Les mots de passe d'apps mobiles vulnérables à la force brute

La société AppBug a réalisé un test sur 100 applications sous iOS et Android disposant d'au moins 1 million de téléchargements. Elle a utilisé une technique de piratage, **la force brute**, pour obtenir le mot de passe du compte utilisateur des applications. La méthode est simple, tester indéfiniment des mots de passe pour trouver le bon. D'habitude les applications mettent en place un nombre limité d'essais, mais sur les 100 programmes testés, **53 ne fixent pas de limites**. L'ensemble de ces apps représente **600 millions de téléchargements**.

La société AppBug a fait part de ces problèmes aux développeurs et aux sociétés éditrices en leur laissant 90 jours pour résoudre cette erreur. La plupart d'entre elles ont réalisé des modifications. Mais, la start-up a publié la liste d'une douzaine d'apps pour qui le bug n'a pas été corrigé. Parmi les applications, on retrouve : **Wunderlist : to do list & tasks, WatchESPN, Expedia Hotels & Flights, CNN, Autocad 360, SoundCloud, Kobo ou Walmart**. Du beau monde qui affiche 300 millions de téléchargements et donc autant de comptes utilisateurs exposés.

La question de la limitation des essais s'est posée notamment avec le piratage d'iCloud d'Apple. Plusieurs célébrités avaient vu leurs comptes hackés et les contenus diffusés sur Internet. Après cette affaire, Apple avait instauré une limitation des tentatives pour se connecter au service. Mais l'expérience d'Apple n'a semble-t-il pas fait tâche d'huile sur les éditeurs et les développeurs d'applications mobiles. Une autre réponse peut se trouver dans la mise en place d'une authentification à double facteur.

A lire aussi :

Un mot de passe sur deux peut être craqué en 24 heures
Les ondes cérébrales pour remplacer les mots de passe ?

Crédit Photo : BrianAJackson-Shutterstock