Des chercheurs brisent le chiffrement d'iMessage d'Apple

Difficilement exploitable et colmatée par Apple en amont de la sortie de iOS 9.3, une vulnérabilité dans le chiffrement du système offrait la possibilité à des hackers aguerris d'intercepter et de déchiffrer des photos et vidéos envoyées via iMessage, révèle le *Washington Post* ce lundi.

La firme de Cupertino aurait été alertée dès 2015 par le professeur Matthew D. Green, qui avait étudié de près un guide de sécurité d'iOS. Il jugeait fragile la procédure utilisée pour le chiffrement et suspectait la présence d'une faille dans l'application de messagerie d'Apple. Quelques mois après ce constat, le système restait vulnérable, à ses yeux.

Clone et force brute

Pour le démontrer, le professeur et des étudiants de l'université américaine Johns Hopkins auraient utilisé des iPhone équipés d'une version antérieure à iOS 9 et mis au point une technique permettant d'extraire des fichiers transmis en utilisant iMessage. La communication ciblée contenait un lien vers une photo stockée dans les serveurs iCloud d'Apple, ainsi qu'une clé pour déchiffrer cette photo.

Les chercheurs auraient créé un logiciel qui imite un serveur Apple, puis mené une attaque par force brute (test de toutes les combinaisons possibles) pour trouver la clé et récupérer la photo sur les serveurs de la firme. Un projet long et chronophage, mais concluant, selon Matthew Green. D'après lui, une technique similaire pouvait être utilisée avec des versions plus récentes d'iOS, mais une telle opération nécessiterait les ressources d'un État puissant…

iOS 9.3 épargné ?

Les chercheurs de l'université Johns Hopkins ont fait savoir que des détails techniques seraient rendus publics, mais pas avant la sortie d'iOS 9.3. Apple, de son côté, a indiqué avoir partiellement colmaté la faille dès l'automne dernier, et qu'elle le serait totalement avec les améliorations de sécurité incluses dans la nouvelle version de son OS mobile lancée ce lundi 21 mars.

La vulnérabilité découverte par les chercheurs démontre, selon eux, qu'exiger d'Apple de casser la sécurité de l'iPhone pour permettre aux autorités fédérales américaines d'accéder aux données de criminels et suspects, n'est pas pertinent, alors qu'il existe des failles dans le chiffrement. Mais le FBI, qui s'oppose à Apple dans l'affaire de San Bernardino, estime qu'exploiter les failles de logiciels n'est pas la solution au meilleur rapport coût-efficacité pour accéder aux données de terminaux dans un cadre légal.

Lire aussi :

Contre le FBI, les experts en chiffrement soutiennent (presque tous) Apple

iMessage et FaceTime passent à l’authentification à deux facteurs

La confidentialité d’iMessage mise en cause par les Français de Quarkslab

crédit photo © tsyhun / Shutterstock.com