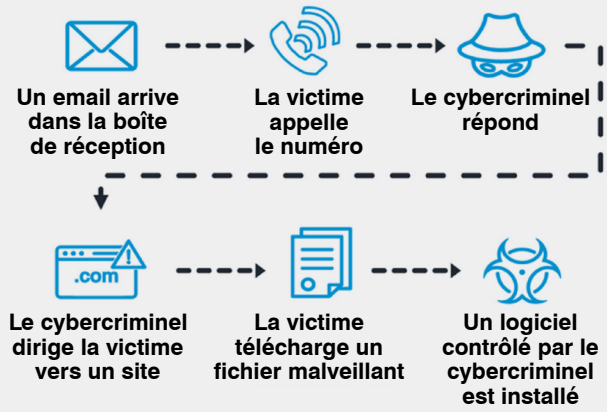
Examinons plus en détail le déroulement de l'attaque.

1. **Le message de leurre.** Un email prétendait confirmer un achat auprès d'une entreprise technologique connue.



Email malveillant initial distribué dans la boîte de réception du destinataire

2. **La séquence d'attaque TOAD.** Si le collaborateur avait appelé ce numéro, le cybercriminel aurait pu l'inciter à cliquer sur une URL malveillante sur son ordinateur afin de déclencher diverses attaques, dont un accès à distance, le vol de données sensibles ou une infection de ransomware.



Aperçu d'une séquence d'attaque TOAD type

Pourquoi ces menaces sont difficiles à détecter

Les menaces TOAD peuvent être difficiles à détecter, car elles comportent rarement des charges virales malveillantes. Qui plus est, les cybercriminels ont souvent recours à des domaines connus appartenant à Google, à Microsoft ou à d'autres services de messagerie légitimes.

Comme cette menace TOAD a été envoyée à partir d'un domaine appartenant à Google, le message a été validé par les dispositifs d'authentification des emails tels que SPF (Sender Policy Framework) et DMARC. Ce message ne contenait pas non plus de charge virale malveillante, ce qui pourrait expliquer pourquoi l'outil de sécurité de l'entreprise de fabrication n'a pas intercepté la menace.

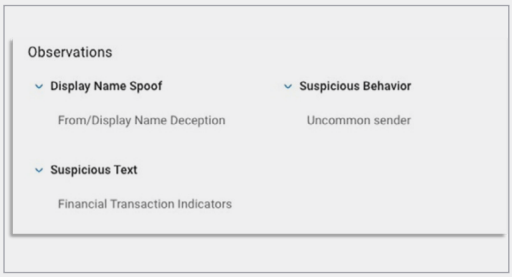
Comment Proofpoint a détecté l'attaque

Proofpoint a recours à l'IA avancée et à l'apprentissage automatique pour analyser et combiner divers indicateurs comportementaux en vue de détecter les menaces TOAD. Cette approche est plus fiable que le simple fait de suivre et de tenir une base de données des numéros de téléphone malveillants précédemment identifiés lors d'attaques TOAD.

Lorsque le moteur d'IA comportementale de Proofpoint a analysé ce message, il a identifié des termes relatifs à une transaction financière et à la nécessité d'agir de manière urgente, deux indicateurs d'un email potentiellement malveillant. Autre indice, les menaces TOAD incluent toujours un numéro de téléphone et exhortent le destinataire à l'appeler rapidement. C'est la raison pour laquelle Proofpoint analyse les messages afin de détecter les numéros de téléphone.

Nous avons procédé à une analyse multicouche, qui a également déterminé que le destinataire n'avait jamais reçu d'email de cet expéditeur, sur la base des schémas de communication antérieurs. En réalité, aucun collaborateur de l'entreprise n'avait jamais reçu d'email de cet expéditeur.

Lors d'attaques TOAD, les cybercriminels envoient souvent des messages qui semblent provenir d'une marque légitime pour essayer d'établir une relation de confiance implicite. Notre analyse a également détecté cette tactique.



Résumé des observations de Proofpoint ayant conduit au signalement

SECTION 4

Détournement de salaires

Le détournement de salaires est une forme d'attaque BEC. Les principales cibles de ces attaques sont les collaborateurs qui traitent les demandes relatives aux salaires. En général, un cybercriminel se fait passer pour un collaborateur qui a besoin de mettre à jour les informations du compte sur lequel est versé son salaire. Les nouvelles informations correspondent en réalité à un compte appartenant au cyberpirate. Une fois le changement effectué, les fonds perdus ne peuvent pas être récupérés par l'entreprise.

Le détournement de salaires n'est pas une nouvelle forme d'attaque BEC, mais sa fréquence s'accélère. Proofpoint continue à observer ce type de menace franchir les défenses d'autres outils de protection de la messagerie. Lors de nos récentes évaluations des menaces, nous avons découvert que plus de 400 de ces attaques avaient échappé à 12 autres outils de protection de la messagerie.

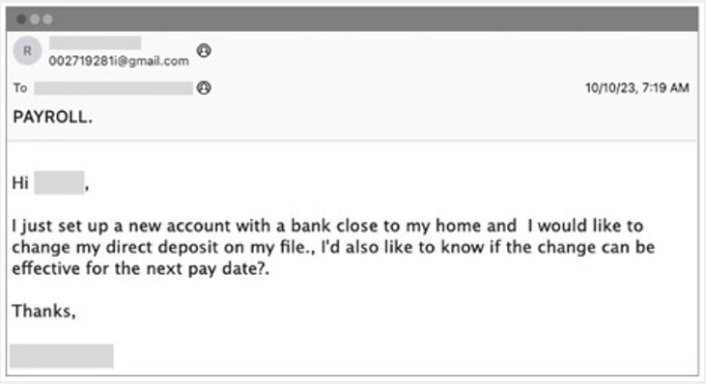
Le scénario

Proofpoint a détecté l'une de ces menaces dans une entreprise du secteur de l'énergie et des services publics comptant 300 collaborateurs. Dans ce cas-ci, un cybercriminel s'est fait passer pour un collaborateur lambda et a envoyé un email au directeur des ressources humaines (RH) de l'entreprise. Non seulement l'outil de protection de la messagerie de l'entreprise a distribué le message, mais son outil de correction après la remise basé sur une API ne l'a pas non plus détecté ni retiré.

Le déroulement de l'attaque

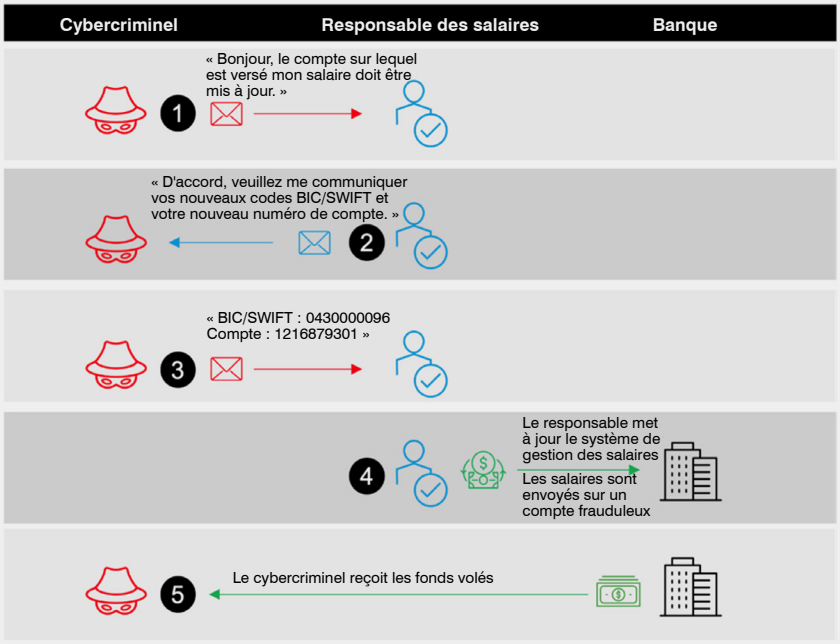
Examinons plus en détail le déroulement de l'attaque.

1. **Le message de leurre.** Le cybercriminel a demandé aux RH la mise à jour des informations du compte sur lequel est versé « son » salaire. Ce message a été envoyé à partir d'un compte qui ressemblait au compte de messagerie personnel d'un collaborateur légitime.



Message malveillant initial distribué dans la boîte de réception du destinataire

2. **La séquence d'attaque de détournement de salaires.** Si le destinataire avait répondu au message, l'objectif du cybercriminel aurait été de le convaincre de transférer des fonds sur un autre compte bancaire n'appartenant pas au collaborateur victime d'une usurpation d'identité.



Séquence d'attaque de détournement de salaires type

Pourquoi ces menaces sont difficiles à détecter

Ces menaces ne comportent généralement pas de charges virales malveillantes telles que des URL ou des pièces jointes. Elles ont également tendance à être envoyées à partir de services de messagerie personnelle comme Google, Yahoo et iCloud. Enfin, elles ciblent des utilisateurs spécifiques.

Par ailleurs, les outils de protection de la messagerie basés sur une API qui recherchent les menaces après la remise sont les plus susceptibles de passer à côté de ce type de menace. Cela s'explique en partie par leur fonctionnement. Pour que ces outils soient efficaces, les équipes informatiques et de sécurité doivent les alimenter manuellement avec un dictionnaire des noms d'affichage possibles de tous les collaborateurs, une tâche très chronophage et difficilement applicable à grande échelle.

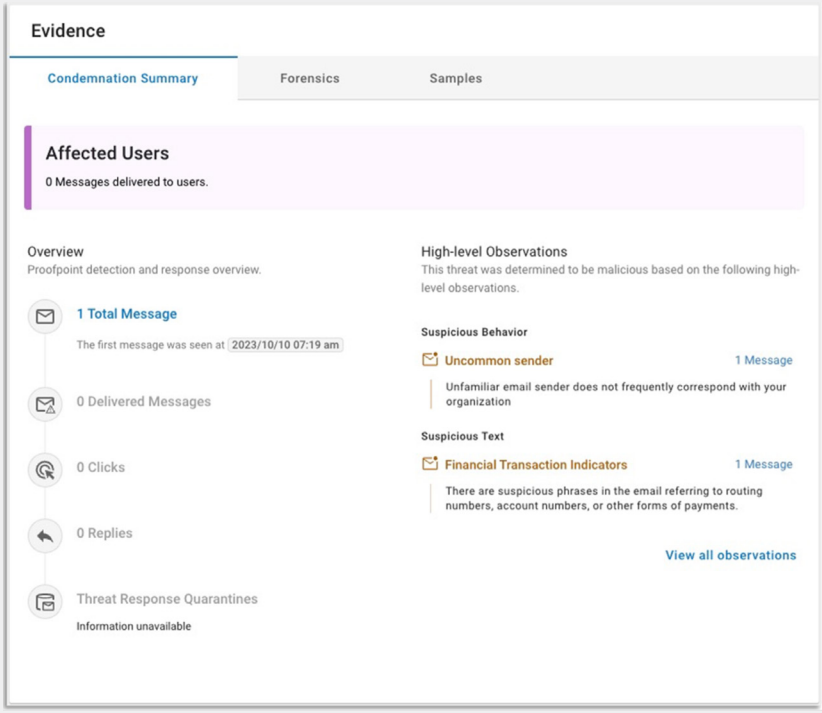
Pour l'éviter, de nombreuses entreprises choisissent de n'activer la prévention de l'usurpation des noms d'affichage que pour leurs cadres dirigeants. Toutefois, les cybercriminels à l'origine du détournement de salaires ne se limitent pas à usurper l'identité de cadres dirigeants, mais ciblent tout collaborateur ayant accès aux fonds de l'entreprise. Dans notre exemple ci-dessus, un cyberpirate a exploité cette faiblesse.

Comment Proofpoint a détecté l'attaque

Pour comprendre le véritable objectif d'un email, un outil de protection de la messagerie doit interpréter le ton et l'intention du message. Pour ce faire, Proofpoint utilise plusieurs signaux de détection, des moteurs d'analyse et l'IA comportementale. Nos moteurs de détection optimisés par l'IA et l'apprentissage automatique sont entraînés en permanence avec des millions d'emails journaliers issus de notre écosystème mondial de threat intelligence.

Parmi les signaux que nous utilisons pour détecter les emails malveillants, on peut citer l'analyse des communications entre un expéditeur et un destinataire ainsi que la fréquence de leurs messages. Dans l'exemple ci-dessus, il était rare que le directeur des RH reçoive des emails de ce collaborateur spécifique à partir de son adresse personnelle.

La plupart des outils de protection de la messagerie utilisent des signaux conçus pour identifier les expéditeurs inhabituels. Ils génèrent donc un nombre élevé de faux positifs. Notre stratégie est différente. Nous combinons de nombreux signaux pour ne pas trop dépendre d'un ou de deux signaux. En combinant le signal permettant d'identifier les expéditeurs inhabituels avec une analyse du langage employé dans le corps du message, Proofpoint extrait le ton et interprète l'intention d'un email.



Synthèse de la menace neutralisée par Proofpoint qui met en évidence les signaux qui nous ont conduits à signaler cette menace

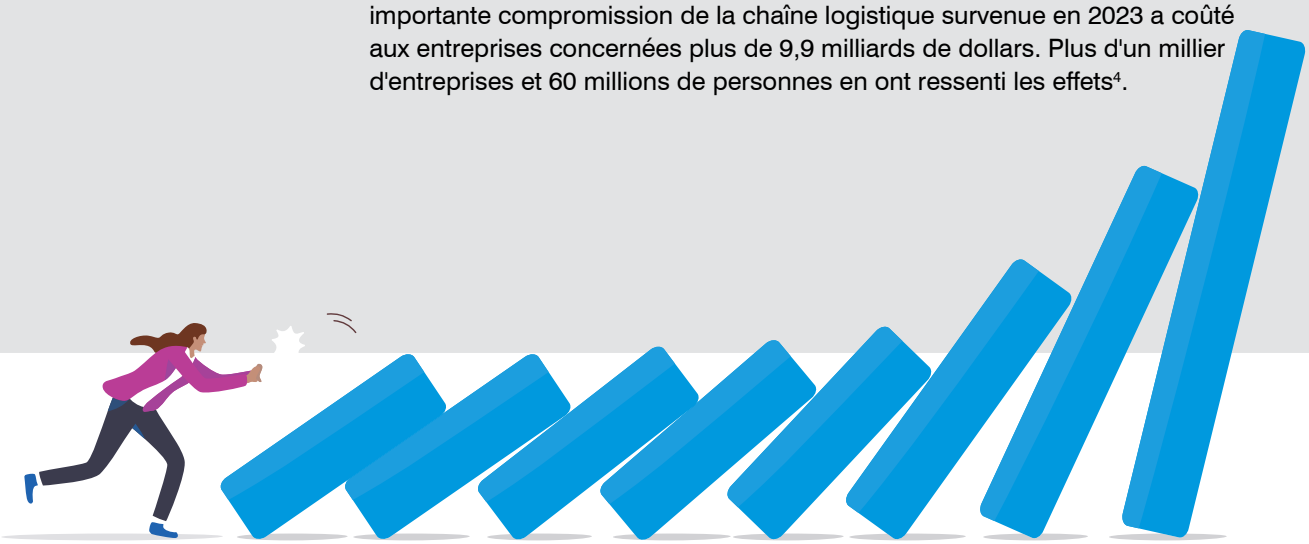
SECTION 5

Compromissions de la chaîne logistique

Les compromissions de la chaîne logistique sont une autre forme d'attaque BEC en plein essor. Lors de ces attaques, un cybercriminel cible une entreprise en compromettant la sécurité de ses fournisseurs et d'autres tiers de sa chaîne logistique. En effet, les cyberpirates savent que les entreprises disposant de chaînes logistiques matures ont tendance à avoir des défenses de cybersécurité plus solides, ce qui en fait des cibles difficiles à atteindre.

Par conséquent, plutôt que de lancer une attaque directe, le cybercriminel infiltre l'une des entités de confiance de l'entreprise et se fait passer pour elle. Le piratage de fils de discussion, ou piratage de conversations, est une technique couramment utilisée, dans le cadre de laquelle les cyberpirates ciblent des comptes de messagerie spécifiques et les compromettent pour pouvoir épier des conversations. Le moment venu, les cybercriminels s'insèrent dans la conversation. Parfois, ils sont assez audacieux pour engager une nouvelle conversation.

Ces attaques gagnent chaque jour en popularité et en sophistication. La plus importante compromission de la chaîne logistique survenue en 2023 a coûté aux entreprises concernées plus de 9,9 milliards de dollars. Plus d'un millier d'entreprises et 60 millions de personnes en ont ressenti les effets[4].



4 TechCrunch, « MOVEit, the Biggest Hack of the Year, by the Numbers » (MOVEit, le plus grand piratage de l'année, en chiffres), août 2023.

Le scénario

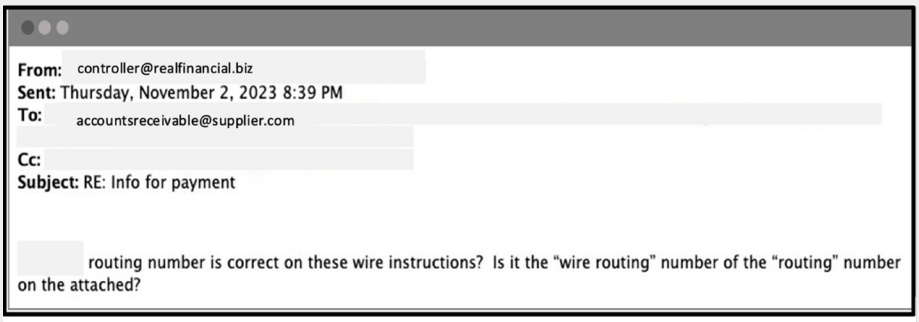
Proofpoint a détecté un message frauduleux semblant avoir été envoyé par un collaborateur du département comptabilité clients d'une petite entreprise de services financiers basée en Floride. Cependant, il s'agissait en réalité d'un cybercriminel qui usurpait l'identité de quelqu'un d'autre. Son objectif était de lancer une attaque de la chaîne logistique contre un important cabinet d'avocats de Boston.

Dans un email envoyé au contrôleur des finances du cabinet d'avocats, le cyberpirate demandait à ce que les paiements soient effectués sur un nouveau compte.

Le déroulement de l'attaque

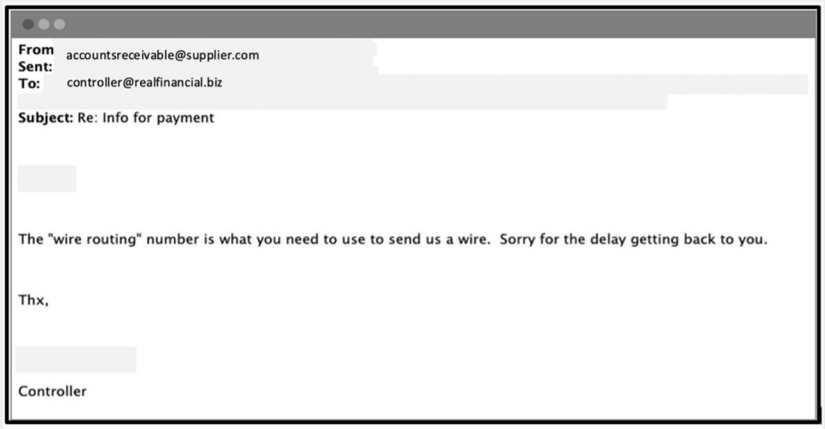
Examinons plus en détail le déroulement de l'attaque.

1. **Le message légitime du client.** Le client a envoyé un email au fournisseur pour confirmer l'exactitude des coordonnées bancaires à utiliser pour les paiements.

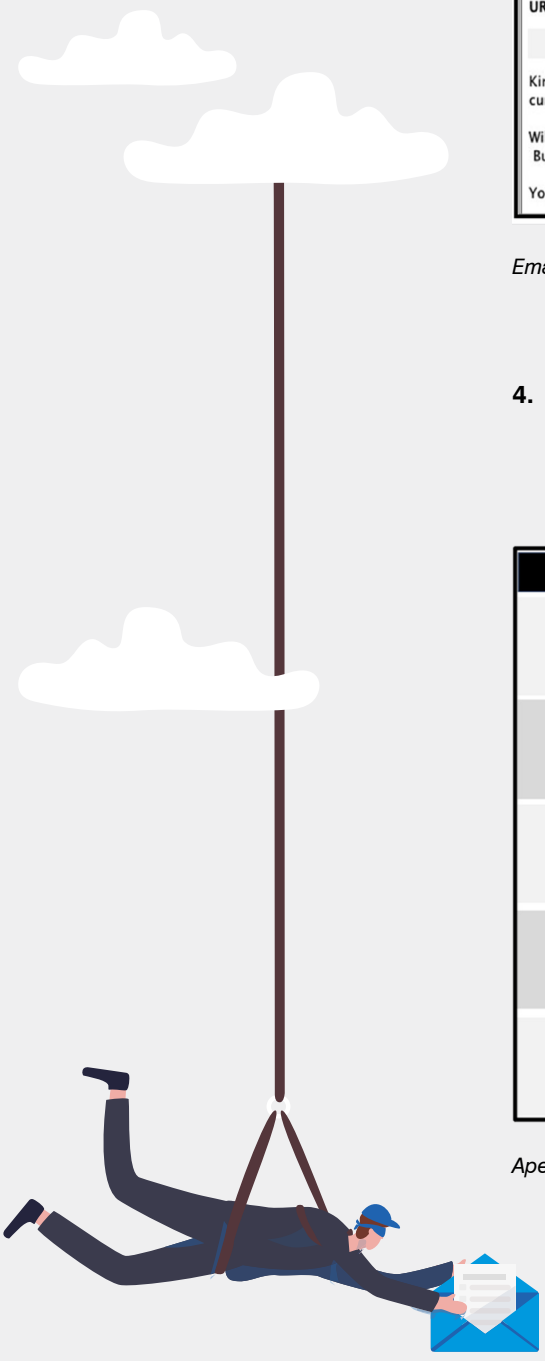


Message légitime du client confirmant les coordonnées bancaires à utiliser pour les paiements

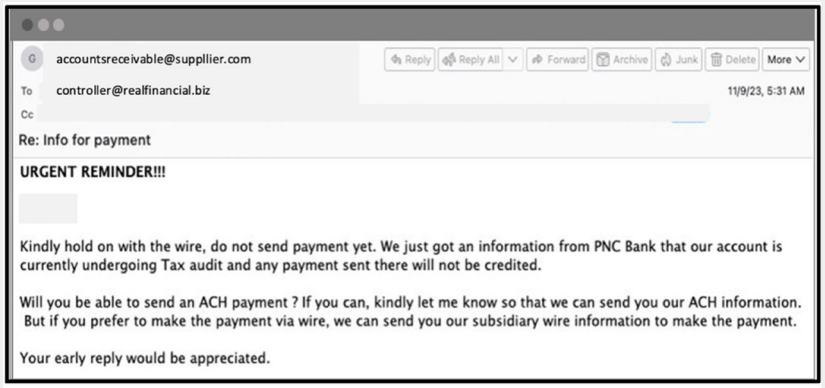
2. **L'email légitime du fournisseur.** Le fournisseur a répondu à la demande de confirmation des coordonnées bancaires à utiliser pour les paiements.



Email légitime du fournisseur en réponse à la demande de confirmation des coordonnées bancaires à utiliser pour les paiements

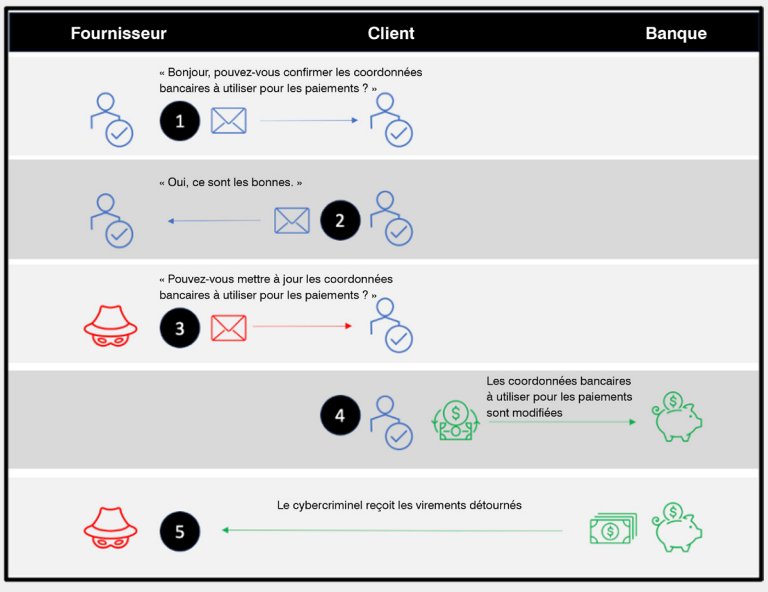


3. **L'email frauduleux du cybercriminel.** Le cybercriminel est entré dans la danse en envoyant un email au client à partir d'un autre compte ressemblant à s'y méprendre à celui du fournisseur. En réalité, cet email était envoyé à partir d'un domaine similaire, qui comportait une lettre supplémentaire dans l'adresse de l'expéditeur. Pour que son email paraisse légitime, le cyberpirate a copié-collé l'ensemble de la conversation en dessous du corps du message.



Email frauduleux du cybercriminel

4. **La séquence d'attaque de compromission de la chaîne logistique.** Le cybercriminel a demandé à ce que les paiements soient effectués sur un autre compte via une chambre de compensation automatisée. Le cyberpirate était le propriétaire de ce nouveau compte.



Aperçu de la séquence d'attaque

Pourquoi ces menaces sont difficiles à détecter

Les attaques de compromission de la chaîne logistique comportent rarement des charges virales malveillantes. C'est l'une des raisons pour lesquelles elles sont difficiles à détecter et à neutraliser. Le cybercriminel a recours à l'ingénierie sociale pour convaincre le destinataire de l'aider à atteindre son objectif.

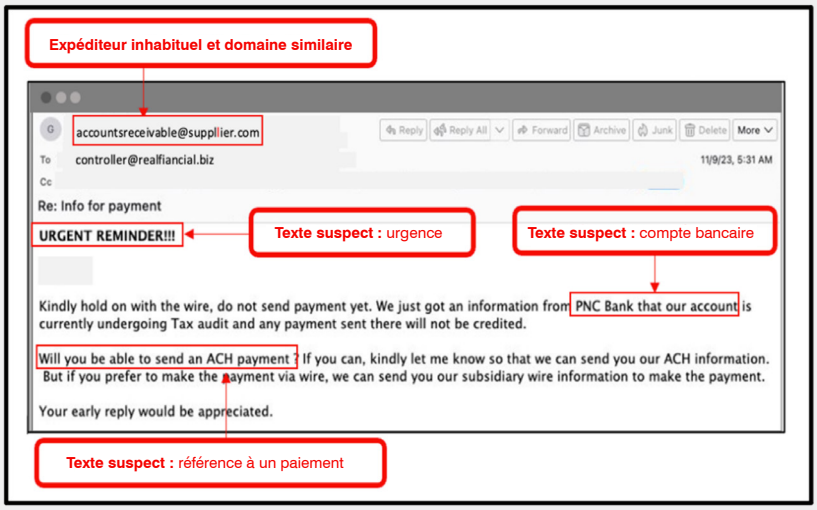
Dans ce scénario, un fournisseur a demandé à un prestataire de modifier les coordonnées bancaires à utiliser pour les paiements. Une telle demande n'est pas inhabituelle. C'est pourquoi les outils de protection de la messagerie basés sur une API peinent à détecter ces attaques. Les outils basés sur une API s'appuient sur des signaux permettant d'identifier les expéditeurs inhabituels, et génèrent donc un nombre élevé de faux positifs et d'alertes. Cette approche limitée basée sur l'IA comportementale aide à comprendre pourquoi un grand nombre d'entreprises se plaignent des nombreuses informations parasites générées par ces signaux.

Pour détecter ces types de messages malveillants, un outil de protection de la messagerie doit interpréter le ton contextuel ainsi que l'intention d'un message. C'est la seule façon de déterminer le véritable objectif d'un message avant qu'il ne soit distribué dans la boîte de réception d'un utilisateur.

Comment Proofpoint a détecté l'attaque

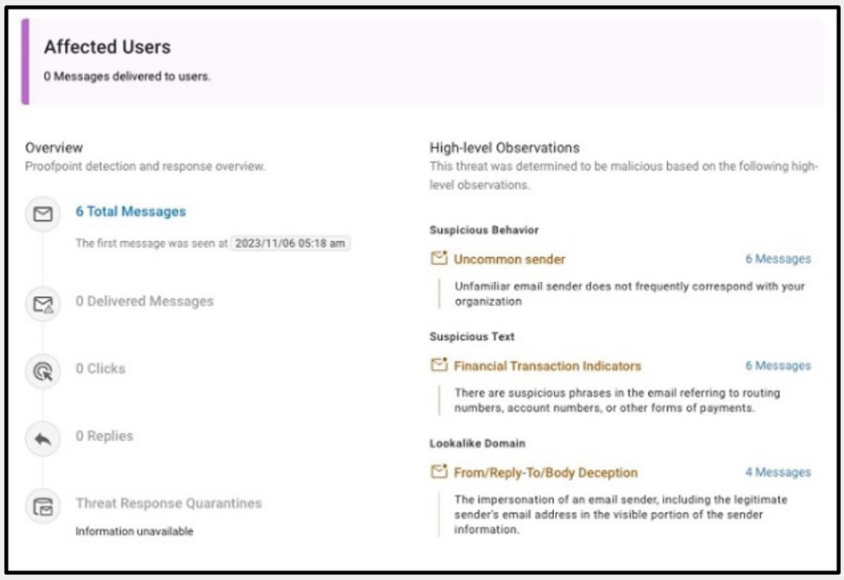
Proofpoint combine les informations de threat intelligence avec l'IA comportementale et l'apprentissage automatique pour déterminer si des emails sont légitimes ou malveillants. Nous entraînons en permanence nos moteurs de détection avec des millions d'emails journaliers issus de notre écosystème mondial de threat intelligence. Cela nous permet de détecter et de bloquer ces types de messages avec un niveau plus élevé de confiance.

Pour réduire les informations parasites, nous combinons plusieurs signaux plutôt que de dépendre d'un ou de deux signaux, ce qui peut générer un nombre élevé de faux positifs. Parmi ces signaux figurent l'analyse des communications entre les expéditeurs et les destinataires ainsi que la fréquence de ces messages. Nous analysons également le langage employé dans le corps du message pour en extraire le ton et en interpréter l'intention. Nous recherchons en outre les domaines similaires et les urgences de paiement.



Plusieurs signaux de détection identifiés dans l'email d'un fournisseur frauduleux

En analysant le contenu et l'intention de l'email ainsi que le langage employé, Proofpoint a déterminé que le message de notre exemple était une demande financière frauduleuse. Cette campagne ne comportait que quelques messages usurpant l'identité d'une personne et ne ciblait qu'un seul client. Aucun autre client de Proofpoint n'avait encore été victime de cette attaque.

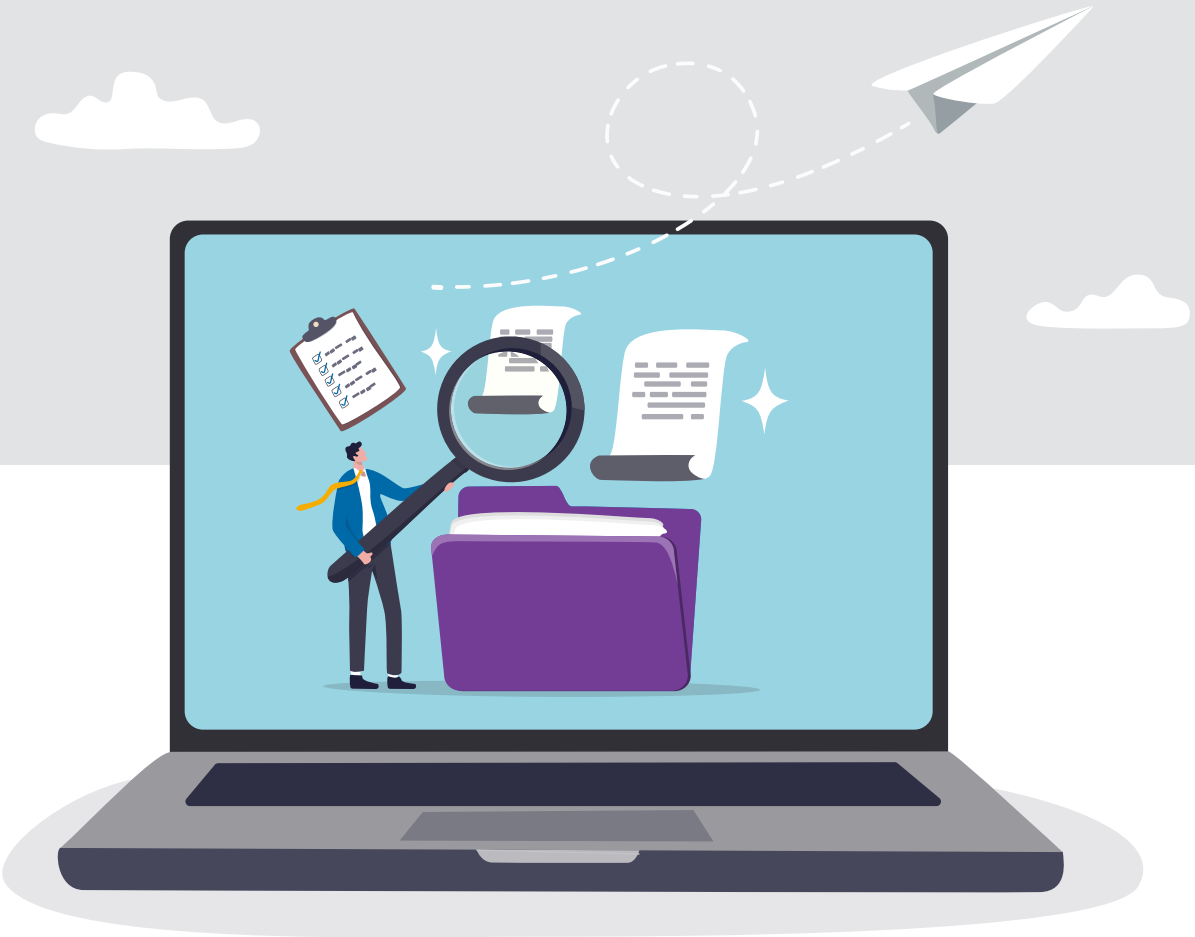


Synthèse de la menace neutralisée qui met en évidence les signaux qui ont conduit Proofpoint à bloquer cette menace

SECTION 6

Conclusion

Toutes ces escroqueries ne font que souligner le besoin critique de mesures de cybersécurité robustes et multicouches.



Pour garder une longueur d'avance sur les menaces en constante évolution, vous devez adopter une approche complète de la protection contre les menaces qui ciblent vos collaborateurs :

- **Détectez les menaces avant leur remise.** Le seul moyen de protéger les utilisateurs est de bloquer les messages malveillants avant leur remise. D'après les recherches menées par Proofpoint, un utilisateur sur sept clique sur un email dans la minute. Optez pour un outil qui allie algorithmes d'apprentissage automatique et threat intelligence avancée pour identifier et bloquer les menaces avancées.
- **Formez vos utilisateurs.** Vos collaborateurs, sous-traitants et partenaires constituent votre première ligne de défense. Assurez-vous qu'ils bénéficient de formations de sensibilisation à la sécurité informatique pour tous les types d'attaques. Rappelez-leur de signaler rapidement tout comportement inhabituel.
- **Réalisez des audits de sécurité réguliers.** Les audits peuvent vous aider à identifier les vulnérabilités potentielles au sein de votre environnement. Ce faisant, assurez-vous de rechercher les irrégularités dans vos configurations et vos journaux d'accès.
- **Configurez votre système afin qu'il détecte les erreurs de configuration.** En plus de rechercher les erreurs de configuration, n'oubliez pas d'activer la correction automatique. Vous pourrez ainsi détecter les modifications non autorisées et les corriger rapidement, ce qui empêchera les cybercriminels de s'implanter durablement dans votre entreprise.
- **Élaborez un plan de réponse aux incidents.** Identifiez plusieurs scénarios d'attaque. Déterminez ensuite comment vous analyserez et corrigerez les incidents. Assurez-vous de tester l'efficacité réelle de votre plan en effectuant régulièrement des exercices de simulation.

Étapes suivantes

Plus que jamais, il est important de protéger votre entreprise contre les menaces email en plein essor. Vous devez adopter une approche proactive pour protéger votre entreprise, vos collaborateurs et vos clients contre les attaques avancées telles que les ransomwares, les menaces BEC et le phishing d'identifiants de connexion.

L'évaluation rapide des risques liés à la messagerie proposée par Proofpoint vous offre une visibilité et des informations complètes sur votre vulnérabilité aux attaques. Elle vous aide à identifier les personnes ciblées par des menaces email au sein de votre entreprise.

N'attendez pas qu'il soit trop tard pour tester la sécurité de votre messagerie. Contactez Proofpoint pour bénéficier d'une **évaluation gratuite des risques liés à la messagerie**.

EN SAVOIR PLUS

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

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 85 % des entreprises de l'index Fortune 100, 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.

0503-006-03-01 07/24