Rapport 2023 de Zscaler ThreatLabz sur le phishing

Sommaire

Note de synthèse

Les escroqueries par phishing, ou hameçonnage, constituent une menace en constante progression alors que les méthodes des cybercriminels sont de plus en plus sophistiquées, et donc plus difficiles à détecter et à neutraliser.

En analysant 280 milliards de transactions quotidiennes et 8 milliards d'attaques quotidiennes neutralisées au cours de l'année 2022, l'équipe ThreatLabz de Zscaler a constaté une augmentation de 47,2 % des tentatives de phishing par rapport à 2021, une tendance à la hausse qui devrait se poursuivre en 2023.

La prévalence plus forte des kits de phishing disponibles sur les marchés noirs et des chatbots optimisés par IA tels que ChatGPT a permis aux hackers d'élaborer rapidement des campagnes de phishing toujours plus ciblées. Ce ciblage renforcé a rendu plus simple le fait de manipuler les utilisateurs en les incitant à effectuer des actions qui compromettent leurs identifiants de sécurité, et les rendent ainsi vulnérables, eux et leurs entreprises.

L'essor de l'IA et des offres PaaS facilite plus que jamais la tâche des cybercriminels qui souhaitent compromettre les organisations et accéder aux données métiers, personnelles et financières sensibles, à des fins d'extorsion. Bien que de nombreuses entreprises disposent désormais d'infrastructures de cybersécurité robustes, elles doivent toutefois les réévaluer à la lumière des tendances actuelles et envisager d'adopter une approche Zero Trust.

Ce rapport vous aidera à identifier les tactiques d'ingénierie sociale et les techniques de codage sophistiquées utilisées dans les attaques de phishing. Vous pourrez ainsi éviter des piratages de données particulièrement coûteux. Poursuivez votre lecture pour découvrir en détail les dernières tendances et observations en matière de phishing, telles que recueillies par l'équipe ThreatLabz tout au long de l'année écoulée. Vous prendrez également connaissance des bonnes pratiques permettant de protéger votre entreprise contre des techniques de phishing qui ne cessent d'évoluer.

Les temps forts de 2022

Les attaques par phishing ont bondi de 47,2 % en 2022 par rapport à 2021.

Les marques de Microsoft, notamment OneDrive et Sharepoint, ainsi que la plateforme de crypto-monnaie Binance et les services de streaming illégaux, ont été les plus ciblés en 2022.

Les États-Unis, le Royaume-Uni, les Pays-Bas, la Russie et le Canada ont été les cinq pays les plus ciblés.

L'enseignement a été le secteur le plus ciblé, subissant une progression de **576 %** des attaques, tandis que la cible principale de l'année dernière, la grande distribution et de la vente en gros, connaît un phishing en recul de **67 %**.

Les attaques sur le thème de la COVID ont représenté **7,2 %** des escroqueries par phishing en 2021, et sont en repli à **3,7 %** en 2022.

Les outils d'IA ont considérablement contribué à la croissance du phishing, en levant les barrières techniques aux exactions des criminels, leur faisant gagner du temps et des ressources.

Les hackers ont évolué au-delà du phishing par SMS (SMiShing) et utilisent désormais le vishing (hameçonnage effectué par téléphone ou message vocal) pour inciter les victimes à exécuter des pièces jointes malveillantes.

Des attaques sophistiquées de type Adversary-in-Middle (AiTM ou attaques par interception) permettent aux hackers de contourner les mesures de sécurité qu'offre l'authentification multifacteur (MFA).

Les escroqueries dans le domaine du recrutement ciblent les demandeurs d'emploi et sont de plus en plus fréquentes.

Principales cibles du phishing en 2022

Zscaler ThreatLabz a analysé des données provenant de divers pays, secteurs d'activité, marques et plateformes afin de cerner les principales cibles des attaques par phishing en 2022.

Tentatives de phishing par pays en 2022

Les dix pays les plus ciblés par les attaques par phishing au cours de l'année dernière sont les suivants :

1. États-Unis
2. Royaume-Uni
3. Pays-Bas
4. Russie
5. Canada
6. Singapour
7. Allemagne
8. France
9. Japon
10. Chine

Les États-Unis sont une fois de plus le pays le plus ciblé par les attaques par phishing, une position qu'ils ont toujours occupée. Nos recherches révèlent que plus de 65 % de toutes les tentatives de phishing ont eu lieu aux États-Unis, un chiffre en progression par rapport aux 60 % de l'année dernière. Le Royaume-Uni a subi une augmentation de 269 % des attaques par phishing.

Plusieurs pays ont vu les tentatives de phishing progresser en 2022, notamment le Canada, qui a connu une envolée de 718 %. Certains experts de ThreatLabz attribuent ce pic au secteur de l'enseignement qui est davantage ciblé. La Russie s'est vue infliger une progression de 198 % et le Japon de 92 %. En revanche, la Hongrie a connu une baisse significative de 90 % des attaques de phishing tandis Singapour enregistre une diminution de près de 48 %.

La diminution des attaques de phishing ciblant Singapour peut être due aux efforts redoublés de son gouvernement en matière de cybersécurité, notamment aux initiatives de la Cyber Security Agency (CSA). Cette agence fournit des lignes directrices et des conseils aux particuliers et aux entreprises concernant la protection contre les cybermenaces. D'autre part, la Personal Data Protection Commission (PDPC) veille à l'application des lois et des réglementations en matière de protection des données.

Illustration 1 : Tentatives de phishing par pays en 2022

Tentatives de phishing par secteur d'activité en 2022

Le secteur de l'enseignement, qui a connu une augmentation de 576 % des tentatives de phishing en 2022, passe du huitième au premier rang des secteurs les plus ciblés, dépassant le secteur le plus ciblé l'an dernier, à savoir la grande distribution et la vente en gros. Les auteurs de phishing ont probablement tiré parti des demandes liées au remboursement des prêts étudiants et d'allègement de dette qui ont été déposées l'année dernière, tout en exploitant les vulnérabilités liées à l'apprentissage à distance. Le secteur de la finance et de l'assurance a également enregistré une progression de 273 % des tentatives de phishing en 2022.

Les tentatives de phishing dans le secteur de la santé ont explosé, passant d'un peu moins de 31 millions à plus de 114 millions. Les patients qui avaient reporté leurs consultations médicales de suivi au cours de la première année de la pandémie de COVID-19 ont repris leurs traitements en 2022, se connectant à leurs comptes en ligne et interagissant potentiellement avec des auteurs de phishing se faisant passer pour des acteurs des soins de santé. En outre, les auteurs d'attaques par ransomware exploitent davantage de tactiques de phishing pour pirater les données des acteurs de la santé.

Les attaques par phishing ont toutefois connu un certain ralentissement en 2022, avec une baisse de 67 % pour la grande distribution et le commerce de gros et de 38 % pour les services. La baisse des attaques contre la grande distribution et le commerce de gros est probablement due à un changement de comportement des consommateurs, suite au volume élevé d'achats en ligne et de dépenses en biens de 2021.

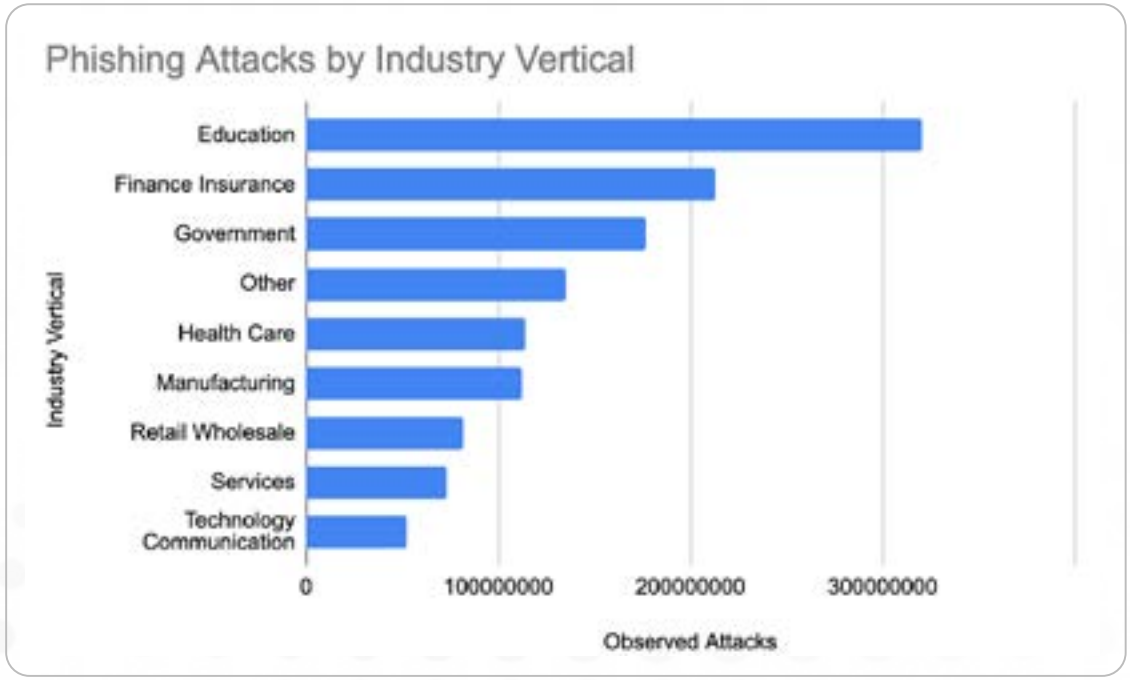
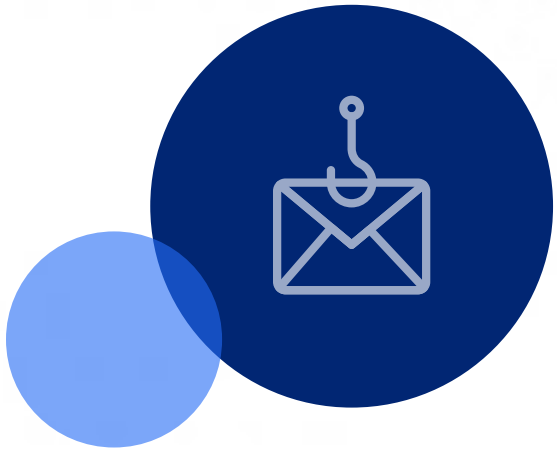


Illustration 2 : Attaques par phishing par secteur d'activité en 2022



Marques les plus usurpées dans le cadre d'attaques par phishing en 2022

Les auteurs de phishing tirent souvent parti des tendances de consommation du grand public et se font passer pour des marques populaires dans le but de tromper les consommateurs vulnérables. Les catégories de marques les plus fréquemment usurpées sont les outils de productivité, les sites de crypto-monnaies, les sites de streaming illégaux, les plateformes de réseaux sociaux et services de messagerie, les institutions financières, les sites gouvernementaux et les services logistiques.

Microsoft a de nouveau été la marque la plus usurpée de l'année, avec un peu moins de 31 % des attaques. Sa marque OneDrive a été utilisée lors de 17 % des attaques, SharePoint 4 % et Microsoft 365 1,7 %. En 2022, Zscaler a observé que les hackers utilisaient davantage OneNote, qui peut être intégré à OneDrive et à d'autres produits Microsoft, pour diffuser des malwares par le biais d'e-mails de phishing. Auparavant, les hackers ciblaient les utilisateurs par le biais de documents avec des macros malveillantes. Cependant, en juillet 2022, Microsoft a désactivé les macros par défaut sur toutes les applications Microsoft 365 (Office), obérant ainsi la capacité de cette approche à diffuser des malwares.

La plateforme de crypto-monnaies Binance a été impliquée dans 17 % des attaques utilisant l'usurpation de marques, les phishers se faisant passer pour de faux représentants de banques ou de sociétés de P2P. Les sites de streaming illégaux ont été associés à 13,6 % des attaques, avec des pics lors d'événements sportifs importants tels que la Coupe du monde FIFA en novembre et décembre 2022.

Bien qu'elles soient encore fréquentes, les attaques sur le thème de la COVID sont en repli. En 2021, les attaques basées sur la thématique de la COVID représentaient 7,2 % des escroqueries par phishing, contre seulement 3,7 % en 2022.

Les 20 marques les plus usurpées par les attaques de phishing en 2022 sont :

1. Microsoft
2. OneDrive
3. Binance
4. Sites de streaming illégaux
5. SharePoint
6. COVID-19
7. Administrations
8. Netflix
9. Facebook
10. Microsoft 365
11. Google
12. Telegram
13. Adobe
14. DHL
15. Amazon
16. American Express
17. WhatsApp
18. Roblox
19. PayPal
20. Docusign

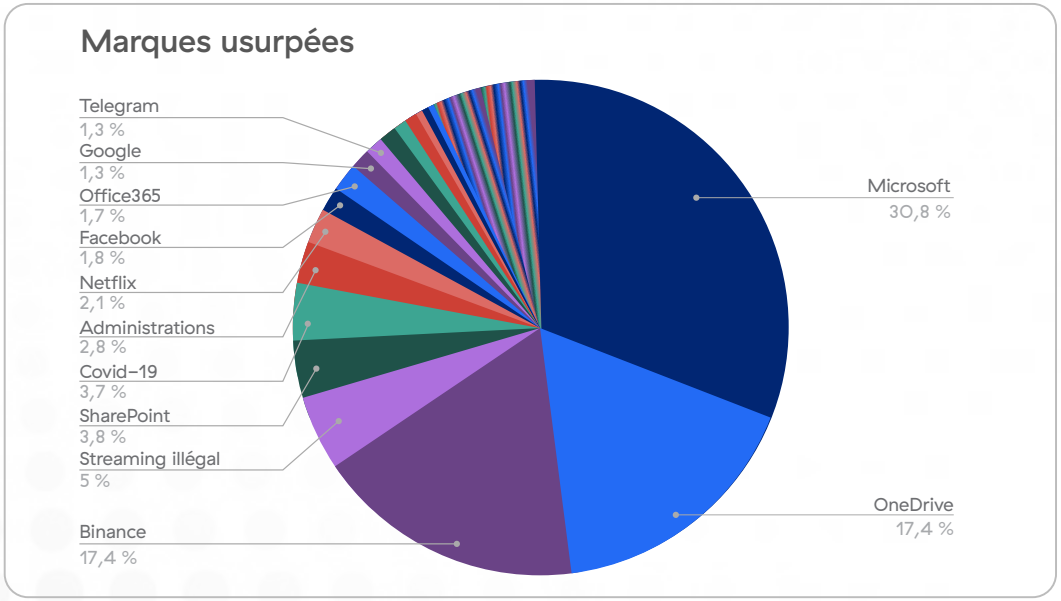


Illustration 3 : Marques les plus usurpées par les attaques de phishing

Principaux domaines référents en 2022

Les hackers utilisent souvent des domaines de confiance pour manipuler les victimes et les rediriger vers des sites de phishing. Ils vont jusqu'à acheter des publicités dans les médias ou sur des moteurs de recherche comme Google et Bing. Ils peuvent également publier des messages sur des forums d'entreprise et des places de marché telles que Walmart et Amazon ou tirer parti de sites/services de partage tels qu'Evernote, Dropbox et GitHub.

Nous avons analysé les domaines référents pour identifier ceux que les hackers privilégient. En 2022, il s'agissait notamment de sites de streaming vidéo, de plateformes de cryptomonnaies et de services financiers, d'outils de conception de sites Web et de formulaires, de sites hébergeant du contenu généré par les utilisateurs, de moteurs de recherche, etc.

Les 20 principaux domaines référents en 2022 étaient :

1. qumucloud.com
2. vimeo.com
3. bittrex-appemail.com
4. bittrex-global-emaill-i.com
5. googlesyndication.com
6. typeform.com
7. mhtestd.gov.zw
8. gutefrage.net
9. dow.com
10. framer.com
11. google.com
12. finanznachrichten.de
13. holldingsglobaloverview marketcap.com
14. hesgoal.com
15. doubleclick.net
16. elonshib.net
17. myftp.biz
18. principal.com
19. marathonbet.ru
20. baidu.comDocuSign

Les 20 domaines référents les plus utilisés dans le cadre d'attaques de phishing

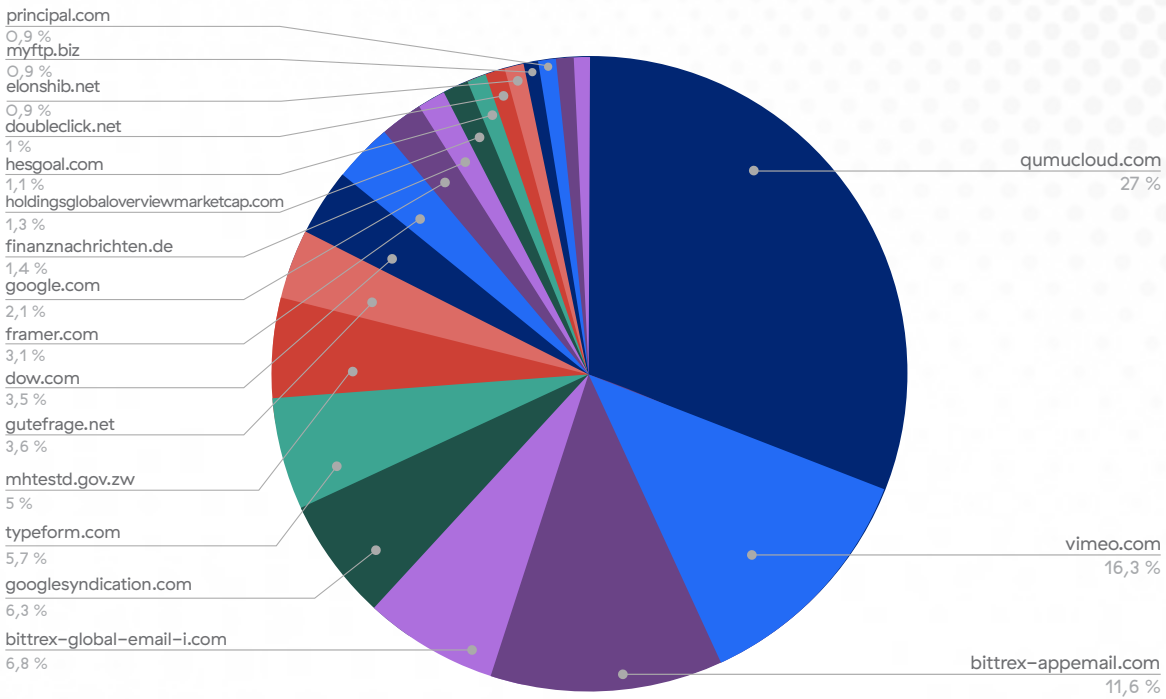


Illustration 4 : Domaines référents les plus couramment utilisés dans le cadre d'attaques par phishing en 2022

Attaques via des systèmes autonomes en 2022

Un système autonome (ou AS pour « Autonomous System ») désigne un réseau ou un groupe de réseaux doté d'une politique de routage unique. Chaque AS possède un identifiant numérique unique, appelé ASN. Dans le cadre de cette analyse, l'équipe ThreatLabz de Zscaler a examiné les ASN hébergeant l'infrastructure de phishing.

Notre analyse a révélé qu'en 2022, 39 % des attaques par phishing utilisaient des sites d'hébergement (contre 50,6 % en 2021), 53 % des FAI (contre 39,2 % en 2021) et 8 % des domaines d'entreprise.

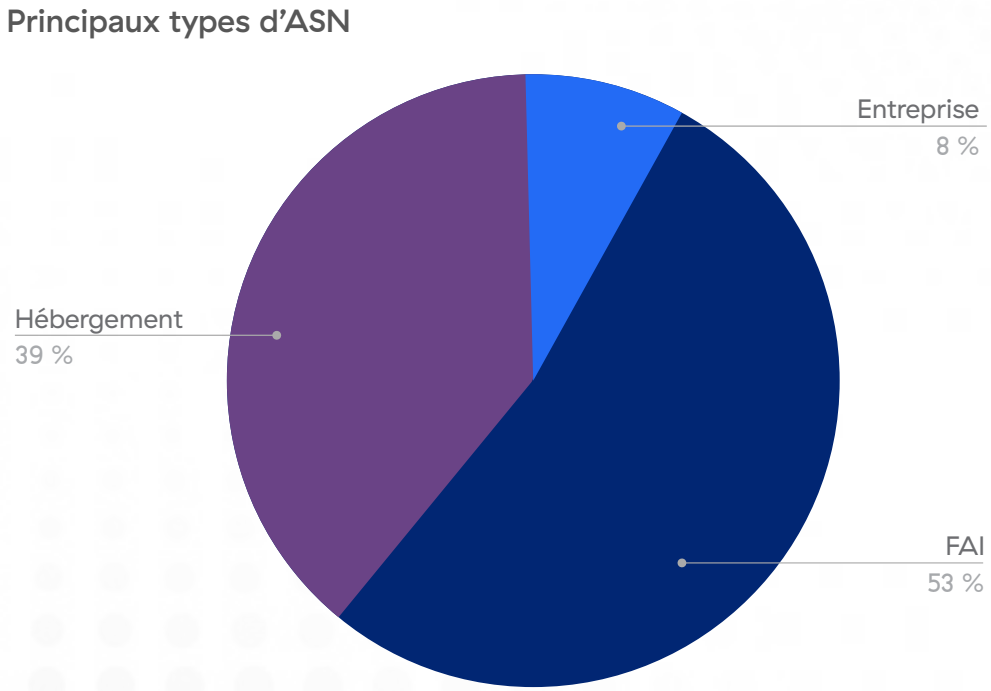


Illustration 5 : ASN pour l'infrastructure de phishing

Évolution des tendances en matière de phishing

Chaque année, les hackers utilisent des tactiques et des approches de plus en plus sophistiquées pour mener leurs escroqueries par phishing. Il est essentiel que votre entreprise et votre équipe se tiennent informées des dernières tendances en matière de menaces afin d'être préparées et de garder une longueur d'avance sur les hackers. Vous trouverez ci-dessous l'essentiel des tendances en matière de phishing observées en 2022.

Attaques de vishing

Les attaques de vishing, ou campagnes de phishing utilisant des appels et des messages vocaux, incitent les victimes à ouvrir des pièces jointes malveillantes. Mi-2022, les hackers ont ciblé les utilisateurs de diverses entreprises basées aux États-Unis à l'aide d'e-mails malveillants sensés notifier un message vocal, afin de dérober leurs données d'identification à Microsoft 365 et Outlook.

Nous avons également observé des campagnes de phishing avec des pièces jointes associées à des messages voix, telles que celle-ci :

Illustration 6 : E-mail de la campagne de vishing

Le fichier .html contient du code JavaScript obscurci :

Illustration 7 : Code de l'e-mail de vishing avec JavaScript furtif

En affichant le code de l'e-mail, vous constatez que si un utilisateur ouvre le fichier, il sera redirigé vers un serveur contrôlé par le hacker :

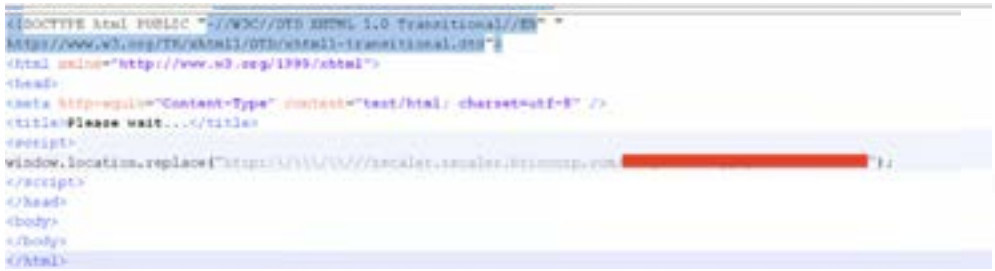


Illustration 8 : Code de l'e-mail de vishing avec affichage du JavaScript

Ceci mène à une page de phishing Microsoft :

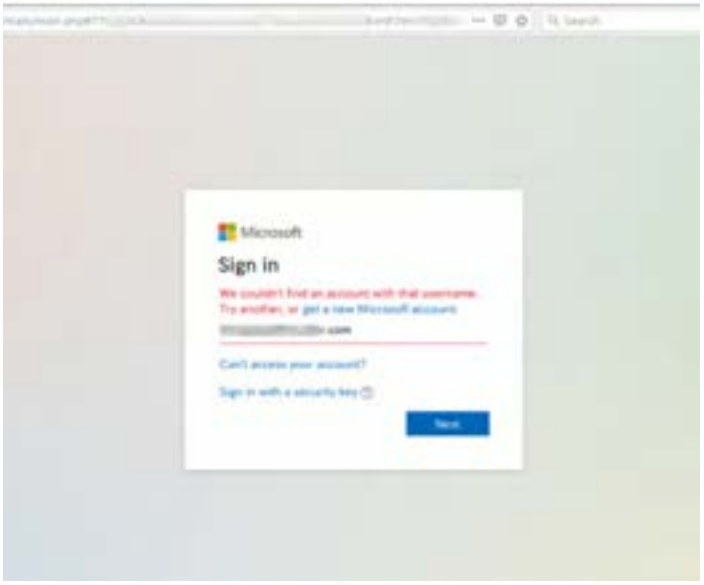


Illustration 9 : Page d'accueil d'une campagne de vishing

ThreatLabz a également découvert une escroquerie par appel vocal, avec un hacker qui s'adresse au collaborateur d'une entreprise en se faisant passer pour un directeur. Dans un premier temps, la victime reçoit un appel téléphonique usurpé avec le message « bonjour » préenregistré, puis l'appel est interrompu. Ensuite, la victime reçoit un message de l'escroc lui signalant que le directeur a des problèmes de connectivité réseau et lui demandant de poursuivre la communication par le biais de la messagerie. L'escroc tente ensuite d'amener la victime à divulguer des informations sur le compte de l'entreprise ou à transférer des fonds.

Pour éviter de tomber dans les pièges des hackers, il est essentiel d'apprendre aux collaborateurs à ne communiquer entre eux que par des canaux officiels et à faire preuve de vigilance face à ce type d'escroquerie.

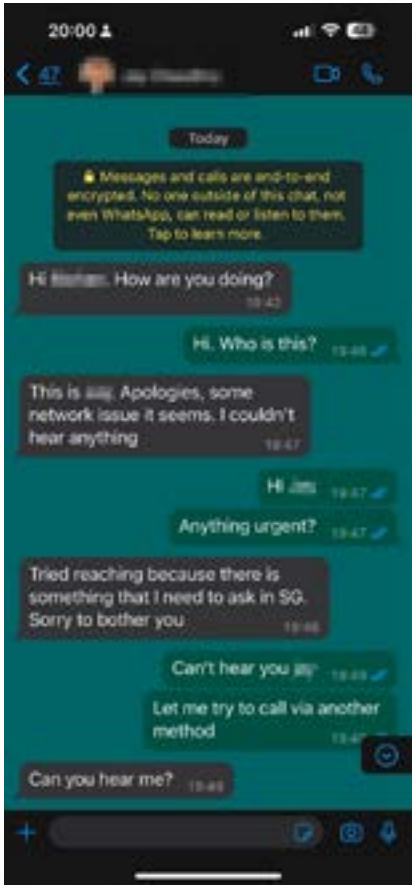


Illustration 10 : Message de vishing

Escroqueries dans le domaine du recrutement

En 2022, ThreatLabz a constaté une augmentation du nombre de demandeurs d'emploi ciblés par une série d'escroqueries liées au recrutement. Ces escroqueries utilisent de fausses offres d'emploi, de faux sites ou portails Web et des formulaires fictifs pour attirer les personnes à la recherche d'un emploi.

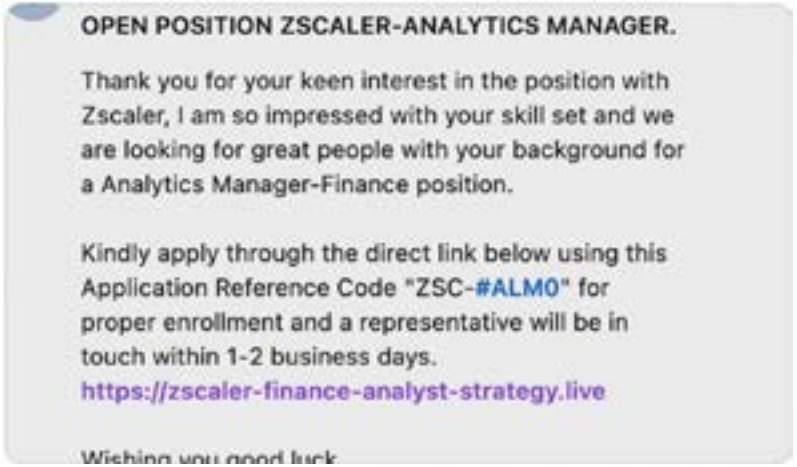


Illustration 11 : Fausse annonce LinkedIn avec une URL de phishing

Ici, le hacker a publié une fausse annonce sur LinkedIn avec une URL de phishing. En visitant cette fausse URL, les victimes potentielles pouvaient postuler à l'emploi.

Une fois que la victime a postulé, le hacker communique avec elle et lui propose un entretien sur Skype, au cours duquel il se fait passer pour un collaborateur des ressources humaines.

Illustration 12 : Faux e-mail de recrutement

En examinant le code source, vous pouvez observer des lignes de code utilisées pour exfiltrer des données de cartes de paiement.

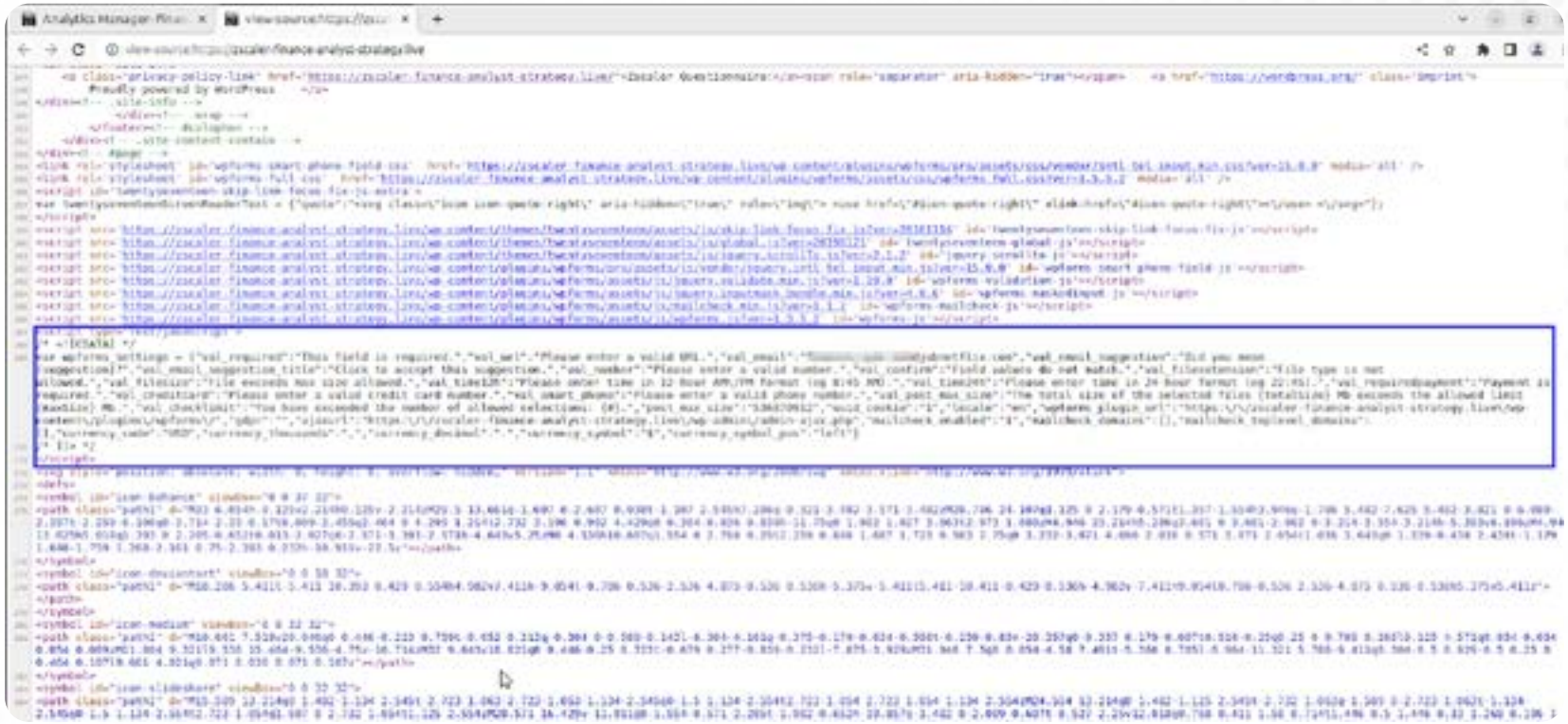


Illustration 13 : Code source du faux e-mail de recrutement

Attaques par phishing de type Adversary-in-the-Middle (AiTM ou attaques par interception)

Découvrez-en davantage sur le phishing de type Adversary-in-the-Middle (AiTM ou attaques par interception).

L'équipe ThreatLabz a découvert une nouvelle variante de campagne de phishing à grande échelle qui recourt à des techniques d'AiTM et à plusieurs tactiques de contournement. Les sites de phishing traditionnels qui recueillent les données d'identification de l'utilisateur ne procèdent à aucune authentification avec le serveur du fournisseur de messagerie. Si l'utilisateur a activé le MFA, le hacker ne pourra pas se connecter au compte en utilisant uniquement les données d'identification dérobées. Pour contourner le MFA, les hackers peuvent recourir à des attaques par phishing de type AiTM.

L'illustration 14 présente un extrait de code d'une page de phishing diffusée par un serveur de phishing AiTM.

Illustration 14 : Code d'une page de phishing diffusée par un serveur de phishing AiTM

Le serveur proxy AiTM malveillant remplace les URL d'une page de destination légitime par des URL contrôlées par le hacker (voir illustration 15) et sert de relais entre la victime et le serveur de destination.

Illustration 15 : URL contrôlées par le hacker et modifiées par le serveur proxy AiTM

Le sous-domaine d'origine (en vert), le nom de domaine d'origine (en bleu, hors domaine de premier niveau) et un identifiant unique généré (en rose) sont réunis par des tirets et deviennent un sous-domaine du site de phishing (en orange).

Nous avons décelé ce phénomène lorsque certaines demandes ont été transmises à la victime avec des modifications incorrectes, comme le montre l'illustration 16.

Illustration 16 : Modifications incorrectes transmises à la victime du phishing

Cela a entraîné une divulgation de l'adresse du serveur contrôlé par le hacker, comme le révèle l'illustration 17.

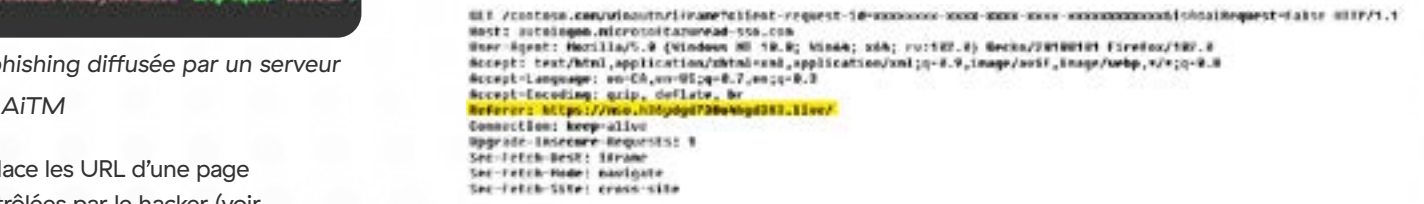


Illustration 17 : Divulgation de l'adresse du serveur contrôlé par le hacker

Attaques par phishing de type Browser-in-the-Browser (BiTB, pour navigateur dans navigateur)

Les attaques par phishing de type BiTB ont également connu une hausse en 2022. Elles simulent une fenêtre de connexion à l'intérieur d'une page principale de phishing qui fait croire à la cible qu'elle doit entrer ses identifiants de connexion unique (SSO) pour continuer à naviguer sur le site Web.

Les hackers utilisent un mix de code HTML/CSS et de cadre iFrame pour créer une fausse fenêtre contextuelle qui simule la fenêtre contextuelle SSO typique de l'utilisateur. Il peut être presque impossible qu'un utilisateur puisse distinguer une fenêtre contextuelle légitime d'une fausse fenêtre de phishing bien conçue.

L'illustration 18 propose un exemple d'attaque BiTB utilisant une fausse fenêtre SSO, générée à l'aide de HTML, pour cibler Steam, une plateforme de jeu vidéo très populaire.

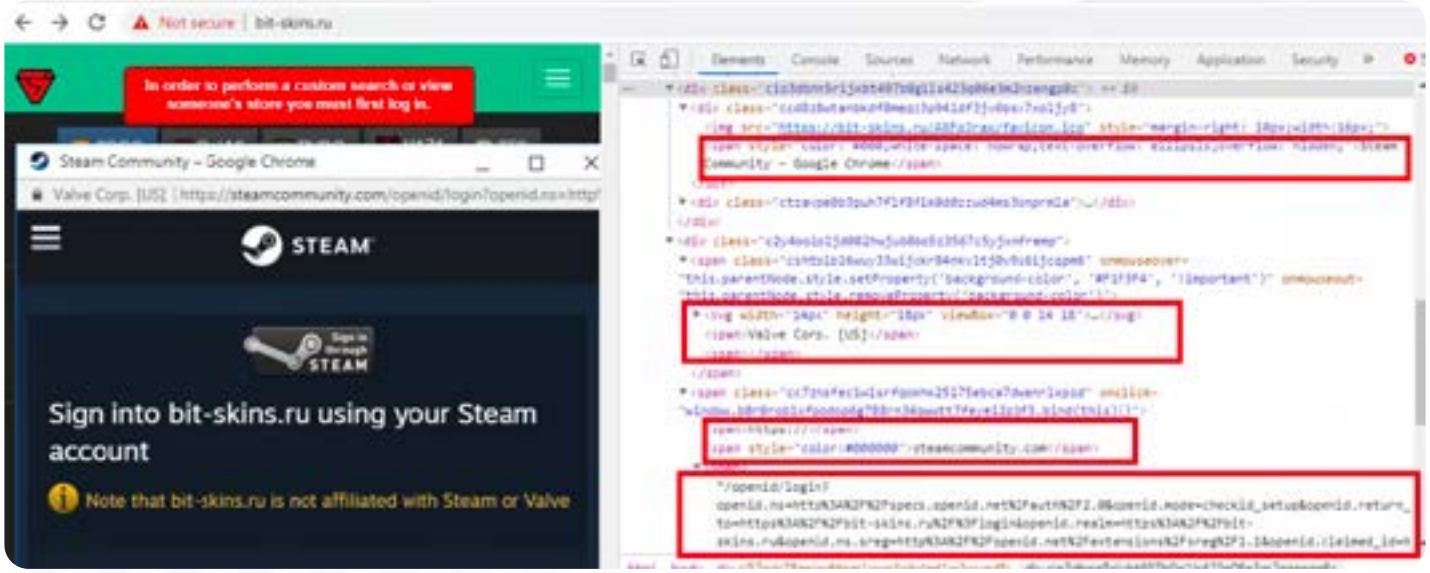


Illustration 18 : Attaque BiTB ou « picture-in-picture » (image dans l'image)

Utilisation de services légitimes pour héberger des sites de phishing

L'équipe de ThreatLabz a également observé des hackers utilisant des services légitimes pour héberger leurs sites de phishing. Certains de ces sites étaient notamment des fournisseurs d'hébergement gratuits tels que OOwebhostapp.com, des services de partage de fichiers tels que transfer.sh, des fournisseurs de services cloud tels qu'amazonaws.com, ou encore des services de raccourcissement d'URL tels que linkedin.com.

En 2022, l'équipe a remarqué que certains hackers utilisaient des services DNS dynamiques qui permettent aux utilisateurs de faire correspondre un nom de domaine à une adresse IP dynamique. Les utilisateurs utilisent principalement ces services pour l'accès à distance ou l'hébergement de sites Web sur des réseaux résidentiels.

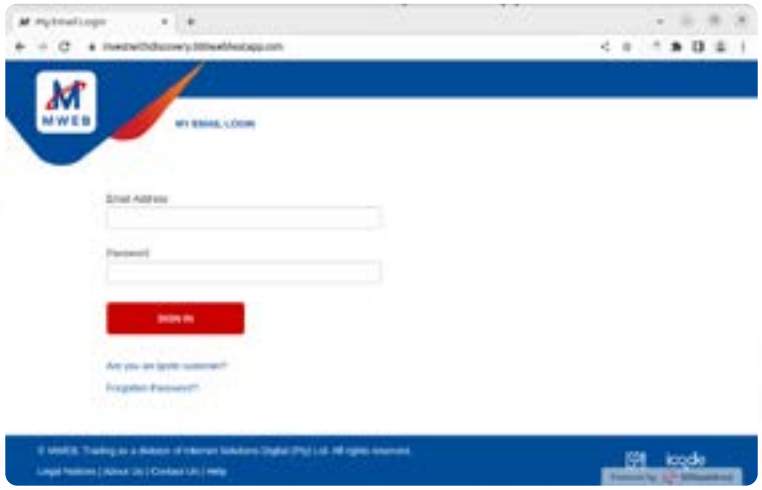


Illustration 19 : Sous-domaines DNS dynamiques pour l'hébergement de pages de phishing (exemple 1)

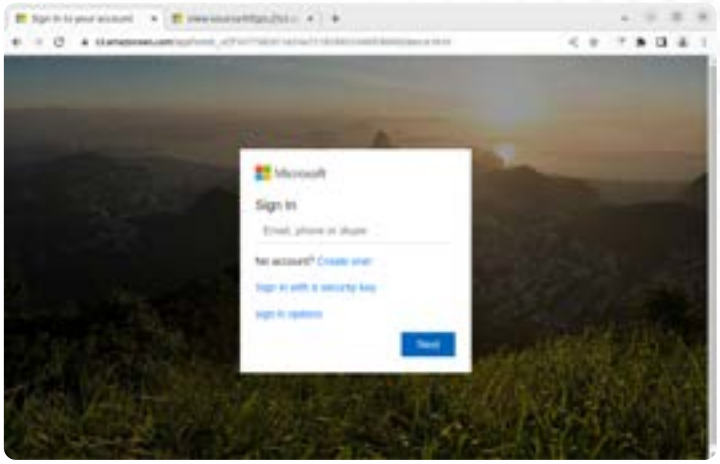


Illustration 20 : Sous-domaines DNS dynamiques pour l'hébergement de pages de phishing (exemple 2)

Les hackers peuvent également utiliser les services DNS dynamiques pour héberger des sites Web de phishing sur des ordinateurs compromis ou des serveurs sans adresse IP fixe.

Illustration 21 : Phishing T&T hébergé à l'aide d'un DNS dynamique

Phishing à l'aide du protocole IPFS (InterPlanetary File System)

L'IPFS est un système de fichiers distribué « peer-to-peer » qui permet aux utilisateurs de stocker et de partager des fichiers sur un réseau décentralisé d'ordinateurs. Par rapport aux systèmes de fichiers centralisés traditionnels, cette approche constitue un moyen plus sécurisé, résilient et efficace de stockage et de fourniture de fichiers.

Dans le système IPFS, les fichiers sont dissociés en fragments et mis à disposition via différents nœuds d'un réseau, ce qui complique le piratage de l'ensemble du système via un unique point vulnérable. L'illustration 22 décrit un cas de phishing IPFS.

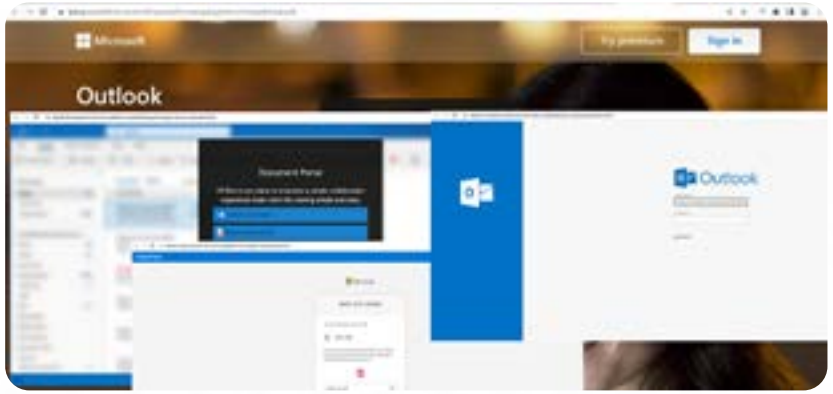


Illustration 22 : Phishing IPFS (exemple 1)

En raison de sa topologie « peer-to-peer », il est beaucoup plus difficile de supprimer une page de phishing hébergée sur un réseau IPFS qu'une page hébergée à l'aide d'une méthode plus traditionnelle.

Nous avons également observé des hackers utilisant Google Translate pour donner à leurs URL une apparence légitime.

Illustration 23 : Exemple de phishing associé à IPFS utilisant Google Translate

Comme le montre l'illustration 23, les hackers ont utilisé Google Translate sur un site de phishing hébergé sur IPFS, et ont ensuite utilisé la page pour détourner des informations d'identification DocuSign.

Utilisation de WebSockets pour exfiltrer des données ciblées par fingerprinting

Le rapport ThreatLabz 2022 de Zscaler sur le phishing aborde la question des kits de phishing et des frameworks Open Source de phishing. Ces kits et frameworks regroupent et proposent les outils nécessaires pour déployer rapidement des centaines ou des milliers de pages de phishing convaincantes et efficaces, même si les compétences techniques du ou des hacker(s) sont limitées.

Certains de ces kits de phishing disposent d'une fonction appelée « cloaking » (camouflage), une technique qui permet aux phishers de dissimuler une page Web de phishing aux yeux des chercheurs en sécurité et des outils de scan, tout en la diffusant auprès de leurs victimes. Le kit de phishing filtre les connexions de chaque visiteur en fonction de l'adresse IP, des mots clés du nom d'hôte, de l'agent utilisateur, etc. En fonction de la correspondance, il diffuse soit une page anodine, soit une page de phishing, évitant ainsi d'être détecté par les chercheurs en sécurité et les outils anti-phishing qui analysent Internet pour identifier les contenus malveillants. Ces méthodes traditionnelles de détection peuvent être contournées par les hackers au moyen de diverses techniques de dissimulation.

Nous avons observé cette année une nouvelle caractéristique liée au fingerprinting (création d'une empreinte) des clients. Voici ce qui se passe lorsqu'un visiteur arrive sur une page de phishing qui procède à une analyse par fingerprinting :

1. L'utilisateur navigue sur la page de phishing.
2. Le serveur renvoie un code JavaScript destiné à prendre l'empreinte du client, et le code JavaScript télécharge celle-ci par l'intermédiaire d'une connexion WebSocket.
3. Le serveur génère un cookie basé sur cette empreinte et renvoie le cookie via WebSocket.
4. Le code JavaScript rafraîchit automatiquement la page sur la base du cookie.
5. L'utilisateur est redirigé vers la page de phishing si les cookies satisfont au contrôle.

Le code JavaScript de fingerprinting est basé sur ce projet Open Source disponible sur GitHub.

```
{
 "type": "vdata",
 "data": {
  "languages": [
   "en-US"
  ],
  "cookieEnabled": true,
  "serviceWorker": true,
  "hardwareConcurrency": 48,
  "javaEnabled": false,
  "referrer": "",
  "etsl": 33,
  "battery": true,
  "hasChrome": false,
  "webXR": true,
  "mediaSession": true,
  "webgl": "ANGLE (Google, Vulkan 1.2.0 (SwiftShader Device (Subzero) (0x0000C0DE)), SwiftShader driver-5.0.0)",
  "timezone": "7",
  "platform": "Linux x86_64",
  "userAgent": "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0",
  "appCodeName": "Mozilla",
  "appName": "Netscape",
  "language": "en-US",
  "deviceMemory": 8,
  "vendor": "Google Inc.",
  "visitorId": "6b3a518d3ab6051e32ce5098746b411e",
  "permissions": {
   "accelerometer": "prompt",
   "ambient_light_sensor": "unknown",
   "background_fetch": "unknown",
   "background_sync": "unknown",
   "bluetooth": "unknown",
   "camera": "prompt",
   "clipboard_write": "unknown",
   "device_info": "unknown",
   "display_capture": "unknown",
   "geolocation": "prompt",
   "gyroscope": "prompt",
   "magnetometer": "prompt",
   "microphone": "prompt",
   "midi": "prompt",
   "nfc": "unknown",
   "notifications": "prompt",
   "persistent_storage": "unknown",
   "push": "prompt",
   "speaker_selection": "unknown",
   "speaker-selection": "unknown",
   "device-info": "unknown",
   "background-fetch": "prompt",
   "background-sync": "prompt",
   "persistent-storage": "prompt",
   "ambient-light-sensor": "unknown",
   "clipboard-write": "prompt",
   "display-capture": "prompt"
  },
```


Illustration 24 : Données de l'empreinte d'une machine

Cette technique peut être neutralisée en surveillant les communications WebSocket et en filtrant les données d'empreintes. Le kit de phishing peut activer une communication Command & Control (C2) pour recevoir des instructions de la part de serveurs de phishing via WebSocket, grâce à une technique appelée « communication par pulsation » (ou « heartbeat communication ») qu'utilise le hacker pour envoyer et recevoir des données en provenance de l'appareil de la victime.

Illustration 25 : Exemple de communication par pulsation

Utilisation de services de formulaires en ligne pour collecter des informations d'identification

Nous avons également observé que les assaillants tiraient parti de services permettant à leurs utilisateurs de collecter des informations par le biais de formulaires. Par exemple, FormSubmit est un service Web qui propose un moyen simple de créer et de gérer des formulaires HTML pour les sites Web. Les entreprises peuvent s'en servir pour créer des formulaires personnalisés comportant divers champs de saisie (zones de texte, cases à cocher, boutons radio, listes déroulantes et possibilités de téléchargement de fichiers), puis envoyer les données du formulaire à une adresse e-mail ou à une URL webhook donnée.

L'exemple de l'illustration 26 révèle comment les hackers peuvent exploiter les services de création de formulaires pour collecter des informations d'identification sans utilisation de serveur.

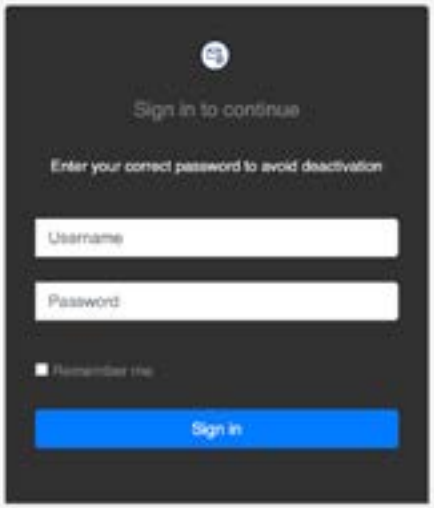


Illustration 26 : Exemple de formulaire

« L'action » du formulaire est « https://submit-form[.]com/Qz1kGknr ».

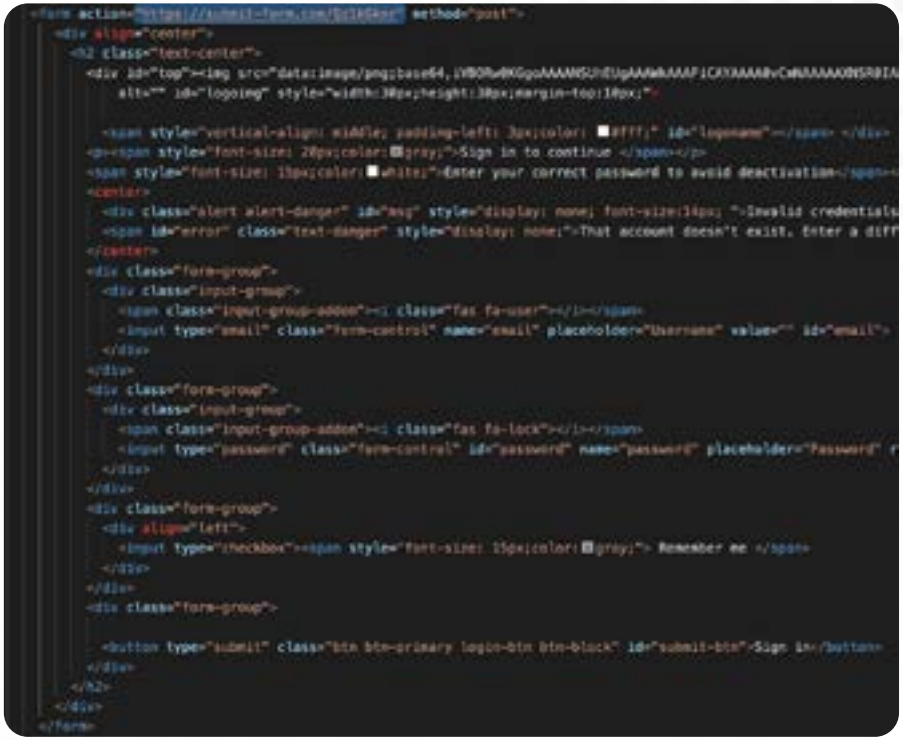


Illustration 27 : Manière dont le hacker exploite le service de formulaire pour intercepter des informations

Phishing utilisant le HTML Smuggling et les fichiers SVG

Le « HTML Smuggling » (contrebande HTML) désigne une technique qui permet aux hackers de contourner les contrôles de sécurité du réseau en intégrant un code malveillant dans un fichier HTML apparemment inoffensif, puis en transmettant des charges malveillantes à un système cible. Les mécanismes de détection analysent et détectent souvent le code JavaScript. C'est pourquoi les hackers se tournent vers la technique « HTML Smuggling » pour diffuser divers types de malware.

Les hackers transforment souvent le code du HTML Smuggling en SVG (Scalable Vector Graphics), un format graphique vectoriel basé sur XML utilisé pour créer des graphiques bidimensionnels qui peuvent être redimensionnés sans perte de résolution. Ils peuvent modifier les fichiers SVG à l'aide d'éditeurs de texte et de logiciels graphiques.

Les hackers peuvent utiliser le code JavaScript pour manipuler les éléments et les attributs SVG afin de créer différents effets d'animation, tels que le déplacement d'objets, le changement de couleurs et la création de transitions. Avec le code JavaScript, les animations SVG peuvent être interactives, ce qui permet aux utilisateurs d'interagir avec les graphiques et de déclencher diverses animations.

Les solutions de détection ne vérifient généralement pas le code JavaScript au sein du SVG, ce qui en fait une option intéressante pour les hackers.

Outils et techniques de phishing

Il existe plusieurs applications autonomes ou extensions de navigateur disponibles en ligne que les hackers utilisent pour copier un site Web légitime et modifier le code d'exfiltration des données pour dérober ces données. Voici quelques exemples :

- **HTTrack,** une application autonome largement utilisée
- **singlefile,** une extension de Google Chrome
- **Webscrapbook,** une extension de navigateur Open Source
- **Save Page WE**, une extension de Google Chrome

Phishing à l'aide d'iFrames

Un iFrame est un élément HTML qui permet aux développeurs Web d'intégrer un autre document HTML dans la page Web consultée. Ceci permet de créer un « cadre dans un cadre » dans lequel le contenu du document intégré s'affiche dans une zone rectangulaire sur la page consultée. En intégrant un contenu de phishing dans un iFrame, les hackers peuvent échapper à toute détection.

Un iFrame peut être utilisé de différentes manières à des fins de phishing :

1. iFrame imbriqué
2. iFrame en tant qu'arrière-plan
3. iFrame en avant-plan, à la manière du BiTB

En outre, nous prévoyons l'arrivée prochaine des « iFrames en tant que composants ». Cette méthode permet de combiner plusieurs iFrames pour générer une page de phishing, avec un iFrame intégré à la page.

Par exemple, le premier iFrame est utilisé pour recueillir un nom d'utilisateur (illustration 28) :

Illustration 28 : iFrame recueillant le nom d'utilisateur

Le second iFrame est utilisé pour recueillir un mot de passe (illustration 29) :

Illustration 29 : iFrame recueillant le mot de passe

Enfin, la page de phishing combine les deux iFrames (illustration 30) :

Illustration 30 : Page de phishing avec des iFrames combinés

Phishing par WebAssembly

WebAssembly désigne un format d'instructions binaires pour une machine virtuelle qui s'exécute dans les navigateurs Web actuels. Il s'agit d'un format de bytecode portable de bas niveau qui peut être exécuté de manière rapide, ce qui le destine à l'exécution d'applications critiques qui exigent des performances élevées sur le Web.

WebAssembly remédie aux limites de JavaScript en tant que langage performant pour les applications Web ; son code peut être écrit dans différents langages, tels que C++, Rust et Go, puis compilé au format bytecode WebAssembly.

Phishing ciblant des lieux géographiques

Les hackers qui souhaitent cibler des utilisateurs se trouvant dans des régions spécifiques ou parlant des langues spécifiques peuvent se tourner vers des API tierces et des services spécifiques pour identifier ces cibles.

Geo Targetly est un service qui permet aux utilisateurs de personnaliser le contenu de leur site Web en fonction de l'emplacement géographique des visiteurs. Pour déterminer le contenu de l'affichage, ils peuvent créer des règles personnalisées basées sur des critères tels que les adresses IP, les paramètres linguistiques et les fuseaux horaires.

Il n'est pas surprenant que les hackers utilisent ce service comme technique de dissimulation dans le cadre de leurs campagnes de phishing.

Utilisation de Punycode ou d'une adresse IP non standard dans les URL pour éviter toute détection

Une adresse IP est tout simplement un nombre de 32 bits qui peut être représenté par différents nombres de chiffres. Le nombre standard est de quatre chiffres, mais il existe également des adresses IP à un, deux ou trois chiffres ; chaque chiffre peut être représenté avec une base différente (binaire, octale, décimale, hexadécimale). Lorsque les auteurs de phishing représentent une adresse IP d'une manière non standard, celle-ci peut échapper à la détection, mais ce problème peut être traité en normalisant les adresses IP.

Phishing utilisant le « Hash in URL »

L'élément « hash » dans une URL fait référence à la partie de l'URL qui vient après le symbole « # ». Également connu sous le nom d'identifiant de fragment, cet élément pointe vers une section spécifique d'une page Web, telle qu'un titre de section ou un paragraphe, et permet à un utilisateur de naviguer directement vers cette section en cliquant sur un lien ou un signet.

Le contenu qui suit le symbole « # » n'est pas envoyé au serveur, de sorte que les modifications apportées au hash ne déclenchent pas de rafraîchissement de la page. Cette fonctionnalité est souvent utilisée dans les applications à page unique et les contenus Web dynamiques.

Les auteurs de phishing ont imaginé deux nouvelles façons d'en tirer parti :

1. Représenter les informations de l'utilisateur avec l'élément hash
    - Les adresses e-mail sont les plus courantes. Lorsque la page de connexion s'affiche, l'adresse e-mail de l'utilisateur est automatiquement renseignée afin de le tromper.
2. Générer des pages de phishing spécifiques, basées sur l'élément hash, personnalisées pour chaque utilisateur.

IA et phishing

Les récentes avancées technologiques en matière d'IA, telles que ChatGPT, permettent aux hackers de développer plus facilement des logiciels malveillants, de générer des attaques de type Business Email Compromise (BEC), de créer des malwares polymorphes, et bien plus encore. Nous avons tenté de générer une page de connexion de phishing à l'aide de ChatGPT, et après seulement trois interactions simples, l'outil a généré cette page Web :

Illustration 31 : Page de phishing générée par ChatGPT

Avec un peu plus de travail, un hacker pourrait ajouter un arrière-plan et modifier la page pour qu'elle ressemble à une véritable page de connexion.

Perspectives pour 2024

1. **Les attaques par IA seront de plus en plus fréquentes** à mesure que les hackers découvriront de nouvelles utilisations pour ces services. Attendez-vous à voir des escroqueries plus sophistiquées sur différents canaux de communication (e-mails, SMS et sites Web). Préparez-vous également à une recrudescence des tentatives de phishing, car les hackers utilisent l'IA pour lancer des attaques plus coordonnées et plus efficaces sur des groupes de personnes plus larges.

2. **Les offres de Phishing-as-a-Service continueront d'évoluer,** les fournisseurs proposant des modèles de phishing personnalisés, un accès à de plus grandes bases de données sur des victimes potentielles et des techniques d'ingénierie sociale plus avancées. Les fournisseurs pourront également proposer des services complémentaires tels que l'installation, l'hébergement et l'analyse de malwares. De plus, ces fournisseurs rivaliseront pour offrir le meilleur rapport qualité-prix, avec des modèles de tarification abordables et un support client 24 h/24, 7 j/7. Il est donc primordial de rester informé des dernières menaces et tendances en matière de phishing.

3. **Les attaques sur appareils mobiles deviendront de plus en plus fréquentes,** les hackers cherchant à exploiter notre dépendance à l'égard de ces dispositifs. Les assaillants développeront des contenus plus adaptés aux appareils mobiles, tels que des applications et des sites Web optimisés, mais aussi des malwares, notamment des spywares et des chevaux de Troie d'accès à distance. Ils trouveront également de nouveaux moyens d'extorquer de l'argent à leurs victimes.

4. **Les attaques de type MFA Bombing et AitM vont se multiplier** à mesure que les assaillants trouveront des moyens de contourner la sécurité MFA. Les attaques de type MFA Bombing submergent les victimes de demandes d'authentification, tandis que les attaques AitM interceptent la session de la victime après son authentification par MFA. Les hackers utiliseront des techniques avancées, dont l'IA, pour prédire et générer des codes de vérification ou identifier des schémas de comportement de l'utilisateur, pour les exploiter et obtenir un accès. Pour se protéger contre ces attaques, il est essentiel d'utiliser des mots de passe forts, d'activer l'authentification à deux facteurs et de surveiller les comptes afin de détecter toute activité suspecte.

5. **Les attaques personnalisées seront de plus en plus difficiles à détecter** à mesure que les hackers développeront des techniques avancées de reconnaissance pour recueillir des informations sur leurs victimes potentielles. Ces informations seront utilisées pour créer des e-mails de phishing sur mesure qui paraîtront plus légitimes et plus convaincants, augmentant ainsi leurs chances de réussite. À mesure que les hackers gagnent en sophistication dans l'art de la personnalisation, les utilisateurs auront de plus en plus de mal à identifier et à éviter les attaques par phishing.

Améliorer vos défenses contre le phishing

Les statistiques révèlent qu'une entreprise moyenne reçoit des dizaines d'e-mails de phishing par jour, avec des pertes financières qui font boule de neige. En effet, les pertes encourues par les attaques de malwares et de ransomwares renchérissent les coûts moyens des attaques par phishing, année après année. Faire face à toutes les menaces décrites dans ce rapport n'est pas une tâche aisée, et bien que vous ne puissiez éliminer complètement le risque de phishing, vous pouvez réduire la probabilité de voir votre entreprise en être victime.

Les principes de base pour maîtriser le risque de phishing portent sur :

Bonnes pratiques : formation et sensibilisation à la sécurité

Les campagnes de phishing connaissent un taux de réussite élevé, car elles ciblent les utilisateurs : il suffit d'un seul collaborateur distrait pour commettre une erreur de jugement et mordre à l'hameçon. Selon une étude réalisée en 2020 par l'université de Stanford, près de 88 % des incidents de données sont imputables à une erreur humaine. Le rapport a également révélé que les jeunes collaborateurs masculins sont les plus vulnérables aux escroqueries par phishing et que l'étourderie est la principale cause d'erreur pour tous les profils. C'est pourquoi une sensibilisation régulière des utilisateurs finaux, plusieurs fois par an, est essentielle pour prévenir les incidents de sécurité. Tous les collaborateurs de votre entreprise doivent être sensibilisés à la manière dont ils peuvent être victimes d'attaques par phishing et se méfier des informations qu'ils communiquent ou des liens sur lesquels ils cliquent lorsqu'ils sont confrontés à des e-mails, sites Web, SMS, applications et appels téléphoniques non fiables.

La mise en place d'une formation continue de sensibilisation à la sécurité et des simulations régulières de phishing sont essentielles pour développer une culture de vigilance et une sensibilisation efficace au phishing. Ces activités vous permettent de dispenser une formation en temps utile aux personnes qui auraient besoin d'un accompagnement supplémentaire pour identifier les tentatives de phishing et modifier leurs comportements à risques. Une autre façon de réduire le nombre d'incidents de phishing consiste à améliorer la capacité des utilisateurs à signaler les e-mails de phishing, ce qui permet aux équipes de sécurité de supprimer plus rapidement la menace dans tous les comptes email de l'entreprise. Par exemple, une alerte peut être lancée en proposant un bouton « Signaler un phishing » directement à partir de la boîte de réception.

ThreatLabz recommande en outre que votre formation de sensibilisation suive les conseils de l'agence américaine Cybersecurity Infrastructure & Security Agency (CISA) qui recommande aux utilisateurs finaux d'être attentifs aux indicateurs suivants :

- **Adresse d'expéditeur suspecte.** L'adresse e-mail d'un expéditeur peut imiter une entreprise légitime. Les cybercriminels utilisent souvent une adresse e-mail qui ressemble beaucoup à celle de sociétés connues, en modifiant ou en omettant quelques caractères.
- **Salutations et signatures génériques.** Une formule de salutation générique, telle que « Cher client » ou « Madame/Monsieur », et l'absence d'informations de contact dans le bloc de signature sont de bons indicateurs d'une attaque par phishing. Une entreprise de confiance s'adressera normalement à vous par votre nom et fournira ses coordonnées.
- **Hyperliens et sites Web usurpés.** Si vous passez votre curseur sur un lien dans le corps de l'e-mail et que ce lien ne correspond pas, il se peut que le lien ait été usurpé. Les sites Web malveillants peuvent sembler identiques à un site légitime, mais l'URL peut utiliser une variante orthographique ou un domaine différent (par exemple, « .com » au lieu de « .net »). En outre, les cybercriminels peuvent utiliser un service de raccourcissement d'URL pour cacher la véritable destination du lien.
- **Orthographe et mise en page.** Une grammaire et une structure de phrase médiocres, des fautes d'orthographe et un formatage incohérent sont autant d'indicateurs d'une éventuelle tentative de phishing. Les institutions dignes de confiance disposent d'un personnel spécialisé qui produit, vérifie et relit les communications adressées aux clients.
- **Pièces jointes suspectes.** Un e-mail non sollicité demandant à un utilisateur de télécharger et d'ouvrir une pièce jointe constitue un mécanisme de diffusion courant des programmes malveillants. Un cybercriminel peut faire naître un faux sentiment d'urgence ou d'importance pour persuader un utilisateur de télécharger ou d'ouvrir une pièce jointe sans la vérifier au préalable.

Bonnes pratiques : fonctions de sécurité

Vos collaborateurs et utilisateurs finaux seront immanquablement ciblés par des tentatives de phishing : les équipes de sécurité doivent donc mettre en place des mesures de protection permettant de détecter et de maîtriser les dommages de ces attaques. Les principales mesures de protection sont notamment :

- **Analyse des e-mails.** Le courrier électronique est de loin le vecteur de phishing le plus courant. Il est donc essentiel de disposer d'un service cloud d'analyse qui inspecte les e-mails en amont de votre edge réseau, avec une protection en temps réel contre les liens malveillants et l'usurpation de nom de domaine.
- **Reporting.** Les attaques par phishing ciblent souvent un large panel d'utilisateurs finaux dans une entreprise pour s'assurer de meilleures chances de réussite. Donnez aux utilisateurs finaux la possibilité de signaler les tentatives de phishing afin de neutraliser les expéditeurs et liens malveillants le plus rapidement possible, idéalement grâce à un bouton de signalement de phishing intégré dans les clients de messagerie des utilisateurs. Mettez en place un processus pour enquêter et répondre aux incidents de phishing, avec notamment un signalement aux agences officielles afin d'aider les gouvernements à combattre les escrocs et à stopper les attaques dirigées contre d'autres entreprises.
- **Authentification multifacteur (MFA).** L'authentification multifacteur reste l'une des défenses les plus efficaces contre le phishing. Avec celle-ci, un mot de passe détourné ne suffit pas, à lui seul, à compromettre un compte. Les applications d'authentification telles que Okta Verify ou Google Authenticator sont particulièrement efficaces et constituent une défense supplémentaire contre les tactiques de type MitM susceptibles d'intercepter les messages SMS.
- **Inspection du trafic chiffré.** Plus de 95 % des attaques utilisent des canaux chiffrés, qui ne sont souvent pas inspectés, ce qui permet aux hackers, experts ou pas, de contourner sans peine les contrôles de sécurité. Les entreprises doivent inspecter tout le trafic, qu'il soit chiffré ou non, afin d'empêcher que des hackers ne compromettent leurs systèmes.
- **Logiciel antivirus.** Les terminaux doivent être protégés par un antivirus régulièrement mis à jour afin d'identifier les fichiers malveillants et d'empêcher leur téléchargement.
- **Protection contre les menaces avancées.** Les antivirus peuvent bloquer les menaces connues mais les hackers peuvent créer de nouvelles variantes inconnues de malware qui peuvent échapper aux outils de détection basés sur des signatures. Déployez une sandbox en mode inline, pour mettre en quarantaine et analyser les fichiers suspects, ainsi qu'un système d'isolation du navigateur qui permet de circonscrire le contenu Web potentiellement malveillant sans perturber les workflows de l'utilisateur final.
- **Filtrage des URL.** Limitez le risque de phishing grâce au filtrage des URL qui applique une politique de gestion de l'accès aux catégories de contenu Web les plus dangereuses, comme les domaines nouvellement enregistrés.
- **Application régulière de correctifs.** Assurez la maintenance des applications, systèmes d'exploitation et outils de sécurité avec les correctifs les plus récents afin de réduire les vulnérabilités et d'actualiser les mesures de protection.
- **Architecture Zero Trust.** S'il est important de déployer une prévention du phishing, il est tout aussi important de déployer des fonctions qui limitent les dommages causés par une attaque réussie. Misez sur une segmentation granulaire, appliquez le principe du moindre privilège et surveillez en permanence le trafic afin d'identifier les acteurs malveillants qui ont pu compromettre votre infrastructure.
- **Veille sur les menaces.** Ces informations de veille s'intègrent à vos outils de sécurité existants afin de proposer des éléments de contexte qui améliorent la détection et la maîtrise du phishing. Ils fournissent également des informations actualisées sur les URL signalées, les indicateurs de compromission (IOC), ainsi que les tactiques, techniques et procédures (TTP) des assaillants. Autant d'éléments pour une prise de décision éclairée et une hiérarchisation pertinente des priorités.

Bonnes pratiques : comment identifier une page de phishing

Les pages de phishing peuvent être identifiées par des indicateurs sur les tactiques que les hackers utilisent pour leurrer les utilisateurs et les moteurs de sécurité, ainsi que par des raccourcis d'URL qu'ils utilisent fréquemment lorsqu'ils génèrent de nouvelles pages de phishing. La création de nouveaux sites de phishing connaît un pic au moment d'évènements majeurs comme les fêtes de fin d'année. Par exemple, pendant la pandémie, les hackers ont lancé une multitude de faux sites Web liés à la COVID-19 qui trompaient les victimes en se faisant passer pour des organisations de santé et des sites de commande de kits de test et de fournitures médicales. Pour détecter les dernières menaces de phishing, vous devez impérativement rester au fait des études et recherches récentes, pour obtenir des informations décisionnelles et des indicateurs actualisés à intégrer dans vos règles de détection et à vos workflows de gestion/réponse des incidents.

Vous trouverez ci-dessous une synthèse des indicateurs que vous (et vos outils anti-phishing) devez surveiller :

La page entière est basée sur une image unique. Les hackers ont souvent recours à des pages web n'affichant qu'une image de fond, souvent une copie d'une page Web légitime. Le seul autre élément figurant sur la page est un formulaire Web destiné à recueillir des informations d'identification. Il s'agit d'une technique très courante utilisée pour cibler les utilisateurs de banques en particulier.

La page n'a pas de titre.

La page comporte une ancre vide pour les liens essentiels. Les pages de phishing utilisent souvent des ancres vides pour des pages importantes telles que l'aide, les FAQ, etc. lorsqu'elles copient le contenu de pages légitimes.

La page comporte un certificat auto-signé.

La page semble être une interface générique de webmail. Les auteurs de phishing utilisent souvent des pages génériques de webmail pour recueillir des identifiants de messagerie, en imitant des sites tels que Webmail, Zimbra, etc.

La page n'est pas chiffrée. Une demande de connexion sur une page « http » est suspecte et doit être signalée.

La page effectue plusieurs redirections avant d'aboutir à une interface de connexion.

La page utilise la technique « HTML Smuggling ». Avec le HTML Smuggling (contrebande HTML), les assaillants dissimulent un blob JavaScript malveillant codé dans une pièce jointe à un e-mail, qui est ensuite assemblé par le navigateur. Ils contournent ainsi les filtres de messagerie. Le HTML Smuggling associé à une invite de connexion constitue un comportement hautement suspect.

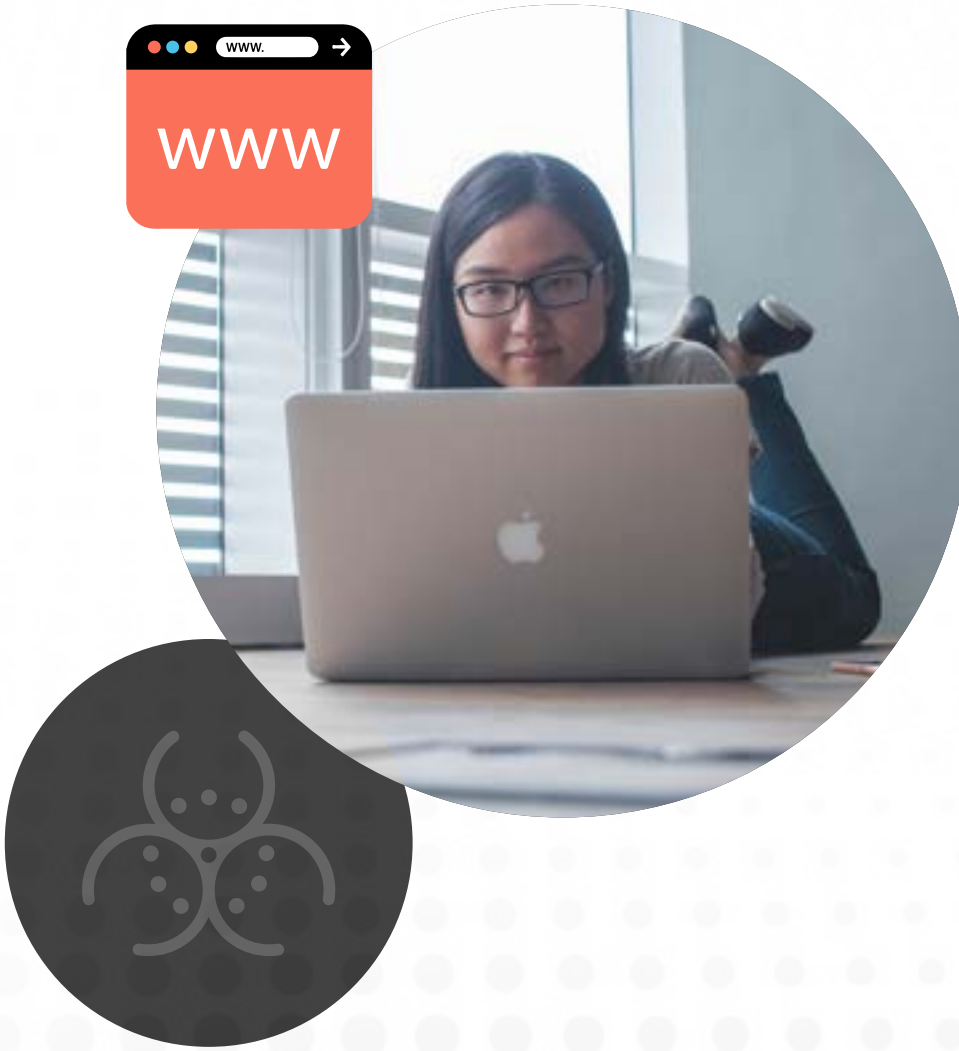
La page contient des balises obscurcies. Les opérateurs de phishing peuvent obscurcir des champs tels que le titre, le copyright, etc.

La page remplace des caractères clés par des « homoglyphes ». Les homoglyphes, des caractères qui ressemblent à d'autres caractères, sont utilisés de manière abusive sur les pages de phishing pour éviter d'être détectés. Cette technique exploite les similitudes entre des caractères appartenant à des scripts différents pour tromper les utilisateurs, ainsi que les moteurs de sécurité qui cherchent à faire correspondre des modèles ASCII.

Comment Zero Trust Exchange de Zscaler peut déjouer les attaques de phishing

La compromission des utilisateurs est une des menaces de sécurité les plus difficiles à contrer. Votre entreprise doit miser sur une prévention du phishing dans le cadre d'une stratégie Zero Trust plus large qui permet de détecter les intrusions actives et de minimiser les dommages causés par les intrusions réussies. Zscaler Zero Trust Exchange™ repose sur une architecture Zero Trust globale qui permet de neutraliser le phishing de diverses manières :

- **Empêcher la compromission :** une inspection TLS/SSL complète à grande échelle, une isolation du navigateur et un contrôle des accès basé sur des politiques permettent d'empêcher l'accès aux sites Web suspects.
- **Éliminer les déplacements en interne :** les utilisateurs sont connectés directement aux applications, et non au réseau, pour limiter la propagation d'une infection potentielle.
- **Bloquer les utilisateurs compromis et les menaces internes :** si un hacker accède à votre système de gestion des identités, Zero Trust Exchange empêche toute tentative d'intrusion sur une application privée grâce à une inspection inline. La solution détecte également les hackers les plus chevronnés grâce à une technologie intégrée de leurre.
- **Prévenir la perte de données :** les données en transit et les données au repos sont inspectées pour empêcher tout détournement par un hacker actif.



Produits Zscaler connexes

Zscaler Internet Access™ permet d'identifier et de stopper les activités malveillantes en acheminant et en inspectant tout le trafic Internet via Zero Trust Exchange. Zscaler bloque les éléments suivants :

- **URL et IP** observées dans Zscaler Cloud, et à partir de sources commerciales et open source d'informations de veille sur les menaces intégrées en natif. Ces informations portent sur les catégories d'URL à haut risque définies par les politiques et couramment utilisées pour le phishing, telles que les domaines nouvellement identifiés et nouvellement activés.
- **Signatures IPS** développées à partir de l'analyse par ThreatLabz des kits et pages de phishing.
- **Nouveaux sites de phishing** identifiés par des analyses de contenu optimisées par IA/ML.

Advanced Threat Protection bloque tous les domaines C2 connus.

Advanced Firewall étend la protection C2 à tous les ports et protocoles, y compris les nouvelles destinations des communications C2.

Browser Isolation crée un espace sécurisé entre les utilisateurs et les sites Web malveillants : le contenu est restitué sous forme d'un flux d'images, pour prévenir toute fuite de données et la propagation de menaces actives.

Advanced Cloud Sandbox empêche la diffusion de programmes malveillants inconnus.

Zscaler Private Access™ protège les applications en limitant le déplacement des menaces en interne, grâce à une segmentation utilisateur–application basée sur le principe du moindre privilège et à une inspection complète du trafic des applications privées.

Zscaler Deception™ détecte et neutralise les hackers qui tentent de se déplacer en interne ou d'élever leurs privilèges. Ces hackers sont leurrés à l'aide de serveurs, applications, répertoires et des comptes d'utilisateurs factices.

Prochaines étapes

Découvrez les risques critiques sur l'ensemble de votre environnement de cloud public grâce au service d'évaluation Zscaler Security Risk Assessment. Bénéficiez d'un inventaire complet de vos ressources dans le cloud, d'une image claire des risques de sécurité pour votre cloud public, d'une synthèse sur le respect des règles de conformité et des conseils sur des mesures correctives à mettre en œuvre.

À propos de ThreatLabZ

ThreatLabZ est l'organisme de recherche en sécurité de Zscaler. Cette équipe experte est responsable de la traque de nouvelles menaces et s'assure de la parfaite protection des milliers d'organisations qui utilisent la plateforme mondiale Zscaler. Au-delà des recherches sur les malwares et des analyses comportementales, l'équipe ThreatLabZ s'investit dans la recherche et le développement de nouveaux prototypes qui assurent une protection avancée contre les menaces sur la plateforme Zscaler. Elle mène régulièrement des audits de sécurité interne pour s'assurer que les produits et l'infrastructure de Zscaler répondent aux normes de conformité de sécurité. ThreatLabZ publie régulièrement des analyses approfondies sur les menaces nouvelles et existantes sur son portail, research.zscaler.fr.

Restez informé des recherches de ThreatLabz en vous abonnant dès aujourd'hui à notre bulletin d'information Trust Issues.

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte de données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quelle que soit leur localisation. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, est la plus importante plateforme de sécurité cloud inline au monde.

En savoir plus sur zscaler.com ou nous suivre sur Twitter @zscaler.com

Annexe

Catégorisation des attaques de phishing

Les attaques de phishing peuvent être catégorisées de différentes manières et peuvent inclure de nombreuses techniques. Cependant, les hackers adaptent leurs approches de manière à duper des utilisateurs de plus en plus avisés et à contourner les outils de défense. Nous mentionnons ici les définitions et les caractéristiques des attaques par phishing les plus courantes.

Les listes ci-dessous décrivent des méthodes d'attaque physique et la menace qu'elles représentent pour les entreprises. La majeure partie de ce rapport se concentre sur les menaces de phishing virtuel qui requièrent une connexion Internet pour leur exécution. Une caractéristique révélatrice des escroqueries par phishing en ligne est qu'elles demandent généralement aux utilisateurs d'envoyer des informations ou de télécharger des malwares par le biais de l'une des méthodes suivantes :

- **Lien :** l'utilisateur clique sur un lien malveillant vers un site de phishing, un fichier hébergé ou un malware.
- **Invite :** l'utilisateur est invité à envoyer des informations sensibles, aboutissant à un vol de données.
- **Pièce jointe :** l'utilisateur ouvre une pièce jointe contenant un malware.

Au moment de planifier vos investissements destinés à maîtriser les incidents de phishing cette année, prenez en compte les types d'attaques de phishing suivants.

A à Z : types courants d'attaques par phishing

1. **Angler phishing :** les hackers se font passer pour le service client d'une entreprise qui souhaite échanger sur des commentaires publiés sur les réseaux sociaux par des clients insatisfaits, en particulier ceux des banques.
2. **CEO fraud (fraude au PDG) ou phishing de type Business Email Compromise (usurpation d'identité par email) :** les hackers ciblent les collaborateurs d'une entreprise en se servant du compte e-mail piraté d'un de ses dirigeants, pour envoyer des factures fictives ou des demandes de paiement par virement bancaire ou sous d'autres formes.
3. **Clone phishing :** les hackers dupliquent des messages électroniques qui semblent provenir de sources de confiance, avec de légères modifications et des pièces jointes ou des liens malveillants.
4. **Malvertising phishing (attaque par publicités frauduleuses) :** les hackers utilisent des scripts intégrés dans des publicités pour injecter des contenus indésirables directement sur les ordinateurs des victimes.
5. **MFA Bombing :** les hackers incitent les utilisateurs dont les informations d'identification sont compromises à vérifier une demande illégitime de MFA. Ces attaques se caractérisent généralement par un flux continu de demandes MFA, parfois accompagnées d'un appel, d'un texte ou d'un e-mail fictif qui incite l'utilisateur à vérifier l'une des demandes à son insu ou par inadvertance.
6. **Pharming ou phishing par cache DNS :** les hackers redirigent les visiteurs vers un site malveillant en modifiant l'adresse IP d'un site Web légitime dans les serveurs DNS (Domain Name System) compromis, ou en envoyant un e-mail de phishing contenant du code malveillant qui redirige la victime vers le site lorsqu'elle saisit n'importe quelle URL sur son ordinateur.

7. **Phishing de type Adversary-in-the-Middle (AitM ou attaques par interception) :** les hackers imitent les actions d'une victime peu méfiante afin d'obtenir ses identifiants de connexion et ses cookies de session.

8. **Phishing de type Browser-in-the-Browser (BitB ou navigateur dans navigateur) :** les hackers affichent une fenêtre de navigateur malveillante à l'intérieur d'une fenêtre de navigateur de manière à imiter un domaine légitime et à reproduire des fenêtres de connexion contextuelles qui semblent provenir de fournisseurs d'authentification tiers.

9. **Phishing de type Credential Harvesting (attaque pour recueillir des identifiants) :** les hackers créent de fausses pages de connexion ou envoient des e-mails de phishing qui imitent des invites de connexion légitimes, pour ainsi dérober les noms d'utilisateur et les mots de passe de victimes sans méfiance.

10. **Phishing de type Doc Clouding (attaque via documents basés sur le cloud) :** les hackers diffusent des documents malveillants à partir de sources cloud classiques comme Google Drive, Box ou OneDrive afin de contourner les outils de sécurité traditionnels et compliquer leur détection par la plupart des équipes de sécurité.

11. **Phishing de type Evil Twin (attaque par jumeau maléfique) :** les hackers imitent un réseau Wi-Fi public de confiance pour observer l'activité en ligne des victimes et voler les données qui transitent par le point d'accès malveillant.

12. **Phishing de type Man-in-the-Middle (MiTM ou attaque de l'homme du milieu) :** les hackers ciblent les utilisateurs d'un serveur ou d'un système spécifique, capturant les données en transit telles que les identifiants, les cookies ou les informations de compte bancaire, en imitant des services en ligne par l'intermédiaire de serveurs proxy.

13. **Phishing de type Reverse Tunnel (attaque par tunnel inversé) :** les hackers utilisent un serveur distant pour créer un tunnel SSH inversé vers l'ordinateur de la victime, ce qui leur permet d'exploiter la machine à diverses fins, comme l'installation de malwares ou le vol de données sensibles, tout en restant dissimulés pour éviter d'être détectés par la victime.

14. **Phishing de type Watering Hole (attaque par point d'eau) :** les hackers ciblent les membres de groupes spécifiques susceptibles de visiter un site précis compromis ou créé par le hacker dans le but de perpétrer son attaque.

15. **Phishing HTTPS :** les hackers utilisent le protocole chiffré « Hypertext Transfer Protocol Secure » pour tromper les utilisateurs confiants et les inciter à cliquer sur des liens URL malveillants.

16. **Phishing par appât :** les hackers utilisent des offres, des noms de fichiers ou des dispositifs alléchants pour attirer des personnes intriguées dans un piège, à la manière d'une attaque par cheval de Troie.

17. **Phishing par chat ou messagerie instantanée :** les hackers utilisent les messages instantanés pour promouvoir leurs escroqueries au sein d'applications, généralement à l'aide de liens URL malveillants.

18. **Phishing par code QR :** les hackers utilisent des codes QR qui, lorsqu'ils sont scannés par le smartphone de la victime, mènent à des sites Web malveillants ou téléchargent des malwares sur l'appareil.

19. **Phishing par e-mail :** les assaillants envoient des messages électroniques d'ingénierie sociale en se faisant passer pour des marques connues. Ces messages contiennent des liens URL malveillants ou des pièces jointes destinées à détourner des informations ou à diffuser des malwares.

20. **Phishing par moteur de recherche :** les hackers ciblent le grand public en créant des sites fictifs de shopping, indexés par les moteurs de recherche. Ils proposent des réductions importantes sur une sélection de produits, et peuvent apparaître comme des pop-ups promotionnels ou contenir de faux avis antidatés. Les victimes peuvent, à leur insu, partager des données personnelles, des informations bancaires, des numéros de carte de crédit ou même effectuer un paiement pour acheter de faux produits. Les escrocs peuvent aller jusqu'à fournir de fausses informations d'expédition et de suivi, et même des produits fictifs bon marché pour prolonger l'existence de ces sites.

21. **Phishing par ransomware :** les hackers envoient des e-mails contenant des pièces jointes ou des liens malveillants qui, lorsqu'ils sont exécutés, téléchargent un ransomware sur l'ordinateur de la victime et exigent un paiement en échange d'une clé de déchiffrement permettant de restaurer le système compromis.

22. **Phishing par USB :** les hackers placent physiquement, ou envoient à leurs cibles, des clés USB contenant des exécutables malveillants qui se chargent lorsqu'ils sont branchés sur un terminal vulnérable.

23. **Smishing (attaque par SMS) :** les hackers utilisent des messages texte (communications SMS) pour diffuser leurs arnaques, généralement à l'aide de liens URL malveillants. L'expéditeur du message semble être une marque connue ou une connaissance du destinataire.

24. **Spear phishing (hameçonnage ciblé) :** les hackers organisent des campagnes qui utilisent des informations accessibles au public pour cibler des personnes travaillant pour des entreprises spécifiques. Ces e-mails trompeurs peuvent contenir de véritables informations et ressembler à des demandes internes légitimes pour inciter les destinataires à effectuer une action souhaitée.

25. **Tailgating (talonnage) :** les assaillants s'introduisent physiquement dans une zone d'accès restreint en suivant une personne autorisée à y pénétrer. Cette forme d'intrusion relève du phishing lorsque quelqu'un est leurré par la méthode d'ingénierie sociale utilisée par l'assaillant (comme se présenter équipé de plusieurs cartons pour une livraison fictive) pour rentrer dans une zone protégée sans vérification.

26. **Vishing :** les hackers passent des appels téléphoniques malveillants qui font appel à l'ingénierie sociale pour inciter les destinataires à effectuer une action, telle qu'un transfert d'argent ou la divulgation d'informations personnelles.

27. **Whaling (fraude au président) :** les hackers ciblent des dirigeants et des personnes très influentes en utilisant des informations accessibles au public. Ils utilisent l'ingénierie sociale pour amener la cible à révéler des secrets d'entreprise qui peuvent être utilisés à des fins frauduleuses ou pour l'amener à effectuer une autre action que le hacker peut utiliser pour atteindre ses objectifs.

La technologie ne peut pas à elle seule éliminer le phishing. Les entreprises doivent suivre l'évolution des escroqueries par phishing afin d'observer comment la sensibilisation des collaborateurs permet de déjouer les techniques malveillantes au fil du temps. Comprendre les différents types d'escroqueries peut aider les professionnels de la sécurité à enseigner aux collaborateurs comment faire preuve de méfiance lorsqu'ils rencontrent ce qui peut sembler être des opportunités, des demandes de vérification ou des notifications push légitimes. Lorsque vous élaborez votre propre stratégie pour réduire les occurrences de phishing, pensez à inclure les types suivants d'escroqueries courantes :

Principales catégories d'escroquerie par phishing

Les escroqueries liées au **cloud** se font passer pour des services de partage de fichiers ou de stockage dans le cloud avec des leurres tels que de fausses demandes d'accès et notifications de compte.

Les escroqueries liées aux **consommateurs** usurpent l'identité de marques de commerce électronique avec des leurres tels que de fausses notifications de compte et des demandes d'adhésion ou des annonces de gains.

Les escroqueries **commerciales** usurpent l'identité de services généraux comme FedEx avec des leurres tels que des notifications de suivi de livraison et des demandes de paiement.

Les escroqueries liées aux **entreprises** usurpent l'identité de sociétés spécifiques avec des leurres tels que de fausses notifications de compte, des actualités sur l'entreprise, des tâches de RH et des demandes de paiement de factures.

Les escroqueries liées aux **rencontres** usurpent l'identité de personnes désireuses de faire des rencontres par le biais d'une plateforme en ligne, avec des leurres tels que de faux profils, des messages, des mentions « j'aime » et « s'abonner ».

Les escroqueries liées aux **services financiers** usurpent l'identité d'institutions financières connues et ciblent des individus avec des leurres tels que de fausses notifications sur leur compte ou des alertes de sécurité.

Les escroqueries liées aux **administrations** usurpent l'identité d'agences ou de collectivité et utilisent des leurres tels que de fausses réclamations concernant des prestations, des prêts à la consommation et des demandes de paiement de créances.

Les escroqueries liées aux **offres d'emploi** usurpent l'identité d'entreprises, vraies ou fausses, cherchant à embaucher de nouveaux employés, avec des leurres tels que de fausses offres d'emploi ou de fausses candidatures.

Les escroqueries liées aux **notifications push ou aux navigateurs** se font passer pour des notifications de navigateurs Web avec des leurres tels que de faux rappels d'installation de mises à jour, des alertes de messages et des publicités pour des produits.

Les escroqueries liées aux **réseaux sociaux** usurpent l'identité de réseaux sociaux/utilisateurs avec des leurres tels que de faux comptes ou des comptes usurpés, des messages privés, des mises en garde ou des notifications de compte et des alertes de sécurité.

Les escroqueries liées au secteur **technique** usurpent l'identité de services généraux ou des marques connues, avec des leurres tels que des notifications de compte, des messages d'erreur et des mises à jour de logiciels.

Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation digitale et permet à ses clients de gagner en agilité, productivité, résilience et sécurité. La plateforme Zero Trust Exchange™ de Zscaler protège des milliers de clients contre les cyberattaques et les pertes des données en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quelle que soit leur localisation. Disponible sur un écosystème de plus de 150 data centers dans le monde, Zero Trust Exchange basé sur le SASE est la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur www.zscaler.fr.

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.fr