Lookout App Defense

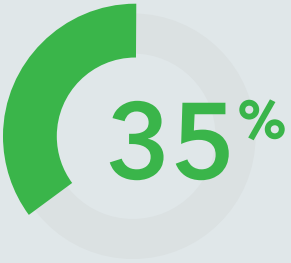
Protégez vos applications mobiles de façon proactive pour empêcher les fuites de données de clients

Applications mobiles : le nouveau champ de bataille des hackers

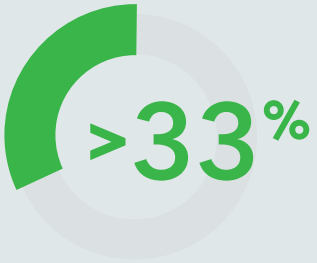
Les applications sur smartphone font désormais partie intégrante de la vie quotidienne et nous permettent de tout gérer, qu'il s'agisse de réserver un voyage ou de gérer les finances. De la même manière, les entreprises misent sur les applications afin de proposer à leurs clients des expériences innovantes et d'améliorer l'intérêt que ces derniers leur portent. Néanmoins, si l'adoption des applications mobiles est en hausse, on observe également une hausse des menaces de cybersécurité. Les hackers ciblent désormais principalement les appareils mobiles pour voler les identifiants de connexion et les données des clients afin d'en tirer profit ou de frauder sur d'autres canaux numériques. L'un des principaux vecteurs de menaces utilisés par les hackers sur mobile est de s'attaquer aux applications elles-mêmes.

11 500

troyens bancaires de plus découverts entre T4 2018 et T1 2019[1]



augmentation des téléchargements d'applications entre 2016 et 2018[2]



transactions bancaires frauduleuses effectuées depuis un mobile[3]

[1] Kaspersky Labs, « Phantom Menace: Mobile Banking Trojan Modifications Reach All-Time High » Kaspersky.com, Kaspersky Labs, 2018, www.kaspersky.com/about/press-releases/2018_phantom-menace.

[1] The State of Mobile 2019: Banking and Finance. App Annie, 2019, The State of Mobile 2019: Banking and Finance, www.appannie.com/en/go/state-of-mobile-2019/.

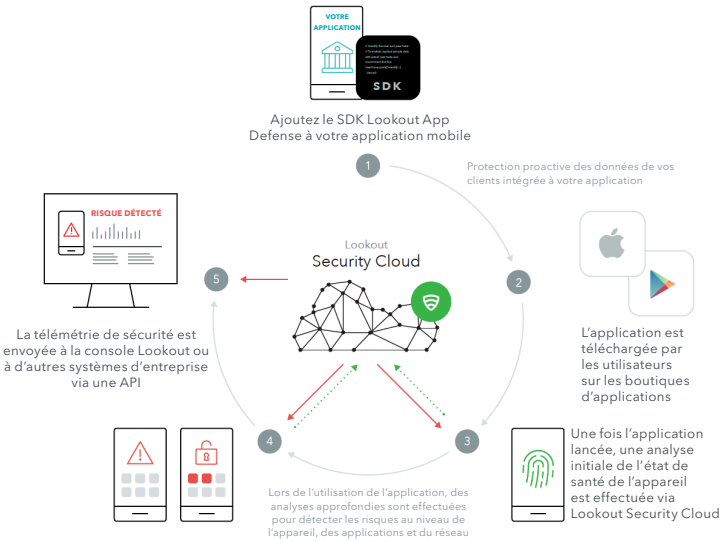
[1] Rapport trimestriel de RSA sur les fraudes. RSA, 2019, Rapport trimestriel de RSA sur les fraudes, https://www.rsa.com/fr-fr/products/fraud-prevention/fraud-prevention.

Kit de développement logiciel Lookout App Defense

La solution Lookout App Defense protège les applications mobiles au moyen d'un SDK léger et intégrable, disponible sur Android et iOS. Une fois le kit de développement logiciel intégré, l'application peut exploiter le Lookout Security Cloud, qui contient des données issues de plus de 180 millions d'appareils et de plus de 90 millions d'applications, en vue de protéger les personnes et les organisations contre les menaces de cybersécurité et les logiciels malveillants susceptibles de provoquer des fuites de données.

Les entreprises profitent de la télémétrie de Lookout en utilisant le SDK pour identifier la menace dans l'application mobile en fonction de sa gravité et de sa nature. Pour s'intégrer avec les outils de sécurité existants tels que les systèmes SIEM et les modèles d'évaluation des risques, l'API Lookout Event Feed propose un flux brut de télémétrie d'événements de sécurité.

Globalement, le kit de développement logiciel peut vous aider à réduire le risque de fraude et de fuite de données, à vous conformer aux normes telles que le RGPD et la DSP2, et à protéger les utilisateurs en identifiant les problèmes potentiels sur leurs appareils lorsqu'ils utilisent l'application.



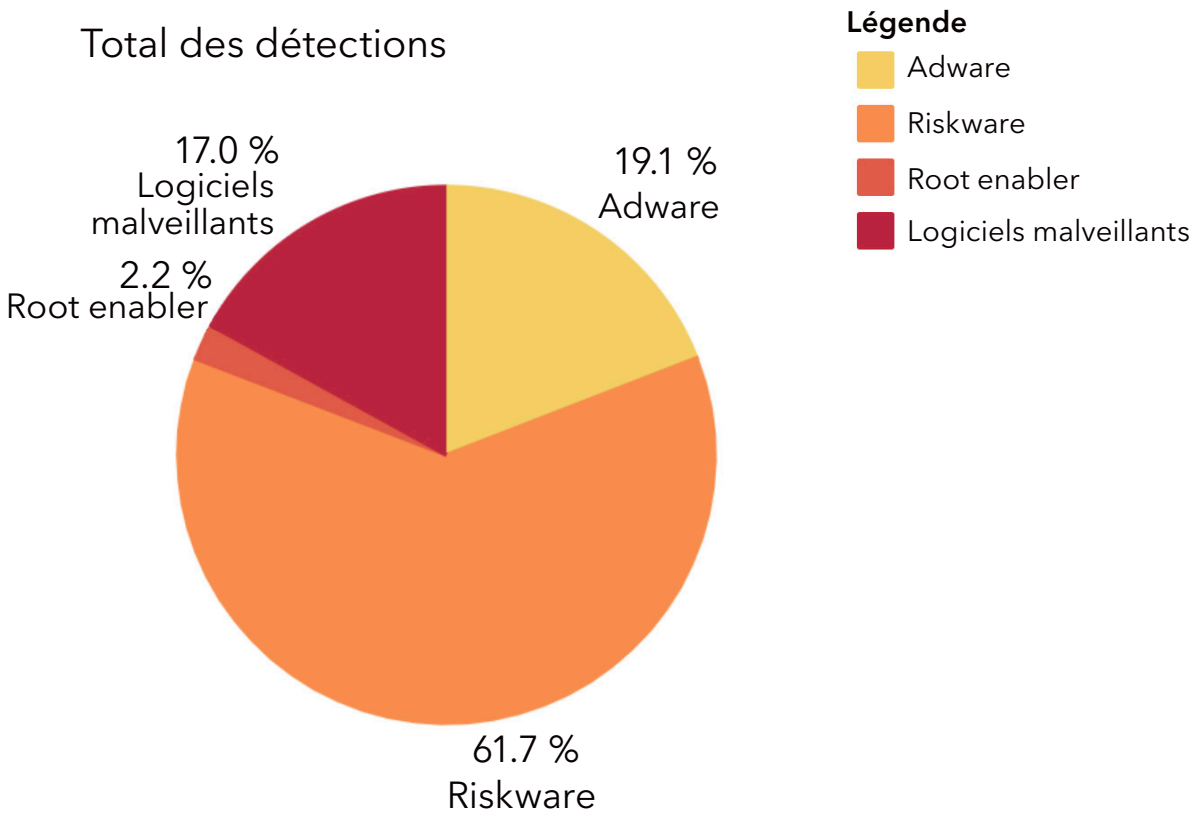
Une protection intégrée aux applications pour faciliter la détection et la correction

La clé d'un kit de développement logiciel efficace est de concevoir des applications mobiles capables de protéger elles-mêmes grâce à un mécanisme d'auto-remediation, non-intrusif ou nuisible pour l'expérience utilisateur. Voici quelques exemples de détections potentielles et d'étapes d'atténuation que l'application pourrait suivre après avoir été alertée par les politiques de Lookout App Defense :

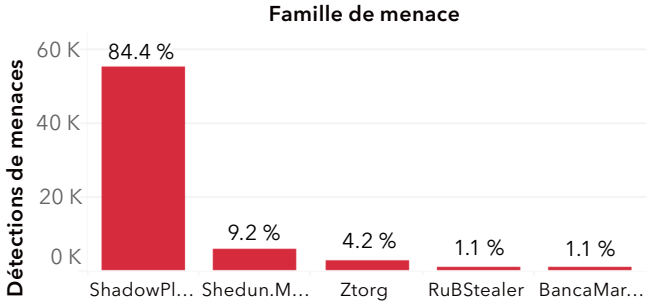
Détection (Gravité)	Correction
Appareil jailbreaké/rooté et élévation des privilèges (Élevée)	Bloquer l'authentification ou mettre fin à la session
Les attaques de type zero-day et man-in-the-middle (Élevée)	Mettre fin à la session et vider le cache
Les appareils comportant des facilitateurs d'accès à la racine, chevaux de Troie, etc. (Moyenne)	Limiter la taille des transactions ou activer l'authentification multifacteur
Les logiciels malveillants tels que les logiciels de publicité, logiciels espions, etc. (Faible)	Aucune correction immédiate - gestion des menaces

Niveau de risque des applications évalué par Lookout

En évaluant le niveau de risque des applications, Lookout assure une visibilité en décomposant les vecteurs de menaces provenant des terminaux des utilisateurs utilisant une application mobile protégée. Cela implique de décomposer les appareils dotés de systèmes d'exploitation vulnérables, qui ont été rootés ou jailbreakés, ou qui sont infectés par des logiciels malveillants, et de classer les familles de logiciels malveillants en fonction de la gravité des menaces. Le diagramme ci-dessous affiche un exemple de données issues de la télémétrie du kit de développement logiciel et du Lookout Security Cloud, pouvant être exploitées par des équipes chargées de la sécurité et des fraudes financières, à mesure qu'elles ajustent leurs modèles de risques et qu'elles renforcent leur défense contre les cybermenaces.



Chevaux de Troie : les 5 principaux



Détections de menaces