Peur d’être surveillés ? mettez à jour votre iPhone

Peur d’être surveillés ? mettez à jour votre iPhone

Apple corrige en urgence iOS, touché par trois failles sévères. Ces dernières étaient exploitées de concert par un spyware de haut vol, Pegasus, vendu par la société israélienne NSO à des gouvernements.

La mésaventure qui vient d'arriver à Apple, obligé de déployer en urgence un correctif pour son OS mobile iOS, ne manquera pas d'alimenter le débat sur l'utilisation des vulnérabilités logicielles par les gouvernements. Et sur le bien-fondé de l'activité de très discrètes petites sociétés spécialisées dans la vente de failles zero day. Avec sa version 9.3.5 d'iOS, la firme de Cupertino vient en effet combler 3 vulnérabilités sévères exploitées probablement depuis des années pour dérober des informations sur les terminaux de la marque.

Selon les chercheurs en sécurité de Lookout, société spécialisée dans la sécurité des terminaux mobiles, et du Citizen Lab, une émanation de l'université de Toronto (Canada), ces failles étaient exploitées conjointement par un logiciel espion. Cette menace, que les chercheurs ont appelée Pegasus, aurait été développé par NSO Group, société basée en Israël et passée, en 2014, sous le contrôle de Francisco Partners Management, un fonds d'investissement américain, pour 120 millions de dollars. L'enquête des chercheurs a pu déterminer que Pegasus a été utilisé pour espionner un dissident aux Emirats Arabes Unis, Ahmed Mansoor. Au-delà de ce cas particulier, le spyware pourrait avoir été utilisé par d'autres gouvernements ou entreprises afin d'espionner des dissidents, des journalistes, des concurrents, des partenaires… Le kit d'attaque est vendu environ 8 millions de dollars pour 300 licences. Cher mais pas hors de portée d'un Etat ou d'une grande entreprise.

NSO : un discret et lucratif business

En novembre dernier, un article de *Reuters* se penchait sur l'activité de la très secrète société NSO, spécialisée dans l'assistance technique aux gouvernements pour l'espionnage de terminaux mobiles. Une société qui a plusieurs fois changé de nom et que Francisco Partners espérait revendre pas moins d'un milliard de dollars. Selon *Reuters*, la société israélienne, fondée en 2010 par Omri Lavie et Shalev Hulio, afficherait 75 M$ de bénéfices opérationnels par an.

Les fonctions de Pegasus. Une image qui serait issue de la documentation de NSO et ui a fuité lors du piratage de Hacking Team.

L'analyse du code semble faire remonter Pegasus à 2013, l'année de la sortie d'iOS 7 ; le malware renfermant des réglages adaptés à cette version de l'OS de Cupertino. « *Pegasus est l'attaque la plus sophistiquée ciblant un terminal que nous ayons jamais rencontrée parce qu'elle exploite la façon dont les terminaux mobiles s'intègrent dans nos vies et tire parti de la combinaison de fonctionnalités présente uniquement sur les mobiles : connexion permanente (WiFi, 3G/4G), communications vocales, caméra, e-mail, messages, GPS, mots de passe et liste de contacts* », écrivent les chercheurs de Lookout et de l'université de Toronto. Modulaire et exploitant le chiffrement pour éviter d'être repéré, Pegasus déroule une séquence d'attaque classique : envoi d'un message texte, ouverture d'un navigateur, chargement d'une page contrefaite (la Croix Rouge, le service de visa britannique, des médias, des sites d'entreprises IT…), exploitation des trois vulnérabilités et installation de codes permettant une surveillance de la cible (avec récupération de données tous azimuts, y compris des données de localisation, l'activation du micro ou de la caméra à distance, selon la documentation de NSO Group !).

Ahmed Mansoor : cible à répétition

C'est la prudence d'Ahmed Mansoor qui a permis la mise au jour de Pegasus : le 10 août, le dissident reçoit un message sur son iPhone accompagné d'un lien lui promettant d'en savoir plus sur les tortures dans les prisons de son pays. Plutôt que de cliquer, Mansoor fait suivre ce message à un chercheur du Citizen Lab, un laboratoire travaillant sur les sujets à la croisée des droits de l'homme et de la cybersécurité. Selon ce labo, c'est la troisième fois qu'Ahmed Mansoor est la cible d'un spyware (après d'autres attaques menées avec des outils conçus par le Britannique Gamma Group en 2011 et par l'Italien Hacking Team en 2012).

Selon les chercheurs du Citizen Lab et de Lookout, Pegasus serait « *hautement configurable* » afin de s'adapter aux spécificités de chaque cible et à l'épaisseur du porte-feuille des 'clients' de NSO. « *En fonction du pays concerné et des fonctions achetées par les utilisateurs, les capacités du spyware peuvent inclure les messages, les appels, les e-mails, les logs et d'autres données issues d'apps comme Gmail, Skype, WhatApp, Viber, FaceTime, Calendar, Line, Mail.ru, WeChat, Tango et d'autres* », écrivent les chercheurs, qui précise que le malware semble en mesure de résister à une montée de version de l'OS (sauf évidemment celle vers iOS 9.3.5) et se montre capable de se mettre à jour pour remplacer des parties de code devenues inopérantes. Selon les premières recherches du Citizen Lab, Pegasus a aussi servi à espionner un journaliste mexicain, travaillant sur la corruption dans son pays, et une personne non identifiée au Kenya.

iOS hyper-sécurisé ? Voire

Au passage, la sécurité légendaire des iPhone est passablement égratignée. Les trois failles, baptisées Trident par les chercheurs de Lookout et du Citizen Lab, montrent que le système d'Apple n'est pas hors de portée des hackers de haut vol. L'installation de Pegasus repose sur l'exploitation d'une vulnérabilité de Safari (corruption de mémoire avec CVE-2016-4655) et de deux failles du noyau d'iOS (CVE-2016-4656 & CVE-2016-4657), détaillent Lookout dans un rapport (PDF).

Rappelons que l'image de l'OS des iPhone et iPad avait bénéficié de la bataille qui avait opposé Apple au FBI concernant une demande de déblocage d'un smartphone frappé de la pomme ayant appartenu à un des auteurs de la tuerie de San Bernardino, aux Etats-Unis. Idem avec le bug bounty lancé l'année dernière par la société Zerodium, un autre de ces prestataires vendant des failles zero day au plus offrant, qui offrait alors un million de dollars pour un code d'exploitation permettant de prendre le contrôle total d'un iPhone. Rappelons que, de son côté, Apple va lancer son propre programme de chasse aux bugs, mais n'offrira au maximum que 200 000 $ de récompense. Vu les tarifs pratiqués par NSO Group et autres sociétés vendeuses de zero day, pas sûr que ce maigre pactole suffise…

Article original de Reynald Fléchaux

Sans information sur l'existence de dysfonctionnements consécutifs à l'installation de IOS 9.3.5 lors de l'écriture de ces lignes, Denis JACOPINI vous recommande fortement l'installation de cette mise à jour si votre téléphone en a les capacités.

Réagissez à cet article

Original de l'article mis en page : Trois failles zero day d'iOS servaient à espionner des dissidents