Les données de millions d'utilisateurs menacées par leurs apps mobiles

Une faille dans la façon dont les applications mobiles stockent les informations en ligne menacerait les données personnelles de millions d'utilisateur. C'est ce qu'ont mis en évidence, depuis la fin mai (et que vient de remonter Reuters), une équipe de chercheurs du Fraunhofer Institute for Secure Information Technology (SIT) et de la Darmstadt University of Technology. En fouinant dans les bases de données de Facebook (Parse) et Amazon principalement, les experts en sécurité ont réussi à récolter 56 millions de jeux de données non protégées.

Des données personnelles à foison

Les données recueillies concernent les noms (complets et vérifiés) et adresses email, des adresses postales, des photos familiales et autres enregistrement audiovisuels, mais aussi des mots de passes, les données privées de Facebook (liens relationnels des contacts), des transactions financières, des fichiers de log ou encore des informations propres aux appareils mobiles (numéro de série, nombre d'application installées…). Autant de données précieuses pour leur valeur marchande et leurs potentiels pour l'usurpation d'identité ou la manipulation des utilisateurs par ingénierie sociale. *« Donc, les utilisateurs devraient être attentifs à la confiance qu'ils accordent aux applications qui prennent soin de leurs données »*, déclare le Dr Eric Bodden, responsable du groupe de recherche.

Le problème vient de la façon dont les développeurs stockent les données personnelles des utilisateurs de leurs applications. Afin de pouvoir les synchroniser entre différents appareils ou plates-formes (Android, iOS, Windows…), ils s'appuient sur des serveurs Baas (Backend-as-a-Service) proposées par les fournisseurs de services Cloud. Lesquels se chargent généralement de fournir, via une API, un jeton de sécurité, sous forme d'une clé numérique, pour authentifier la connexion de l'utilisateur à travers l'application utilisée.

Une clé de sécurité à portée de main

Or, il s'avère que l'API d'authentification n'est pas nécessairement intégrée dans les règles de l'art. Sur les 750□000 applications Android et iOS que les chercheurs ont testées, *« une vaste majorité »* se contente d'une méthode d'authentification faible en intégrant en leur sein la clé de sécurité permettant d'accéder aux données des serveurs Baas. *« Comme les chercheurs l'ont montré, il est assez facile d'extraire cette clé pour toute personne ayant une connaissance un peu approfondie du codage d'application mobile »*, note Eric Bodden dans la FAQ dédiée à la découverte de la faille.

Les chercheurs se gardent de publier la liste des applications mal sécurisées. Et ont évidemment alerté les fournisseurs de services Cloud d'un côté, et les autorités allemandes de l'autre (le German Federal Office for Information Security, en l'occurrence). *« Avec l'aide d'Amazon et Facebook, nous avons également informé les développeurs des applications concernées et ce sont vraiment eux qui doivent prendre les mesures adéquates parce qu'ils ont sous-estimé le danger »*, ajoute Eric Bodden. La balle est en effet

dans leur camp. Ce qui n'interdit pas l'utilisateur de regarder à deux fois ce qu'il décide de mettre, ou pas, dans le Cloud.

Lire également
Sécurité des données et Chief Digital Officer dans le top des jobs en or
5 règles de base pour sécuriser les appareils mobiles
Enquête : Le paiement mobile NFC sécurisé, vraiment ?

crédit photo : Anan Chincho – shutterstock