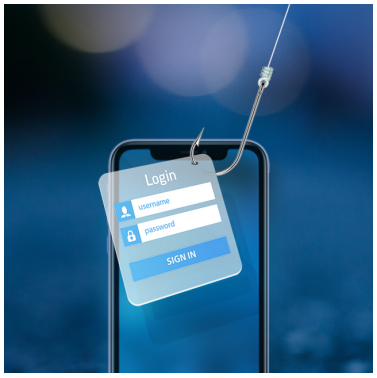
ZIMPERIUM®
ADVANCED MOBILE SECURITY

Le phishing mobile suit la voie de moindre résistance

Permettre aux entreprises de gérer efficacement les risques liés à la mobilité

Les phishing[1] représente une menace pendant au moins un quart de siècle, mais la pandémie de COVID-19 a triplé la fréquence des attaques de phishing rien qu'en 2020. Et ce chiffre continuera d'augmenter. L'utilisation des terminaux mobiles ayant dépassé celle des ordinateurs de bureau[2], les cybercriminels considèrent le mobile comme première cible pour les attaques de phishing.

Le Département de la Défense a déclaré que huit courriels entrants sur dix destinés au Département ont dû être bloqués[3]. En comparaison, le Pentagone a anticipé une prévision de 13 milliards d'e-mails en une seule année[4]. Et d'après Verizon[5], plus de 90 % de violations commencent par une attaque de phishing.



Les terminaux mobiles ne demeurent plus des appareils exclusivement personnels, ils ont été adoptés par l'entreprise dans le cadre des politiques BYOD, abréviation de l'anglais « bring your own device », PAP pour « prenez vos appareils personnels » ou encore AVEC pour « apportez votre équipement personnel de communication » et d'applications axées sur l'entreprise, de la vérification d'identité jusqu'à l'accès aux données. Grâce à cette adoption, les équipes de la DSI déploient souvent des applications destinées aux entreprises, avec des contrôles de sécurité restreints afin de prendre en charge les points d'accès aux données itinérantes. Sauf que cette portée de contrôles de sécurité est axée sur les applications d'entreprise, les applications grand public les plus utilisées ne sont donc pas protégées contre les attaques. En bref, les cybercriminels attaquent les courriels personnels, les SMS et les applications de messagerie personnelle comme points d'entrée non protégés dans les données de l'entreprise.

Jusqu'à l'an 2020, 87 % des entreprises ont déclaré leur dépendance de la capacité de leurs employés à accéder aux applications professionnelles mobiles depuis leur appareil mobile[6], ***et plus de 60 % de tous les courriels, professionnels et personnels, ont été consultés sur des appareils mobiles***[7]. Associez cela au fait que plus de 52 % des entreprises reconnaissent que les appareils mobiles sont difficiles à sécuriser[8], il est évident que le facteur de commodité offert par les appareils mobiles fait également multiplier les risques pour la sécurité des données. Et l'essor d'accès aux données d'entreprise sur des terminaux mobiles, bien au-delà de l'infrastructure de sécurité existante, a laissé ces surfaces d'attaque prêtes pour le phishing, laissant en péril les données personnelles et celles de l'entreprise.

Il n'en reste pas moins que les cybercriminels trouvent que les utilisateurs de téléphones mobiles constituent des cibles parfaites pour les attaques de phishing à cause de l'absence de sécurité au niveau des applications de communication grand public.

Et selon le rapport annuel d'enquête sur les compromissions de données de Verizon[9], ceci est attribuable au fait que la technologie mobile est une cible très souvent oubliée, qui ouvre les terminaux aux attaques de phishing contrairement aux technologies de bureau traditionnelles.

---

[1] Phishing.org. History of phishing. http://www.phishing.org/history-of-phishing
[2] Statcounter. Desktop vs Mobile vs Tablet Market Share Worldwide
Desktop vs Mobile vs Tablet Market Share Worldwide. Apr 2018 - Apr 2019. Data cited from May 2019. http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet
[3] Department of Defense. Norton: Secure, operate, and defend are the fundamentals.
https://www.disa.mil/NewsandEvents/2017/AFCEA-Luncheon
[4] Inc. Government Agencies Are Under Siege From Phishing Attacks. Could Your Company Be Next? https://www.inc.com/adam-levin/government-agencies-are-under-siege-from-phishing-attacks-could-your-company-be-next.html
[5] Verizon. 2019 Data Breach Investigations Report. May 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[6] BYOD Usage in the Enterprise. https://syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the-Enterprise.pdf
[7] BYOTop 10 Email Clients in March 2019. https://uplandsoftware.com/adestra/resources/blog/top-10-email-clients/
[8] Enforce Endpoint Compliance and Cyber Hygiene With Duo Device Trust. https://blogs.cisco.com/security/enforce-endpoint-compliance-and-cyber-hygiene-with-duo-device-trust
[9] Ibid.

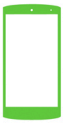
« Les attaques qui se sont avérées fructueuses sur les PC sont maintenant testées sur des utilisateurs involontaires d'appareils mobiles pour voir ce qui fonctionne - et grâce au nombre croissant d'appareils mobiles mal protégés, les cibles faciles ne manquent pas »

- Stacy Collett, CSO Online

HAUT 5 POURQUOI LE PHISHING EST-IL SI REDOUTABLE SUR MOBILE ?

1 Les utilisateurs s'en chargent

Les utilisateurs de terminaux mobiles prennent généralement en charge la gestion de leurs propres appareils, qui ne sont pas soumis aux politiques de correction et de mise à jour automatisées que l'on trouve sur les ordinateurs de bureau et les ordinateurs portables de l'entreprise,



Less Usable Screen Space 2

À cause de la taille minuscule de l'écran, il est très compliqué de voir les adresses web complètes sur un navigateur et les adresses électroniques réelles de l'expéditeur dans les courriers électroniques.

3 Une confiance excessive

Les utilisateurs renouent un lien personnel avec leurs appareils mobiles, ce qui développe une sorte de confiance infondée dans l'appareil, ainsi que dans les données et dans le contenu qui y sont stockés.

Don't Ask, Just Tell 4

La conception de l'interface graphique favorise la mise en place d'actions comme accepter, répondre, envoyer et liker avec des informations limitées.

5 Envoyer des messages en étant distrait

L'utilisation d'appareils mobiles en marchant, en parlant, en conduisant, etc. signifie que les utilisateurs répondent également aux demandes en étant distraits. En éliminant le besoin de visualiser l'application d'origine, les utilisateurs de terminaux mobiles sont plus susceptibles d'intéragir aveuglément avec l'alerte.

Zimperium zIPS protège contre les attaques de type « zero day » (ou vulnérabilités du jour zéro) et les attaques de phishing personnalisées et adaptées.

Même si l'éducation à la sécurité informatique représente souvent la première ligne de défense contre le phishing mobile, elle ne permet pas à elle seule de résister à l'assaut des tentatives de phishing dont sont victimes les entreprises. Finalement, les attaques de phishing restent plus sophistiquées et plus difficiles à détecter, même avec la meilleure éducation de l'utilisateur final. Afin de pouvoir protéger leurs données et les utilisateurs de leurs terminaux, les entreprises doivent aborder la sécurité des appareils mobiles en combinant plusieurs technologies de sécurité.

Grâce à son moteur breveté z9, le moteur d'apprentissage automatique de Zimperium constitue la pierre angulaire de la sécurité de Zimperium zIPS. Il permet de détecter le phishing sur les terminaux mobiles et de prévenir les attaques de type « zero-day », ce qui échappe généralement aux solutions existantes. Aussi, la détection et la prévention basées sur des modèles établis à partir d'algorithmes d'apprentissage automatique, le machine learning, sont effectuées sur l'appareil, sans avoir besoin d'accéder au réseau, ce qui protège les utilisateurs contre des tentatives de phishing jusqu'alors inconnues et améliore leur confiance dans la sécurité des appareils mobiles. Le moteur d'apprentissage automatique Zimperium z9 est renforcé par une couche d'analyse statique, augmentant la vitesse et l'efficacité de la détection et de la prévention du phishing mobile.

Grâce au moteur z9, zIPS est capable de détecter les menaces connues et inconnues en analysant les petits écarts des statistiques du système d'exploitation, de la mémoire, du processeur et d'autres paramètres système d'un appareil mobile.

Les cybercriminels effectuent des attaques de type Phishing pour un but bien déterminé

- Le phishing mobile a augmenté de plus de 300 % en 2020.
- 32 % des violations avérées de données sont dues au phishing.
- 37.9 % des utilisateurs échouent aux tests de phishing.
- Un nouveau site de phishing est lancé toutes les 20 secondes.
- Le Département de la défense a déclaré recevoir 34 millions d'e-mails infectés par des logiciels malveillants par jour.
- 78 % des incidents de cyber-espionnage sont liés au phishing.

zIPS de Zimperium fournit une protection puissante et très évolutive contre le phishing mobile, protégeant ainsi les terminaux mobiles contre les stratégies courantes d'infiltration de données. zIPS contrôle tous les liens, qu'il s'agisse d'un e-mail, d'un texte, d'un média social ou d'une application de messagerie, dans le but d'établir si le lien et la source sont légitimes et si l'utilisateur peut cliquer dessus en toute sécurité. La solution zIPS est axée sur le terminal mobile lui-même, offrant la garantie de la sécurité totale des applications professionnelles et grand public tout en augmentant la confiance en matière de sécurité.

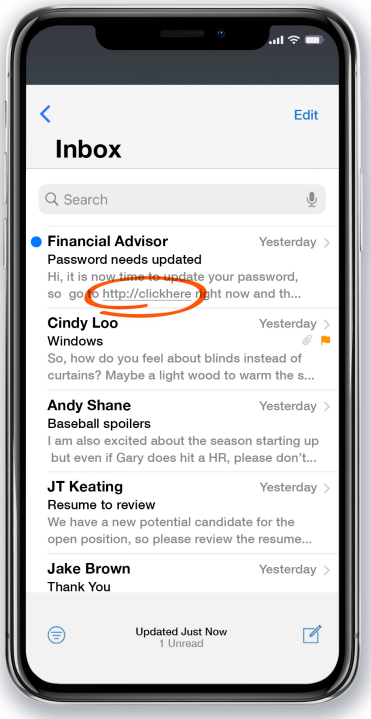
Intuitive et facile à comprendre, la protection zIPS des terminaux mobiles avise l'utilisateur du terminal au cas où une URL est malveillante avant que la connexion ne soit terminée, grâce à un ensemble d'alertes simples et contextuelles, ce qui aide les utilisateurs à adopter les meilleures habitudes en matière de sécurité mobile. Et la solution Zimperium zIPS apporte cette couche de sécurité sans même lire ni analyser les données des messages, ce qui assure la sécurité et la confidentialité des données personnelles.

Faisant partie du niveau 2 du modèle de maturité Mobile Threat Defense (MTD) de Zimperium, la protection contre le phishing mobile est une mesure proactive destinée à toute organisation qui cherche à renforcer la confiance dans la sécurité mobile tout en permettant à ses collaborateurs d'accéder aux données de l'entreprise et de les utiliser depuis leurs appareils mobiles.

Boostez la confiance en matière de sécurité grâce à une protection accrue contre le phishing mobile

En raison de l'augmentation de l'utilisation des appareils mobiles pour accéder aux données de l'entreprise et de l'augmentation des attaques de phishing de manière unanime, la surface d'attaque des organisations moyennes demeure vulnérable jusqu'à ce que des contrôles appropriés de sécurité soient implémentés sur tous les appareils.

- 25 % des courriels de phishing contournent la sécurité des clients de messagerie par défaut.
- Les URL de phishing ont été présentées aux utilisateurs via troiscampagnes d'ingénierie sociale distinctes et ciblées.
- En moyenne, les utilisateurs de terminaux mobiles ciblés font objet de 2 liens de phishing par mois.



Il serait temps de traiter les terminaux mobiles en adoptant la même attitude en matière de sécurité que celle des terminaux traditionnels et d'accroître la confiance des entreprises grâce à une sécurité renforcée des dispositifs mobiles par apprentissage automatique. Les clients de Zimperium sont protégés contre les attaques de phishing les plus avancées ou encore méconnues.

- Grâce à une solution Zimperium zIPS active de lutte contre le phishing mobile, les entreprises ont constaté une nette diminution de plus de **95 %** des attaques de phishing réussies.
- Améliorez la **visibilité** de **toutes les tentatives de phishing** sur tous les terminaux mobiles activement surveillés.
- Le score de sécurité de Zimperium permet aux SOC de comprendre la position globale du risque et de compléter tout de même les capacités par une formation de sensibilisation des utilisateurs finaux.

« L'approche holistique de Zimperium en matière de détection des attaques de phishing axée sur les appareils mobiles des utilisateurs permet de bloquer les attaques de phishing qui utilisent comme vecteurs le texte, les médias sociaux et les e-mails personnels et professionnels. Ceci est faisable tout en assurant la confidentialité des utilisateurs. »

- Radar 2020 de GigaOm pour la prévention et la détection du phishing

Résumé

Le phishing mobile représente une préoccupation de premier plan pour les professionnels de la sécurité informatique des secteurs public et privé et continue d'être utilisé comme vecteur d'attaque contre les entreprises, quelle que soit leur taille.

Défendre les utilisateurs mobiles et leurs appareils contre les attaques de phishing doit être une grande priorité, en réunissant à la fois des technologies avancées et la formation des utilisateurs à la sécurité. Si vous souhaitez en savoir plus sur la façon dont Zimperium peut aider à protéger votre agence contre le phishing mobile, nous vous invitons à nous contacter. Nos experts en sécurité mobile seront là pour vous aider.

ZIMPERIUM®