La double authentification affaiblie par la synchronisation

Des chercheurs de l'Université libre d'Amsterdam (Vrije Universiteit Amsterdam, VU) on démontré que la synchronisation multiplateforme peut miner la double authentification d'utilisateurs de téléphones mobiles sous Android et iOS. Et ce en partant du postulat que l'ordinateur utilisé pour la synchronisation est exposé à une attaque MitB (*man-in-the-browser*, ou homme dans le navigateur).

Contourner la chaîne d'authentification

Pour la première attaque, indiquent les chercheurs dans leur analyse, la fonction d'installation à distance d'applications de Google Play a été utilisée depuis un PC. Une application malveillante spécifique a été installée sur le smartphone Android ciblé, puis l'application a été activée. Celle-ci peut alors intercepter le mot de passe à usage unique et l'envoyer sous forme de SMS à un serveur contrôlé par l'attaquant. Il peut alors contourner la chaîne d'authentification à deux facteurs proposée par le site ou le service en ligne concerné, bancaire inclus.

De même pour l'attaque contre iOS, une application douteuse a été publiée et installée à partir d'un ordinateur compromis depuis l'App Store d'Apple, via la fonction d'installation à distance d'iTunes. Ensuite, l'application a été installée sur un iPhone. Une telle application peut être utilisée pour lire des SMS. Cette attaque exploite une fonction de continuité d'OS X qui permet de synchroniser des SMS entre un Mac et un iPhone. Là encore la double authentification est mise à mal.

Ces vulnérabilités nommées « *2FA synchronization vulnerabilities* » par les scientifiques, ont été communiquées à Google et Apple entre l'été et l'automne 2015. Pour les chercheurs, *« les fournisseurs devraient être extrêmement prudents avant d'opter pour l'activation par défaut ou en option de nouvelles fonctionnalités de synchronisation, et informer leurs utiliseurs des risques liés à cette utilisation »*.

Lire aussi :

Protection des données : l'ambivalence perdure après Snowden

crédit photo © wk1003mike-Shutterstock