Lookout assure la protection des contenus et contre le phishing

Comprendre le phishing et les menaces de contenu sur mobile

Les attaquants se servent en premier lieu du phishing pour accéder au réseau de votre entreprise. Il est assez simple de piéger un utilisateur final et de le faire cliquer sur un lien redirigeant vers des sites Web ou des téléchargements malveillants. De fait, il ressort de données exclusives de Lookout que, dans le cadre de tests de phishing, jusqu'à un quart des employés a pu être trompé, en cliquant sur des liens de phishing. Les attaquants se sont rendu compte que l'e-mail est la technique la moins coûteuse pour les attaques de phishing. Nombreuses sont les entreprises qui ont déjà investi dans des systèmes de protection des e-mails au moyen de pare-feu, de passerelles ou de filtres antispam, qui permettent également d'empêcher les attaques de phishing sur les appareils mobiles servant uniquement à consulter les e-mails professionnels. Toutefois, ces méthodes sont de moins en moins pertinentes, car les employés peuvent, sur un même appareil, accéder à leur messagerie et leurs applications professionnelles et personnelles.

La problématique du phishing par mobile est à la fois différente et plus complexe, car celui-ci offre aux attaquants de nouveaux angles d'attaque, en plus de la messagerie d'entreprise :

E-mail personnel – envoi d'un e-mail de phishing au compte de messagerie personnel, qui contourne les systèmes de protection généralement installés sur les systèmes de messagerie gratuits et pousse l'utilisateur à cliquer sur un lien compromettant les données et donnant l'accès aux données d'entreprise depuis l'appareil

SMS – envoi à un utilisateur non méfiant d'un SMS contenant un lien court dirigeant vers un site Web malveillant ou déclenchant le téléchargement d'une application malveillante ou d'un surveillanceware

Réseaux publicitaires malveillants – intégration d'URL dans des applications mobiles afin de communiquer avec d'autres services et d'enrichir l'expérience des utilisateurs, par exemple par l'envoi d'instructions, la connexion à des sites d'achats en ligne ou l'affichage de publicités pertinentes. En revanche, si l'application est programmée pour accéder à une URL malveillante, cela peut provoquer le téléchargement de plug-ins de logiciels malveillants ou espions.

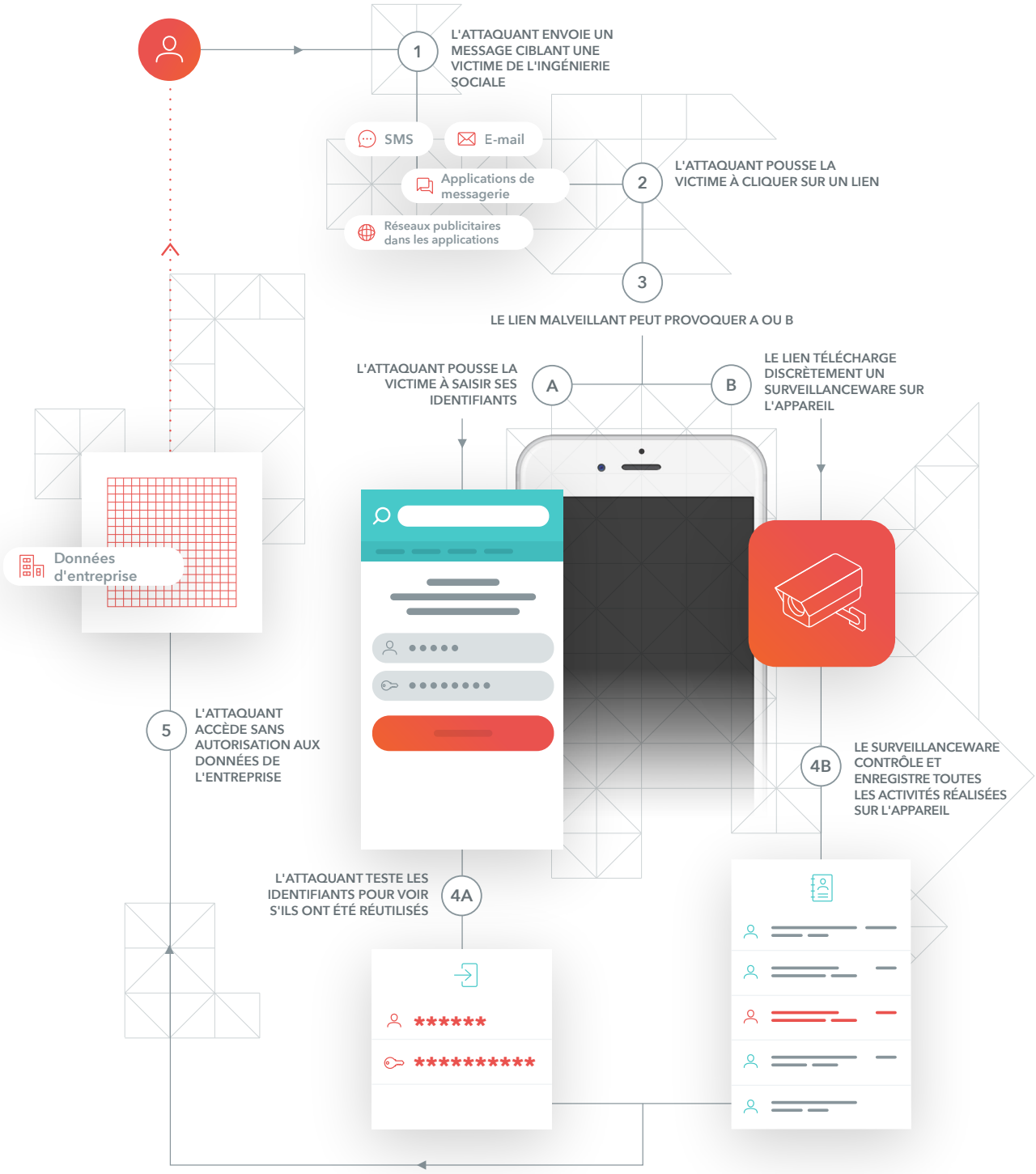
Plates-formes de messagerie – envoi d'un message à un utilisateur via WhatsApp, Facebook Messenger ou Instagram, afin de l'inciter à télécharger un logiciel espion

Bonnes pratiques en matière de sécurité pour éviter le phishing et les menaces de contenu sur mobile

1. Mettre en place un bon système de protection des comptes professionnels de messagerie sur les PC et la passerelle Web afin d'éviter les infections par pièces jointes et URL malveillantes
2. Déployer une protection complète contre le phishing par mobile sur les appareils Android et iOS, et couvrant les e-mails personnels, les SMS, les plates-formes de messagerie et les applications mobiles
3. Planifier la formation en interne des employés sur l'identification des attaques de phishing et d'ingénierie sociale via différents canaux, dont les e-mails, les SMS et les réseaux sociaux

Qu'est-ce qu'une attaque de phishing par mobile ?

Les attaquants ne se cantonnent plus aux e-mails, et les appareils mobiles s'imposent rapidement comme le principal vecteur des attaques de phishing menées dans le but d'installer des surveillancewares et d'accéder aux données et aux réseaux des entreprises.



Pourquoi les entreprises doivent-elles se protéger contre le phishing par mobile ?

D'après IBM, les utilisateurs d'appareils mobiles ont trois fois plus de risques d'être victimes du phishing. De fait, 56 % des utilisateurs de Lookout ont déjà reçu et cliqué sur une URL de phishing sur leur appareil mobile. En moyenne, en un an, ces utilisateurs ont cliqué sur six URL de phishing sur leur appareil mobile.

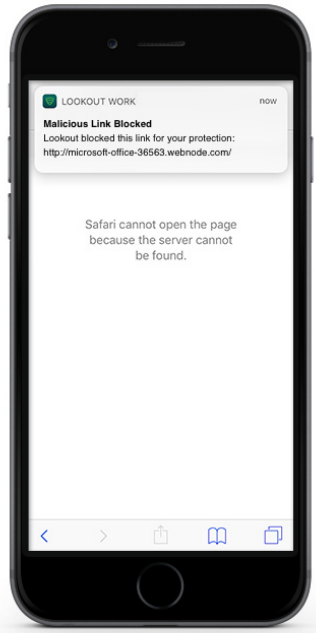
85 % Le taux de clic sur des URL malveillantes sur un appareil mobile par des utilisateurs de Lookout a ainsi augmenté de 85 % en moyenne par an depuis 2011

Or, si un attaquant parvient à inciter un utilisateur à fournir ses identifiants, il peut accéder aux systèmes de l'entreprise et parcourir sans être détecté vos infrastructures et vos données.

Quelle est la protection offerte par Lookout contre le phishing ?

La protection des contenus et contre le phishing de Lookout, fonctionnalité complète de Mobile Endpoint Security, a été conçue pour protéger les entreprises contre les attaques de phishing, quel que soit le canal, y compris les e-mails (professionnels et personnels), les SMS, les applications de messagerie et les URL intégrées dans des applications.

Lookout inspecte toutes les connexions sortantes effectuées depuis des appareils mobiles et les applications installées sur le réseau lorsqu'un utilisateur cherche à se connecter. Là où cette approche se démarque, c'est qu'elle ne nécessite pas d'inspecter le contenu des messages, et n'enfreint donc pas la vie privée des utilisateurs finaux. Lookout compare l'URL à laquelle l'utilisateur cherche à accéder avec toutes les URL malveillantes connues et identifiées par le Lookout Security Cloud. Si elle est malveillante, Lookout le signale à l'utilisateur final avant la fin de la connexion. Cette alerte en temps réel protège contre l'exposition aux contenus risqués, comme les applications ou les sites Web malveillants dont les vulnérabilités sont connues.



La console de Lookout permet aux administrateurs de bloquer les utilisateurs cherchant à se connecter sur leur appareil mobile à des URL malveillantes connues hébergées sur des sites Web à risque et susceptibles de tenter de voler leurs identifiants.

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 et les logiciels espions

Avant le blocage, les administrateurs peuvent également choisir d'informer les utilisateurs sur les sites Web à risque. Si la protection des contenus et contre le phishing est désactivée sur l'appareil d'un utilisateur, les administrateurs peuvent marquer l'appareil comme non conforme jusqu'à la réactivation de la protection.

Pourquoi choisir Lookout ?

Pour protéger également vos appareils mobiles contre le phishing en ajoutant une ligne de protection puissante contre le phishing, qui couvre les e-mails personnels, les SMS, les plates-formes de messagerie et les applications.

Pour accélérer votre transformation digitale, car vous pourrez utiliser en toute confiance des appareils mobiles au travail et les protéger contre les contenus malveillants, que les employés soient connectés au réseau protégé de l'entreprise ou non.

Pour bénéficier d'une protection complète à grande échelle, couvrant tout le spectre des risques mobiles, y compris les menaces Web et de contenu, l'un des vecteurs mobiles les plus souvent utilisés par les attaquants pour exfiltrer des données d'entreprises.

Ce qui rend Lookout différent

- Grâce à notre présence mondiale et à l'importance que nous accordons au mobile, Lookout a réuni l'un des ensembles de données sur la sécurité mobile les plus importants au monde. Lookout a ainsi collecté les données de sécurité de plus de 150 millions d'appareils à travers le monde et de plus de 50 millions d'applications, avec jusqu'à 90 000 nouvelles applications ajoutées chaque jour.
- Ce réseau de capteurs mondial intègre la notion de prévisibilité à notre plate-forme en laissant l'intelligence artificielle identifier les modèles complexes synonymes de risque, modèles qui autrement échapperaient aux analystes humains.
- La mobilité a fait entrer l'informatique dans une nouvelle ère et nécessite une nouvelle solution de sécurité conçue exclusivement pour ses besoins. Lookout sécurise les appareils mobiles depuis 2007 et possède une solide expérience en la matière.

En fournissant aux équipes informatiques et de sécurité la visibilité dont elles ont besoin, Lookout offre à votre entreprise la possibilité d'intégrer la mobilité à son écosystème en toute sécurité sans sacrifier la productivité. Pour savoir dès aujourd'hui comment sécuriser votre parc mobile, contactez-nous à l'adresse info@lookout.com