600 millions d'iPhone affectés par des backdoors ?

Un chercheur en sécurité aurait découvert des backdoors installées dans iOS par… Apple. **Jonathan Zdziarski** a exposé sa découverte à l'occasion de la conférence Hackers On Planet Earth (HOPE/X) qui s'est déroulée à New York du 18 au 20 juillet derniers. Selon lui, pas moins de **600 millions de terminaux iPhone et iPad sont affectés** par ces portes dérobées.

Lesquelles permettent à Apple *« d'accéder aux données du terminal de l'utilisateur dans le cadre de l'application de la loi »* comme on peut le lire sur la diapo 6 des 58 (en PDF) qui illustrent son intervention. Autrement dit, **Apple s'est donné les moyens d'accéder aux données de ses clients** et les mettre, au besoin, à disposition des autorités américaines comme le stipule la firme de Cupertino dans ses lignes directrices d'application de la loi américaine.

Accès à quasiment toutes les données

A la décharge d'Apple, l'expert en sécurité reconnaît que le constructeur *« a tout mis en œuvre pour rendre les terminaux iOS raisonnablement sécurisés face aux attaquants classiques »* et que *« **l'iPhone 5 et iOS 7 sont plus protégés de tout le monde sauf d'Apple et du gouvernement** »*. L'homme est bien placé pour le savoir. Auteur de plusieurs ouvrages sur la sécurité d'iOS, dont *Hacking and securing iOS applications*, il a également participé aux développements des premiers *jailbreaks*, ces outils qui permettent de déverrouiller l'accès aux droits d'administration des terminaux mobiles estampillés de la pomme. Il est également connu comme le hacker NeverGas dans la communauté de développeurs iOS.

A quelles données Apple a-t-il accès par défaut à tous les appareils équipés d'iOS 4 et les versions suivantes ? A **tous les fichiers produits par l'utilisateur** (qui ne sont pas chiffrés par le système comme ils devraient l'être), du moins tant que l'appareil est allumé, y compris en veille. Autrement dit, SMS, photos, vidéos, contacts, enregistrements audio et historiques des appels sont accessibles. *« Votre appareil est presque toujours disposé à fournir toutes les données, car il est presque toujours authentifiée, même s'il est verrouillé »*, indique le chercheur. En revanche, Apple n'a pas accès aux emails, agenda et autres données intégrées dans les applications tierces, selon Jonathan Zdziarski.

Une violation de la confiance de l'utilisateur

Apple s'est donc visiblement arrangé pour accéder aux données de ses clients, à leur insu, afin de pouvoir répondre aux exigences des autorités de sécurité. Ce qui a probablement **facilité le travail de la NSA** d'installer ses propres outils d'espionnage sur les terminaux iOS, comme l'avait rapporté *Der Spiegel* en début d'année, sur la base des documents exfiltrés par le lanceur d'alerte Edward Snowden. De plus, un certain nombre de prestataires spécialisés dans l'accès aux données des terminaux à des fins judiciaires sont capables d'exploiter les backdoors d'Apple pour proposer leurs propres services. Et Jonathan Zdziarski de citer Cellebrite, AccessData (Mobile Phone Examiner) ou

encore Elcomsoft parmi ceux-là.

Il n'en reste pas moins que Jonathan Zdziarski voit dans la stratégie d'Apple « ***une violation de la confiance de l'utilisateur*** *et sa vie privée [et qu'il] n'y a aucune excuse pour faire fuir des données personnelles ou autoriser la surveillance des paquets sans que l'utilisateur en soit informé et qu'il donne son consentement* ». En conclusion, *« la sécurité renforcée d'iOS a été compromise… par Apple… dans sa conception »*.

En réponse à cette présentation, Apple a démenti les allégations de Jonathan Zsziarski, dans un communiqué. «
Nous avons conçu iOS pour que ses fonctions de diagnostic ne compromettent pas la vie privée ni la sécurité de l'utilisateur, mais fournissent tout de même les informations nécessaires aux départements informatiques des entreprises, aux développeurs ainsi qu'à Apple afin d'être en mesure de résoudre les problèmes techniques. Un utilisateur doit déverrouiller son appareil et accepter de faire confiance à un nouvel ordinateur avant que celui-ci ne puisse accéder à ces données de diagnostic. L'utilisateur doit accepter de partager ces informations, et les données ne dont jamais transférées sans son consentement ». La firme rappelle par ailleurs qu'elle *« n'a jamais travaillé avec une agence gouvernementale de quelque pays que ce soit pour créer une porte dérobée dans nos produits ou services*. **»**

Lire également
Faille de sécurité béante sur iPhone
La NSA, éditeur de spywares pour téléphones mobiles