Lookout

LE SPECTRE DES RISQUES MOBILES

Comprendre l'étendue des risques de la mobilité pour les données d'entreprise

Lookout a créé la Matrice des risques mobiles pour aider les sociétés à comprendre les différents éléments et vecteurs qui composent le spectre des risques mobiles. Ces informations offrent aux entreprises une meilleure visibilité sur la prévalence et l'impact des menaces et des vulnérabilités mobiles.

LA MATRICE DES RISQUES MOBILES

Vecteurs

Composantes du risque

	APPLICATIONS	APPAREIL	RÉSEAU	WEB ET CONTENU
MENACES	**Menaces applicatives** 1 Les applications malveillantes peuvent dérober des informations, endommager les appareils et accorder des accès à distance non autorisés.	**Menaces pesant sur l'appareil** Les menaces pesant sur l'appareil peuvent entraîner des pertes de données majeures à cause des autorisations accrues dont bénéficient les hackers.	**Menaces pesant sur le réseau** 5 Les données sont menacées via les connexions au Wi-Fi ou au réseau mobile.	**Menaces Web et de contenu** Ces menaces incluent les URL malveillantes ouvertes à partir d'e-mails ou de messages SMS de phishing.
VULNÉRABILITÉS LOGICIELLES	**Vulnérabilités applicatives** Même les éditeurs de logiciels connus développent des applications pouvant comporter des failles de sécurité qui mettent en danger les données des utilisateurs et des entreprises.	**Vulnérabilité de l'appareil** 2 Les appareils d'entreprise sont particulièrement exposés durant la « fenêtre de vulnérabilité », c'est-à-dire entre le lancement d'un nouveau correctif et son installation.	**Vulnérabilité du réseau** Les appareils mobiles sont plus souvent confrontés à des réseaux plus hostiles que les ordinateurs portables et ne bénéficient pas du même niveau de protection.	**Vulnérabilités du Web et du contenu** Les formats de contenu incorrects, notamment dans les pages Web, les vidéos et les photos, peuvent permettre l'accès non autorisé aux appareils.
COMPORTEMENT ET CONFIGURATIONS	**Comportements et configurations de l'application** 3 Les applications mobiles peuvent faire fuiter des données, telles que des contacts.	**Comportements et configurations de l'appareil** 4 Certains comportements, tels que le débogage USB pour Android ou l'installation d'applications depuis des boutiques d'applications non officielles font courir un risque aux données d'entreprise.	**Comportements et configurations du réseau** Se connecter à un routeur mal configuré, un portail captif inconnu ou un réseau qui déchiffre le trafic pour filtrer le contenu.	**Comportements et configurations du Web et du contenu** Consulter des sites Web peu fiables qui ne chiffrent pas les informations de connexion et font fuiter des données d'entreprise augmente le risque d'activités malveillantes

PRÉVALENCE DES RISQUES MOBILES

47 SUR 1 000 APPAREILS D'ENTREPRISE ANDROID ONT ÉTÉ CONFRONTÉS À DES MENACES APPLICATIVES

Sur deux trimestres (4e trimestre 2016 et 1er trimestre 2017), 47 appareils d'entreprise Android sur 1 000 protégés par Lookout Mobile Endpoint Security ont été confrontés à des menaces applicatives. 1

57 % DES UTILISATEURS iOS N'ONT PAS MIS À JOUR LEUR SYSTÈME D'EXPLOITATION AU-DELÀ DE LA VERSION 10.3

Entre le 27 mars 2017, date de lancement d'iOS 10.3, et le 14 avril 2017, seuls 43 % des utilisateurs ont effectué la mise à jour vers la dernière version d'iOS. Or, la version 10.3.1 corrige une faille d'exécution qui peut être exploitée par le biais du Wi-Fi. Cette statistique est basée sur les données concernant les utilisateurs iOS de Lookout Personal. 2

30 % DES APPLICATIONS DES APPAREILS D'ENTREPRISE iOS ONT ACCÈS AUX CONTACTS

Sur les appareils d'entreprise iOS protégés par Lookout Mobile Endpoint Security, 75 % des applications ont accès à l'appareil photo, 38 % au GPS, 8 % aux calendriers et 10 % au micro. De plus, 43 % des appareils d'entreprise iOS sont connectés à Facebook et 14 % à Twitter. 3

5 SUR 1 000 APPAREILS D'ENTREPRISE ANDROID ONT ÉTÉ ROOTÉS

Seul 1 appareil d'entreprise iOS sur 1 000 a été jailbreaké. 4

JUSQU'À 1 % DES APPAREILS MOBILES D'ENTREPRISE ONT ÉTÉ CONFRONTÉS À DES MENACES BASÉES SUR LE RÉSEAU

L'étude de Lookout révèle qu'un peu moins de 1 % des appareils mobiles d'entreprise ont été confrontés à des menaces réseau l'an dernier. 5

À PROPOS DES DONNÉES :

Les données analysées sont issues d'un vaste sous-ensemble mondial d'appareils personnels ou d'entreprise protégés par Lookout. Elles ont été recueillies entre le 15 avril 2016 et le 16 avril 2017. Les données d'entreprise proviennent d'appareils Android et iOS d'institutions financières, de prestataires de soins de santé, d'organismes gouvernementaux et d'entreprises d'autres secteurs. Les données personnelles proviennent de plus de 100 millions d'appareils Android et iOS d'utilisateurs du monde entier. Toutes les données ont été extraites anonymement. Nous n'avons accédé à aucune donnée et aucun réseau ou système d'entreprise pour réaliser cette analyse.

À PROPOS DE LOOKOUT :

Lookout est une société de cybersécurité qui permet à des dizaines de millions d'individus, d'entreprises et d'agences gouvernementales d'être à la fois mobiles et sécurisés. Alimenté par un ensemble de données de code mobile provenant du monde entier (40 millions d'applications, et sûrement davantage), Lookout Security Cloud peut identifier les connexions qui autrement resteraient invisibles, prédire les attaques mobiles et les arrêter avant qu'elles n'entraînent des dommages irréversibles. Les principaux opérateurs de réseaux mobiles du monde, dont AT&T, Deutsche Telekom, EE, KDDI, Orange, Sprint, T-Mobile et Telstra, ont sélectionné Lookout comme leur solution de sécurité mobile préférée. Lookout a par ailleurs établi des partenariats avec des entreprises de pointe telles que AirWatch, Ingram Micro, Microsoft et MobileIron. Lookout a son siège social à San Francisco et possède des bureaux à Amsterdam, Boston, Londres, Sydney, Tokyo, Toronto et Washington, D.C. Pour en savoir plus, consultez le site www.lookout.com, abonnez-vous à la newsletter Lookout et suivez Lookout sur Facebook, Twitter et LinkedIn.