Comment Lookout Phishing and Content Protection fonctionne

Comprendre le phishing et les menaces 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 et de le faire cliquer sur un lien redirigeant vers des sites Web ou des téléchargements malveillants. En effet, il ressort de données analysées par 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 terminaux 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 à leurs applications professionnelles et personnelles.

La problématique du phishing sur mobile est à la fois différente et plus complexe, car ce dernier 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 logiciel de surveillance.

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'achat 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.

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

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

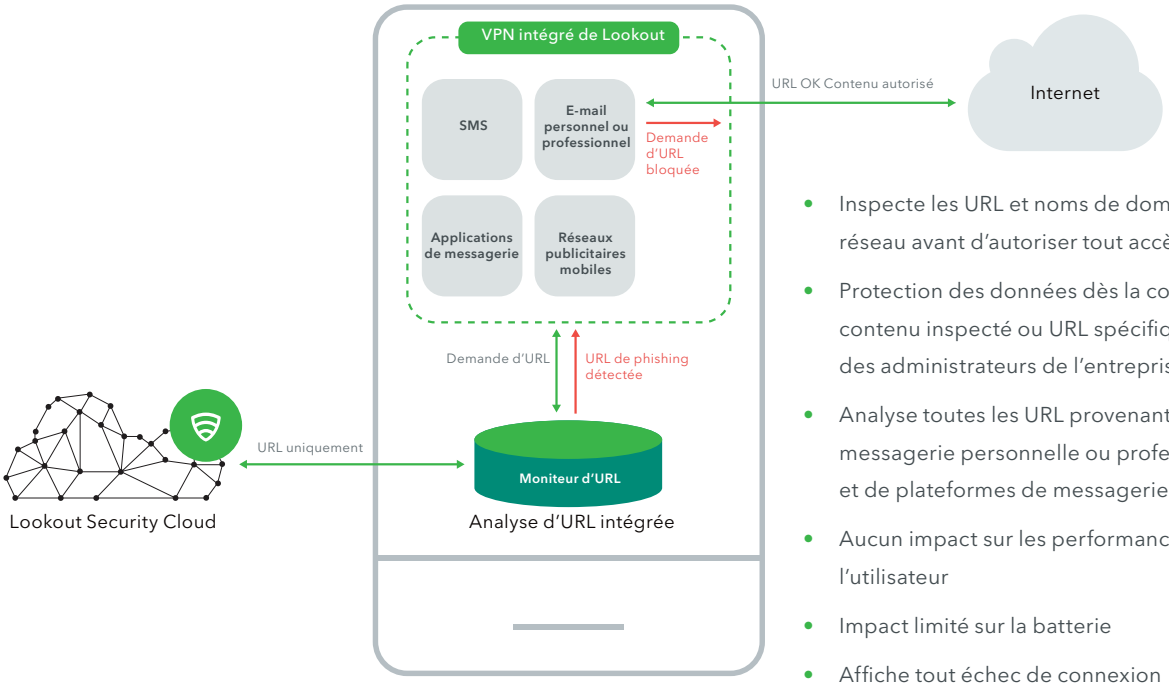
D'après IDC, plus de 30 % des entreprises ont signalé que leurs employés avaient été la cible de phishing sur mobile en 2018[1]. De fait, 56 % des utilisateurs de Lookout ont déjà reçu et cliqué sur une URL de phishing sur leur appareil mobile. En moyenne, en un an, ces utilisateurs ont cliqué sur six URL de phishing à partir de leurs appareils mobiles.

Le taux de clic sur des URL malveillantes par des utilisateurs de Lookout à partir d'un terminal mobile a ainsi augmenté de 85 % par an en moyenne depuis 2011.

[1]Source : IDC 2018 U.S. Enterprise Mobility Decision Maker Software Survey

Fonctionnement

Les moteurs à intelligence artificielle de Lookout protègent non seulement les entreprises des menaces zero-day et de cybersécurité connues, mais détectent aussi les tentatives de phishing en temps réel. L'intelligence artificielle contre le phishing de Lookout parcourt Internet à la recherche de nouveaux sites de phishing en cours de création. Grâce à son approche de recherche continue, Lookout détecte ces sites Web malveillants dès leur conception, avant qu'un utilisateur ne soit ciblé et qu'une attaque ne soit exécutée.



- Inspecte les URL et noms de domaine dans le trafic réseau avant d'autoriser tout accès
- Protection des données dès la conception, aucun contenu inspecté ou URL spécifique partagée avec des administrateurs de l'entreprise
- Analyse toutes les URL provenant d'applications de messagerie personnelle ou professionnelle, de SMS et de plateformes de messagerie
- Aucun impact sur les performances perceptible par l'utilisateur
- Impact limité sur la batterie
- Affiche tout échec de connexion

Sur un appareil, la solution de protection des contenus et contre le phishing de Lookout inspecte toutes les demandes d'URL provenant d'e-mails (professionnels ou personnels), de messages SMS, d'applications de messagerie et celles intégrées aux navigateurs d'applications, en bloquant de façon dynamique les demandes d'accès à des sites Web que Lookout a identifiés comme étant malveillants.

Cette solution de Lookout utilise un VPN local qui analyse le trafic et détecte toute tentative d'accès d'un navigateur ou d'une application d'un appareil à une URL suspecte. Pour assurer la confidentialité de l'utilisateur, seule l'existence d'un problème et le nombre de détections sont signalés à la console MES. Cette fonctionnalité ne permet pas aux administrateurs d'afficher l'historique de navigation ou le trafic d'un appareil. Dans l'application Lookout for Work, cette fonctionnalité est appelée « Safe Browsing ».

Confidentialité et collecte de données

Lookout applique au développement des produits une approche de protection des données dès la conception (Privacy by Design[2]). Nous collectons uniquement les données nécessaires au respect de notre engagement de sécurité. Nous nous assurons que les données sont protégées en transit et au repos. Nous effectuons également des contrôles de confidentialité efficaces pour réduire autant que possible la collecte de données à caractère personnel et leur présentation aux administrateurs.

Pour gagner la confiance des utilisateurs finaux et assurer la conformité réglementaire, Lookout s'engage à obtenir les certifications et autorisations les plus exigeantes. Nos engagements en matière de conformité comprennent les suivants :

- EU-U.S. Privacy Shield (Bouclier de protection des données UE-États-Unis), octobre 2016
- FedRAMP In Process, mars 2017
- Certification ISO 27001, juin 2017
- Certification ISO 27018, décembre 2017
- RGPD, conforme à la réglementation RGPD (UE) 2016/679

[2] https://en.wikipedia.org/wiki/Privacy_by_design

L'analyse d'URL en question

La solution Lookout Phishing and Content Protection exploite une combinaison d'analyses d'URL (en provenance d'e-mails, de messages SMS, de réseaux publicitaires et de plateformes de messagerie) effectuées par intelligence artificielle directement sur les terminaux ou sur le Cloud. Aucun contenu de ces applications n'est collecté, stocké ou partagé avec les administrateurs d'entreprise. Aucun trafic ou contenu n'est redirigé hors du terminal ou via une passerelle Web, quelle qu'elle soit.

Engagement de Lookout par rapport au RGPD

Le Règlement général sur la protection des données (RGPD) impose de nouvelles règles pour la protection des informations des résidents de l'Union européenne en matière de vie privée. Lookout déploie tous les efforts commercialement raisonnables et prend les mesures techniques et organisationnelles préconisées pour respecter ce règlement (Règlement (UE) 2016/679).

Le RGPD inclut des exigences relatives à la collecte, au stockage, à l'utilisation et à la sécurisation des informations à caractère personnel par les entreprises. Nous nous concentrons sur les principales exigences ci-dessous, en phase avec la conformité au RGPD.

Pourquoi choisir Lookout ?

Protégez vos terminaux mobiles en ajoutant une ligne de protection puissante contre le phishing, qui couvre les e-mails personnels, les SMS, les plateformes de messagerie et les applications.

Accélérez votre transformation numérique en utilisant en toute confiance des terminaux mobiles au travail et en les protégeant contre les contenus malveillants, que les employés soient connectés au réseau protégé de leur entreprise ou non.

Bénéficiez d'une protection complète à grande échelle, couvrant tout le spectre des risques mobiles, y compris les menaces web, l'un des vecteurs mobiles que les attaquants utilisent le plus souvent 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 170 millions d'appareils à travers le monde et de plus de 70 millions d'applications, avec jusqu'à 90 000 nouvelles applications ajoutées quotidiennement.
- Ce réseau de capteurs mondial intègre la notion de prévisibilité à notre plateforme 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 permet à votre entreprise d'intégrer la mobilité à son écosystème en toute sécurité et sans sacrifier la productivité. Pour apprendre dès aujourd'hui à sécuriser votre parc mobile, contactez-nous à l'adresse lookout.com/fr.