La sécurité de iOS compromise lors des connexions à un PC

iOS, l'OS mobile des iPhone et iPad, est réputé être plutôt bien sécurisé, grà¢ce à son **bon niveau d'isolation** et au **travail d'Apple pour éviter la présence de malwares** sur l'App Store. Mais, selon une équipe de chercheurs du Georgia Institute of Technology, cette barrière de défense peut être contournée lorsqu'un terminal iOS est connecté via USB à un PC infecté (qu'il soit sous Windows ou OS X). Déjà à l'origine avec son équipe d'une compromission de l'iPhone via une app infectieuse qui avait brièvement échappé à la vigilance d'Apple l'an dernier, Tielei Wang revient avec **une méthode ne reposant plus directement sur le téléchargement d'une app infectée**, mais sur la connexion par USB d'un iPhone à un ordinateur infecté.

La démarche de Wang et des autres chercheurs de Georgia Tech consiste à tromper l'iPhone ou l'iPad connecté pour l'autoriser à télécharger une application malveillante à l'insu de l'utilisateur. Cette attaque, de type Man-in-the-Middle, **contourne l'App Store** en utilisant les certificats autorisés par Apple pour permettre à des entreprises de créer leurs propres circuits de distribution d'apps (donc à signer ces dernières). « *Infecter un grand nombre de terminaux iOS via des botnets est possible* », assurent les auteurs. Selon une analyse de ces derniers sur plus de 500 000 adresses IP de PC zombies, 23 % d'entre eux sont parfois connectés à des appareils iOS.

Cookies en libre service

Selon Tielei Wang, **Apple a été prévenu** de l'existence de cette faille en 2013 et a apporté certaines modifications à son process. Avec notamment l'apparition d'un message avertissant l'utilisateur des risques lors de la première connexion à un PC spécifique.

L'équipe de Tielei Wang a également mis au jour une autre faiblesse, toujours lors de connexions via USB à des ordinateurs. En plus d'iTunes, le PC a alors également accès au périphérique iOS via un protocole baptisé **Apple File Connection**. Or, via ce dernier, les chercheurs sont parvenus à **récupérer des cookies https**, renfermant les informations de connexion des utilisateurs. Notamment ceux de Facebook ou Gmail. « *Nous pensons qu'Apple a trop fait confiance aux connexions USB* », a expliqué Tielei Wang à nos confrères de CIO.com.

A lire aussi :

Android grignote la mainmise d'iOS en entreprise

iOS 7 faillible sur les pièces jointes et Siri