EBOOK

Le cloud en ligne de mire

Comment les cybercriminels exploitent les vulnérabilités liées au partage de fichiers, aux identités et à la chaîne logistique dans Microsoft 365

proofpoint.

Introduction

Dans le monde numérique actuel, Microsoft 365 est un outil de productivité incontournable. Malheureusement, sa popularité en a fait une cible de choix pour les cybercriminels. Bien que Microsoft 365 regorge de fonctionnalités natives pour bloquer les cyberattaques, ces outils ne sont pas à la hauteur des attaques sophistiquées actuelles.

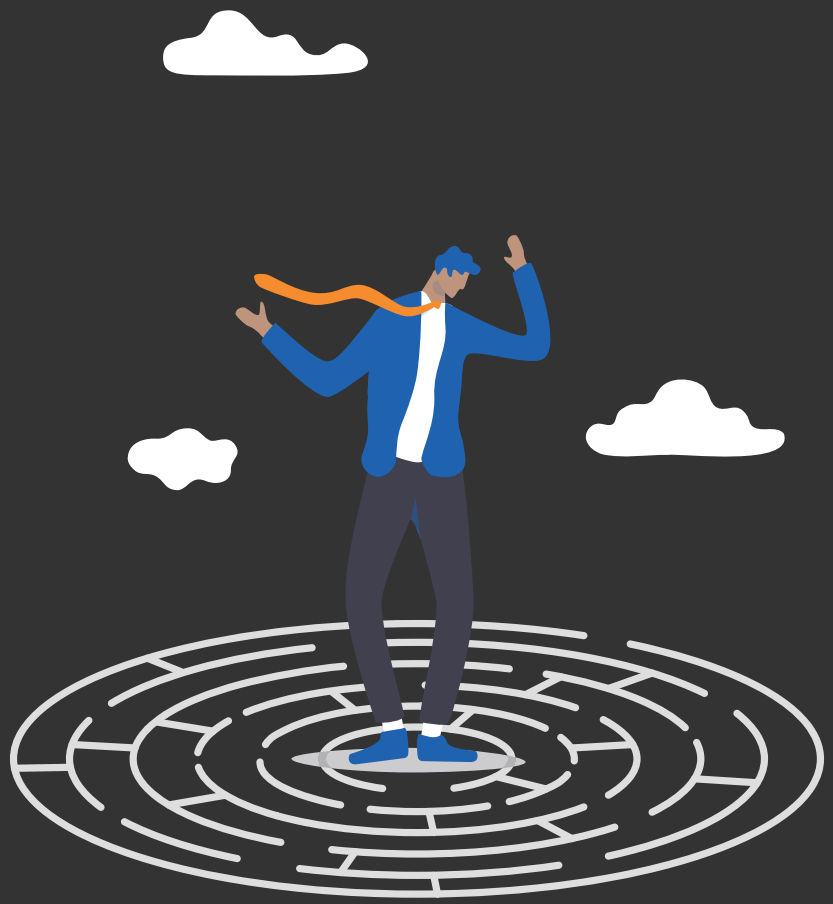
Les attaques centrées sur les personnes ciblant Microsoft 365 coûtent chaque année des millions de dollars aux entreprises et provoquent la frustration tant des utilisateurs que des équipes de sécurité. À tel point que des experts du secteur, comme Gartner, estiment que les outils intégrés pour le cloud devraient être renforcés par des solutions tierces[1].

La raison pour laquelle les outils intégrés ne suffisent plus est simple : les cybercriminels sont passés maîtres dans l'art de cibler les personnes. Et cela les rend de plus en plus difficiles à contrer.

La compromission d'utilisateurs est généralement la première étape d'une série bien plus vaste d'événements qui se produisent lorsqu'une entreprise est infiltrée. Baptisés « chaîne de cyberattaque », ces événements commencent par la compromission d'utilisateurs et évoluent vers l'utilisation abusive de privilèges, le vol de données et plus encore.

Étapes de la chaîne de cyberattaque

1 Gartner, « Market Guide for Email Security » (Guide du marché de la protection de la messagerie), février 2023.



Cet eBook s'intéresse à cinq types d'attaques centrées sur les personnes qui ouvrent la porte aux cybercriminels et, par la même occasion, exposent les entreprises à des risques de compromissions plus graves. Ils sont très difficiles à détecter au moyen des seules fonctionnalités de Microsoft 365.

1. Piratage de la messagerie en entreprise (BEC, Business Email Compromise)
2. Attaques par téléphone (TOAD, Telephone-Oriented Attack Delivery)
3. Partage de fichiers malveillants
4. Prise de contrôle de comptes
5. Compromission de comptes fournisseurs

Chaque section inclut plusieurs exemples qui illustrent à quel point ces attaques peuvent être variées et inventives. Ces exemples montrent également comment n'importe quel utilisateur de Microsoft 365 ou presque peut être victime d'un cybercriminel chevronné s'il ne met pas en place des mesures de sécurité supplémentaires.

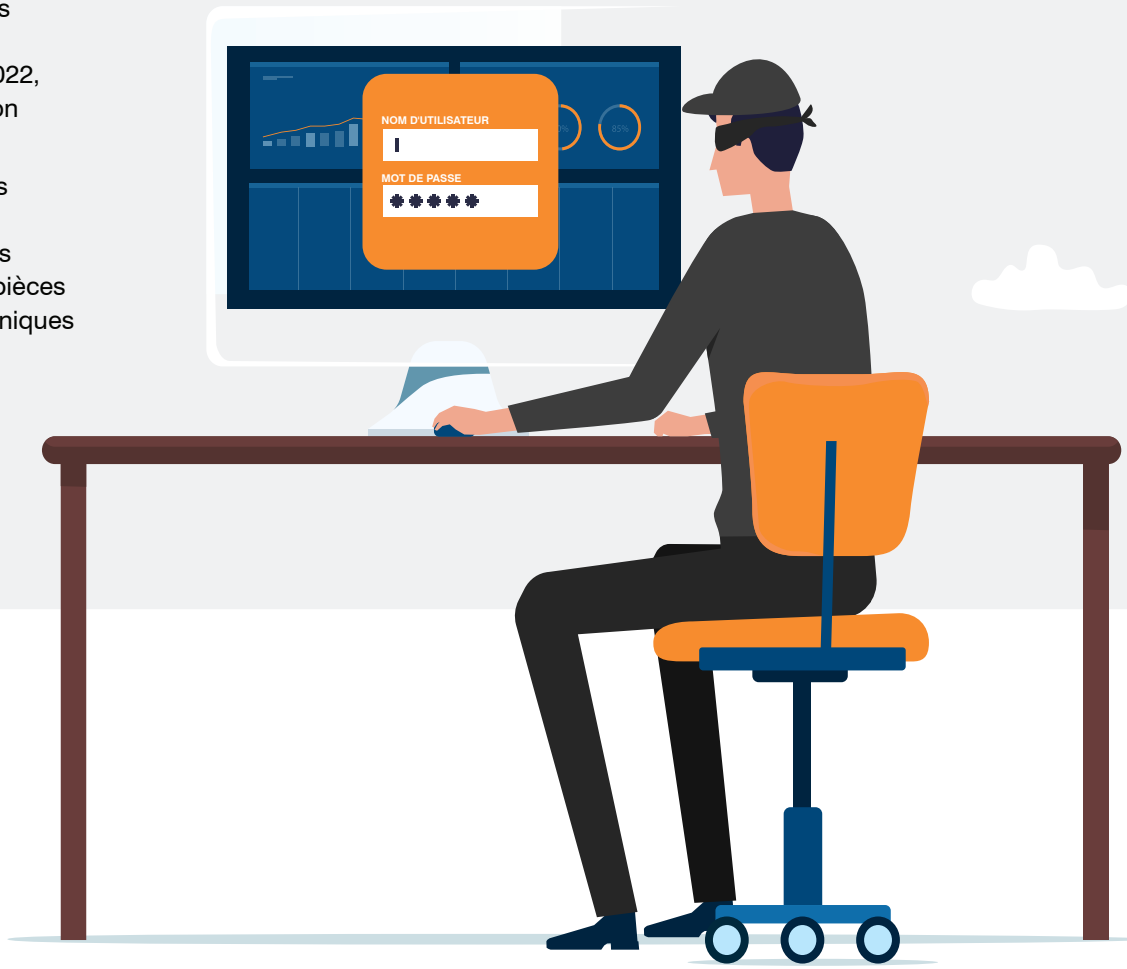
Tous ces exemples correspondent à des menaces réelles observées par Proofpoint dans le cadre d'évaluations des risques réalisées pour des entreprises.

SECTION 1

PIRATAGE DE LA MESSAGERIE EN ENTREPRISE (BEC)

Le piratage de la messagerie en entreprise (BEC) fait partie des types d'attaques les plus coûteux ciblant les entreprises de toutes tailles et de tous secteurs. Chaque année, les pertes continuent de suivre une tendance à la hausse. En 2022, le FBI a découvert que les entreprises ont perdu 2,7 milliards de dollars en raison d'attaques BEC. Cela représente 300 millions de dollars de plus qu'en 2021.

Bon nombre des attaques BEC actuelles sont très sophistiquées, bien financées et soutenues par une planification et des recherches minutieuses. Elles sont également très difficiles à détecter. En effet, les cybercriminels n'envoient pas les charges virales que nous avons l'habitude d'analyser, à savoir des URL ou des pièces jointes malveillantes, mais ont recours à l'usurpation d'identité et à d'autres techniques d'ingénierie sociale.



2 FBI, « 2022 Internet Crime Report » (Rapport 2022 sur la cybercriminalité), 2023.

Environnement :
Microsoft 365

Catégorie de menace :
Ingénierie sociale

Type d'attaque :
Détournement de salaires

Cible :
Responsable des rémunérations et avantages sociaux

Attaque de détournement de salaires

Les attaques de détournement de salaires sont des fraudes par email qui ciblent généralement des collaborateurs du département financier, fiscal, de paie ou des ressources humaines. Lors de ces attaques, les cybercriminels cherchent à gagner la confiance des collaborateurs afin de modifier des coordonnées bancaires et de voler les salaires de membres du personnel. Comme ils emploient des tactiques d'ingénierie sociale, ils peuvent être extrêmement difficiles à détecter. Les attaques de détournement de salaires sont considérées comme un risque de niveau moyen pour les entreprises.

Exemple d'attaque de détournement de salaires

Dans le cadre de cette attaque, un fraudeur a envoyé un email à un responsable des rémunérations et avantages sociaux à partir d'un compte Gmail en se faisant passer pour un collaborateur demandant le versement de son salaire sur un nouveau compte bancaire. Dans cet exemple, le fraudeur et la victime ont même été autorisés à échanger plusieurs messages. Lors des évaluations et des validations de concept (PoC) réalisées par Proofpoint, les contrôles natifs de protection de la messagerie Microsoft ne sont pas parvenus à bloquer ces types d'attaques.

Environnement :
Microsoft 365

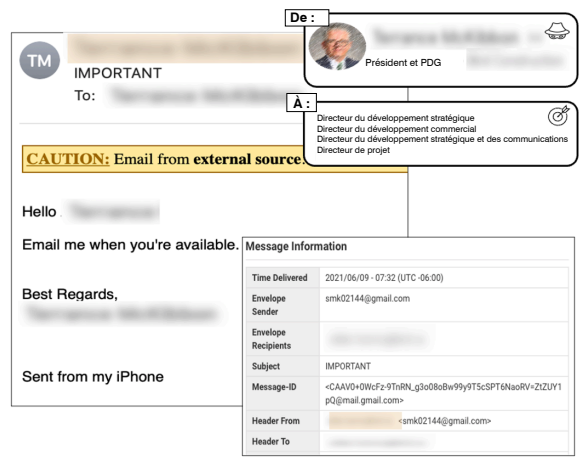
Catégorie de menace :
Ingénierie sociale

Type d'attaque :
Usurpation d'identité

Cible :
Responsables stratégie et développement commercial

Attaque d'usurpation de l'identité d'un cadre dirigeant

Lorsqu'un cybercriminel réussit à se faire passer pour un collaborateur, la fraude peut s'avérer coûteuse pour l'entreprise. Mais lorsque des cyberpirates usurpent l'identité de cadres dirigeants, les pertes peuvent être bien plus lourdes. Ces dernières années, ces attaques ont connu une hausse spectaculaire. Depuis mars 2020, Proofpoint a observé des usurpations par email touchant plus de 7 000 PDG. Plus de la moitié des clients de Proofpoint ont vu au moins un des comptes de messagerie de leurs cadres dirigeants utilisé dans une tentative d'escroquerie.



Exemple d'attaque d'usurpation de l'identité d'un cadre dirigeant

Dans cet exemple, un cybercriminel a envoyé un email à des collaborateurs à partir d'un compte Gmail en se faisant passer pour un PDG qui avait besoin qu'ils réalisent une action. Si les collaborateurs avaient réagi à l'email, le fraudeur aurait facilement pu extraire des données ou détourner de l'argent. Lors des évaluations et des validations de concept réalisées par Proofpoint, les contrôles natifs de protection de la messagerie Microsoft ne sont pas parvenus à bloquer ces types d'attaques.

Environnement :
Microsoft 365

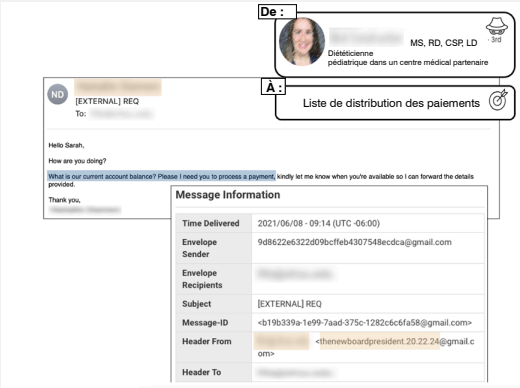
Catégorie de menace :
Ingénierie sociale

Type d'attaque :
Fraude aux factures

Cible :
Département financier

Fraude aux factures fournisseurs

La plupart des attaques BEC ciblent des particuliers, comme la fraude aux cartes cadeaux. Toutefois, les escroqueries BEC B2B qui visent des fournisseurs sont hautement ciblées. Dès lors, même si leur volume peut être moins important, les pertes financières qui en découlent peuvent être dévastatrices. Proofpoint a bloqué plusieurs tentatives de fraude aux factures fournisseurs qui auraient pu coûter des millions de dollars aux entreprises.
Lors de ces attaques, les cybercriminels envoient des factures factices ou de nouvelles coordonnées bancaires afin que les versements soient effectués sur un compte dont ils ont le contrôle.



Exemple de fraude aux factures fournisseurs

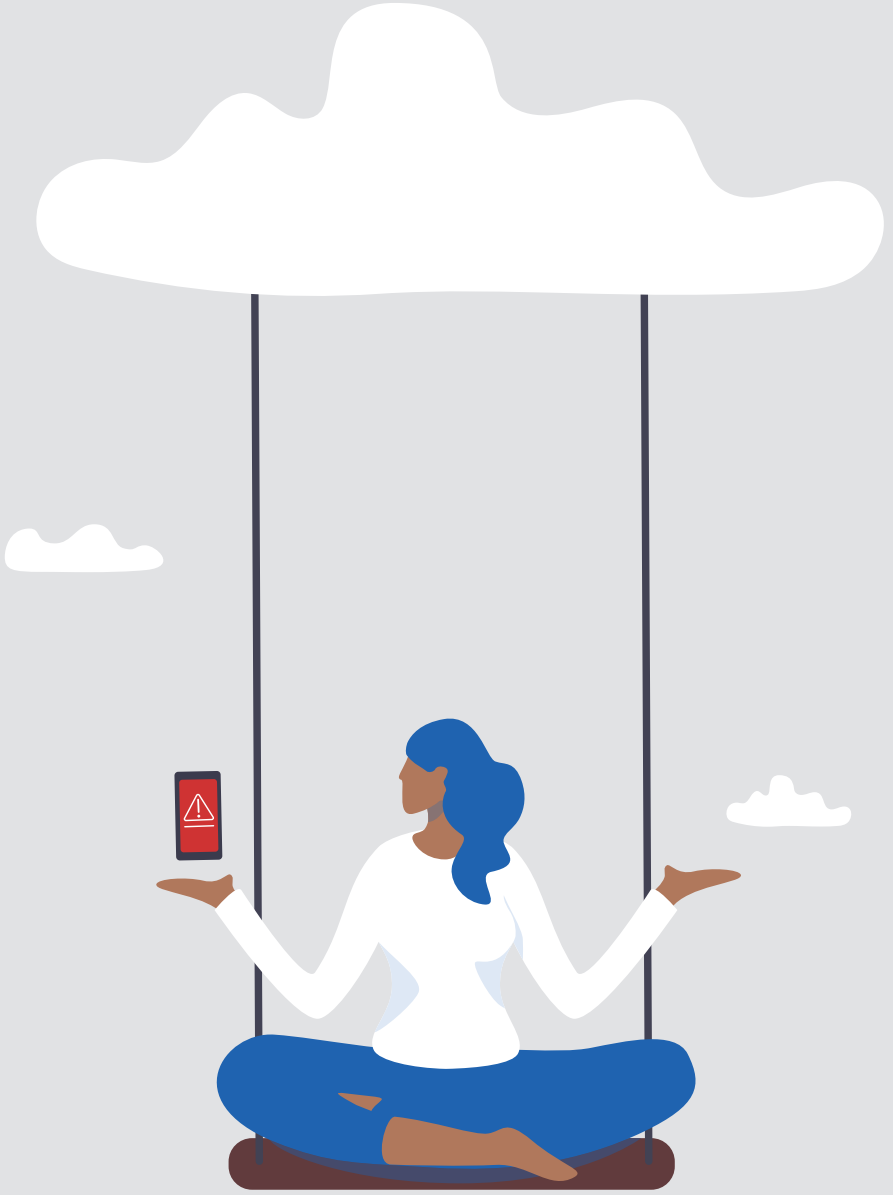
Dans cet exemple, le cybercriminel s'est fait passer pour un ancien collaborateur travaillant désormais dans une entreprise partenaire qui avait besoin qu'un paiement soit traité. Ce message, qui a été envoyé au département financier à partir d'un compte Gmail, a échappé aux contrôles natifs de protection de la messagerie Microsoft.

Les cyberpirates utilisent souvent Gmail ou d'autres services de messagerie gratuits lorsqu'ils procèdent à de telles tentatives de fraude, car cela les aide à contourner les dispositifs d'authentification des emails avec des technologies telles que SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail). Les cybercriminels peuvent également envoyer des URL ou des pièces jointes malveillantes pour accéder à des informations financières ou à d'autres données de valeur.

SECTION 2

ATTAQUES PAR TÉLÉPHONE

Lors d'une attaque par téléphone (TOAD), une cible reçoit un message contenant généralement une fausse facture ou alerte. Le message contient également le numéro d'un service client à contacter en cas de questions ou pour corriger une erreur. Si la cible appelle le numéro, elle se retrouve en ligne avec un cybercriminel. Pendant les pics d'activité, Proofpoint a détecté plus de 13 millions de messages TOAD envoyés par mois en 2022. Ce chiffre ne cesse d'augmenter depuis l'apparition de cette technique en 2021[3].



3 Proofpoint, rapport « Le facteur humain », 2023.

Environnement :
Microsoft 365

Catégorie de menace :
Ingénierie sociale

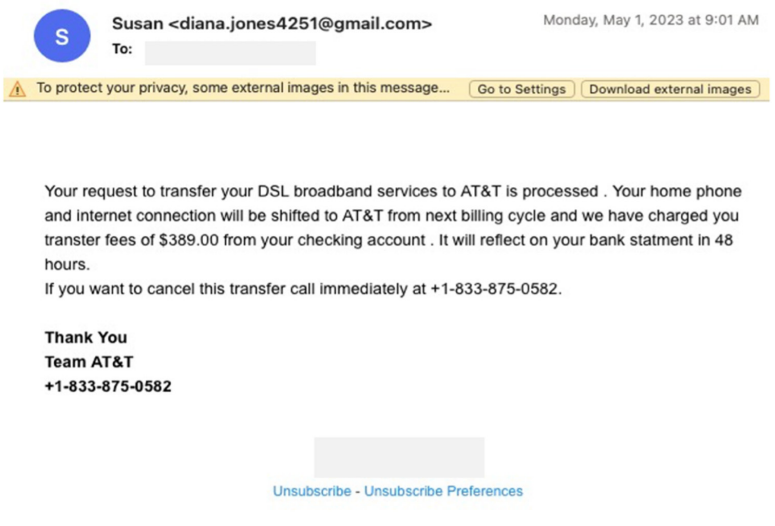
Type d'attaque :
TOAD

Cible :
Utilisateur de Microsoft 365

Menace TOAD

La fraude par email appuyée par de faux représentants d'un service client dans un centre d'appels est à la fois prolifique et rentable. Dans de nombreux cas, les victimes perdent des dizaines de milliers de dollars volés directement sur leur compte bancaire. 68,4 millions d'Américains auraient perdu 39,5 milliards de dollars en raison de fraudes par téléphone entre 2021 et 2022[4].

Deux types de menaces émanant de centres d'appels sont régulièrement observés par Proofpoint. Le premier utilise des logiciels d'assistance à distance gratuits et légitimes pour voler de l'argent. Le second a recours à des malwares maquillés en documents pour compromettre un ordinateur et peut entraîner la distribution de malwares secondaires.



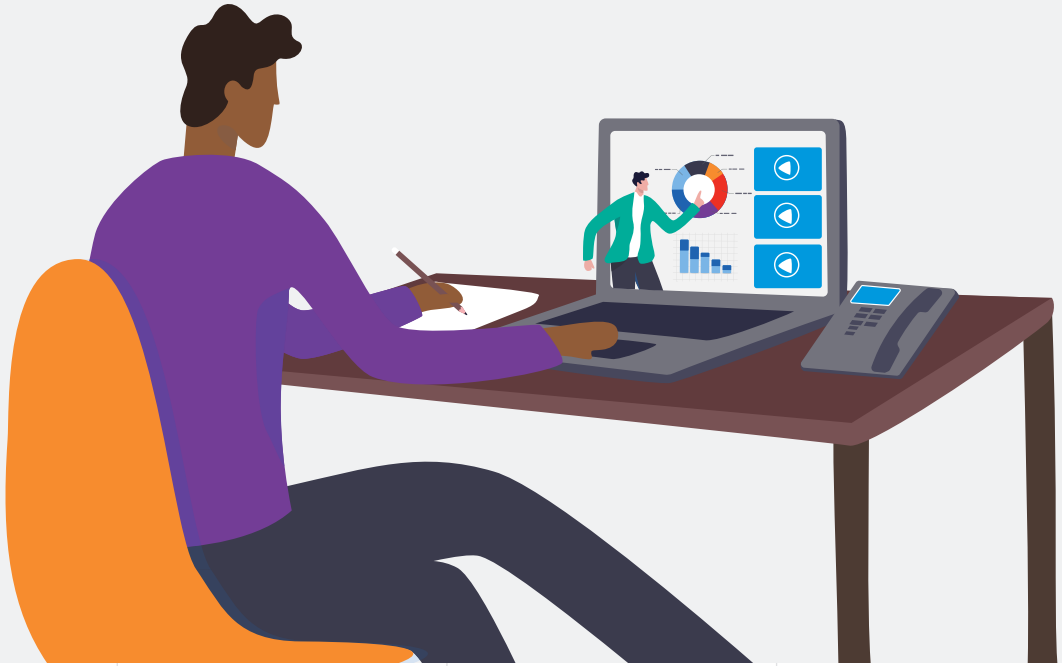
Exemple d'attaque TOAD

4 Truecaller, « U.S. Spam & Scam Report » (Rapport sur le spam et les escroqueries aux États-Unis), 2022.

Dans une attaque type émanant d'un centre d'appels, un utilisateur reçoit généralement un message prétendument urgent, comme celui ci-avant. Ce message inclut souvent un reçu pour un achat conséquent et semble avoir été envoyé par une entreprise légitime. Le destinataire est invité à appeler un numéro figurant dans l'email pour annuler la transaction ou contester l'achat.

Si l'utilisateur appelle le numéro de téléphone indiqué dans l'email, un faux représentant du service client le guide vers un site Web ou une boutique d'applications mobiles. Les étapes suivantes observées par les chercheurs Proofpoint sont variées : téléchargement de malwares, transfert d'argent ou activation d'un accès à distance par les victimes.

Microsoft passe à côté de ces messages, car ils ne contiennent pas de charge virale ni d'URL malveillantes.



SECTION 3

PARTAGE DE FICHIERS MALVEILLANTS

Les attaques par partage de fichiers malveillants constituent l'un des types d'attaques basées sur des URL les plus courants. Les données internes sur les menaces de Proofpoint montrent que des URL sont utilisées dans trois quarts des cyberattaques. Des URL de partage de fichiers sont impliquées dans plus de 50 % de ces attaques.

Étant donné que les utilisateurs font naturellement confiance à des services comme Microsoft OneDrive et Microsoft SharePoint, les cybercriminels emploient régulièrement des liens vers ces services. Microsoft se trouve dans une situation particulière face à ces attaques. Non seulement il héberge involontairement ces fichiers malveillants, mais il leur permet également d'échapper à la détection de ses solutions de protection de la messagerie.

En 2021, nous avons découvert que plus de 45 millions de menaces basées sur des URL envoyées à nos clients comportaient du contenu malveillant hébergé par Microsoft.

Environnement :
Microsoft 365

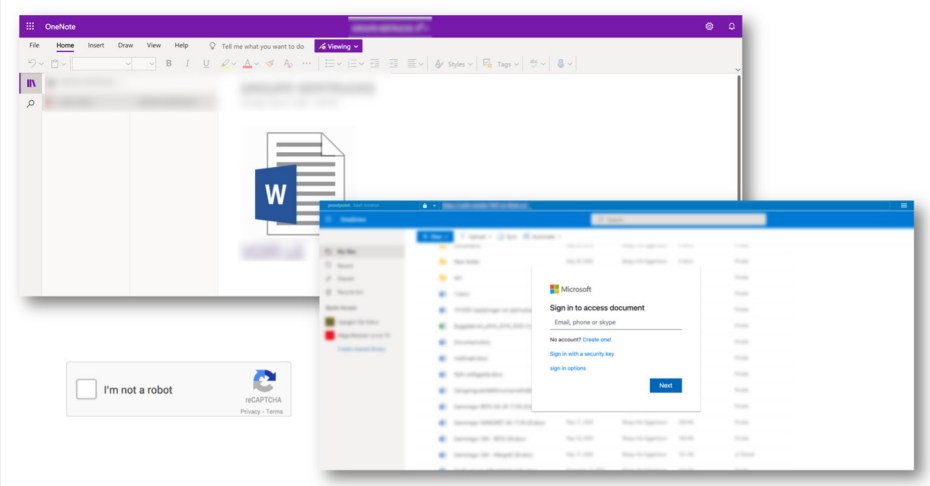
Catégorie de menace :
Partage de fichiers via une URL

Type d'attaque :
Phishing d'identifiants de connexion

Cible :
Utilisateurs d'une boîte email partagée

Phishing d'identifiants de connexion OneNote

D'après les données de Proofpoint, l'utilisation de CAPTCHA par les cybercriminels a été multipliée par 50 en un an[5]. Lors de ces attaques, les cyberpirates tentent de voler les identifiants de connexion d'utilisateurs en leur envoyant des liens vers des documents factices. Lorsque des utilisateurs cliquent sur ces liens, un CAPTCHA s'affiche. Une fois la case cochée, ils sont dirigés vers une fausse page Microsoft qui les invite à saisir leurs identifiants de connexion.



Exemple de page Microsoft OneNote contenant un lien vers un faux document Word

5 Proofpoint, rapport « Le facteur humain », 2022.

Dans cet exemple, un cybercriminel s'est fait passer pour un fournisseur tiers envoyant une requête à la boîte email partagée d'un opérateur de télécommunications. En envoyant un lien vers un faux document Word contenant un CAPTCHA, l'objectif du cyberpirate était que les utilisateurs de la boîte email divulguent leurs identifiants de connexion. Transmis via OneDrive, le lien vers la page malveillante contournait les contrôles de sécurité natifs de Microsoft.

Étonnamment, même après avoir été signalée par Proofpoint, la page OneDrive était toujours en ligne un mois plus tard. Ce n'est qu'une des millions de pages de partage de fichiers frauduleuses qui usurpent la marque Microsoft chaque mois.

Environnement :
Microsoft 365

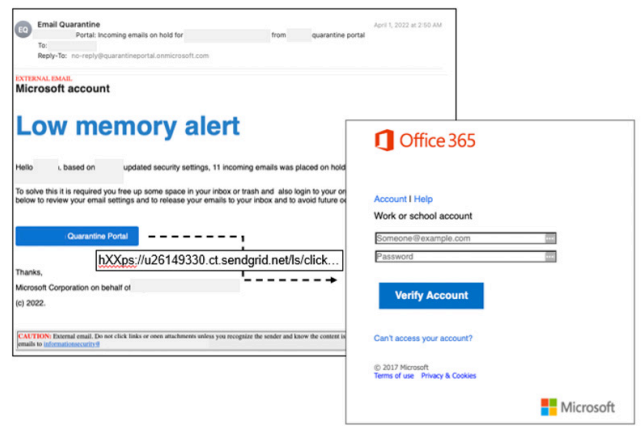
Catégorie de menace :
Utilisation abusive de services cloud légitimes

Type d'attaque :
Phishing d'identifiants de connexion

Cible :
Utilisateurs de Microsoft 365

Phishing d'identifiants de connexion via l'utilisation abusive de services cloud légitimes

Le vol d'identifiants de connexion Microsoft 365 est une tactique courante utilisée par les cybercriminels pour compromettre des comptes d'utilisateurs. Une fois qu'ils contrôlent le compte de leur victime, les cyberpirates peuvent obtenir des informations leur permettant d'envoyer des messages très convaincants. Ils peuvent ainsi voler des données de valeur et détourner des fonds.



Exemple d'un vol d'identifiants de connexion usurpant la marque Microsoft par le biais d'un service cloud légitime

Dans cet exemple, le cybercriminel a utilisé SendGrid comme hôte et a envoyé son message à partir d'un domaine Microsoft usurpé (onmicrosoft.com) pour qu'il paraisse légitime. En bas du message, il a même inclus Microsoft Corporation dans la signature.

Il convient de noter que lorsque les cyberpirates utilisent des services cloud légitimes, leurs attaques échappent souvent à la détection de Microsoft. Cela est dû à la façon dont Microsoft traite les liens. La fonction Liens fiables de Microsoft n'effectue pas de sandboxing prédictif au moment où les utilisateurs cliquent. Elle s'appuie uniquement sur la réputation, de sorte qu'elle n'est pas capable de détecter les menaces inédites émanant de services cloud et de partage de fichiers légitimes.

SECTION 4

PRISE DE CONTRÔLE DE COMPTES

La prise de contrôle de comptes est une tactique couramment employée par les cybercriminels. Lors de ces attaques, un cyberpirate vole les identifiants de connexion au compte d'un utilisateur afin de pouvoir usurper son identité professionnelle. Une seule paire d'identifiants de connexion est très précieuse pour les cybercriminels, car elle offre un accès aux emails, au stockage de documents et à d'autres services avec authentification unique. Avec un tel accès, les conséquences d'une attaque réussie peuvent être dévastatrices. En 2021, les entreprises ont perdu en moyenne 6,2 millions de dollars en raison de compromissions de comptes cloud[6]. Et ces attaques sont en plein essor. En 2022, Verizon a découvert que 76 % des attaques d'ingénierie sociale impliquaient le vol d'identifiants de connexion[7].

6 Ponemon Institute, rapport « The Cost of Cloud Compromise and Shadow IT » (Le coût de la compromission de comptes cloud et du Shadow IT), 2021.
7 Verizon, « Data Breach Investigations Report » (Rapport d'enquête sur les compromissions de données), 2023.

Environnement :
Microsoft 365

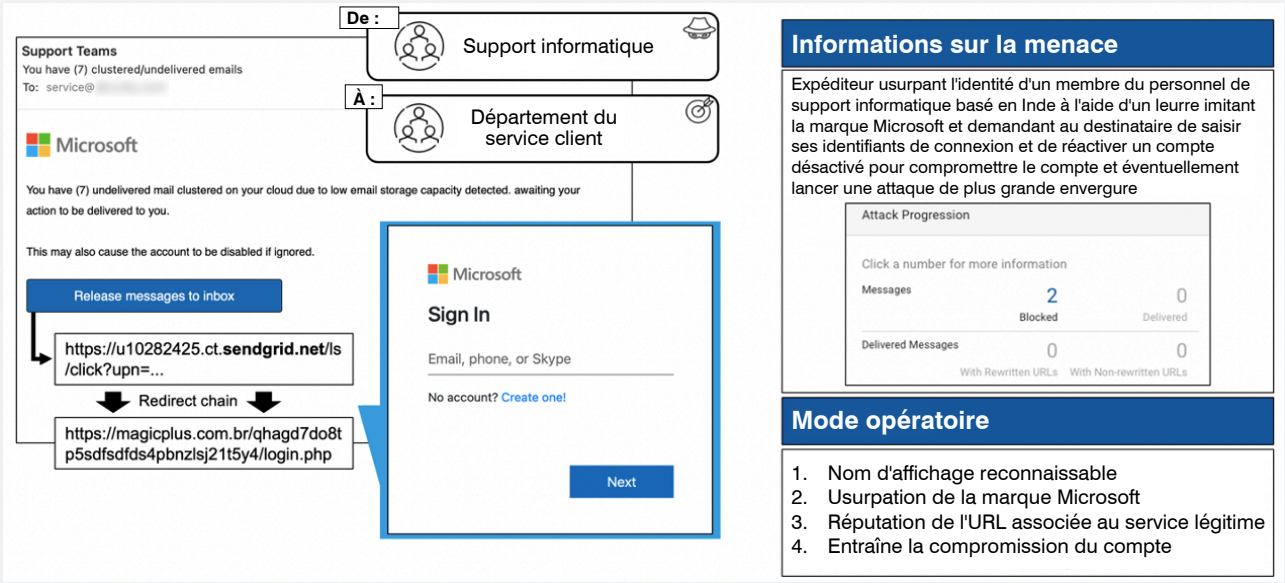
Catégorie de menace :
Attaque basée sur des URL

Type d'attaque :
Vol d'identifiants de connexion

Cible :
Département du service client

Attaque de collecte d'identifiants de connexion Microsoft 365

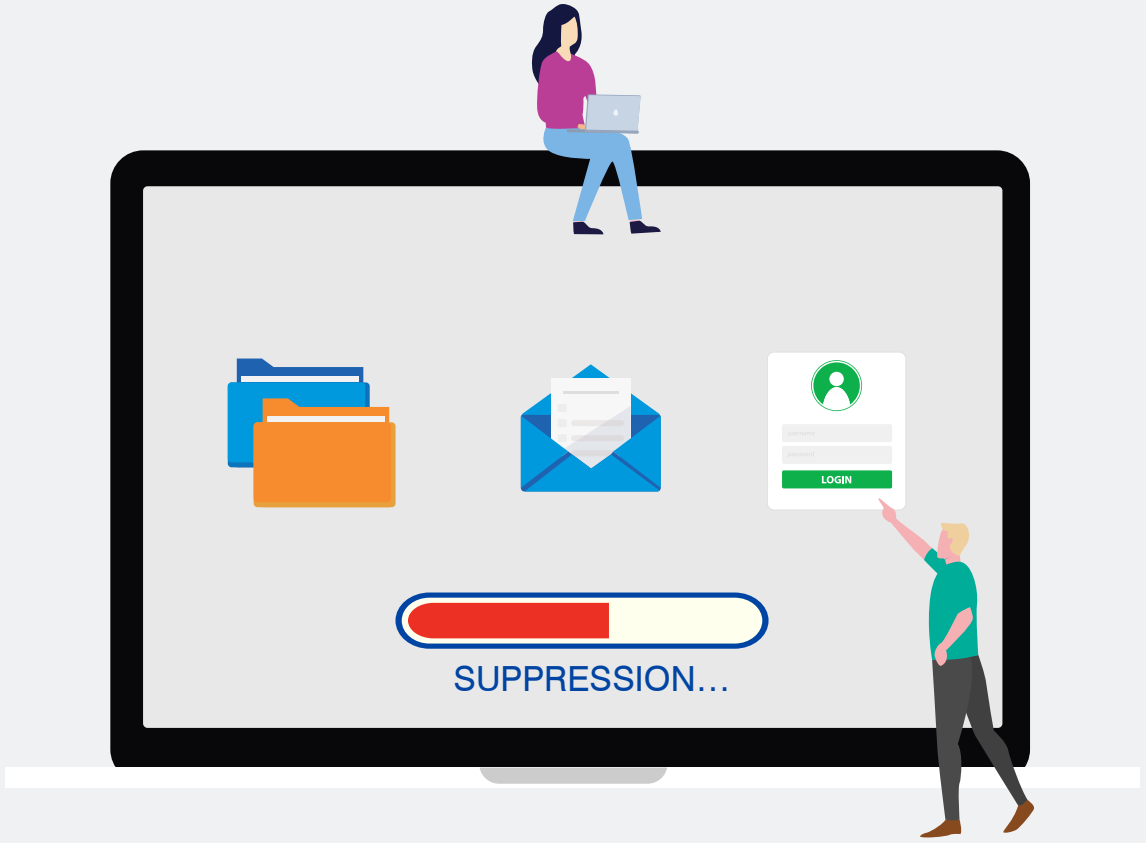
De nombreuses attaques de collecte d'identifiants de connexion utilisent la même tactique : elles imitent Microsoft afin de contourner ses mécanismes de défense. L'exploitation de la familiarité et de la confiance des utilisateurs dans des marques de premier plan est l'une des formes les plus simples d'ingénierie sociale. Les cybercriminels sont nombreux à usurper la marque Microsoft. D'après les recherches menées par Proofpoint, Microsoft occupait quatre des cinq premières places du classement des marques les plus usurpées en 2022[8].



Exemple d'attaque de collecte d'identifiants de connexion

8 Proofpoint, rapport « Le facteur humain », 2023.

Cette tentative de vol d'identifiants de connexion a échappé aux contrôles natifs de protection de la messagerie de Microsoft. Le cybercriminel a envoyé un message à un collaborateur d'un centre de support client en se faisant passer pour un membre du personnel du support informatique. Pour paraître authentique, le message du cyberpirate utilisait un nom d'affichage reconnaissable et la marque Microsoft. Proofpoint constate souvent que les cybercriminels utilisent une URL légitime (dans cet exemple, sendgrid.net) pour contourner les fonctionnalités d'analyse des URL de Microsoft.



Environnement :
Microsoft 365

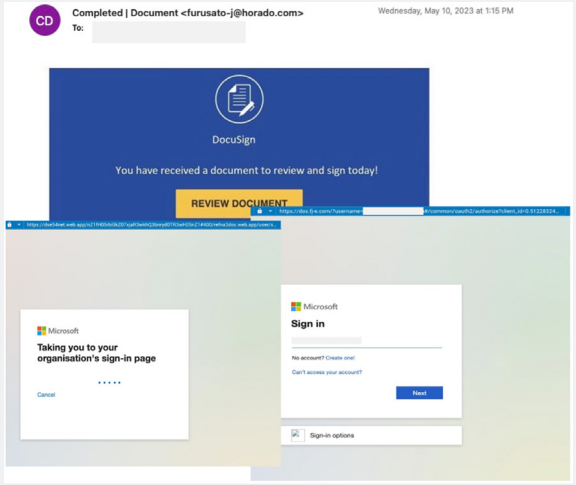
Catégorie de menace :
Phishing de l'authentification multifacteur (MFA)

Type d'attaque :
Phishing d'identifiants de connexion

Cible :
Utilisateurs de Microsoft 365

Phishing de l'authentification multifacteur (MFA)

L'authentification multifacteur (MFA) ne suffit plus à empêcher les prises de contrôle de comptes. Les cybercriminels la contournent de plus en plus facilement. Selon les recherches menées par Proofpoint, pendant les pics d'activité, le contournement de la MFA représentait plus d'un million de messages par mois en 2022[9].



Exemple de phishing de la MFA avec une URL qui redirige vers une fausse page de connexion Microsoft

Cette attaque a échappé aux contrôles de sécurité natifs de Microsoft, car elle ressemblait à une page DocuSign avec un lien permettant à l'utilisateur d'apposer sa signature. Plutôt que de diriger l'utilisateur vers DocuSign, l'URL pointe vers une fausse page de connexion Microsoft.

Pour mener cette attaque, le cyberpirate a utilisé EvilProxy, un framework de phishing ayant recours à un proxy inverse pour personnaliser les pages de renvoi pour chaque destinataire et ainsi collecter des identifiants de connexion et contourner la protection MFA. Ce kit relativement récent est disponible à la vente sur des forums d'exploits et, une fois les identifiants MFA collectés, il offre un accès persistant à un compte, même en cas de réinitialisation du mot de passe.

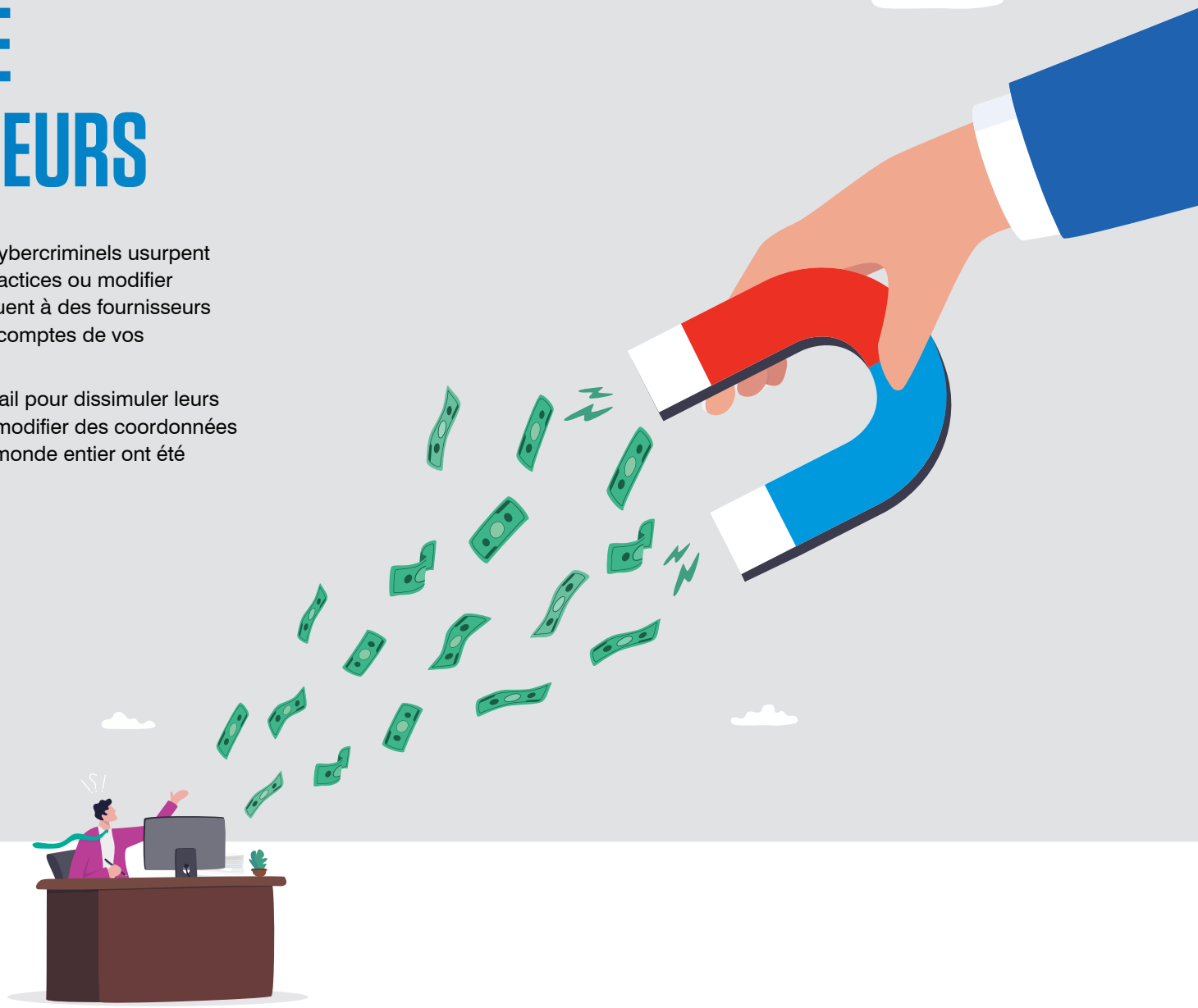
9 Proofpoint, rapport « Le facteur humain », 2023.

SECTION 5

COMPROMISSION DE COMPTES FOURNISSEURS

Comme nous l'avons déjà évoqué, lors d'attaques BEC, les cybercriminels usurpent souvent l'identité de fournisseurs pour envoyer des factures factices ou modifier des coordonnées bancaires. Il arrive également qu'ils s'attaquent à des fournisseurs ou à d'autres tiers de confiance en vue de compromettre les comptes de vos collaborateurs ou de voler de l'argent et des données.

Une fois à l'intérieur de votre réseau, ils créent des règles email pour dissimuler leurs activités, accéder à des éléments de propriété intellectuelle, modifier des coordonnées bancaires et plus encore. En 2022, 69 % des entreprises du monde entier ont été victimes d'une attaque provenant de leur chaîne logistique[10].



10 Proofpoint, rapport « State of the Phish », 2023.

Environnement :
Microsoft 365

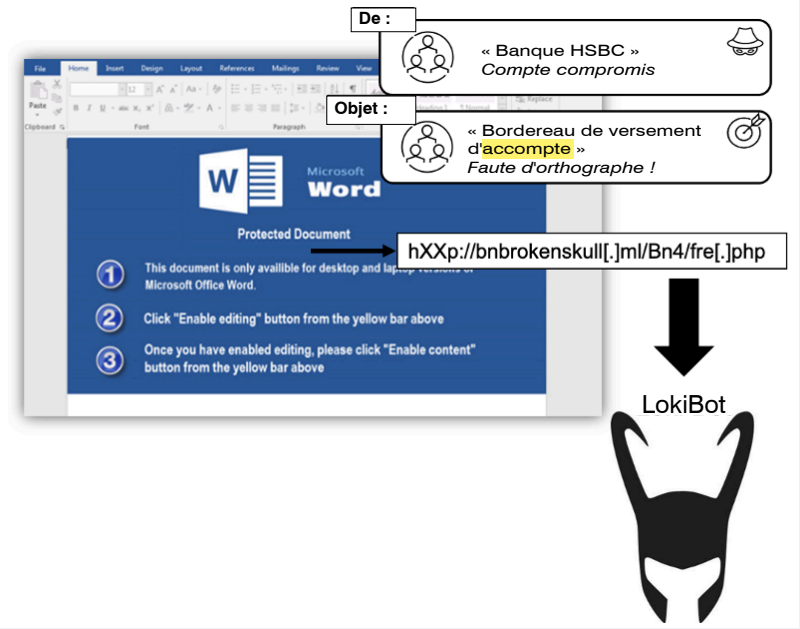
Catégorie de menace :
Attaque basée sur des URL

Type d'attaque :
Téléchargeur

Cible :
Dissimulée en copie cachée (CCI) de l'email

Pièce jointe malveillante

Les malwares font partie des techniques permettant d'infiltrer un réseau. Proofpoint a récemment effectué une analyse interne des données de près de 4 600 entreprises. Nous avons découvert que 85 % d'entre elles avaient été victimes d'une fraude aux fournisseurs par email sur une période de sept jours se terminant le 31 janvier 2023. Des malwares étaient impliqués dans environ 13 % de ces attaques[11].



Exemple d'attaque LokiBot

11 Proofpoint, « Risque caché : comment reconnaître et prévenir les attaques de la chaîne logistique », avril 2023.

Cette attaque a été envoyée à partir d'un compte de messagerie compromis dans une banque mondiale. Le message contenait un lien vers un document Word qui exploitait diverses vulnérabilités de l'Éditeur d'équations pour télécharger LokiBot, un bot capable de voler des mots de passe depuis des navigateurs, des applications FTP/SSH et des comptes de messagerie.

Microsoft est passé à côté de cette attaque, car le message a été envoyé à partir d'un domaine légitime, de sorte que l'analyse statique de la réputation ne l'a pas identifié comme malveillant. Le message est également passé outre les vérifications d'authentification SPF. Par ailleurs, la charge virale utilisait des techniques de contournement de l'environnement sandbox et d'obfuscation de fichiers.

Environnement :
Microsoft 365

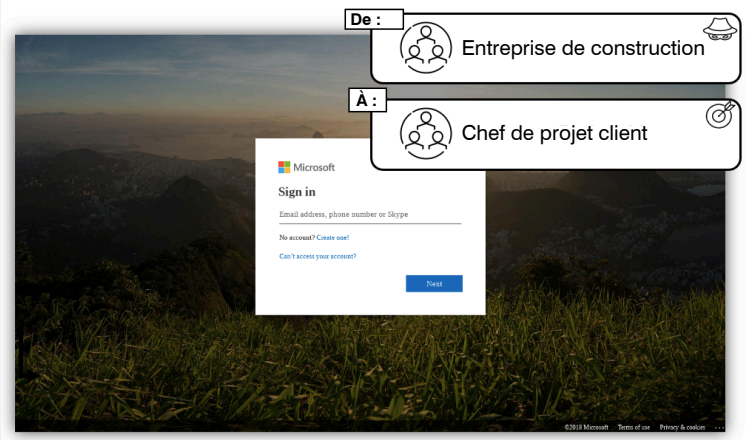
Catégorie de menace :
Attaque basée sur des URL

Type d'attaque :
Phishing d'identifiants de connexion

Cible :
Chef de projet client

Phishing d'identifiants de connexion

Les cybercriminels exploitent également des comptes fournisseurs compromis pour voler des identifiants de connexion utilisateur. Dans ces cas-là, les conséquences peuvent être encore plus préjudiciables. Malheureusement, les utilisateurs se sentent souvent libres d'interagir avec ces menaces car, même après une inspection plus approfondie, ces messages semblent légitimes, étant donné qu'ils sont envoyés à partir d'un domaine légitime.



Page imitant une page de connexion Microsoft 365

L'attaque ci-dessus a été envoyée à partir d'un compte compromis appartenant à une entreprise de construction légitime. Ce compte envoie régulièrement des emails à un chef de projet qui fait partie de ses clients. L'email malveillant contenait une URL vers une page qui imitait la marque Microsoft afin de collecter des identifiants de connexion Microsoft 365.

Cette menace a été distribuée dans la boîte de réception du chef de projet pour plusieurs raisons. Pour commencer, l'analyse de la réputation réalisée par Microsoft ne détecte généralement pas les nouvelles URL malveillantes, même lorsqu'elles usurpent la marque Microsoft. Qui plus est, ce message a été envoyé à partir du domaine d'un fournisseur légitime. L'analyse statique de la réputation effectuée par Microsoft n'a donc pas identifié l'expéditeur comme malveillant. L'enveloppe n'a pas déclenché de cas d'utilisation d'usurpation d'identité évidents.

Environnement :
Microsoft 365

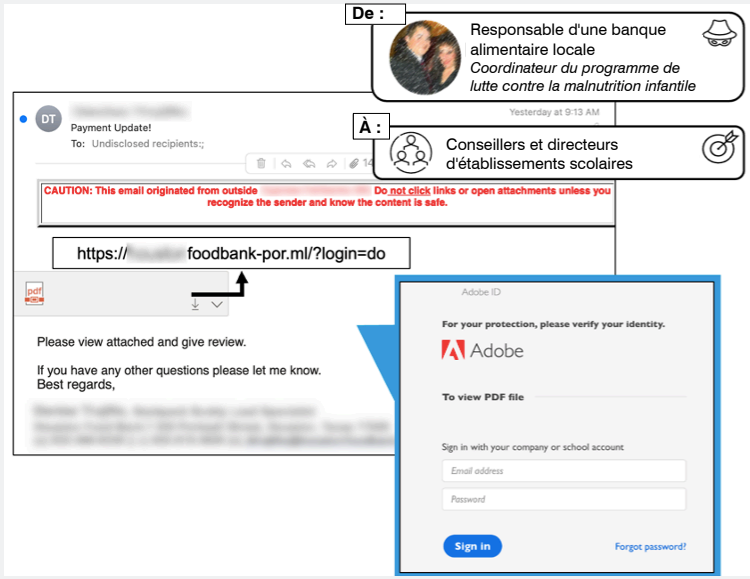
Catégorie de menace :
Attaque basée sur une pièce jointe contenant une URL

Type d'attaque :
Phishing d'identifiants de connexion

Cible :
Conseillers et directeurs d'établissements scolaires

Attaque via une URL intégrée

Tous les cybercriminels ne ciblent pas Microsoft 365. Avec la croissance des applications cloud, il est souvent plus facile d'exploiter des comptes cloud, qui sont moins protégés que Microsoft 365. Pour accroître la probabilité que sa victime active une attaque, le cyberpirate envoie un message à partir du compte compromis d'un partenaire.



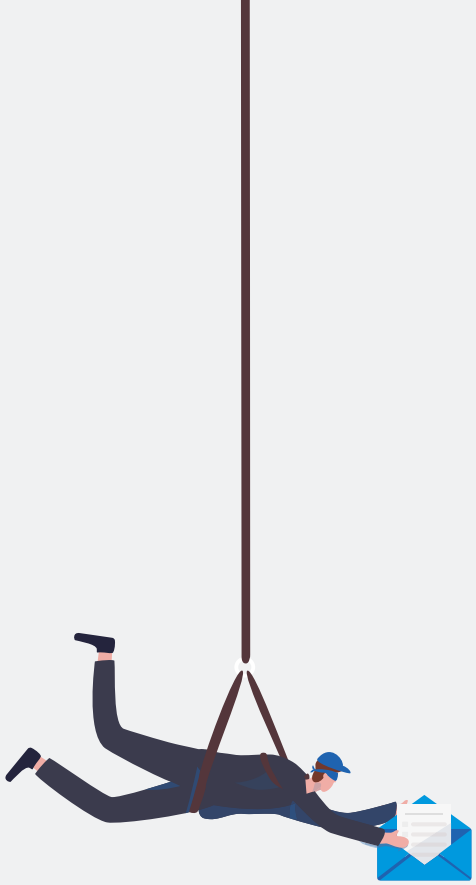
Informations sur la menace

Attaque de phishing envoyée à partir d'un compte partenaire compromis visant à établir une relation de confiance et à inciter les destinataires à divulguer leurs identifiants de connexion, ce qui peut entraîner une fuite de données

Mode opératoire

1. Envoyé à partir d'un compte partenaire compromis
2. Passé outre les vérifications d'authentification SPF/DKIM
3. Nom de confiance avec correspondance régulière
4. Entraîne la compromission du compte

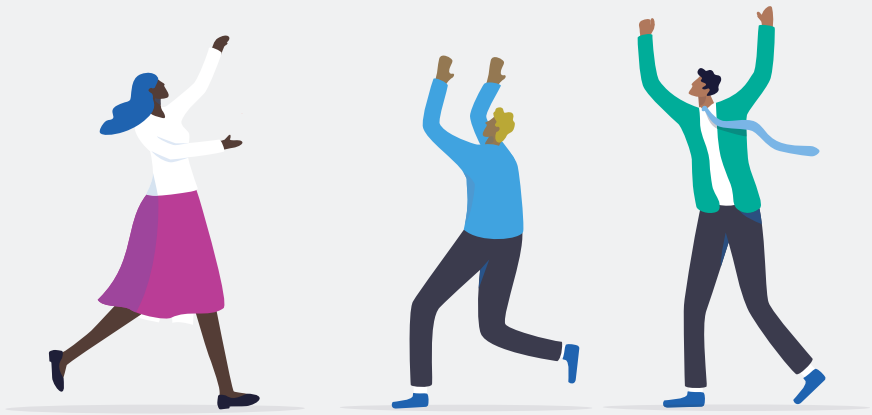
Page imitant une page de connexion Adobe



Cette attaque de collecte d'identifiants de connexion a été envoyée à partir du compte compromis d'un partenaire légitime à qui l'utilisateur envoie régulièrement des emails. Comme illustré ci-dessus, un lien intégré au message dirige l'utilisateur vers une page qui usurpe la marque Adobe dans le but de collecter les identifiants de connexion de l'utilisateur.

Microsoft n'a pas bloqué l'attaque pour plusieurs raisons. Pour commencer, elle a été envoyée à partir du compte d'un partenaire légitime, de sorte qu'elle est passée outre les vérifications d'authentification SPF/DKIM. Et comme l'utilisateur correspondait régulièrement avec ce compte, ce dernier était réputé de confiance. L'analyse statique de la réputation réalisée par Microsoft ne l'a donc pas identifié comme malveillant.

Par ailleurs, le cybercriminel est parvenu à contourner le sandboxing en intégrant la charge virale (URL) à la pièce jointe, et non à l'email lui-même. L'URL n'a pas été détectée par l'analyse de la réputation réalisée par Microsoft, qui peut passer à côté des nouvelles URL malveillantes.



Environnement :
Microsoft 365

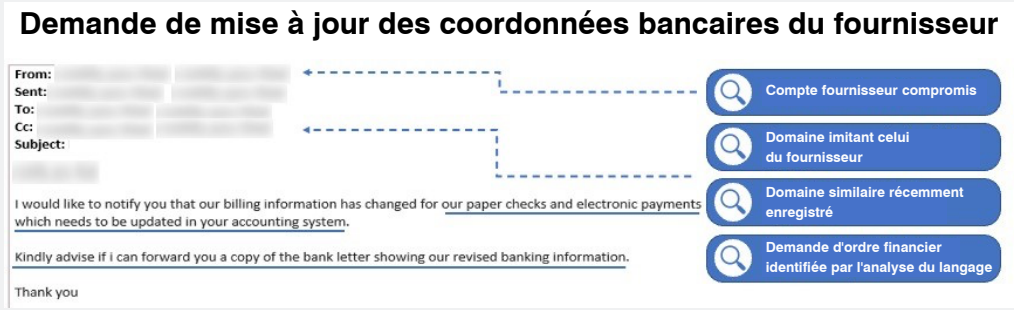
Catégorie de menace :
Ingénierie sociale, compromission de compte fournisseur

Type d'attaque :
Fraude aux factures

Cible :
Chargés de compte

Attaque d'usurpation de l'identité d'un fournisseur

Les utilisateurs sont plus susceptibles de répondre à un email malveillant lorsque celui-ci semble avoir été envoyé par quelqu'un qu'ils connaissent. Lorsque l'une de ces attaques est envoyée par un fournisseur en apparence légitime, elle devient encore plus dangereuse.



Email initial du cybercriminel

Réponse du client, envoyée à un domaine similaire

Le message initial a été envoyé à un groupe mondial de la grande distribution à partir du compte d'un fournisseur légitime. L'expéditeur demandait la modification de ses coordonnées bancaires. Cette demande en apparence inoffensive était en réalité malveillante, car le compte de l'expéditeur avait été compromis. Le cybercriminel tentait de rediriger les emails de réponse vers un domaine similaire récemment enregistré, dans le but d'intercepter des informations sensibles et de détourner des fonds.

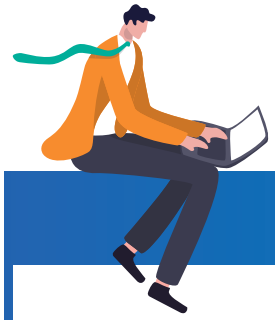
Microsoft n'a pas bloqué cette menace, car elle a été envoyée par un client légitime et est ainsi passée outre les vérifications d'authentification SPF/DKIM. Et comme l'utilisateur correspondait régulièrement avec ce compte, ce dernier était réputé de confiance. L'analyse statique de la réputation réalisée par Microsoft ne l'a donc pas identifié comme malveillant.

CONCLUSION

Les fonctionnalités de sécurité intégrées de Microsoft 365 sont un bon point de départ pour protéger votre entreprise, mais face à la multiplication et à l'évolution des menaces, des couches de protection supplémentaires sont nécessaires.

Les cybercriminels ne dépendent plus de techniques isolées. Ils combinent des tactiques sophistiquées pour exploiter les personnes. Ils sont également à l'affût de relations dont ils peuvent profiter, de liens de confiance dont ils peuvent abuser et d'accès qu'ils peuvent exploiter. Pour les stopper, vous avez donc besoin d'une approche multicouche centrée sur les personnes qui couvre l'ensemble de la chaîne d'attaque.

Pour découvrir comment Proofpoint peut renforcer la sécurité native de Microsoft 365 et protéger vos collaborateurs des cyberattaques avancées, consultez notre site à l'adresse proofpoint.com/fr.

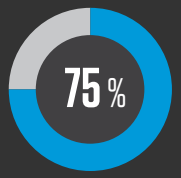


Pourquoi Proofpoint

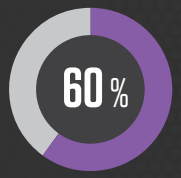
Chaque jour, nous analysons plus de :

2,6 Mrd D'EMAILS	**49 Mrd** D'URL	**1,9 Mrd** DE PIÈCES JOINTES
1,7 Mrd DE MESSAGES MOBILES	**430 Mio** DE DOMAINES WEB	**143 000** COMPTES DE RÉSEAUX SOCIAUX

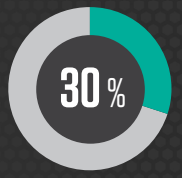
Nos solutions ont été adoptées par plus de :



DU CLASSEMENT FORTUNE 100



DU CLASSEMENT FORTUNE 1000



DU CLASSEMENT FORTUNE GLOBAL 2000

8 000 GRANDES ENTREPRISES

200 000 PETITES ENTREPRISES

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 75 % 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**.