Lookout®

LIVRE BLANC

Pourquoi les services financiers doivent protéger proactivement leurs applications mobiles

Une révolution numérique touche actuellement les institutions financières grand public où les traditionnelles interactions directes avec les clients sont délaissées au profit de l'utilisation des appareils mobiles. D'après une étude de la Réserve fédérale intitulée « Consumers and Mobile Financial Services », 43 % des personnes disposant d'un appareil mobile et d'un compte bancaire utilisent des services de banque mobile. La banque mobile propose des services offrant une liberté sans précédent à ses clients, tels que des dépôts de chèques mobiles, des virements quasi instantanés de personne à personne et un accès aux comptes personnels en temps réel.

Les applications mobiles orientées clients offrent les avantages clés suivants aux banques et autres établissements financiers :

- Amélioration de la fidélisation des clients. Les clients étant davantage fidélisés, ils connaissent mieux la valeur ajoutée qu'offrent les établissements bancaires. Une étude réalisée par J.D. Power and Associates révèle une augmentation de la satisfaction client vis-à-vis de la banque mobile de 84 points.
- Renforcement de l'image de marque et de la notoriété. Un utilisateur moyen passe plus de quatre heures par jour sur son téléphone portable. Même si une application bancaire n'est pas ouverte et en cours d'exécution, sa marque et son logo figurent toujours parmi les applications installées sur l'appareil d'un client et restent donc toujours à l'esprit du client.
- Baisse du coût des services. En automatisant les interactions directes, les établissements de services financiers peuvent réduire les coûts consacrés à l'assistance client et réinvestir les économies réalisées dans des initiatives génératrices de revenus.

Au vu du développement de nouvelles fonctionnalités pour les applications mobiles, la sécurité doit rester un enjeu majeur pour les développeurs d'applications afin de protéger les identifiants des clients contre toute tentative de vol de la part d'acteurs malveillants.

Menaces pesant sur les applications bancaires orientées clients

Un acteur malveillant peut utiliser quatre méthodes différentes pour compromettre les identifiants et données d'un client utilisant une application mobile :

1. **Appareil compromis.** Via un appareil compromis (jailbreaké ou rooté), les attaquants peuvent désactiver ses fonctionnalités de sécurité, qui en temps normal empêchent tout accès aux données personnelles d'une application, modifier les processus en cours d'exécution sur l'appareil qui interagissent avec l'application pour ensuite accéder à ses données, et installer un code malveillant pour exécuter toutes les actions précédentes et plus encore.
2. **Logiciel malveillant.** Via une application malveillante installée sur un appareil, les attaquants peuvent accéder à toutes les applications en cours d'exécution sur un appareil, et notamment aux applications d'entreprise. En rendant ces applications trop permissives ou en utilisant un exploit pour infecter un appareil, ils peuvent accéder à ses données.
3. **Version d'une application légitime contenant un cheval de Troie.** Les attaquants peuvent utiliser la version légitime d'une application disponible sur Google Play ou l'App Store d'Apple, la modifier, puis la transférer sur un app store tiers dont le processus de contrôle des applications est moins rigoureux. Ils peuvent aussi directement envoyer l'application à un client en utilisant la méthode du phishing. Les clients seront alors invités à télécharger une fausse version de l'application qui communiquera identifiants et données à l'attaquant plutôt qu'à l'établissement financier.
4. **Attaque réseau.** Les attaquants peuvent déchiffrer, consulter ou modifier le trafic, notamment les identifiants d'un client, après avoir exploité les vulnérabilités des systèmes de communication chiffré. Ce type d'exploit est connu comme attaque de type man-in-the-middle (MITM).

Les chevaux de Troie bancaires sont actifs sur les appareils des clients

En exploitant les données de notre réseau de capteurs unique composé de plus de 150 millions d'appareils mobiles dans le monde, Lookout a analysé 30 000 appareils mobiles sur lesquels sont installées une ou plusieurs applications bancaires orientées clients. Pendant un an, une étude s'est intéressée à l'historique des menaces mobiles dont ont été victimes ces appareils et a révélé que 10 % des clients de banques mobiles ont été confrontés à une menace ou à un risque mobile.

Figure 1.1 : Menaces auxquelles les clients ont été confrontés

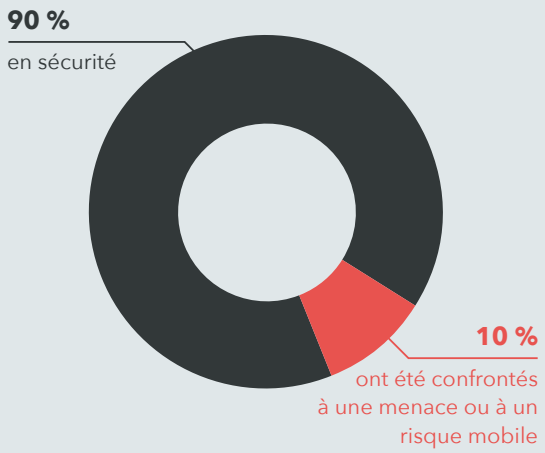
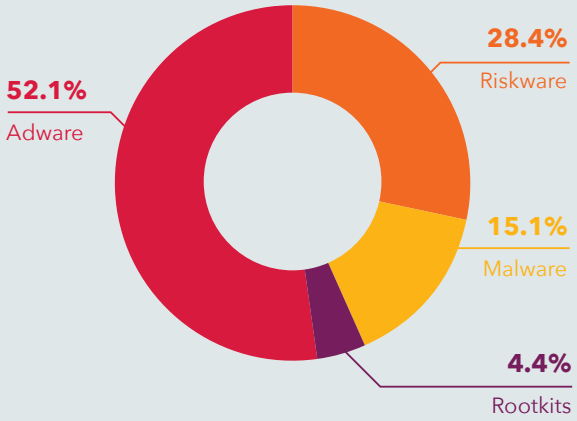


Figure 1.2 : Types de menaces rencontrées



Pendant la réalisation de cette étude, Lookout a détecté des appareils qui ont été été confrontés à un ou plusieurs chevaux de Troie bancaires ciblés, tels que BancaMarStealer, PlayBanker, Shunbad, SvPeng et TauSpy.

Tableau 1 : Chevaux de Troie bancaires détectés

Famille de chevaux de Troie	Description
BancaMarStealer	Voleur d'identifiants de connexion rudimentaire qui recueille des SMS pour intercepter les messages mTAN (Mobile Transaction Authentication Number).
PlayBanker	Cheval de Troie qui génère des notifications push pour inciter la victime à télécharger des versions pirates d'applications bancaires légitimes.
Shunbad	Cheval de Troie qui imite des applications bancaires et dérobe des messages SMS et des données de contact.
SvPeng	Cheval de Troie qui s'exécute en arrière-plan et qui surveille l'utilisation d'applications bancaires légitimes, puis qui superpose un écran de connexion factice pour intercepter les identifiants bancaires d'une victime.
TauSpy	Voleur d'identifiants de connexion rudimentaire qui recueille des SMS pour intercepter les messages mTAN (Mobile Transaction Authentication Number).

Pour réduire proactivement le piratage de comptes, renforcer la confiance des clients et prévenir toute menace mobile, les établissements financiers doivent utiliser une solution leur permettant de protéger leurs applications orientées clients.

Le développement d'applications internes néglige parfois la sécurité

Les développeurs d'applications sont plus concernés par l'expérience utilisateur et l'optimisation des fonctionnalités que par la mise en place de mesures de sécurité permettant de prévenir toute menace mobile. Ils doivent avant tout s'assurer que le code de leur application ne contient aucune vulnérabilité, mais ils ont généralement tendance à négliger la sécurité de l'appareil même.

Toute faille au niveau des identifiants d'un client ou des données va entraîner une succession de problèmes pour les établissements bancaires, notamment des pertes financières pour cause de fraude ou des clients se tournant vers la concurrence, une érosion de l'image de marque due à une mauvaise publicité, et des sanctions financières pour non-respect des réglementations en vigueur.

Une solution de protection pour vos applications sur laquelle vous pouvez compter

Lookout App Defense protège proactivement les applications mobiles des établissements de services financiers sans compromettre les données des applications mobiles orientées clients. Pour cela, il fournit une visibilité totale et une sécurité avancée face au spectre des risques mobiles.

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.

Lookout App Defense exploite toute la puissance de Lookout Security Cloud pour proposer une solution offrant un déploiement intuitif et permettant de protéger les utilisateurs contre le piratage de leurs données lorsqu'ils réalisent des transactions via des applications mobiles.

Lookout App Defense comprend quatre fonctionnalités uniques :

Le réseau mondial d'appareils Lookout. Des millions d'appareils mobiles utilisent Lookout Personal dans plus de 150 pays et Lookout App Defense utilise cette même technologie sous-jacente. Cette énorme empreinte permet à Lookout de bénéficier d'une visibilité anticipée et exclusive sur les menaces mobiles existantes et émergentes. Ce réseau d'appareils permet à Lookout de mieux suivre les acteurs des menaces existantes et d'identifier les menaces Zero Day pour protéger les utilisateurs et minimiser la divulgation de données sensibles.

L'ensemble de données Lookout et la technologie de machine learning (ML). De nombreux fournisseurs de sécurité prétendent utiliser des fonctionnalités de machine learning, or les algorithmes de machine learning ne sont pas la cause du problème, mais bien les données. Sans un ensemble de données suffisamment étendues pour former des modèles ML, une solution sera inefficace à grande échelle. Lookout dispose de l'ensemble de données requis et a implémenté le ML à grande échelle.

Une architecture Cloud-first et d'assistance pour appareils mobiles. Lookout a conçu et optimisé sa plate-forme pour l'environnement mobile. Son approche en matière de sécurité consiste à exploiter le Cloud pour réaliser une analyse approfondie des menaces et implémenter des solutions d'analyse efficaces sur les appareils lors du lancement d'une application.

Un déploiement rapide et fluide. Lookout App Defense a été optimisé pour que le personnel autre que le personnel de sécurité puisse facilement et en quelques minutes déployer le kit de développement logiciel dans les applications orientées clients. Les développeurs d'applications n'ont pas besoin d'être des experts en sécurité pour sécuriser les données et fonctionnalités des applications mobiles orientées clients.