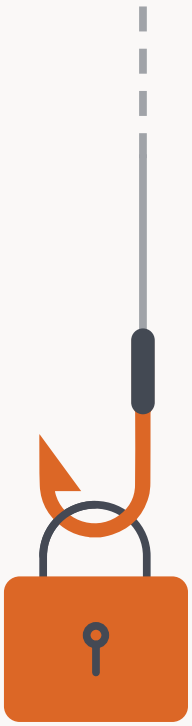
Les tendances du phishing en 2021

En 2021, le phishing a infiltré toutes les formes de communication, des e-mails aux SMS, aux médias sociaux et même à la publicité.

L'ingénierie sociale, qui se limitait autrefois aux e-mails d'entreprise, est devenue la première cybermenace qui touche les entreprises aujourd'hui, sur toutes les plateformes, y compris les ordinateurs de bureau et les téléphones portables.

Pourquoi ? Il est en effet plus facile pour un attaquant d'exploiter une personne et de capturer des données par le biais d'une attaque de phishing que d'exploiter un système d'exploitation robuste. Les informations d'identification de l'utilisateur ont beaucoup plus de valeur pour un pirate à l'ère de l'entreprise sur le cloud, car elles permettent d'accéder à des données sensibles qui sont stockées et gérées au-delà de l'appareil, dans des applications SaaS, des référentiels de stockage de fichiers en ligne et des centres de données.

Les attaques de phishing ont évolué bien au-delà des courriels mal formulés offrant des "gains de loterie non réclamés". Non seulement elles sont plus personnalisées et plus convaincantes, mais elles atteignent les utilisateurs dans un plus grand nombre d'endroits qu'auparavant et vont de plus en plus au-delà des consommateurs pour cibler les informations d'identification et les données des entreprises. Cela est dû en grande partie à l'adoption du mobile.



Les attaques de phishing trompent un nombre croissant d'utilisateurs

La majeure partie du trafic web provient des mobiles. Il n'est donc pas surprenant que les pirates l'utilisent à leur avantage en concevant des attaques spécifiques aux plateformes mobiles. Les appareils mobiles ont des écrans plus petits et comportent un certain nombre de raccourcis visuels, ce qui signifie qu'il est beaucoup plus difficile de repérer les URL suspectes ou les expéditeurs malveillants que sur un ordinateur de bureau. Les utilisateurs sont également plus distraits et plus vulnérables sur les appareils mobiles en raison de leur nature portable et de leur caractère intrinsèquement personnel.

Les attaquants continuent de produire des sites de phishing de plus en plus convaincants, qui ciblent les utilisateurs de téléphones portables : 1 utilisateur de téléphone portable sur 10 est victime d'une attaque de phishing. Cela signifie qu'ils ne se contentent pas de les recevoir, mais qu'ils cliquent dessus.

On constate une augmentation de 160 % des utilisateurs mobiles victimes de phishing au cours des 12 derniers mois. Cela ne reflète pas le volume des attaques en ligne, mais plutôt le rythme auquel les gens s'y laissent prendre. Cette augmentation du nombre de personnes qui mordent à l'hameçon est probablement due à l'évolution des techniques des attaquants. Ils utilisent désormais des applications de confiance pour diffuser leurs messages, enregistrent des domaines attrayants et imitent des marques connues pour toucher davantage d'utilisateurs avec moins d'investissement.

1 sur 10

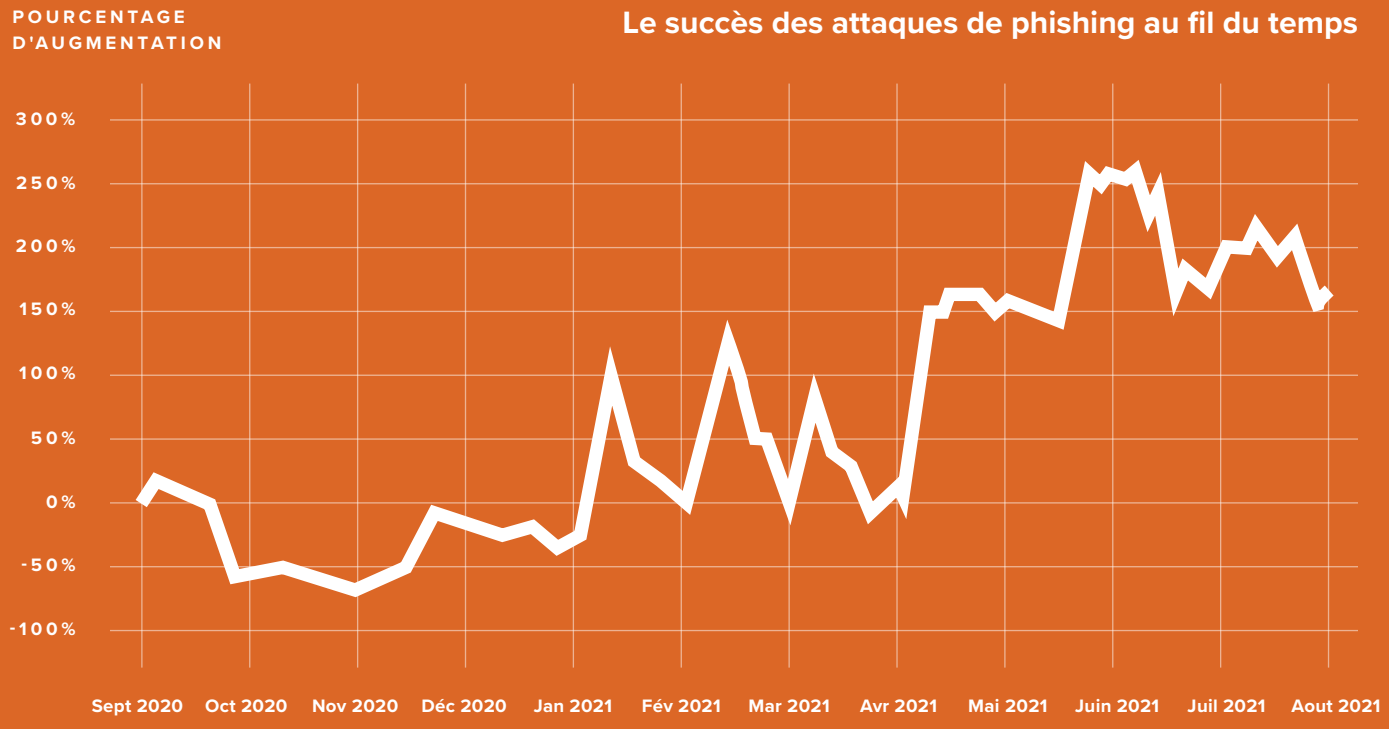
clique sur des liens de phishing lorsqu'elle est sur son appareil mobile.

Source : Wandera, une entreprise Jamf

Le nombre d'utilisateurs mobiles victimes d'attaques de phishing a augmenté de 160 % d'année en année.

Source : Wandera, une entreprise Jamf

Le succès des attaques de phishing au fil du temps



Source : Wandera, une entreprise Jamf

Les attaques de phishing sont plus difficiles à repérer sur les appareils portables

Les appareils portables, utilisés pour le travail à distance, rendent le phishing plus difficile à détecter.

- L'utilisation accrue des appareils mobiles entraîne une réduction de la taille des écrans, ce qui laisse moins de place pour évaluer la légitimité d'un site Web
- Les améliorations apportées à la conception de l'interface utilisateur ont conduit à des décisions de conception qui masquent généralement la barre d'adresse déjà minuscule lorsque l'utilisateur fait défiler l'écran vers le bas
- Les utilisateurs distraits qui travaillent sur plusieurs appareils, communiquent et collaborent sur une grande variété d'applications ont tendance à se précipiter sur les différentes pages et notifications. En outre, de nombreux développeurs d'applications choisissent de mettre en évidence le bouton "Accepter" ou "OK" ce qui conduit les utilisateurs à accepter automatiquement sans les examiner
- Les visuels simplifiés qui donnent la priorité au contenu plutôt qu'aux métadonnées empêchent l'utilisateur de voir ou d'évaluer la destination du lien avant de cliquer
- Les raccourcisseurs d'URL tels que Bitly ou Owly - couramment utilisés dans les messages texte - masquent le domaine complet

Le phishing est diffusé en dehors des e-mails, là où les gens ne s'y attendent pas

La sécurité traditionnelle a abordé le phishing comme un problème d'e-mails d'entreprise. Les solutions se trouvaient dans l'appareil de messagerie lui-même et non sur le périphérique. Lorsque les gens sont devenus mobiles, ils ont (1) commencé à utiliser davantage d'applications, qui n'étaient pas protégées, et (2) ils se trouvaient en dehors du périmètre et ne bénéficiaient donc d'aucune des protections mises en place autour du campus physique.

Les appareils informatiques de l'utilisateur final offrent de plus en plus une plateforme de communication consolidée - où vous pouvez disposer d'un grand nombre d'applications de messagerie et de médias sociaux avec des messages directs dans l'application. Les MacBooks utilisant le silicium d'Apple peuvent exécuter non seulement les applications macOS, mais aussi les applications iOS, Windows, etc. pour offrir une expérience informatique cohérente. Les applications de messagerie ont tendance à être une zone négligée dans les défenses de l'entreprise, et donc attrayante pour les attaquants.

Le fait de se concentrer sur le mobile a permis aux pirates de quitter le domaine de confiance qu'est l'e-mail pour se tourner vers la multitude de nouvelles méthodes de distribution telles que les SMS, WhatsApp, Messenger, Instagram et LinkedIn, des services auxquels les utilisateurs font confiance.

Le cadenas est utilisé pour tromper davantage les utilisateurs

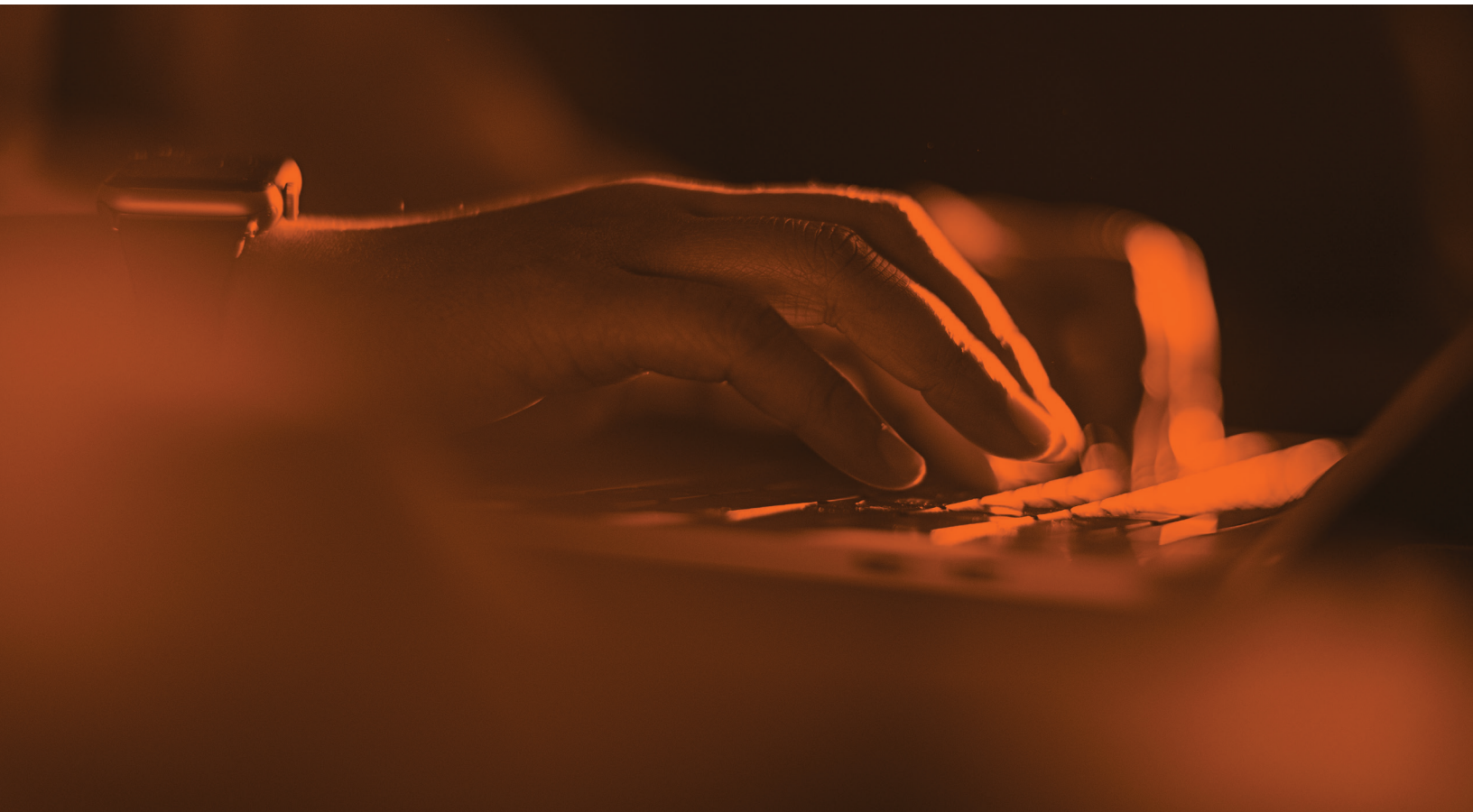
Vérifier deux fois la présence d'un cadenas dans la barre d'adresse était autrefois un moyen facile de repérer un mauvais domaine, mais il existe désormais une multitude de services gratuits en ligne que les attaquants peuvent utiliser pour obtenir rapidement et facilement une certification SSL pour des sites de phishing malveillants. Malheureusement, cela est efficace car les utilisateurs pensent que le symbole du cadenas précédant une URL est un indicateur fiable de la sécurité d'un site web. Une fois l'obstacle du coût supprimé, il n'y a aucune raison pour qu'un attaquant ne crypte pas ses mauvais sites.

93 % des domaines de phishing sont hébergés sur un site web "sécurisé" avec un cadenas dans la barre d'URL

Source : Wandera, une entreprise Jamf

Aujourd'hui, 93 % des sites de phishing réussis utilisent la vérification HTTPS pour dissimuler leur nature trompeuse contre 65 % en 2018.

Source : Wandera, une entreprise Jamf



Le punycode rend les mauvais domaines plus difficiles à identifier.

Les attaquants utilisent de plus en plus le punycode pour rendre leurs domaines de phishing plus difficiles à détecter. Le punycode convertit les mots qui utilisent des caractères unicode (dans des langues comme le cyrillique, le grec et l'hébreu, par exemple) en caractères ASCII afin que les ordinateurs puissent les comprendre.

L'origine des attaques punycode remonte à l'époque où les navigateurs ne prenaient pas en charge l'unicode et n'utilisaient que l'ASCII pour afficher les URL ; les attaquants ont commencé à utiliser ces jeux de caractères parce qu'ils pouvaient enregistrer des domaines qui ressemblaient beaucoup à des domaines existants/de confiance et que le navigateur pouvait finalement être utilisé pour tromper l'utilisateur en lui faisant croire qu'il communiquait avec un site alors qu'en fait, il communiquait avec un autre. Les caractères Unicode permettent d'obtenir des noms de domaine qui semblent familiers à l'œil nu mais qui, en réalité, pointent vers un serveur différent ou renvoient à un domaine inconnu.

D'après nos données, au cours des 12 derniers mois, 2 % des attaques de phishing zero day réussies contenaient du punycode. Vous trouverez ci-dessous quelques exemples. Pouvez-vous repérer les caractères unicode dans les domaines ci-dessous ?

2% des attaques de phishing dont les utilisateurs ont été victimes contenaient du punycode

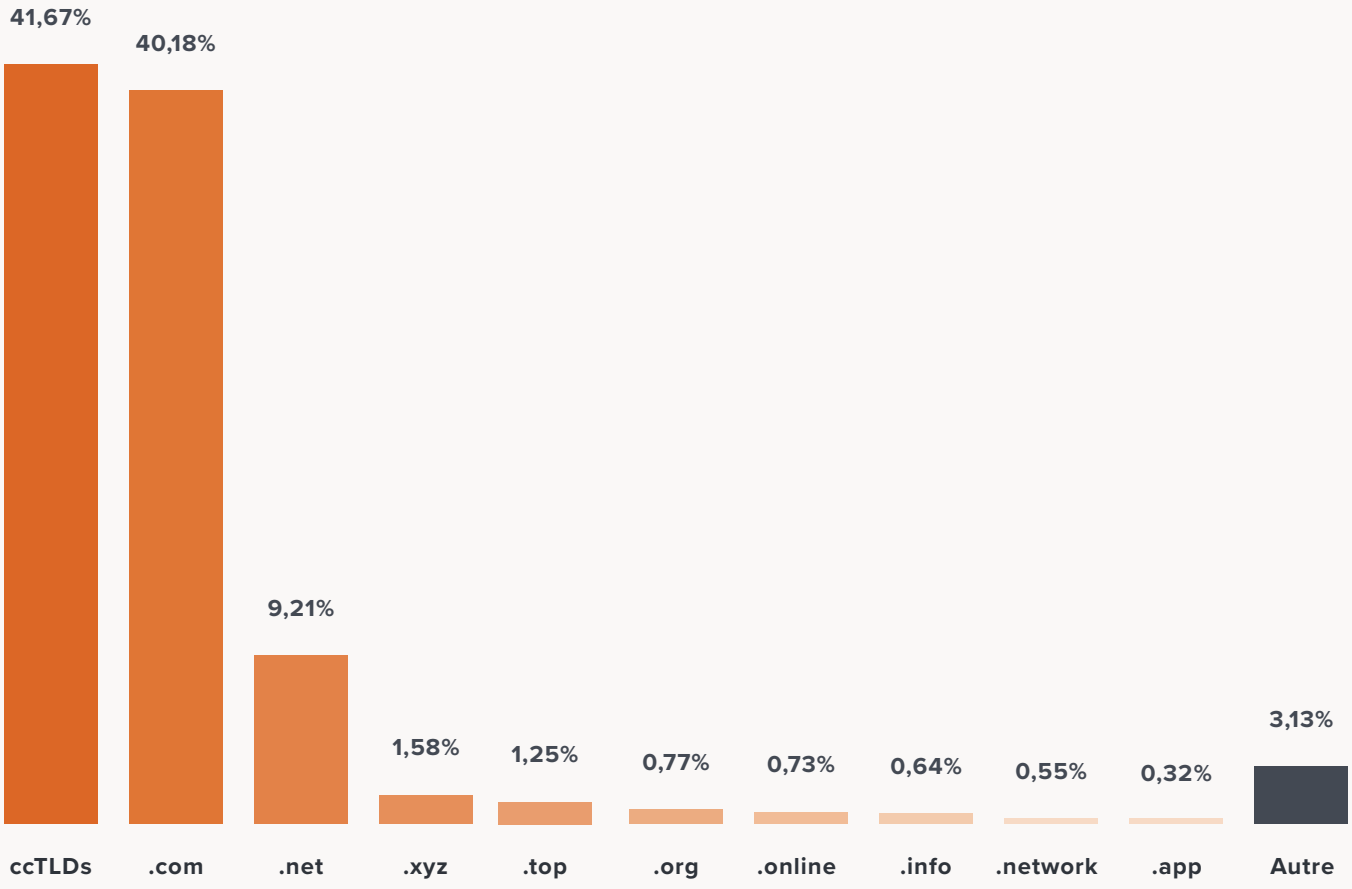
Source: Wandera, a Jamf Company

MARQUE	CE QUE L'UTILISATEUR VOIT (UNICODE)	LE PUNYCODE « DÉCODÉ »
Google	https://googĺe.com	xn--googe-95a.com
Starbucks	https://starƅucks.com	xn--starucks-hpd.com
Rolex	https://rolẹx.com	xn--rolx-nu5a.com
Paypal	https://t.paypal.com	t.xn--ayal-9ndc.com
Facebook	https://www.facebook.com⁄login.en.do	www.facebook.xn--comlogin-g03d.en.do

Les domaines de premier niveau (TLD) obscurs aggravent la situation

Les domaines de premier niveau (TLD) se résumaient autrefois à .com, .net, .org, etc. Ces dernières années, de plus en plus de domaines utilisant des codes de pays différents (ccTLD) et des TLD spécifiques aux entreprises (par exemple, .attorney, .technology, .airline) ont commencé à apparaître. Vous trouverez ci-dessous la part des domaines de premier niveau que nous avons observés dans des attaques de phishing réussies. Le danger est que les utilisateurs puissent voir une marque qu'ils reconnaissent mais avec un TLD qui n'est pas le TLD habituel. Par exemple, un pirate pourrait enregistrer microsoft.xyz pour héberger une attaque de phishing sur le thème de Microsoft et, lorsqu'il est découvert, le remplacer par microsoft.info ou microsoft.network, et ainsi de suite. .

Vous trouverez ci-dessous la part des TLD utilisés dans les attaques de phishing réussies détectées sur notre plateforme au cours des 12 derniers mois. Les TLD courants .com et .net sont les plus populaires, ainsi qu'une consolidation des ccTLD tels que .ru, .uk et .co.



Source : Wandera, une entreprise

Ce qu'il faut retenir : Si l'on additionne le cadenas, le punycode et les TLD non conventionnels, on voit combien il est facile de créer un domaine de phishing convaincant qui imite même les plus grandes marques.

Les 10 marques les plus utilisées dans les attaques de phishing réussies

Pour augmenter le taux de réussite d'une attaque, les acteurs malveillants doivent être sélectifs lorsqu'ils décident des entreprises à imiter.

Les attaquants délaissent les attaques régionales au profit de celles qui intègrent des marques mondiales, axées sur la technologie. Les gens sont plus susceptibles d'être victimes d'une attaque de phishing lorsque l'appât est un site qui a leur confiance. La technologie de signature unique étant intégrée à un nombre croissant d'applications, les identifiants d'Apple, de Google, d'Amazon, de Microsoft, etc. donnent accès à bien plus qu'une simple messagerie électronique... ils ouvrent des couches supplémentaires de données personnelles et professionnelles.

Les acteurs malveillants ciblent de plus en plus les applications utilisées pour le travail, comme Office 365 et les applications G Suite de Google. À l'heure où les entreprises s'efforcent de déplacer leurs actifs professionnels vers le cloud, il s'agit d'une préoccupation majeure. Une seule erreur de la part d'un employé qui reçoit une attaque de phishing intelligente (par exemple, lui demandant de confirmer ses identifiants de connexion à Google Drive) peut permettre à un pirate d'accéder aux actifs de l'entreprise stockés sur ces types d'applications cloud populaires.

Les trois principales marques utilisées dans les attaques de phishing qui ont réussi à inciter les utilisateurs à agir sur le lien de phishing en 2021 sont Apple, PayPal et Amazon, qui représentent respectivement 43%, 27% et 9% de ces attaques.

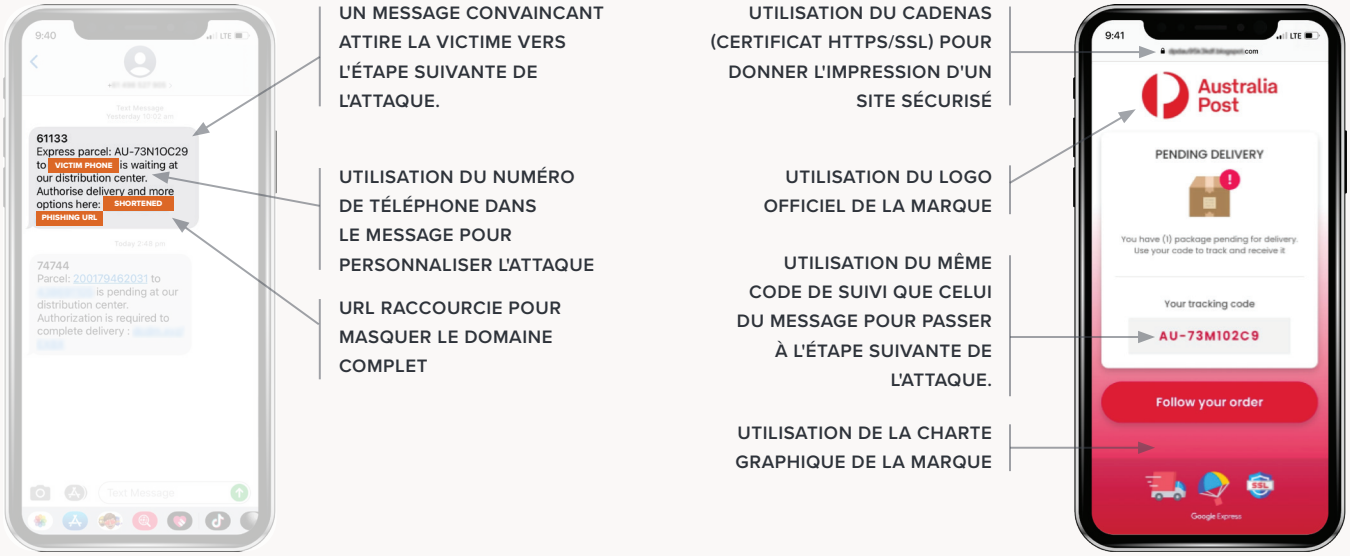
Les 10 marques les plus utilisées dans les campagnes de phishing en 2021

1. **Apple**
2. **PayPal**
3. **Amazon**
4. **Chase**
5. **Facebook**
6. **Google**
7. **Twitter**
8. **Netflix**
9. **Microsoft**
10. **Wells Fargo**

Source : Wandera, une entreprise Jamf

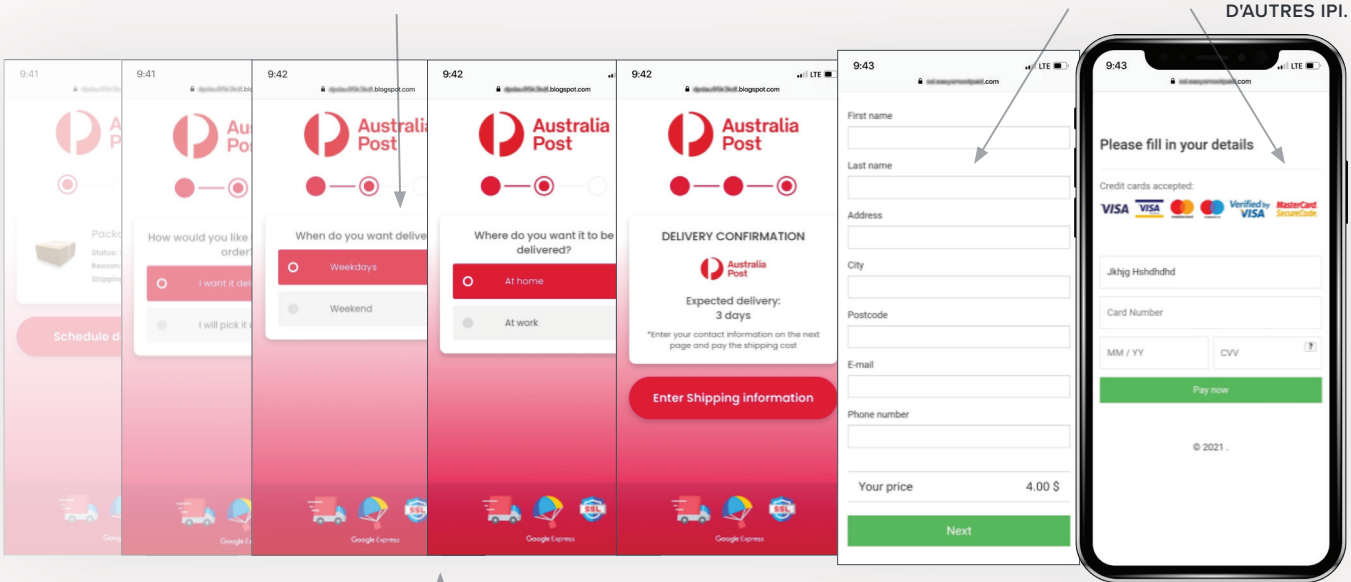
Coup de projecteur sur une campagne de phishing - Australia Post

Nos chercheurs ont enquêté sur une campagne de phishing lorsque plusieurs SMS suspects ont été signalés. Les messages avaient pour thème la livraison de colis et utilisaient la marque bien connue Australia Post (Australia Post est l'équivalent de USPS aux États-Unis ou de Royal Mail au Royaume-Uni, de sorte que les victimes potentielles sont toutes les personnes qui vivent en Australie et reçoivent du courrier). Il s'agit d'une attaque opportuniste étant donné que les gens comptaient beaucoup sur la livraison à domicile pendant les verrouillages stricts et répétés du COVID-19 en Australie.



SITE WEB INTERACTIF AVEC UNE ICONOGRAPHIE, DES POLICES, DES COULEURS DE MARQUE, ETC. COHÉRENTES.

SOUMISSION DE DÉTAILS PERSONNELS, Y COMPRIS DES INFORMATIONS D'IDENTIFICATION, DES DONNÉES FINANCIÈRES ET D'AUTRES IPI.



PRÉPARATION D'UN EXPLOIT D'INGÉNIERIE SOCIALE

Source : Wandera, une entreprise Jamf

Il existe de nombreuses campagnes de phishing mal conçues. Parfois, le message ne correspond même pas au contenu de la page, ou le contenu de la page est une arnaque très générique. Cette attaque de phishing est un peu plus sophistiquée, car il y a une continuité entre le message et le contenu de la page pour faire croire à la victime qu'elle doit autoriser la livraison d'un colis.

Bien qu'il s'agisse d'une attaque bien exécutée, il y a ici quelques signes évidents d'un phishing. Tout d'abord, l'URL n'utilise pas le domaine auspost. Deuxièmement, la marque est convaincante, mais elle ne correspond pas parfaitement au site Web légitime d'Australia Post. Troisièmement, l'utilisateur est redirigé vers un autre domaine hors marque qui demande un paiement alors qu'un paiement ne serait pas normalement nécessaire pour autoriser une livraison. Enfin, les Australiens écrivent center "centre" ; les plus petits détails peuvent trahir une attaque de phishing, alors gardez l'œil ouvert !

N'oubliez jamais : dans ces situations, lorsque vous recevez un message convaincant, nous vous recommandons d'aller directement sur l'application ou le site web de votre service plutôt que de cliquer à partir d'un e-mail ou d'un message.

Un petit rappel à la réalité

De nombreux sites de phishing ne sont publiés en ligne que pendant quelques heures avant que les pirates ne se déplacent vers un tout nouveau serveur d'hébergement. Cela leur permet d'échapper à la détection et de maintenir des campagnes en cours sans être bloqués. Le risque pour les utilisateurs est le plus élevé au cours de ces premières heures critiques, avant que les renseignements statiques sur les menaces, basés sur des listes, ne soient mis à jour.

Dans l'attaque d'Australia Post ci-dessus, lorsque le domaine de phishing est signalé et supprimé, il suffit à l'attaquant d'enregistrer un nouveau domaine et de relancer l'attaque, jusqu'à ce que ce nouveau domaine soit également signalé et qu'il recommence. Lorsque l'on pense au nombre de domaines de premier niveau existants et aux nombreux sous-domaines que l'on voit dans les URL légitimes (tels que login., mobile. ou en.), il est facile de comprendre comment un attaquant peut maintenir une campagne de ce type. Mélangez-les et créez votre propre URL de phishing à partir des quelques exemples ci-dessous, puis demandez-vous si vous mordriez à l'hameçon si vous le voyiez.

SOUS-DOMAINE	MARQUE	DOMAINE DE PREMIER NIVEAU
tracking.	aus-post	.com
feedback.	auspost	.net
mobile.	australiapost	.review

Recommandations

Les attaques de phishing exploitent la partie la plus vulnérable d'une entreprise : ses employés. Les employés sont souvent l'atout le plus précieux d'une entreprise, mais lorsqu'il s'agit de protéger les données, ils constituent également la plus grande faiblesse en matière de sécurité.

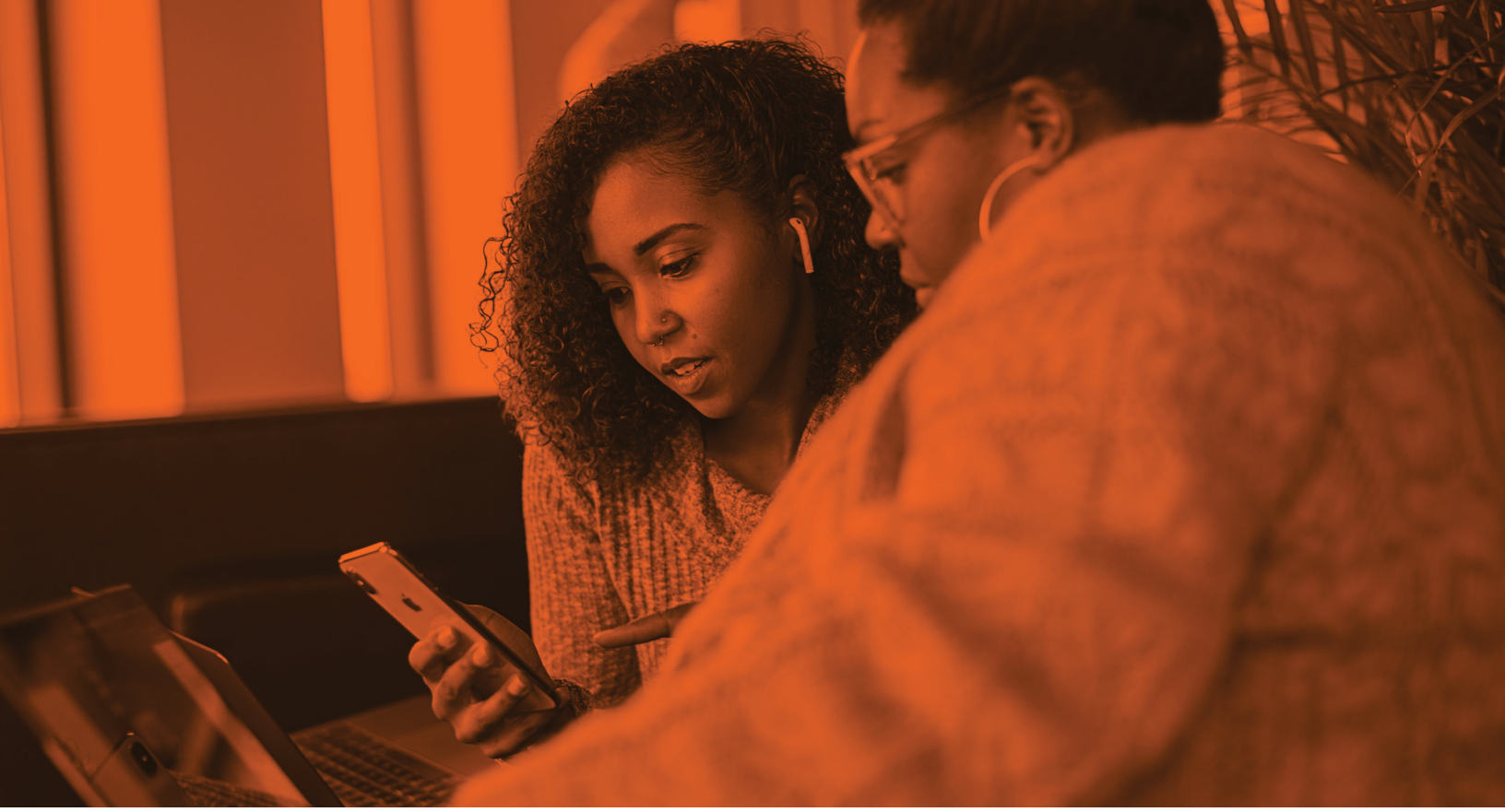
C'est pourquoi une solution de phishing de type zero-day solution", c'est-à-dire une solution qui fonctionne sur toutes les applications de communication, et pas seulement sur le courrier électronique, est essentielle pour mettre fin aux attaques courantes et aux attaques plus sophistiquées lancées contre votre entreprise.

Vous avez été victime de phishing, et maintenant ?

- Changez tous vos mots de passe pour les comptes qui ont été compromis ainsi que pour les comptes qui utilisent des mots de passe identiques ou similaires à ceux qui ont été capturés par le pirate
- Si vous avez saisi les informations de votre carte de crédit sur la page de phishing, annulez votre carte
- Mettez votre ordinateur hors ligne ou supprimez votre compte de messagerie pour éviter de diffuser les liens de phishing dans vos listes de contacts
- Contactez l'entreprise ou la personne qui a été imitée dans l'attaque - il peut s'agir de votre PDG, d'un collègue de travail ou d'un représentant de votre banque. Plutôt que de répondre au message, choisissez une autre méthode de communication, comme un appel téléphonique, pour vérifier qu'il s'agit bien de cette personne
- Soyez attentif aux alertes de vol d'identité et placez une alerte à la fraude sur votre compte de crédit

Le meilleur remède est la prévention. Restez à l'abri du phishing en suivant ces conseils :

- Ne cliquez pas sur les liens suspects
- Regardez attentivement les caractères de l'URL. Si vous avez des doutes, copiez l'URL de votre navigateur dans un éditeur compatible avec l'unicode afin de rechercher plus efficacement les attaques par punycode
- Faites attention aux messages prétendant provenir des grandes marques technologiques. Vérifiez si le message est conforme à leur ton, leur vocabulaire, leur dialecte régional, etc
- N'entrez pas les informations de votre carte de crédit dans des services inconnus ou non fiables
- Si un lien vous dirige vers le site de votre banque, ouvrez-le dans une fenêtre séparée en tapant le nom manuellement, ou utilisez l'application officielle
- Ne tombez pas dans les escroqueries évidentes qui prétendent que vous avez gagné un prix
- Vérifiez la barre d'adresse pour détecter les URL suspectes ou copiées, par exemple, my.apple.pay.com



À propos de cette étude

L'objectif était de mieux comprendre l'état du phishing mobile et les informations les plus à risque. Les informations et les statistiques contenues dans ce document sont le résultat de notre analyse des tendances du phishing sur un échantillon de 500 000 appareils protégés dans 90 pays au sein de la base de clients de Wandera, a Jamf company, sur une période de 12 mois. Cette analyse a été réalisée au troisième trimestre de 2021. Les métadonnées analysées dans cette recherche proviennent de journaux agrégés qui ne contiennent pas d'informations permettant d'identifier les personnes ou les entreprises.

Notre intention avec cette analyse n'est pas de susciter la peur, mais plutôt de vous éduquer, vous et vos utilisateurs, sur les options disponibles et sur la meilleure façon de sécuriser tous les aspects des données des appareils, des utilisateurs et des entreprises. Contactez-nous pour savoir comment vous pouvez mettre en place des mesures de protection et renforcer votre dispositif de sécurité.

Découvrez comment Jamf et Threat Defense constituent une solution complète et adaptée pour protéger les utilisateurs Apple contre les intentions malveillantes, tout en maintenant un impact minimal sur l'expérience de l'utilisateur final impact minimal sur l'expérience de l'utilisateur final. Ou bien, demandez un essai et voyez comment vous pouvez protéger vos utilisateurs.

Demander un essai