DSP2

LA SÉCURISATION DES APPLICATIONS BANCAIRES SUR MOBILE DÉSORMAIS NÉCESSAIRE

Vue d'ensemble de la situation

Les clients utilisent de plus en plus les applications bancaires sur mobile comme moyen principal pour gérer leurs finances, transférer de l'argent, déposer des chèques ou encore payer des factures. Malheureusement, les cybercriminels ont repéré cette tendance et se sont mis à cibler les utilisateurs d'applications mobiles en priorité. C'est pourquoi des réglementations plus strictes imposent désormais une sécurité supplémentaire aux applications mobiles bancaires et de paiement.

Statistiques clés de 2018

50 %

TAUX D'ÉVOLUTION DES PERSONNES QUI UTILISENT SEULEMENT DES APPLICATIONS BANCAIRES SUR MOBILE[1]

68 %

PROPORTION DE PERSONNES ISSUES DE LA GÉNÉRATION Y QUI SOUHAITENT REMPLACER LEUR PORTEFEUILLE PAR LEUR SMARTPHONE[2]

600 %

TAUX D'ÉVOLUTION DES TRANSACTIONS FRAUDULEUSES SURVENUES SUR DES APPLICATIONS MOBILES ENTRE 2015 ET 2018[3]

65 %

TOTAL DE TRANSACTIONS FRAUDULEUSES QUI SURVIENNENT SUR MOBILE[3]

87 %

PROPORTION DE CONSOMMATEURS QUI PRÉFÈRENT LES BANQUES TRADITIONNELLES PAR RAPPORT AUX APPLICATIONS MOBILES[5]

Ensemble d'exigences de sécurité clés de l'ABE concernant la directive DSP2

DÉTECTER LES LOGICIELS MALVEILLANTS

Les banques doivent mettre en œuvre des mécanismes de surveillance des transactions capables de détecter les logiciels malveillants dès l'étape d'authentification

(DSP2, Normes techniques de réglementation, Article 2)

SÉCURISER LES ENVIRONNEMENTS D'EXÉCUTION

Afin d'atténuer l'impact des appareils compromis, les banques doivent mettre en place des mesures de sécurité telles que la sécurisation des environnements d'exécution

(DSP2, Normes techniques de réglementation, Article 9)

Exemples de la vie réelle[4]

15/100

NOMBRE D'APPAREILS DONT DES APPLICATIONS RENOMMÉES DE SERVICES FINANCIERS ONT ÉTÉ CONFRONTÉES À UNE MENACE

62 %

PART DE LA POPULATION QUI ESTIME QUE L'APPLICATION VENMO EST PEU SÉCURISÉE

56 000

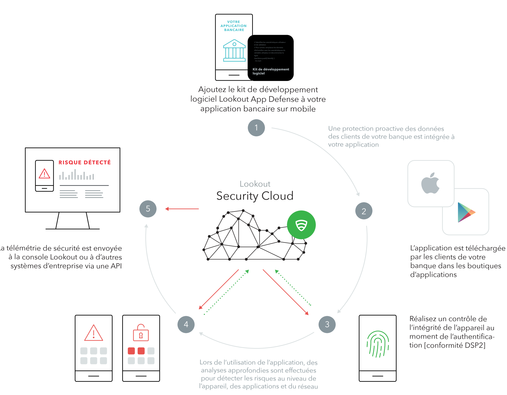
NOMBRE D'APPAREILS DONT UNE APPLICATION QUI SE SITUE PARMI LES 5 PLUS UTILISÉES A ÉTÉ CONFRONTÉE À UN CHEVAL DE TROIE, À UN SURVEILLANCEWARE OU À UN LOGICIEL ESPION

Étapes à suivre pour que les applications bancaires sur mobile soient conformes à la directive DSP2

- Exploiter une stratégie de déploiement rapide et fluide
- Augmenter la protection contre les menaces connues et inconnues qui touchent les applications
- Activer les mesures de protection plus rapidement
- Intégrer la sécurité au niveau de l'application mobile
- Mettre en œuvre des politiques de sécurité fondées sur un vaste ensemble mobile
- Garantir la sécurité à l'échelle du client

Comment Lookout protège les applications bancaires sur mobile

Lookout App Defense réalise une analyse de sécurité au moment de l'authentification de l'utilisateur final afin de vérifier la présence d'un logiciel malveillant et/ou d'un appareil compromis



Lookout

1 David Schiff, et al. « PwC's 2018 Digital Banking Consumer Survey: Mobile Users Set the Agenda. » PwC's 2018 Digital Banking Consumer Survey: Mobile Users Set the Agenda. PwC, juin 2018, www.pwc.com/us/en/industries/financial-services/library/digital-banking-consumer-survey.html. Dernier accès janv. 2019.

2 « Mobile Banking One of Top Three Most Used Apps by Americans, 2018 Citi Mobile Banking Study Reveals. » About | Citi | Timeline. 26 avril 2018. Dernier accès janvier 2019. https://www.citigroup.com/citi/news/2018/180426a.htm.

3 « Prévention des fraudes | RSA Fraud & Risk Intelligence Suite. » RSA PRÉVENTION DES FRAUDES RSA® Fraud & Risk Intelligence Suite. 2018. Dernier accès janvier 2019. https://www.rsa.com/fr-fr/products/fraud-prevention

4 « Lookout App Defense. » Sécurité mobile. Dernier accès 14 janvier 2019. https://www.lookout.com/products/app-defense.

5 Tina Orem, « 65% of Fraud Transactions Happen on Mobile, Study Finds. » Credit Union Times, 31 mai 2018. Dernier accès 19 janvier 2019. https://www.cutimes.com/2018/05/31/65-of-fraud-transactions-happen-on-mobile-study-fi/?slreturn=20190022141719.