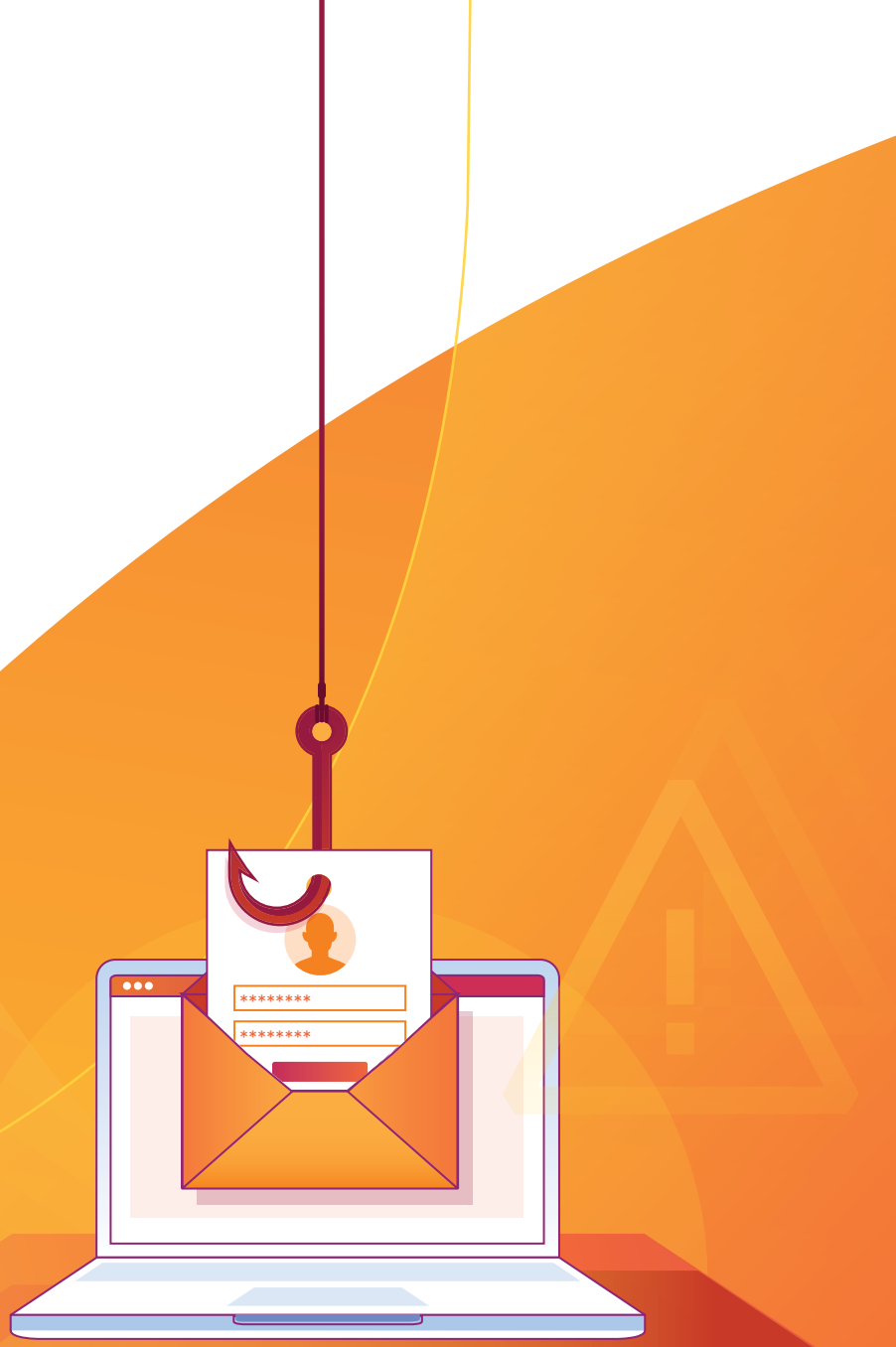
CLOUDFLARE

Rapport sur les menaces de phishing en 2023



Sommaire

Cliquez sur la section pour passer directement à la page désirée

À propos du rapport

Sommaire

Le courrier électronique est l'application professionnelle la plus exploitée. Premier vecteur d'attaque initial des incidents de cybersécurité, il contient de grandes quantités de secrets professionnels, d'informations d'identification personnelle (Personally Identifiable Information, PII), de données financières et d'autres informations sensibles, précieuses pour les acteurs malveillants.

Pour couronner le tout, le courrier électronique constitue l'une des applications les plus difficiles à sécuriser. Si l'opération était simple, nous verrions beaucoup moins de gros titres concernant le fait que les pertes dues aux attaques BEC (Business Email Compromise, compromission du courrier électronique professionnel) dépassent les 50 milliards de dollars[1] et moins de violations attribuées à un utilisateur s'étant fait prendre au piège d'un phishing. Une fois qu'un acteur malveillant a infiltré un compte e-mail, il peut effectuer des mouvements latéraux et affecter une vaste gamme de systèmes internes.

Afin d'examiner les tendances principales en matière de phishing, ce premier **rapport Cloudflare sur les menaces de phishing** s'appuie sur notre système d'information sur les menaces, qui intègre des données issues des 112 milliards de menaces que le réseau mondial de Cloudflare bloque quotidiennement. Dans le cadre de ce rapport, nous avons étudié un échantillon de plus de **279 millions d'indicateurs de menaces véhiculées par e-mail[2], 250 millions de messages malveillants[3], près d'un milliard d'occurrences d'usurpation de marque[4] et d'autres points de données rassemblés sur près de 13 milliards traités entre mai 2022 et mai 2023**.

En outre, le rapport est étayé par une étude commandée par Cloudflare et conduite par la firme Forrester Consulting. Entre janvier et février 2023, **Forrester Consulting a ainsi interrogé 316 décisionnaires en matière de sécurité (officiant dans les régions Amérique du Nord, EMEA et APAC)**[5] sur la situation actuelle du phishing.

Les pages suivantes détailleront les trois points à retenir de notre étude ci-dessous :

- **Les liens constituent la tactique de phishing n° 1 des acteurs malveillants**, qui évoluent dans la manière dont ils tentent d'amener leurs victimes à cliquer et concernant le moment où ils modifient le lien dans un but hostile.
- **L'usurpation d'identité** prend plusieurs formes **et peut facilement contourner les normes d'authentification d'e-mails**.
- Les acteurs malveillants peuvent feindre d'être des centaines d'organisations différentes, mais elles **se font principalement passer pour des entités auxquelles nous faisons confiance (et dont nous avons besoin)**.

Ne vous méprenez pas toutefois : **les acteurs malveillants ne s'attaquent pas qu'aux entreprises**. Nous avons, par exemple, observé davantage de messages provenant d'une source se faisant passer pour les Nations unies plutôt que pour la Bourse de New York[4]. De même, lors des trois mois précédant les élections américaines de mi-mandat de 2022, nous avons bloqué près de 150 000 e-mails de phishing ciblant des responsables de campagne.

Nous espérons que nos découvertes et nos recommandations vous aideront à lutter contre l'élément principal soutenant l'ensemble des attaques de phishing : **la confiance**.

Assurez-vous que la personne ou l'entité avec laquelle vous communiquez est bien celle qu'elle prétend être, que les informations que vous partagez sont légitimes et que son canal de communication (c'est-à-dire la manière dont elle vous contacte) n'a pas été compromis.

Conclusions principales

Méthode n° 1

Les liens trompeurs constituaient la méthode d'attaque n° 1 pour les cyberacteurs, avec un total de 35,6 % des menaces.[2]

89 %

des mesures d'authentification des e-mails n'arrêtent pas les menaces. La majorité (89 %) des messages indésirables ont réussi à « passer » les contrôles SPF, DKIM ou DMARC[8].

Plus de 1 000 entreprises

Les acteurs malveillants se sont fait passer pour plus de 1 000 entreprises différentes dans leurs tentatives d'usurpation de marque. Toutefois, dans la majeure partie des incidents (51,7 %), ils n'ont choisi leur identité factice que parmi les 20 plus grandes marques du monde.[4]

Catégorie de menace n° 2

Un tiers (30 %) des menaces détectées se basaient sur des domaines nouvellement enregistrés, c'est-à-dire la deuxième catégorie de menace.[7]

39,6 millions

Les menaces d'usurpation d'identité sont en hausse, avec une augmentation de 10,3 % à 14, 2 % (soit 39,6 millions) du total des indicateurs de menace par rapport à l'année précédente.[6]

Entreprises de confiance

La marque la plus usurpée s'avère être l'une des entreprises de logiciels les plus respectées au monde : Microsoft. Les autres entreprises principalement citées dans les cas d'usurpation d'identité comprenaient, entre autres, Google, Salesforce et Notion.so.[4]

Menaces de phishing multicanales

90 % des décisionnaires en sécurité interrogés conviennent que le type et la portée des menaces de phishing se développent, avec 89 % se disant préoccupés par les menaces de phishing multicanales.[5]

Vue d'ensemble des principales menaces véhiculées par e-mail

Sommaire

Vous trouverez ci-dessous un instantané des principales catégories de menace que nous avons observées entre le 2 mai 2022 et le 2 mai 2023.[2]

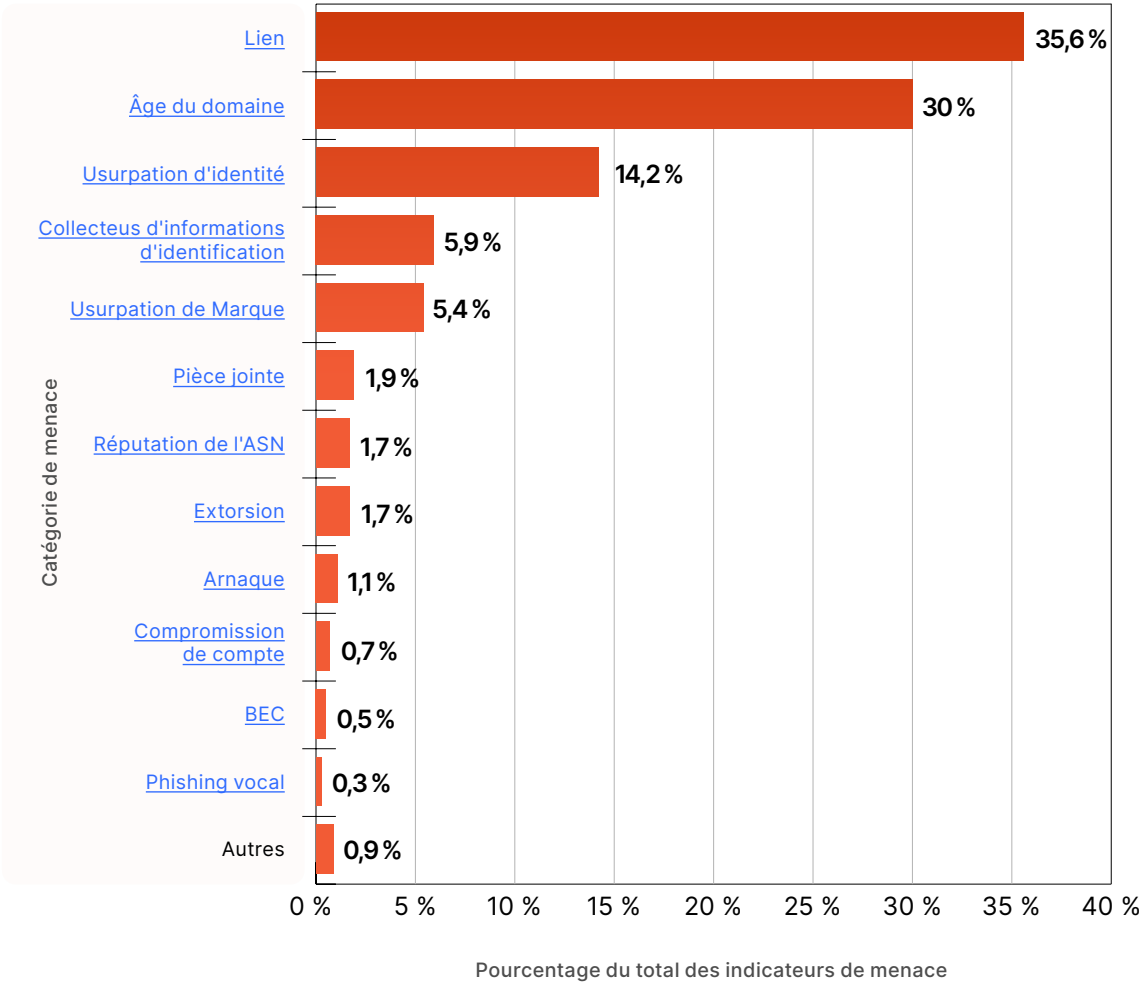
Les acteurs malveillants s'appuient souvent sur une combinaison d'ingénierie sociale et de techniques pour faire paraître leurs messages comme légitimes à la fois aux yeux du système du destinataire, mais aussi à ceux du système de l'expéditeur. Nous examinons donc de nombreux signaux de données pour identifier et bloquer les e-mails indésirables. Ces signaux comprennent :

- **L'analyse structurelle** des en-têtes, du corps des messages, des images, des liens, des pièces jointes et des contenus, parmi bien d'autres éléments, à l'aide d'instruments heuristiques et de modèles d'apprentissage automatique spécialement conçus pour ces signaux.
- **L'analyse des sentiments**, afin de détecter les changements dans les tendances et les comportements (c.-à-d. les habitudes d'écriture et les expressions).
- **Les graphiques de confiance** qui évaluent les graphes sociaux, l'historique d'expédition, ainsi que les cas d'usurpation potentielle de l'identité des partenaires.

À partir de ces signaux, nous catégorisons les indicateurs de menace sous **plus de 30** types différents.

Poursuivez votre lecture pour plus d'informations sur ces catégories principales, et notamment : les liens trompeurs, l'âge du domaine, l'usurpation d'identité, l'usurpation de marque, la compromission de compte et les attaques BEC.

Nombre de détections par catégorie de menace



Vous trouverez une description détaillée des catégories susmentionnées en annexe.

Menace principale : liens trompeurs

Sommaire

Les liens trompeurs constituaient la principale catégorie de menaces véhiculées par e-mail. Ils figuraient ainsi dans 35,6 % de nos détections. Ces liens constituaient également la première catégorie de menace l'année précédente (mai 2021 – avril 2022), en totalisant 38,4 % de l'ensemble des indicateurs.

Il est naturel de vouloir cliquer sur un lien envoyé par une personne que « vous connaissez », notamment si l'e-mail concerné arrive en temps opportun et ressemble aux e-mails précédents. Toutefois, un clic sur le mauvais lien peut avoir diverses conséquences :

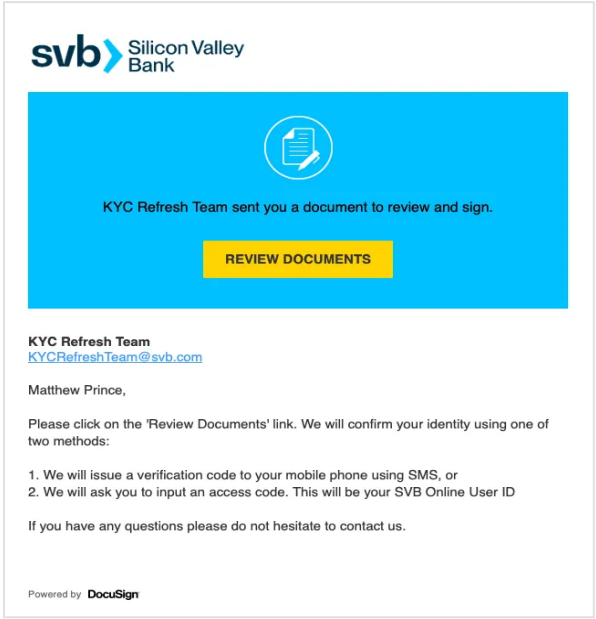
- **La captation de vos identifiants**, si vous saisissez ces derniers sur une page contrôlée par un acteur malveillant.
- **L'exécution de code à distance** (Remote Code Execution ou RCE), qui permet à un acteur malveillant d'installer un logiciel malveillant ou un rançongiciel, de dérober des données ou d'effectuer d'autres actions.
- **La compromission du réseau**, résultant de la prise de contrôle d'un poste de travail.

Les utilisateurs continuent néanmoins de cliquer sur ces liens, car il s'agit d'un comportement ancré dans notre nature. Comme le remarque le Verizon 2023 Data Breach Investigations Report (DBIR, rapport de l'enquête Verizon 2023 sur les violations de données),

« Le facteur humain représente toujours l'écrasante majorité des incidents et joue un rôle dans 74 % de l'ensemble des violations ».[12]

En détail : des escrocs exploitent une crise en temps réel

Basée sur DocuSign, la campagne SVB de mars 2023, qui a visé des dizaines d'individus dans plusieurs entreprises (dont le cofondateur et CEO de Cloudflare, Matthew Prince), s'appuyait sur du code HTML contenant un lien initial et une chaîne de redirection complexe à quatre niveaux.



Nous avons automatiquement bloqué cette campagne pour les clients de la solution Cloudflare Email Security, mais la chaîne se lançait lorsqu'un utilisateur cliquait sur le lien « Review Documents » (Voir les documents). Le clic conduisait l'utilisateur à un lien d'analyse traçable exécuté par Sizmek sur l'Amazon Advertising Server bs[.]serving-sys[.]com.

Le lien redirigeait l'utilisateur vers une application Google Firebase hébergée sur le domaine na2signing[.]web[.]app. Le code HTMP du domaine na2signing[.]web[.]app redirigeait ensuite l'utilisateur vers un site WordPress, exécuté sur un autre redirecteur hébergé sur eaglelodgealaska[.]com.

Après cette dernière redirection, l'utilisateur était alors conduit sur le site web docusigning[.]kirklandellis[.]net, contrôlé par l'acteur malveillant .

Tendance à surveiller : le phishing multicanal peut commencer par un lien « inoffensif »

Nous remarquons de plus en plus d'attaques cibler les utilisateurs via plusieurs canaux de communication, le premier d'entre eux étant généralement un lien. **Nous désignons ce type d'attaque par le nom de « phishing multicanal »**. À ce sujet, d'après l'étude que nous avons commandée auprès de Forrester Consulting, **89 % des décisionnaires en sécurité se disent préoccupés par ces menaces de phishing multicanal**[5] :

Près de 8 sur 10

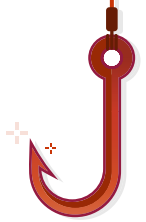
déclarent que leur entreprise est exposée sur divers canaux : messagerie instantanée/collaboration cloud/outils de productivité/mobile/SMS/canaux sociaux.

Seule 1 sur 4

parmi les personnes interrogées avait le sentiment que son entreprise était totalement préparée à faire face aux menaces de phishing véhiculées via plusieurs canaux.

Définitions des attaques

- **Attaque multicanale**
  Une attaque de phishing tentant d'exploiter un utilisateur en le sollicitant via plusieurs applications.
- **Attaque multivecteurs**
  Une tentative visant à obtenir un accès non autorisé en attaquant simultanément plusieurs points d'entrée.
- **Attaque multimodes**
  Les différentes étapes du cycle de vie d'une attaque à mesure que l'acteur malveillant progresse vers son objectif final.



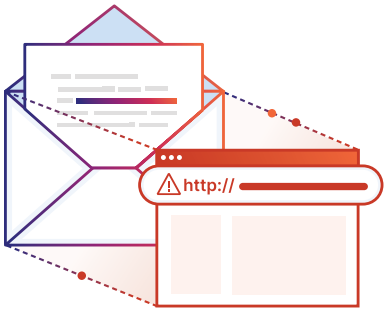
Tendance à surveiller : le phishing multicanal peut commencer par un lien « inoffensif »

Le phishing « différé », dans lequel le lien reste inoffensif lorsque l'e-mail est envoyé pour la première fois, constitue un bon aperçu de l'attaque multicanale. Prenons un exemple :

Quelques semaines avant le lancement

Configuration :

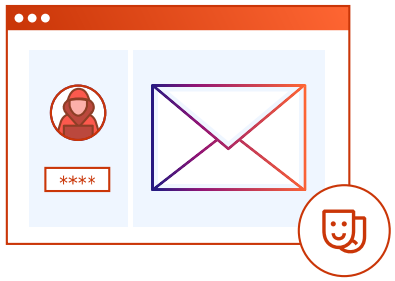
l'acteur malveillant met en place une infrastructure (par exemple, en enregistrant un domaine, en configurant une méthode d'authentification des e-mails et en créant une page web inoffensive) en préparation d'une future tentative de phishing.À ce stade les systèmes de courrier électronique ne décèlent aucune preuve d'attaque.



Dimanche

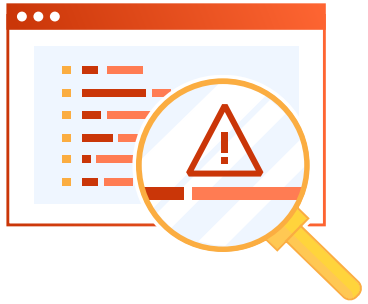
Lancement de l'attaque, première partie, dimanche matin :

l'acteur malveillant adresse un e-mail provenant du domaine nouvellement créé et comportant un lien pointant vers la page web toujours inoffensive. Les systèmes de courrier électronique n'identifient pas l'e-mail comme suspect.



Lancement de l'attaque, deuxième partie, dimanche soir :

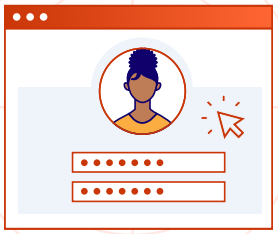
une fois l'e-mail arrivé à destination, la page web est « rendue malveillante », par exemple, en la mettant à jour afin de lui ajouter une fausse page de connexion destinée à capter des identifiants.



Lundi

Démarrage de l'attaque :

les collaborateurs commencent leur semaine en consultant l'e-mail. Il suffit que l'un d'entre eux clique sur le lien et saisisse ses identifiants pour que l'attaque réussisse.

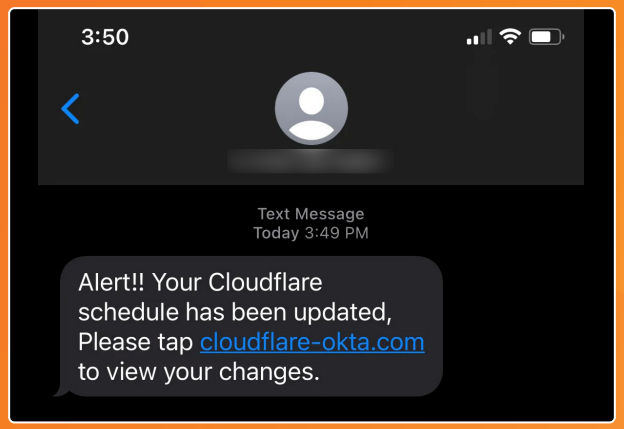


Sommaire

En détail : une tentative de phishing multicanal sur Cloudflare

En juillet 2022, l'équipe de sécurité de Cloudflare a **reçu** des rapports de collaborateurs recevant des SMS d'aspect légitime pointant vers ce qui semblait être une page de connexion Okta de Cloudflare.

Les messages texte pointaient vers un domaine d'apparence officielle (cloudflare-okta[.]com), **enregistré moins de 40 minutes** avant le début de la campagne de phishing.

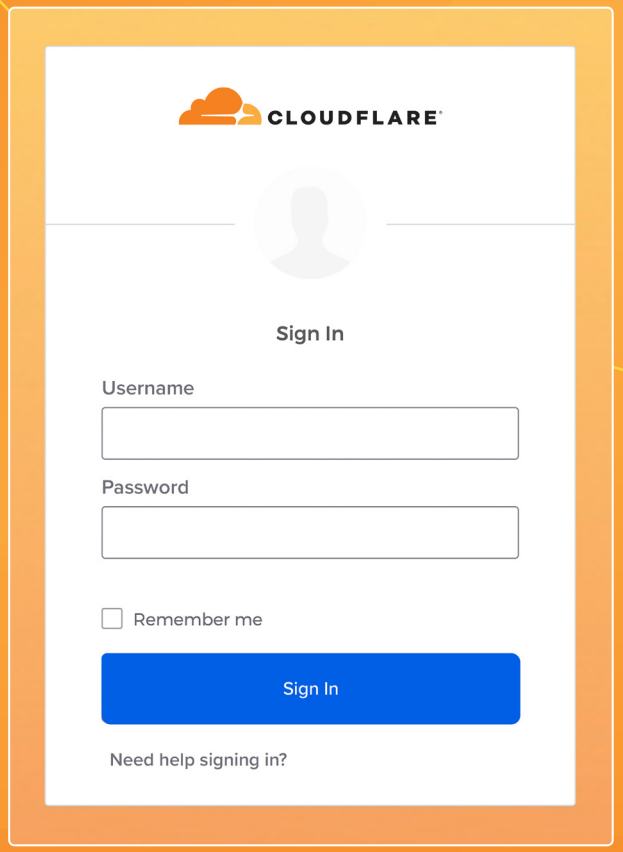


Message texte reçu par les collaborateurs de Cloudflare et pointant vers une fausse page de connexion Okta

Si l'un de nos collaborateurs avait cliqué sur le lien, ce dernier l'aurait conduit à une page de phishing apparemment identique à une page de connexion Okta légitime, invitant les visiteurs à saisir leurs identifiants (Cloudflare utilise Okta comme fournisseur d'identité).

En définitive, si l'une des victimes visées avait entrepris de saisir ses identifiants et un mot de passe temporaire à usage unique (Time-Based One Time Password, TOTP) sur le site de phishing, ce dernier aurait lancé le téléchargement de la charge utile du phishing, contenant entre autres le logiciel d'accès à distance AnyDesk. Une fois installé, ce logiciel aurait permis à un acteur malveillant de contrôler l'appareil de l'utilisateur à distance.

Toutefois, Cloudflare n'utilise pas de codes TOTP (à la place, chaque collaborateur se voit remettre une clé de sécurité physique conforme à la norme FIDO2). Les pirates n'ont donc pas pu satisfaire notre condition de détention d'une clé physique ni passer notre plateforme **SASE**, Cloudflare One.



Fausse page de connexion Okta, quasiment identique à la véritable version

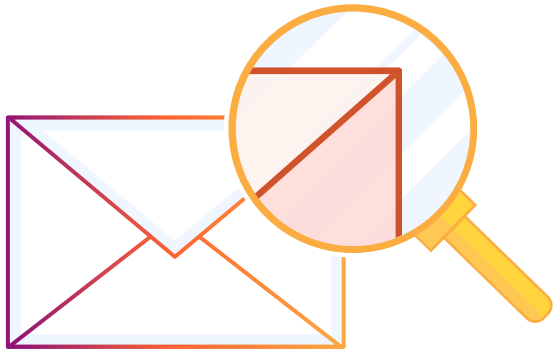
Menace principale : usurpation d'identité

Sommaire

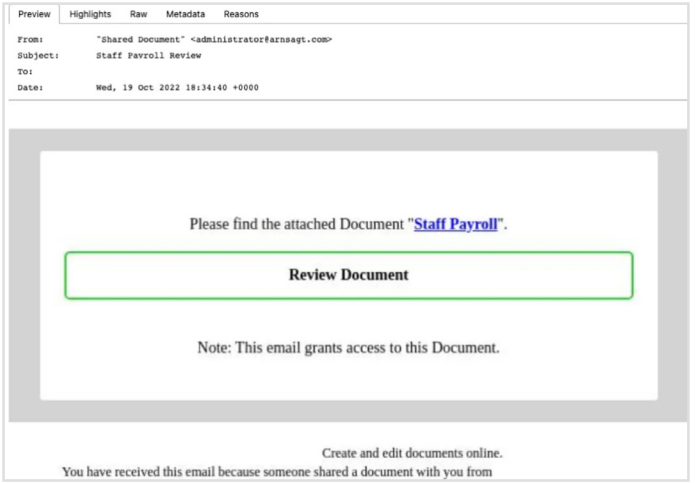
De plus en plus d'attaques s'appuient sur l'**usurpation d'identité (c'est-à-dire, le fait d'utiliser l'identité de quelqu'un d'autre)**, désormais devenue la troisième catégorie la plus courante parmi les menaces véhiculées par e-mail. Nous avons constaté la présence de l'usurpation d'identité dans **14,2 % des détections** enregistrées entre le 2 mai 2022 et le 2 mai 2023, soit un bon de 10,3 % par rapport à l'année précédente[6]. Ce type d'attaque adopte plusieurs formes, dont l'**usurpation de marque** et les attaques **BEC** (Business Email Compromise, compromission du courrier électronique professionnel).

Les principaux défis auxquels les entreprises font face en matière de prévention du phishing sont le nombre d'attaques et la difficulté liée au fait de différencier les e-mails et les sites web légitimes de leurs contreparties frauduleuses.

Qu'ils mettent en œuvre des campagnes d'envergure ou des tentatives de compromission de comptes extrêmement ciblées, **les acteurs malveillants d'aujourd'hui trouveront des moyens d'exploiter la confiance que de nombreux utilisateurs placent dans les messages envoyés par des expéditeurs « connus ».**



En détail : le phishing s'en prend à la démocratie



Lors des trois mois précédant les élections américaines de mi-mandat de 2022, Cloudflare a empêché près de 150 000 e-mails de phishing de se retrouver dans la boîte de réception de divers responsables de campagne. Ces e-mails comprenaient une tentative de phishing ciblant les collaborateurs d'un candidat au Congrès américain.

Ces derniers ont reçu un e-mail avec l'intitulé « Staff Payroll Review » (Examen des salaires des collaborateurs), qui les invitait à cliquer sur un lien vers un document. L'e-mail intégrait un pied de page valide et sa charte graphique était cohérente avec celle de la campagne.

Nos modèles ont toutefois découvert plusieurs disparités dans les métadonnées de ce dernier, notamment un lien pointant vers un domaine nouvellement enregistré.

Notre système a bloqué l'e-mail et ainsi empêché une potentielle perte de données et de ressources financières.

Sommaire

Tendance à surveiller : les menaces BEC montent en flèche partout dans le monde

De nos jours, de nombreuses entreprises ont déjà entendu parler des attaques par compromission du courrier électronique professionnel (Business Email Compromise, BEC), une forme spécifique de phishing motivée par le gain financier. Pourtant, les attaques BEC continuent de provoquer d'importants dégâts.

Pourquoi ? Les attaques BEC ne s'appuient pas sur des liens trompeurs ni des pièces jointes malveillantes, mais **tirent plutôt parti d'une compréhension approfondie des comportements du destinataire en matière de courrier électronique et des processus de l'entreprise**. Cette connaissance peut également s'étendre à la compromission de la chaîne logistique et des partenaires de confiance de la cible.

Pour prendre un exemple, la compromission de compte (susceptible d'être exploitée par les attaques BEC) désigne l'opération par laquelle un acteur malveillant prend le contrôle du compte e-mail d'un utilisateur. S'il s'agit du compte e-mail d'un partenaire, on peut alors également parler d'attaques par compromission du courrier électronique fournisseurs (Vendor Email Compromise, VEC). Les comptes compromis peuvent en cibler d'autres, car la source ne change pas.

Imaginez un fournisseur auquel vous faites confiance depuis longtemps : vous correspondez régulièrement par e-mail concernant vos projets communs, voire au sujet de ses plans pour le week-end. Un jour, vous vous retrouvez à payer une facture « factice », qui ressemble en tout point aux factures passées, si ce n'est au niveau du code bancaire. Cette situation résulte du fait qu'un acteur malveillant s'est dissimulé « dans » votre compte e-mail depuis des *semaines, voire des mois*.

Les menaces BEC ne représentaient qu'un faible volume (0,5 %) du total de nos détections[7], mais nous pensons que ce chiffre est dû au fait que nos technologies identifient ces menaces plus tôt au cours du cycle d'attaque (par exemple, avant que l'acteur malveillant n'ait eu l'occasion d'envoyer une facture frauduleuse afin de détourner un paiement).

Les entreprises qui ne parviennent pas à déjouer les attaques BEC seront confrontées à des pertes financières plus lourdes que jamais auparavant :

Plus de 50 milliards de dollars de pertes

Entre octobre 2013 et décembre 2022, le total des pertes nationales et internationales dues aux attaques BEC s'est monté à plus de 50 milliards de dollars.[1]

Une augmentation de 17 %

De décembre 2021 à décembre 2022, les pertes dévoilées et identifiées au niveau mondial comme résultant d'attaques BEC mondiales ont connu une augmentation de 17 %.[1]

Un coût plus élevé que les rançongiciels

Un total de 2 385 plaintes liées à des rançongiciels ont été déposées en 2022 pour un total de plus de 34,3 millions de dollars, par rapport aux 21 832 plaintes relatives aux attaques BEC totalisant des pertes de 2,7 milliards de dollars.[11]

71 % des entreprises

71 % des entreprises ont fait les frais d'une tentative ou d'une véritable attaque BEC en 2022.[12]

Menace principale : usurpation de marque

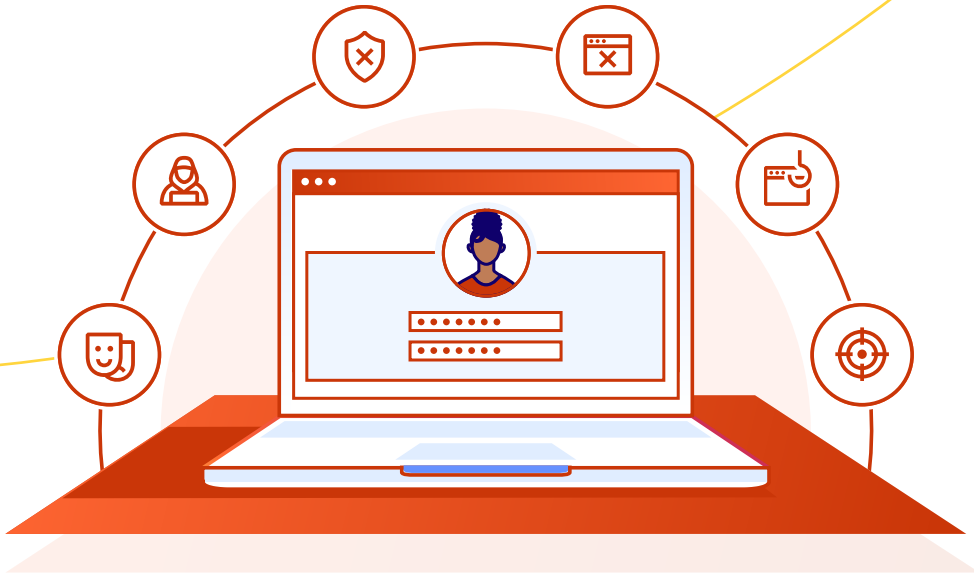
Sommaire

Dans notre ensemble de données, les acteurs malveillants se sont fait passer pour près de **1 000 entreprises différentes** sur environ milliard de tentatives d'usurpation d'identité à l'encontre de clients Cloudflare.

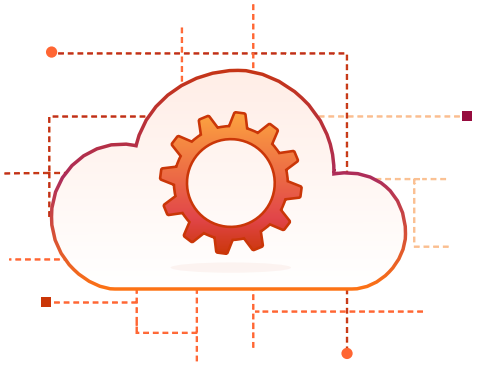
Toutefois, la majorité du temps **(51,7 %)**, ils n'ont usurpé l'identité que d'une des 20 entreprises mentionnées ci-dessous, **Microsoft**[4] en tête. Non seulement les pirates se font souvent passer pour Microsoft, mais ils utilisent également les propres outils de Microsoft pour commettre leurs fraudes.

Marques les plus usurpées:

1. Microsoft
2. Organisation mondiale de la santé
3. Google
4. SpaceX
5. Salesforce
6. Apple
7. Amazon
8. T-Mobile
9. YouTube
10. MasterCard
11. Notion.so
12. Comcast
13. Line Pay
14. MasterClass
15. Box
16. Truist Financial Corp
17. Facebook
18. Instagram
19. AT&T
20. Louis Vuitton

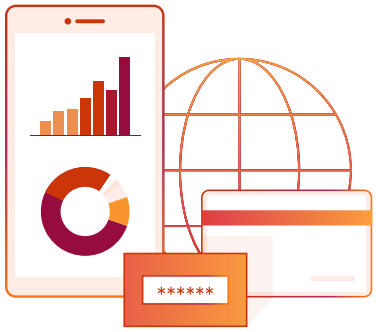


En détail : l'usurpation de marque dans certains secteurs essentiels



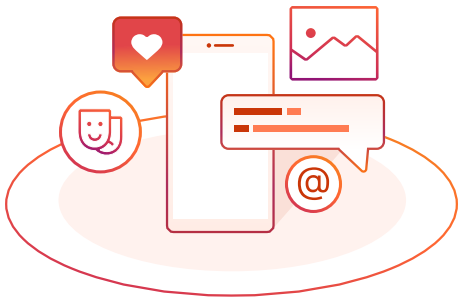
Marques de SaaS les plus usurpées :

1. Salesforce
2. Notion.so
3. Box
4. 1Password
5. Zoom
6. Rapid7
7. Marketo
8. ServiceNow
9. NetSuite
10. workday



Marques de services financiers les plus usurpées :

1. MasterCard
2. Truist Financial
3. Investec
4. Generali Group
5. Bitcoin
6. OpenSea
7. Bank of America
8. Binance
9. Visa
10. Nationwide



Marques de réseaux sociaux les plus usurpées :

1. YouTube
2. Facebook
3. Instagram
4. WhatsApp
5. Pinterest
6. Parler
7. Twitter
8. LinkedIn
9. Discord
10. Reddit

Chiffre basé sur le volume d'indicateurs d'usurpation de marque contenus dans les e-mails observés par le service de sécurité du courrier électronique Area 1 de Cloudflare entre le 2 mai 2022 et le 2 mai 2023

En détail : l'usurpation de marque dans le monde

Marques de la région EMEA les plus usurpées :

1. Organisation mondiale de la santé
2. Louis Vuitton
3. Investec
4. Chanel
5. Generali Group

Marques de la région APAC les plus usurpées :

1. LINE
2. JCB Global
3. State Bank of India
4. Toyota
5. Toshiba

Marques de la région LATAM les plus usurpées :

1. Banco Bradesco
2. Atento
3. LATAM Airlines
4. California Supermercados
5. Locaweb

Chiffre basé sur le volume d'indicateurs d'usurpation de marque contenus dans les e-mails observés par le service de sécurité du courrier électronique Area 1 de Cloudflare entre le 2 mai 2022 et le 2 mai 2023

Tendance à surveiller : l'usurpation de marque déjoue les mesures courantes de protection du courrier électronique

Le problème de l'usurpation de marque peut être partiellement traité à l'aide de mesures d'authentification des e-mails, mais ces dernières présentent de nombreuses limitations. Les acteurs malveillants peuvent, par exemple, facilement configurer leurs e-mails de manière à passer les normes d'authentification.

> Au final, **la majorité (89 %) des messages indésirables ont réussi à « passer »** les contrôles SPF, DKIM ou DMARC.[8]

Vous trouverez ci-dessous quelques moyens par lesquels un pirate usurpant une marque peut contourner l'authentification des e-mails :

- **Les méthodes SPF, DKIM et DMARC n'empêchent pas** l'usurpation par voie de similarité, qu'il s'agisse d'un e-mail, d'un domaine ou d'un nom d'affichage.
- **La méthode DKIM ne protège pas contre les attaques par rejeu**, un type d'attaque capable de « piéger » un réseau afin de l'amener à considérer que le message répondait bien aux protocoles.
- **La méthode DMARC n'empêche pas l'usurpation** du domaine d'une autre entreprise.
- **Ces normes n'inspectent pas le contenu,** elles permettent uniquement de déterminer sur le domaine de l'expéditeur est correctement configuré.

L'un des autres moyens par lesquels un acteur malveillant peut usurper avec succès l'identité d'une marque ou envoyer n'importe autre type d'e-mail de phishing consiste à utiliser un **domaine récemment enregistré** (Newly Registered Domain, NRD). Des milliers de domaines sont enregistrés chaque jour[13], la campagne de phishing multicanal contre Cloudflare (décrite plus haut) n'était qu'un exemple d'attaque NRD n'ayant pas porté ses fruits.

Les menaces dues à l'**« âge du domaine »** (en association avec divers autres points de données) **représentaient la deuxième catégorie de menace**, détectée dans **30 % de l'ensemble des e-mails indésirables**. *(Dans le cadre de ce rapport, nous avons considéré comme NRD les domaines enregistrés ou faisant état d'un changement de propriétaire dans les 48 heures précédant l'envoi de l'e-mail).*

Les attaques de phishing de tous types ont tellement gagné en sophistication que les approches traditionnelles visant à lutter contre elles ne suffisent plus à bloquer les attaques les plus dangereuses.

Pour garder une longueur d'avance sur ces dernières et sur les autres menaces avancées, poursuivez votre lecture et découvrez nos recommandations.

Recommandations

Sommaire

1 Sécurisez vos e-mails à l'aide d'une approche Zero Trust

Malgré l'omniprésence des e-mails, de nombreuses entreprises suivent toujours un modèle de sécurité de type « château entouré de douves » qui fait, par défaut, confiance aux messages provenant de certains individus et systèmes.

Dans le modèle de sécurité Zero Trust, vos systèmes ne font confiance à rien ni personne. Aucun utilisateur ou appareil ne dispose d'un accès totalement libre, ni jugé digne de confiance, à l'ensemble des applications (dont la plateforme de courrier électronique) ou des ressources du réseau. Ce changement d'état d'esprit s'avère particulièrement essentiel en présence d'environnements multicloud et d'effectifs en télétravail ou hybrides.

N'accordez pas votre confiance aux e-mails sur la seule base qu'ils passent les mesures d'authentification du courrier électronique, qu'ils proviennent de domaines réputés ou qu'ils ont été envoyés par un utilisateur avec lequel vous avez déjà un historique de communication. Choisissez une solution de sécurité des e-mails ancrée dans le modèle Zero Trust afin de compliquer la tâche aux acteurs malveillants qui tentent d'exploiter la confiance existante accordée aux expéditeurs « connus ».

2 Renforcez vos e-mails cloud à l'aide de plusieurs mesures de contrôle anti-phishing

Une défense multicouches peut répondre de manière préventive aux secteurs à haut risque des scénarios d'exposition des e-mails, notamment les suivants :

- Blocage en temps réel des attaques jamais observées auparavant, sans nécessiter « d'ajuster » la configuration d'une passerelle SEG ou d'attendre les mises à jour des politiques.
- Révélation des fraudes financières non liées à un logiciel malveillant, comme les attaques VEC et le phishing sur la chaîne logistique.
- Isolement automatique des pièces jointes ou des liens suspects contenus dans les e-mails.
- Identification et blocage de l'exfiltration de données, notamment via les plateformes de courrier électronique dans le cloud et les outils collaboratifs.
- Identification des comptes et des domaines compromis dont les acteurs malveillants se servent pour lancer leurs campagnes.

De plus en plus d'entreprises choisissent une approche superposée pour leur protection contre le phishing. Comme le remarque le rapport The Forrester Wave™: Enterprise Email Security (Sécurité du courrier électronique au sein des entreprises) du deuxième trimestre 2023, « les fournisseurs de sécurité du courrier électronique avec lesquels vous travaillez doivent apporter la preuve de leur capacité à se connecter et à partager les données les uns avec les autres, ainsi qu'avec les outils principaux de votre pile technologique de sécurité. »[15]

3 Adoptez une authentification multifacteurs résistante au phishing

N'importe quelle forme d'authentification multifacteurs (Multi-Factor Authentication, MFA) vaut mieux que rien, mais toutes les MFA ne proposent pas le même niveau de sécurité. Les clés de sécurité physiques figurent parmi les méthodes d'authentification les plus sécurisées pour empêcher les attaques de phishing d'arriver à leurs fins. Elles peuvent protéger le réseau, même si les acteurs malveillants mettent la main sur des noms d'utilisateur et des mots de passe. Vous pouvez également envisager de remplacer vos méthodes MFA existantes, comme les SMS ou les mots de passe temporaires à usage unique, par des méthodes plus éprouvées, comme les déploiements de MFA conformes à la norme FIDO.

La mise en œuvre du principe du moindre privilège peut également garantir que les pirates qui parviennent à passer les mesures de contrôle MFA ne puissent accéder qu'à un ensemble limité d'applications. De même, le partitionnement du réseau via la microsegmentation peut empêcher les mouvements latéraux et contenir les violations à un stade précoce.

4 Rendre les erreurs humaines plus difficiles à commettre

Plus l'entreprise est grande, plus chacune de vos équipes souhaitera utiliser ses propres outils et ses logiciels de prédilection.Devancez les désirs de vos collaborateurs et de vos équipes, peu importe leur localisation géographique, en sécurisant davantage les outils que vous utilisez déjà et en les empêchant de commettre des erreurs.

Pour prendre un exemple, l'isolement des liens envoyés par e-mail, qui intègre la sécurité du courrier électronique et la technologie d'isolement de navigateur à distance (Remote Browser Isolation, RBI), peut automatiquement bloquer et isoler les domaines hébergeant des liens de phishing, plutôt que de devoir faire confiance aux utilisateurs pour qu'ils arrêtent de cliquer sur ces liens.

5 Établissez une culture de la paranoïa, exempte de toute recherche de responsabilité

Encourager en permanence une approche ouverte, transparente et axée autour du concept de « problème remarqué, problème signalé » quant à la collaboration avec vos équipes chargées de l'informatique et de la réponse aux incidents de sécurité peut vous aider à englober tous vos collaborateurs au sein de la « cyber-équipe ».

Chaque minute compte lors d'une attaque. L'établissement d'une culture de la paranoïa (sans notion de recherche de responsabilité) visant à signaler toute activité suspecte, mais aussi les erreurs légitimes, à un stade précoce et contribue souvent à faire en sorte que les incidents (qu'ils surviennent fréquemment ou non) soient détectés aussitôt que possible.

En savoir plus

Pour découvrir quelles attaques de phishing échappent à vos systèmes actuels de sécurité du courrier électronique, demandez une évaluation gratuite des risques de phishing. L'évaluation ne nécessite aucune installation de matériel ou de logiciel et n'aura aucune incidence sur votre flux d'e-mails.

Pour en apprendre davantage sur la manière dont Cloudflare assure une protection Zero Trust contre les menaces véhiculées par e-mail, rendez-nous visite ici.

Annexe : glossaire des menaces

Compromission de compte : l'événement au cours duquel un acteur malveillant prend le contrôle du compte e-mail d'un utilisateur. Il est également désigné sous le nom de *compromission de compte e-mail* (Email Account Compromise, EAC), un proche parent de la *compromission du courrier électronique professionnel* (Business Email Compromise, BEC). Les acteurs malveillants emploient une vaste gamme de techniques, comme les tentatives de connexion par force brute à l'aide d'un dictionnaire, les attaques de captation d'identifiants et le vol d'identifiants. Les détails essentiels de cet événement résident dans le fait que les identifiants du compte e-mail de l'utilisateur se retrouvent compromis par le biais d'actions malveillantes. Le pirate se sert ensuite de ce compte compromis pour envoyer du contenu malveillant à de nouvelles cibles.

Réputation ASN : le score général attribué à un numéro de système autonome (Autonomous System Number, ASN) en fonction de son comportement. Les ASN à l'origine d'importants volumes de courrier indésirable ou d'e-mails malveillants, par exemple, auront tendance à avoir moins bonne réputation et donc des scores plus faibles. Les ASN aux scores de réputation bas sont souvent utilisés pour lancer des attaques.

Pièce jointe : un fichier joint à un e-mail qui, une fois ouvert ou exécuté dans le contexte d'une attaque, inclut un appel à l'action (p. ex., piéger une victime afin de l'amener à cliquer sur un lien) ou effectue une série d'actions définies par un acteur malveillant. Si la victime ouvre une pièce jointe ou clique sur un lien malveillant en pièce jointe, elle pourrait en définitive installer un logiciel malveillant susceptible de donner lieu à une attaque par rançongiciel ou à d'éventuelles opérations consécutives par le biais de backdoors ou d'un RAT (Remote Access Trojan, cheval de Troie d'accès à distance).

Usurpation de marque : une forme *d'usurpation d'identité* dans laquelle un acteur malveillant envoie un message de phishing se faisant passer pour une entreprise ou une marque reconnue. L'usurpation de marque est conduite à l'aide d'une vaste gamme de techniques. Une tactique courante est *l'usurpation de nom d'affichage*, au cours de laquelle le nom d'affichage de l'expéditeur figurant dans les en-têtes visibles de l'e-mail inclut une marque légitime. Les pirates peuvent également employer *l'usurpation de domaine*. Dans ce cas, l'acteur malveillant enregistre un domaine d'apparence similaire à celui du domaine de la marque usurpée et s'en sert pour envoyer des messages de phishing.

Les pirates font souvent usage de diverses formes de dissimulation, comme la mystification d'homographe, lors de leurs attaques par usurpation de marque. Ils peuvent également enregistrer le même domaine que celui de la marque usurpée, mais à un domaine de premier niveau (Top Level Domain, TLD) différent. Il est possible de tirer parti de ces techniques dans l'ensemble des sections d'un e-mail, notamment le nom d'affichage de l'expéditeur, l'adresse e-mail (dont le nom du domaine de l'expéditeur), la ligne d'objet, le corps de texte (HTML et texte brut), l'hypertexte des liens et les hyperliens eux-mêmes (c.-à-d. les URL en elles-mêmes).

Compromission de courrier électronique professionnel (Business Email Compromise, BEC) : une attaque par e-mail ciblée de plus en plus courante, efficace et coûteuse, conçue pour amener les destinataires à transférer des fonds, généralement par le biais de factures falsifiées, vers des comptes contrôlés par des acteurs malveillants. Les attaques BEC se divisent en diverses catégories en fonction de leur degré de sophistication, de l'utilisation d'une adresse e-mail usurpée à la compromission d'un fournisseur lors d'une attaque sur la chaîne logistique.

Capteurs d'identifiants : des sites configurés par un acteur malveillant afin de duper les utilisateurs et de les amener à renseigner leurs identifiants de connexion. Cette attaque particulière présente à l'utilisateur une page imitant une page de connexion à un compte e-mail ou à tout autre compte. Les utilisateurs inconscients du danger peuvent saisir leurs identifiants et ainsi fournir aux pirates un accès à leurs comptes. Comme les utilisateurs réutilisent souvent leurs mots de passe sur plusieurs comptes, un membre de votre entreprise qui communiquerait ses identifiants à un capteur pourrait fournir un accès à de nombreux comptes à l'acteur malveillant.

Réputation de domaine (en lien avec *l'âge du domaine*) : le score général attribué à un domaine. Pour prendre un exemple, les domaines qui envoient un grand nombre de nouveaux e-mails immédiatement après leur enregistrement auront tendance à avoir moins bonne réputation et donc un score plus faible. A contrario, les domaines plus anciens et connus ont tendance à avoir une réputation positive et, par conséquent, un score plus élevé. Les domaines aux scores de réputation bas sont souvent utilisés pour lancer des attaques.

Extorsion : cette tactique est couramment utilisée pour forcer un individu ou une entreprise à effectuer un ensemble d'actions qu'ils n'accompliraient pas en temps normal. L'opération s'effectue généralement sous la contrainte, par exemple, en demandant à la victime de verser une rançon lors d'une attaque DDoS. Le niveau d'extorsion peut conduire à une vaste gamme de compromissions, en fonction des intentions et des ressources de l'acteur malveillant.

Usurpation d'identité : cet événement survient lorsqu'un acteur malveillant ou toute autre personne animée d'une intention malveillante envoie un e-mail en se faisant passer pour quelqu'un d'autre. Les mécanismes et les tactiques de cette opération varient fortement. Certaines techniques comprennent l'enregistrement de domaines à l'aspect similaire (*usurpation de domaine*), proprement *usurpés* ou mettant en œuvre une supercherie au niveau du nom d'affichage afin de donner l'illusion de provenir d'un domaine de confiance. D'autres variations reposent sur le fait d'envoyer des e-mails à l'aide de domaines-écrans et de plateformes de services web réputées.

Lien : lorsqu'un utilisateur clique sur un lien trompeur, ce dernier ouvre le navigateur par défaut de l'utilisateur et procède au rendu des données référencées dans le lien. Il peut également ouvrir directement une application (p. ex. un PDF). Comme le texte affiché pour un lien (c.-à-d. l'hypertexte) peut être arbitrairement défini en HTML, les pirates peuvent faire croire qu'une URL pointe vers un site inoffensif, alors qu'elle est en réalité malveillante. Les liens malveillants peuvent conduire à l'exécution de code arbitraire ou à l'exécution de code à distance (Remote Code Execution, RCE), à une captation d'identifiants, à une fraude au clic, à une installation indésirable et à d'autres formes de compromission.

Arnaque : une large catégorie de fraude par phishing. L'aspect fondamental de l'opération consiste à duper une victime afin qu'elle verse de l'argent au pirate sous la promesse d'un produit, d'un service, d'un bien ou même d'une importante somme d'argent en retour. Le dénominateur commun réside dans le transfert de fonds en suivant une méthode atypique pour l'expéditeur. Les changements de pratiques de paiement ou les soudaines demandes de versement par virement bancaire peuvent également être des indicateurs.

Phishing vocal : également appelée « vishing » (pour « Voice Phishing »), cette opération désigne généralement la pratique visant à laisser de faux messages vocaux dans l'espoir que la victime rappellera pour fournir des données personnelles (comme ses coordonnées bancaires et les informations de sa carte de paiement), qui seront ensuite utilisées dans d'autres attaques. Dans nos détections de menaces relatives à la sécurité des e-mails, nous avons observé des acteurs malveillants combiner les vecteurs e-mail et vocal en envoyant des e-mails contenant des enregistrements audio en pièce jointe, un fichier multimédia ou un lien vers un fichier. Nous avons observé des pirates envoyer des e-mails ne contenant aucun contenu malveillant, mais uniquement un numéro de téléphone.

Autres : pour ce rapport, les autres catégories d'indicateurs de menace, assorties de chiffres statistiquement insignifiants, ont été regroupées dans la catégorie « Autres ». Ces catégories comprennent le « Command and Control » ou prise de contrôle directe (toute tentative de lancer un processus sur un système hôte), la politique IP (détection basée sur une politique spécifique au client) et le développement de cibles (la collecte d'informations par un acteur malveillant afin de faciliter la réussite d'une attaque future), parmi bien d'autres.

Notes de fin

Sommaire

[1] “Business Email Compromise: The $50 Billion Scam” (Compromission du courrier électronique professionnel : l'arnaque à 50 milliards). IC3.gov, 9 juin 2023. https://www.ic3.gov/Media/Y2023/PSA230609

[2] Chiffre basé sur un échantillon d'indicateurs de menace (« catégories ») détectés par le service de sécurité du courrier électronique de Cloudflare entre le 2 mai 2022 et le 2 mai 2023. Ces indicateurs présentent des dispositions d'e-mails « Malicious » (malveillant), « BEC », « spoof » (usurpation) ou « spam » (courrier indésirable). Chaque message peut contenir plusieurs catégories de menace, comme « l'usurpation d’identité », l'« usurpation de marque », les liens (« Link ») et d'autres catégories décrites en annexe.

[3] Chiffre basé sur les messages catégorisés comme « Malveillant » ou « Malveillant-BEC » par le service de sécurité du courrier électronique de Cloudflare entre le 1er mai 2022 et le 30 avril 2023.

[4] Chiffre basé sur le volume agrégé d'usurpations de marque (voir annexe) observées par le service de sécurité du courrier électronique de Cloudflare entre le 2 mai 2022 et le 2 mai 2023. Pour notre analyse : les cas d'usurpation de la marque « Microsoft » comprenaient également les cas d'usurpation des marques « Windows », « Outlook », « Office365 », « Microsoft Teams », « Windows Defender », « SharePoint », « Yammer », « OneDrive », « Skype » et « OneNote ». Les cas d'usurpation de la marque « Google » comprenaient également les cas d'usurpation des marques « Gmail » et « Hangouts ». Les cas d'usurpation de la marque « Amazon » comprenaient également les cas d'usurpation de la marque « Amazon Fresh ». Les cas d'usurpation de la marque « Apple » comprenaient également les cas d'usurpation des marques « iTunes » et « iCloud ». Les cas d'usurpation de la marque « Salesforce » comprenaient également les cas d'usurpation de la marque « ExactTarget ».

[5] Source : Forrester Opportunity Snapshot : une étude personnalisée commandée par Cloudflare, “Leverage Zero Trust to Combat Multichannel Phishing Threats” (Tirer parti du Zero Trust pour combattre le phishing multicanal), mai 2023. *Méthodologie : cette étude Opportunity Snapshot a été commandée par Cloudflare. Pour créer ce profil, Forrester Consulting a complété les recherches Forrester existantes par des questions personnalisées, avant d'interroger 316 professionnels mondiaux de niveau manager ou supérieur et responsables de la stratégie de sécurité de leur entreprise. L'étude personnalisée a débuté en janvier 2023 et s'est terminée en février 2023.*

[6] Chiffre basé sur un échantillon d'indicateurs de menace classés dans la catégorie « IdentityDeception » (usurpation d'identité, voir annexe) par le service de sécurité du courrier électronique de Cloudflare entre le 2 mai 2022 et le 2 mai 2023, et dans la catégorie « IdentityDeception » entre le 1er mai 2021 et le 30 avril 2022 par Area 1 Security. Area 1 Security a été acquise par Cloudflare en avril 2022.

[7] Chiffre basé sur un échantillon d'indicateurs de menace classés dans la catégorie « BEC » ou « BECType1 » (voir annexe) par le service de sécurité du courrier électronique de Cloudflare entre le 2 mai 2022 et le 2 mai 2023, et dans la catégorie « BEC » ou « BECType1 » entre le 1er mai 2021 et le 30 avril 2022 par Area 1 Security. Area 1 Security a été acquise par Cloudflare en avril 2022.

[8] Chiffre basé sur un échantillon de messages présentant une disposition « Malicious » (malveillant), « BEC », « spoof » (usurpation) ou « spam » (courrier indésirable) par le service de sécurité du courrier électronique de Cloudflare entre le 2 mai 2022 et le 2 mai 2023, et ayant également passé avec succès les mesures d'authentification des e-mails SPF, DKIM et/ou DMARC.

[9] Chiffre basé sur un échantillon d'indicateurs de menace classés dans la catégorie « Links » (liens, voir annexe) par le service de sécurité du courrier électronique de Cloudflare entre le 2 mai 2022 et le 2 mai 2023, et dans la catégorie « Links » entre le 1er mai 2021 et le 30 avril 2022 par Area 1 Security. Area 1 Security a été acquise par Cloudflare en avril 2022.

[10] “2023 Verizon Data Breach Investigations Report” (DBIR, rapport de l'enquête Verizon 2023 sur les violations de données). Verizon.com, dernier accès le 15 juin 2023. https://www.verizon.com/business/resources/reports/dbir/

[11] “Federal Bureau of Investigation Internet Crime Report 2022” (rapport du FBI sur la cybercriminalité en 2022). IC3.gov, dernier accès le 15 juin 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[12] “2023 AFP Payments Fraud and Control Survey” (étude AFP sur la fraude et le contrôle des paiements en 2023). AFPonline.org, dernier accès le 15 juin 2023. https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

[13] “The Domain Name Industry Brief: Q1 2023 Data and Analysis” (Présentation du secteur des noms de domaine : données du premier trimestre 2023 et analyse). Verisign.com, dernier accès le 15 juin 2023. https://www.verisign.com/en_US/domain-names/dnib/index.xhtml?section=executive-summary

[14] Chiffre basé sur un échantillon d'indicateurs de menace classés dans la catégorie « DomainAge » (âge du domaine, voir annexe) par le service de sécurité du courrier électronique de Cloudflare entre le 2 mai 2022 et le 2 mai 2023.

[15] Source : Forrester Research, “The Forrester Wave™: Enterprise Email Security, Q2 2023” (The Forrester Wave™ : sécurité du courrier électronique professionnel, deuxième trimestre 2023). 12 juin 2023. *The Forrester New Wave™ est la propriété intellectuelle de Forrester Research, Inc. Forrester et Forrester Wave™ sont des marques commerciales de Forrester Research, Inc. Forrester n'apporte son soutien à aucun des fournisseurs, produits ou services présentés dans la publication The Forrester New Wave™. Les informations reposent sur les meilleures ressources disponibles. Ces avis constituent le reflet de l'évaluation prononcée au moment de l'analyse et sont susceptibles d'évoluer.*

Téléphone : +33 7 57 90 52 73
E-mail : enterprise@cloudflare.com
Site : www.cloudflare.com/fr-fr/

RÉV. : BDES-4838.2023AUG03