Lookout®

LE SPECTRE DES RISQUES MOBILES

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

Lookout a développé une matrice des risques mobiles pour aider les organisations à comprendre les composants et vecteurs constituant le spectre des risques mobiles, mais aussi pour fournir des données qui aideront les entreprises à mieux comprendre la prévalence et l'impact des menaces et vulnérabilités mobiles.

LA MATRICE DES RISQUES MOBILES

Composantes du risque

Vecteurs

	WEB ET CONTENU	APPLICATIONS	APPAREIL	RÉSEAU
MENACES	• Phishing • Drive-by-download • Sites Web et fichiers malveillants	• Logiciel espion et surveillanceware • Chevaux de Troie • Autres applications malveillantes	• Élévation des privilèges • Jailbreak/root à distance	• Man-in-the-middle • Fausse antenne-relais de téléphonie mobile • Installation de l'AC racine
VULNÉRABILITÉS LOGICIELLES	• Format de contenu incorrect qui déclenche des vulnérabilités du système d'exploitation ou des applications	• Applications obsolètes • SDK (kits de développement logiciel) vulnérables • Mauvaises pratiques de codage	• Système d'exploitation obsolète • Matériel en fin de vie • Applications préinstallées vulnérables	• Vulnérabilités du matériel réseau • Vulnérabilités des piles de protocoles
COMPORTEMENT ET CONFIGURATIONS	• Ouvrir des pièces jointes et cliquer sur des liens vers des contenus potentiellement dangereux	• Applications qui font fuir les données • Applications qui compromettent la sécurité de l'entreprise • Applications non conformes aux réglementations	• Jailbreak/root initié par l'utilisateur • Pas de code pin/mot de passe • Débogage USB	• Proxies, VPN, AC racine • Connexion automatique à des réseaux non cryptés

PRÉVALENCE DES RISQUES MOBILES

203 SUR 1 000 APPAREILS D'ENTREPRISE ONT ÉTÉ CONFRONTÉS À DES MENACES URL

203 appareils d'entreprise (Android et iOS) sur 1 000 ont été confrontés à des menaces URL (T1 à T3 2021).

17 % DES APPLICATIONS DES APPAREILS D'ENTREPRISE ONT ACCÈS AUX CONTACTS

Sur les appareils d'entreprise protégés par Lookout Mobile Endpoint Security, 25% des applications ont accès à l'appareil photo, 38% au GPS, 2% aux calendriers et 5% au micro. De plus, 4% des appareils d'entreprise sont connectés à Facebook et 2% à Twitter.

16 SUR 1 000 APPAREILS D'ENTREPRISE ANDROID ONT ÉTÉ CONFRONTÉS À DES MENACES LIÉES AUX APPLICATIONS

Sur deux trimestres (T1 à T3 2021), 16 appareils d'entreprise Android sur 1 000 ont été confrontés à des menaces liées aux applications..

58 % DES UTILISATEURS D'IOS N'ONT PAS MIS À JOURLEUR SYSTÈME D'EXPLOITATION AU-DELÀ DE LA VERSION 15.0

Entre le 20 septembre 2021, date de lancement de la version 15.0, et le 17 novembre 2021, seuls 42 % des utilisateurs ont effectué la mise à jour vers la dernière version.

2 SUR 1 000 APPAREILS D'ENTREPRISE ONT ÉTÉ CONFRONTÉS À DES MENACES RÉSEAU

2 appareils mobiles d'entreprise sur 1 000 ont été confrontés à des menaces réseau l'an dernier.

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 1er janvier 2021 et le 31 octobre 2021. 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 185 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 entreprise de sécurité intégrée du terminal au Cloud (endpoint-to-cloud). Notre mission est de sécuriser et développer l'avenir numérique dans un monde où la confidentialité est primordiale et où la mobilité et le Cloud jouent un rôle clé dans notre travail et nos loisirs. Nous permettons aux consommateurs et aux employés de protéger leurs données et de rester connectés en toute sécurité sans porter atteinte à leur confidentialité et à leur confiance. Des millions de consommateurs, de multinationales, d'organismes gouvernementaux et de partenaires font confiance à Lookout, notamment AT&T, Verizon, Vmware, Vodafone, Microsoft, Google et Apple. Lookout a son siège social à San Francisco et a également des bureaux à Amsterdam, Boston, Londres, Sydney, Tokyo, Toronto et Washington D.C. Pour en savoir plus, visitez le site www.lookout.com/fr et suivez Lookout sur son blog, LinkedIn et Twitter.