Lookout®

LIVRE BLANC

Le phishing par mobile: mythes et réalité dans les entreprises d'aujourd'hui

Les appareils mobiles constituent pour les criminels auteurs d'attaques de phishing un nouvel angle d'attaque rentable. En effet, les attaquants parviennent à contourner les systèmes existants de protection contre le phishing afin de cibler les appareils mobiles. Ces attaques mettent en lumière les failles de sécurité et exposent les données sensibles et à caractère personnel à un rythme alarmant.

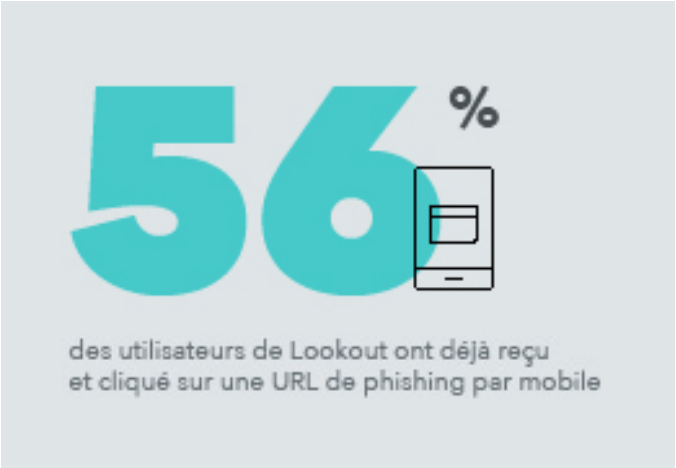
La plupart des entreprises se protègent contre les attaques de phishing par e-mails en utilisant des pare-feu traditionnels, des passerelles sécurisées pour les e-mails et des protections des points de terminaison. De plus, les utilisateurs identifient de mieux en mieux les attaques de phishing. Cependant, les appareils mobiles compliquent nettement l'identification et le blocage des attaques de ce type, tant pour les personnes que pour les technologies de protection existantes.

La problématique du phishing par mobile est à la fois différente et plus complexe

Les appareils mobiles se connectent hors des pare-feu traditionnels, ne disposent généralement pas de solutions de protection des points de terminaison, et ont accès à pléthore de nouvelles plates-formes de messagerie qui ne fonctionnent pas sur PC. L'interface utilisateur des mobiles n'offre pas non plus le niveau de détail nécessaire pour identifier les attaques de phishing. Par exemple, il n'est pas possible de balayer les hyperliens pour afficher leur destination. Par conséquent, d'après IBM, les utilisateurs d'appareils mobiles ont trois fois plus de risques d'être victimes du phishing.

Enfin, ces appareils mobiles sont la cible favorite des attaques de phishing en raison de la quantité énorme de données personnelles et professionnelles qu'ils contiennent.

De fait, et même s'ils ont été formés et bénéficient d'une protection traditionnelle contre le phishing, 56 % des utilisateurs de Lookout ont déjà reçu et cliqué sur une URL de phishing sur leur appareil mobile entre 2011 et 2016. Heureusement pour eux, Lookout a pu déjouer ces attaques. Un bémol toutefois, le taux de réception et de clic sur des URL de phishing sur un appareil mobile par des utilisateurs de Lookout a augmenté en moyenne de 85 % par an depuis 2011.



Bien souvent, les entreprises n'ont pas conscience de la complexité du problème du phishing par mobile. Avant de pouvoir mettre en place une protection complète contre le phishing sur tous les canaux, y compris les appareils mobiles, les professionnels de la sécurité et de l'informatique doivent comprendre en quoi les idées reçues qui ont cours sur le phishing brouillent les cartes. En revenant aux faits, ils pourront prendre des décisions éclairées et protéger leurs données d'entreprise.

TABLE DES MATIÈRES

1re idée reçue sur le phishing par mobile

Les protections contre le phishing couvrent également les appareils mobiles.

2e idée reçue sur le phishing par mobile

Les attaques de phishing ne se produisent que par e-mail.

1er fait sur le phishing par mobile

Lors d'une attaque de phishing, il est plus facile de piéger une personne sur un appareil mobile que sur un PC.

2e fait sur le phishing par mobile

Les attaques de phishing des auteurs de logiciels malveillants mobiles aboutissent, en particulier celles des acteurs mAPT.

3e fait sur le phishing par mobile

Les entreprises doivent faire preuve de vigilance vis-à-vis des applications (et pas seulement des personnes) accédant à leur insu à des URL de phishing avant de les soumettre aux utilisateurs de mobiles peu méfiants.

1re idée reçue sur le phishing par mobile

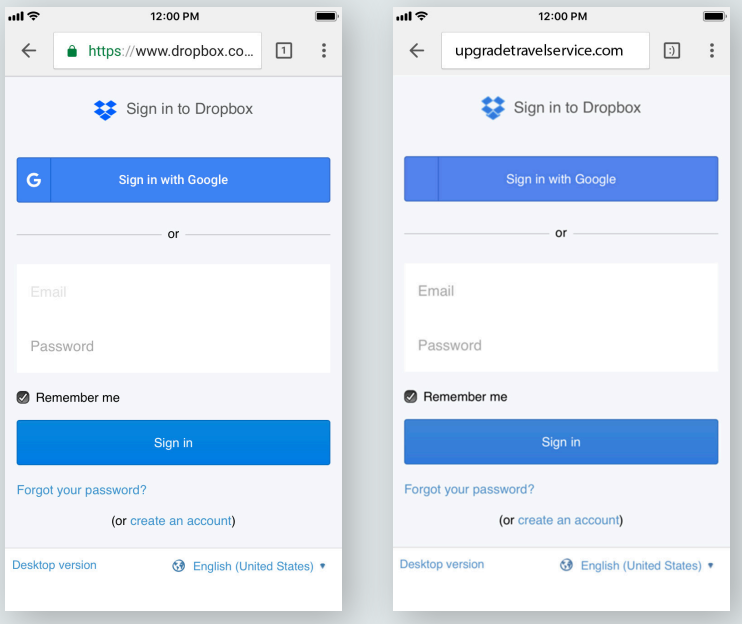
La protection actuelle contre le phishing est efficace sur les appareils mobiles

Les entreprises ont pris l'habitude d'utiliser des pare-feu traditionnels, des passerelles sécurisées pour les e-mails et des antivirus pour les points de terminaison. Elles forment également leurs utilisateurs pour éviter qu'ils ne reçoivent ou donnent suite à des messages de phishing. Cette approche est efficace sur les postes fixes, comme les ordinateurs portables, entièrement détenus et gérés par les entreprises. Cependant, comme le savent parfaitement les RSSI, les appareils mobiles répondent à des paramètres différents.

De nos jours, tous les appareils mobiles, même ceux appartenant à des entreprises, sont également utilisés à titre privé. Les employés utilisent souvent le même smartphone pour travailler, payer leur déjeuner, envoyer des e-mails personnels, prendre des photos de famille, aller sur les réseaux sociaux, lire des avis de clients, trouver les adresses de réunions et survoler des rapports financiers. Les applications de jeux, de rencontre et de messagerie côtoient les lecteurs de documents, les e-mails professionnels, les applications de partage de fichiers et autres applications contenant les données les plus importantes de votre entreprise.

Par exemple, l'e-mail est sans aucun doute le premier point d'attaque des auteurs de phishing. Or, à l'heure actuelle, plus de 66 % des e-mails sont d'abord ouverts sur un appareil mobile, d'après le rapport de MovableInk sur les préférences en matière d'appareils des consommateurs américains. Si les entreprises ont mis l'accent sur la protection des e-mails d'entreprise, la lecture des e-mails personnels sur des mobiles ouvre un nouveau boulevard aux attaquants.

Les fournisseurs de messagerie privée les plus réputés ont mis en place des protections de base contre le phishing, mais les attaquants parviennent à les contourner et à inciter les employés à fournir des données sensibles ou à télécharger des applications malveillantes, ce qui ouvre une brèche vers les données d'entreprise. Des attaquants astucieux ciblent les comptes de messagerie privée pour exécuter leurs attaques de phishing d'entreprise, car ils savent que les protections robustes dont sont dotées les messageries d'entreprise ne s'étendent pas aux comptes privés. Ils savent également que les deux comptes sont cependant disponibles sur les appareils mobiles.



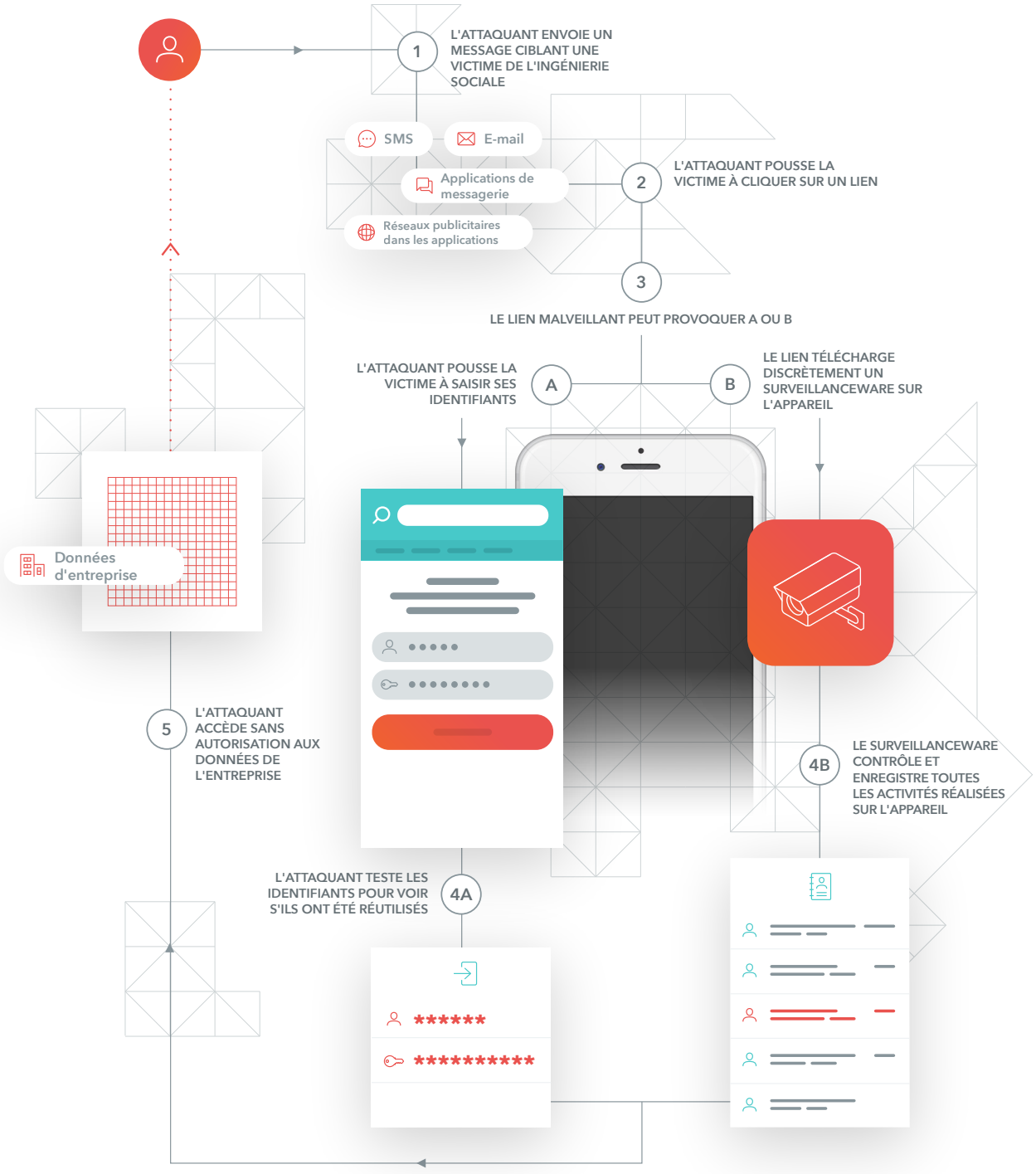
Lorsque la barre d'adresse disparaît et masque l'URL, ces deux pages de connexion sont pratiquement identiques sur un mobile.

Lorsqu'on se rend compte à quel point les sites de phishing (ou les pages Web conçues pour inciter les personnes à fournir leurs données) peuvent être convaincants, on s'étonne moins que ce soit une méthode aussi efficace pour les attaquants. Cela devient très clair lorsqu'on observe les pages de connexion suivantes : il peut être très difficile de démêler le vrai du faux, même pour des experts, a fortiori sur des appareils mobiles, dont l'écran est assez petit.

De plus, l'e-mail n'est que l'un des moyens de conduire des attaques de phishing, et les appareils mobiles ouvrent un tout nouvel éventail de points d'accès pour les attaquants.

La kill-chain du phishing par mobile

Il suffit d'un clic maladroit pour compromettre un appareil mobile. Il peut s'agir d'une URL malveillante tronquée dans la fenêtre de navigation, d'une URL à laquelle une application accède dans son back-end, se connectant sans s'en rendre compte à un réseau publicitaire malveillant, ou d'un lien contenu dans un e-mail privé qui incite les utilisateurs à saisir leurs identifiants professionnels, pour permettre à un attaquant de naviguer dans votre infrastructure et ainsi, d'accéder à vos données stratégiques.



2e idée reçue sur le phishing par mobile
Les attaques de phishing ne se produisent que par e-mail

Contrairement à une idée répandue, les attaques de phishing ne se cantonnent pas aux e-mails. Les appareils mobiles ont ouvert un nouveau boulevard aux auteurs d'attaques malveillantes. Désormais, les attaquants utilisent les SMS et les MMS pour leurs attaques de phishing, ainsi que certaines des applications et plates-formes de messagerie et de réseaux sociaux privés les plus populaires et les plus utilisés, comme WhatsApp, Facebook Messenger et Instagram.

Les employés se font avoir par les attaques de phishing par SMS. D'après une étude de Lookout, plus de 25 % des employés ont déjà cliqué sur un lien contenu dans un SMS envoyé par un numéro de téléphone maquillé pour ressembler à un numéro local.

Les experts de la sécurité doivent tenir compte de ces nouveaux modes d'attaque, sous peine de mettre leur entreprise en danger. Vous le comprendrez mieux en jetant un œil à quelques exemples récents de phishing qui ont réellement eu lieu et n'impliquaient pas les e-mails.

ViperRAT

ViperRAT est une forme sophistiquée de surveillanceware. Les acteurs malveillants qui se cachent derrière ViperRAT incitent leurs victimes à télécharger une application malveillante en se faisant passer pour des femmes sur des réseaux sociaux. Après avoir noué une relation, les attaquants envoient à leur victime un message sur les réseaux sociaux, en demandant de télécharger une application pour « discuter plus facilement ».

Les catégories d'informations volées par ViperRAT permettent aux attaquants de savoir où la personne se trouve et à qui elle est liée (y compris les photos de profil des contacts), de connaître les messages envoyés et l'historique de navigation, de faire des captures d'écran qui interceptent des données d'autres applications installées sur l'appareil, d'entendre des fichiers audio joués ou les discussions tenues à proximité de l'appareil, et d'accéder à pléthore d'images, en particulier tout ce vers quoi l'appareil photo du mobile est dirigé.

En savoir plus sur ViperRAT

Campagne de phishing Facebook

Des chercheurs de F-Secure ont identifié une campagne de phishing qui ciblait les utilisateurs iOS et Android. L'attaquant envoyait à sa victime un message par Facebook Messenger disant qu'elle figurait dans une vidéo sur YouTube. Si la victime cliquait sur le lien depuis un appareil iOS ou Android, le dispositif détectait le type de l'appareil et proposait une page ressemblant à la page de connexion de Facebook afin d'intercepter les identifiants de la victime. Sur PC, le rendu aurait été différent. Ce type d'attaque peut se baser sur l'ingénierie sociale pour inciter les victimes à fournir leurs identifiants pour n'importe quel service, y compris les services utilisés par les entreprises.

En savoir plus sur la campagne de phishing Facebook

Ces quelques exemples parmi tant d'autres d'attaques de phishing démontrent que les attaquants voient au-delà des e-mails et ciblent les appareils mobiles. Ils rappellent également pourquoi les appareils mobiles s'imposent de plus en plus comme le principal vecteur de ces attaques :

- Ils ouvrent la voie à de nouvelles plates-formes de messagerie, comme celle que nous venons d'évoquer
- Les appareils ne sont souvent pas gérés par l'entreprise, et en général, ne disposent pas d'un système de protection des points de terminaison : ils sont donc moins bien protégés contre les attaques
- La surveillance est souvent bien plus efficace sur mobile, du fait des fonctionnalités offertes par les appareils mobiles (ex. services de géolocalisation, caméra à l'avant et à l'arrière, micro, appels vocaux, messages textes, e-mails, applications) et parce que les gens les emportent pratiquement toujours avec eux

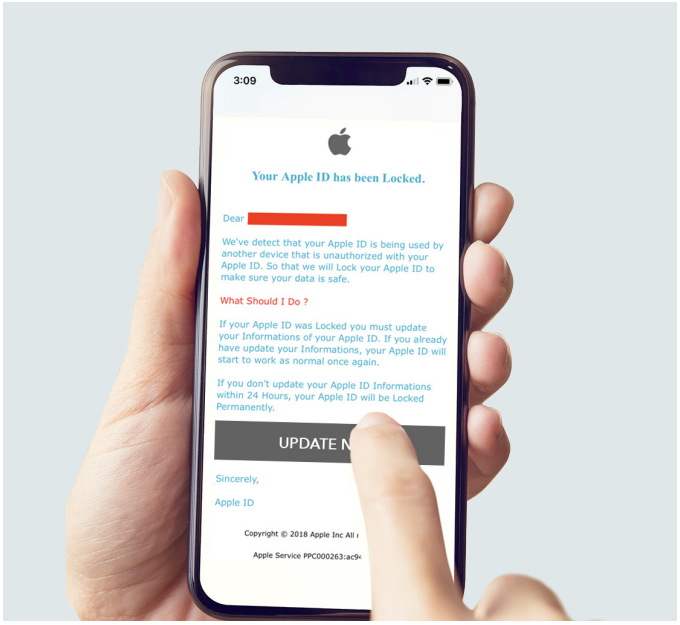
1er fait sur le phishing par mobile

Lors d'une attaque de phishing, il est plus facile de piéger une personne sur un appareil mobile que sur un PC

Les caractéristiques, les fonctionnalités et même la taille de l'écran des appareils mobiles d'aujourd'hui sont à l'avantage des auteurs d'attaques de phishing. Sur les appareils mobiles, il est plus difficile de distinguer le vrai du faux, et ils sont utilisés hors du cadre traditionnel de protection de l'entreprise.

Exemple 1

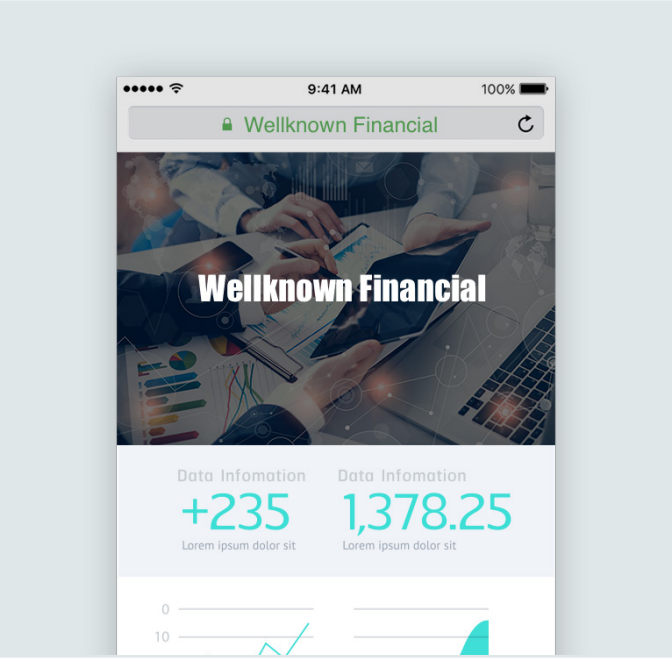
Des études ont démontré que les gens ont trois fois plus de risques de cliquer sur un lien suspect à partir d'un téléphone que sur un PC. Contrairement aux PC, sur lesquels les utilisateurs peuvent « balayer » les hyperliens pour afficher le lien complet, il est bien plus difficile de contrôler les liens sur mobile avant de cliquer dessus. Si l'on ajoute à cela le fait qu'en raison de l'affichage Web des applications mobiles (comme Facebook), il est pratiquement impossible de voir l'URL consultée, on comprend très vite pourquoi les attaquants privilégient les mobiles.



Ce qui se passe ici : sur un mobile, il est très difficile de voir ce vers quoi un lien redirige. Par exemple, sur iOS il suffit de toucher, sans appuyer, sur un lien pour activer 3D Touch et charger la page. Si l'attaquant utilise une page de phishing suffisamment convaincante, l'utilisateur aura du mal à distinguer les sites usurpés des véritables sites Web.

Exemple 2

Depuis un grand écran, on peut remarquer qu'une URL s'intitule « wellknownfinancial.com----------sidebidon.xyz » au lieu de « wellknownfinancial.com » mais sur un navigateur mobile, l'URL de la barre d'adresse est tronquée et dans les deux cas, on ne voit que « wellknownfinancial.com--- ». Dans certains cas, le navigateur remplace même l'URL par le nom de l'entreprise exploitant le site auquel vous accédez, comme on le voit à droite. Il est donc encore plus difficile de s'assurer que l'URL est légitime.



Ce qui se passe ici : La barre d'adresse affiche uniquement le nom de l'entreprise, et pas l'URL

De plus, les navigateurs mobiles dissimulent souvent les URL en masquant la barre d'adresse lorsque l'utilisateur fait défiler l'écran et en limitant le nombre de caractères affichés dans la barre de navigation en fonction de la largeur de l'écran. Dans ce cas de figure, le design amélioré facilite la tâche des auteurs d'attaques de phishing.

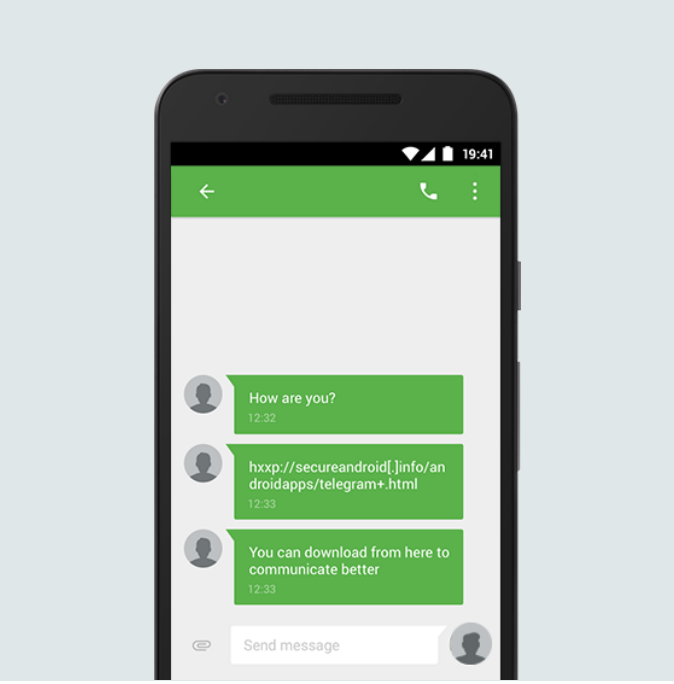
Exemple 3

Lorsqu'un appareil mobile est protégé par un pare-feu et qu'un utilisateur clique sur un lien de phishing, le pare-feu bloque la connexion de l'employé. Cependant, les mobiles sont précisément mobiles et par conséquent, les employés passent plus de temps hors de la protection du pare-feu. Les appareils mobiles se trouvent la plupart du temps en dehors du cadre de protection traditionnel, et dans ce cas, si un employé est confronté à une URL malveillante (par exemple, en rentrant chez lui), il n'est plus protégé par le pare-feu. Il est donc plus facile pour les attaquants d'accéder sans autorisation aux données si l'entreprise ne prévoit qu'un cadre traditionnel de protection.

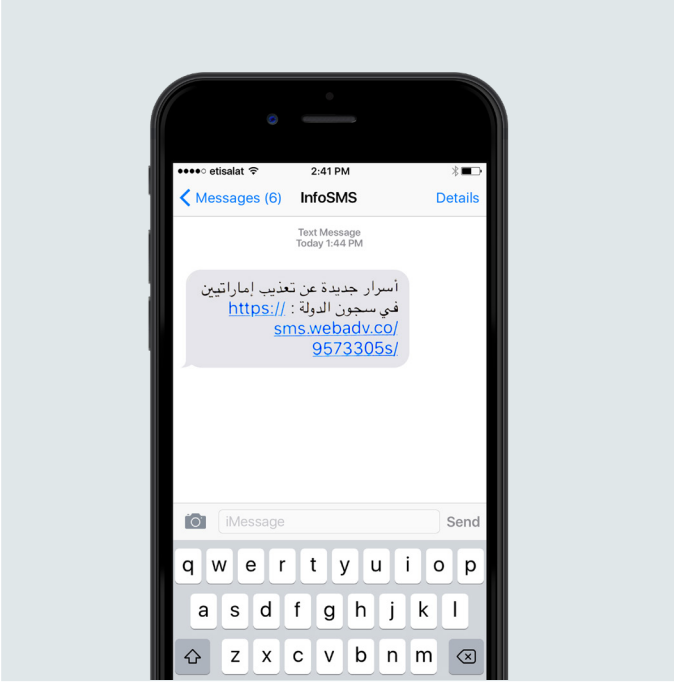
2e fait sur le phishing par mobile

Les attaques de phishing des auteurs de logiciels malveillants mobiles aboutissent, en particulier celles des acteurs mAPT

Le phishing par mobile est de plus en plus souvent le fer de lance d'attaques sophistiquées à grande échelle. Certaines des attaques les plus actives proviennent de menaces persistantes avancées sur mobile, ou mAPT. Le terme « menace persistante avancée » désigne un groupe, en général un État-nation, ayant la capacité et l'intention de cibler de façon efficace et persistante d'autres États-nations, grandes entreprises, entreprises ou personnes, afin d'extraire des informations, généralement à des fins d'enrichissement ou d'espionnage. On les appelle mAPT lorsque ces attaques ciblent des mobiles. Voici quelques exemples récents :



SMS Dark Caracal



SMS de phishing Pegasus intercepté par Citizen Lab.

- **Dark Caracal**
  Dark Caracal envoie des messages de phishing par WhatsApp et Facebook pour inciter les victimes à cliquer sur des liens malveillants et télécharger un logiciel Android malveillant. Ce logiciel Android malveillant, appelé Pallas, surveille ensuite l'appareil de la victime et collecte des quantités énormes de données.

  Dark Caracal cible les gouvernements, les armées, les services publics, les institutions financières, les sociétés de production et les sous-traitants de la défense. Il intercepte des quantités énormes de données, dont des documents, des enregistrements d'appel, des enregistrements audio, des contenus clients envoyés par messagerie sécurisée, des coordonnées, des messages texte, des photos et des données de comptes.

- **Pegasus**
  Le surveillanceware Pegasus a suscité l'attention partout dans le monde en raison de sa gravité. Les opérateurs qui répandaient Pegasus envoyaient à leurs victimes un message de phishing par SMS. Lorsque la victime cliquait dessus, cela déclenchait une chaîne d'événements silencieux débouchant sur l'une des attaques les plus sophistiquées jamais vues par Lookout compromettant les appareils iOS. De la même façon, une fois sur l'appareil, Pegasus contrôlait toutes les activités se déroulant sur l'appareil et collectait de grandes quantités de données sensibles.

Il est important de sensibiliser les utilisateurs, car les attaques par mAPT sont extrêmement sophistiquées.

3e fait sur le phishing par mobile

Les entreprises doivent faire preuve de vigilance vis-à-vis des applications (et pas seulement des personnes) accédant à leur insu à des URL malveillantes avant de les soumettre aux utilisateurs de mobiles non méfiants

Les utilisateurs finaux ne sont pas les seuls à utiliser ou accéder à des URL (ex. en cliquant dessus). Les applications se servent d'URL dans leur code base pour communiquer et extraire des informations en temps réel. Les attaquants peuvent exploiter cette fonctionnalité pour piéger des personnes. C'est un nouvel angle d'attaque dont les entreprises doivent s'inquiéter : l'accès par des « applications bénignes » à des URL malveillantes.

Par exemple, les applications utilisent souvent la publicité pour générer des revenus. Pour cela, elles intègrent des SDK (développements logiciels) publicitaires à leur code. Ces SDK se connectent à des URL en arrière-plan pour afficher des publicités destinées aux utilisateurs finaux. Or, si une application bénigne utilise un SDK publicitaire exploité par un attaquant, ce dernier peut s'en servir pour fournir des URL malveillantes et afficher des publicités visant à inciter les utilisateurs finaux à fournir des données sensibles.

Mais si ces menaces exploitent les fonctionnalités en arrière-plan, il n'est pas nécessaire pour une attaque de phishing d'être dissimulée pour être efficace.

Comment Lookout peut-il résoudre le problème du phishing ?

La protection des contenus et contre le phishing de Lookout, incluse dans Mobile Endpoint Security, a été conçue pour protéger les entreprises contre les attaques de phishing.

Protection des contenus et contre le phishing

Détection – Détection des tentatives de phishing, quelle que soit la source, sur les appareils mobiles, y compris les e-mails (privés et professionnels), les SMS, les applications de messagerie instantanée, les réseaux sociaux, etc., et élaboration de politiques de protection contre le phishing.

Protection – Blocage des connexions d'appareils aux URL malveillantes connues hébergées sur des sites à risque, et susceptibles d'intercepter des identifiants ou d'exécuter d'autres actes malveillants.

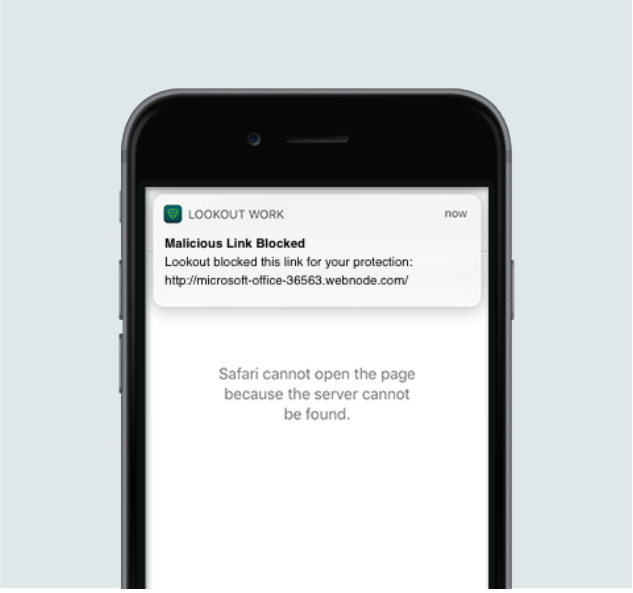
- Ces URL malveillantes englobent les publicités frauduleuses, les botnets, les centres de commande et de contrôle, les liens compromis et redirigeant vers des logiciels malveillants, les call home de logiciels malveillants, les points de distribution de logiciels malveillants, le phishing/la fraude, les URL spam, les contenus à risque comme les applications ou sites Web malveillants dont les vulnérabilités sont connues, et les logiciels espions

Correction – Alerte en temps réel des utilisateurs lors de l'accès aux URL.
Ces alertes en temps réel leur évitent de s'exposer à des tentatives de phishing ou des sites malveillants.

Analyse – Meilleure visibilité de la fréquence et de la gravité des clics d'utilisateurs sur des liens de phishing et malveillants, et suivi de l'activation ou non de la protection des contenus et contre le phishing sur les appareils. Les appareils ne présentant pas cette fonctionnalité sont signalés comme non conformes, ce qui permet une correction classique par l'entreprise, via intégration aux principaux fournisseurs d'EMM.

Fonctionnement

La protection des contenus et contre le phishing bloque toutes les tentatives de connexion vers des URL malveillantes et de phishing à l'échelle du réseau, lorsqu'un appareil ou un employé essaye de se connecter. Là où cette approche se démarque, et ce n'est pas négligeable, c'est qu'elle ne nécessite pas d'inspecter le contenu des messages. En effet, de nombreux réseaux sociaux et plates-formes de messagerie utilisés sur les appareils mobiles, comme les SMS, WhatsApp, Facebook Messenger et les e-mails personnels, sont des données extrêmement sensibles et privées des utilisateurs. En inspectant uniquement l'URL au moment où la personne ou l'appareil tente de se connecter, la protection des contenus et contre le phishing de Lookout préserve la vie privée des utilisateurs. En inspectant ces URL à l'échelle du réseau, Lookout parvient à protéger les utilisateurs contre les URL malveillantes ou de phishing contenues dans tous les e-mails, messages textes, réseaux sociaux et autres applications.



Les avantages de la protection des contenus et contre le phishing de Lookout

Lookout Mobile Endpoint Security a toujours cherché à vous offrir une parfaite visibilité sur tout le spectre des risques mobiles et vous permet d'appliquer des politiques pour réduire ces risques de façon mesurable, tout en s'intégrant à vos solutions existantes de gestion de la sécurité et de la mobilité. Vous en profiterez encore mieux avec notre fonctionnalité de protection des contenus et contre le phishing. Caractéristiques :

- Ajoute une ligne de protection puissante contre le phishing et les sites Web malveillants, et étend votre protection existante aux appareils mobiles en couvrant les e-mails personnels, les réseaux sociaux et les plates-formes de messagerie.
- Permet aux entreprises d'utiliser en toute confiance les smartphones au travail et les protège contre les contenus malveillants, que les employés soient connectés au réseau protégé de l'entreprise ou non.
- Offre une protection complète à grande échelle, couvrant tout le spectre des risques mobiles, y compris les menaces qui pèsent sur le Web et les contenus, l'un des vecteurs mobiles les plus souvent utilisés par les attaquants pour exfiltrer des données d'entreprises.
- Respecte les principes de minimisation et de collecte ciblée des données, et propose des contrôles efficaces des données d'ordre privé, avec notamment la possibilité de limiter la collecte de toute donnée personnelle associée aux utilisateurs ou aux appareils.

En optant pour Lookout Mobile Endpoint Security, qui intègre la protection des contenus et contre le phishing, vous doterez votre entreprise d'une solution éprouvée de limitation des risques et d'optimisation de la mobilité au sein de votre entreprise en toute sécurité.

Une protection véritable

Le mobile a véritablement transformé la façon dont les entreprises conduisent leurs activités. Les entreprises cherchent activement à promouvoir la productivité et la flexibilité de leurs employés, tout en protégeant les données sensibles, les données relatives aux employés et aux clients, et les infrastructures stratégiques du réseau.

- La protection des contenus et contre le phishing de Lookout répond à des besoins concrets et des problèmes actuels auxquels sont confrontés au quotidien les administrateurs.
- Ces derniers veulent laisser leurs employés naviguer librement sur le Web depuis leur appareil mobile, mais également bloquer les sites Web connus pour leurs activités malveillantes.
- Les administrateurs s'inquiètent de voir les employés utiliser différents navigateurs sur leurs appareils mobiles, sans être informés des sites Web à risque. Ils veulent donc s'assurer que les utilisateurs reçoivent un avertissement sur leur mobile avant de continuer vers ces sites.
- Les services de sécurité veulent instaurer une parité de la protection sur tous les points de terminaison, et cette solution comble les lacunes au niveau du mobile.
- Les services informatiques ne seront pas contraints de faire transiter le trafic de manière à placer les appareils mobiles derrière un pare-feu, une solution qui amoindrit la qualité de l'expérience d'utilisation et pose des problèmes de performance pour les employés. Au contraire, notre solution permet aux entreprises de bénéficier pleinement de la transformation digitale, en laissant les employés utiliser leurs appareils mobiles, qu'ils soient BYOD ou COPE.

Lookout Mobile Endpoint Security a été conçu comme une protection contre les défis de sécurité posés par l'arrivée de la mobilité dans l'entreprise. Cette dernière fonctionnalité permet aux professionnels de l'informatique et de la sécurité de résoudre les problèmes causés par le phishing par mobile.

Passez à l'étape suivante : découvrez comment Lookout peut vous aider

Les acteurs malveillants recourent à des formes sophistiquées de phishing pour franchir les portes bien gardées des entreprises.

Si les professionnels de la sécurité et de l'informatique reconnaissent généralement les risques liés aux attaques de phishing, bon nombre d'entreprises ont choisi de mettre l'accent sur la protection des points de terminaison traditionnels, comme les PC. Mais cela ne suffit pas.

La problématique du phishing par mobile est à la fois différente et plus complexe que celle des points de terminaison traditionnels. Les entreprises en quête d'une protection complète contre le phishing, sur tous les canaux, y compris les appareils mobiles, ne doivent pas camper sur leurs acquis. Lookout Mobile Endpoint Security vous offre le niveau de protection dont vous avez besoin.

Pour savoir dès aujourd'hui comment sécuriser votre parc mobile, contactez-nous à l'adresse lookout.com

*À propos des données : données provenant de l'analyse de 67 M d'appareils mobiles protégés par Lookout Personal entre 2011 et 2016. Toutes les données sont anonymes. Nous n'avons accédé à aucune donnée ni aucun réseau ou système d'entreprise pour réaliser cette analyse.