Wirelurker, Masque : la sécurité d'iOS ébranlée ?

Coup sur coup, le système d'exploitation des terminaux mobiles d'Apple a été secoué par deux affaires affectant sa sécurité. La première se nomme **Wirelurker**. Il s'agit du nom d'un malware découvert par les équipes de Palo Alto Networks qui vise les terminaux iOS **via la connexion USB avec Mac OS X** en installant des applications tierces malveillantes. Si cette menace reste limitée à la Chine et se révèle réellement virulente sur les seuls terminaux jailbreakés (avec le vol de données sensibles comme des informations bancaires, identifiants, etc), les cybercriminels ont trouvé un moyen de percer la muraille d'iOS, y compris sur des terminaux non débloqués. Et les experts estiment que ce malware a encore une marge de progression.

A quelques heures d'intervalle, une autre attaque a été détaillée par la société Fire Eye. Baptisée **Masque**, cette technique permet l'**installation de logiciels malveillants** déguisés en programmes légitimes et capables de remplacer des applications déjà présentes sur l'appareil. Masque peut fonctionner sans ordinateur, ni connexion filaire. Il suffit d'un simple lien hypertexte pour déclencher le téléchargement d'une application malicieuse. Afin de tromper l'utilisateur et le pousser à valider l'installation, les pirates reprennent au détail près l'interface d'une application légitime (dans le cas présent, une fausse application Gmail). La **faiblesse d'iOS se trouve dans la gestion des certificats de conformité**. Ces derniers ne sont pas vérifiés lors de l'installation d'une application qui dispose du même identifiant (de type '.com.google.Gmail') qu'un logiciel déjà installé.

Des prémisses et des correctifs

Ce n'est pas la première fois que l'OS mobile d'Apple fait face à des critiques en matière de sécurité. En août dernier, des chercheurs du Georgia Institute of Technology montraient déjà la faisabilité d'une **attaque via la connexion USB** entre un iPhone et un ordinateur compromis. 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). En juillet dernier, c'est un expert en sécurité, Jonathan Zdiarski qui lançait une petite bombe en expliquant avoir trouvé, dans iOS, des backdoors installées par Apple. Selon lui, pas moins de 600 millions de terminaux iPhone et iPad étaient affectés par ces portes dérobées. Ces dernières ont probablement facilité le travail de la NSA pour installer ses propres outils d'espionnage sur les terminaux iOS.

Face à ces différentes affaires de sécurité, la communication d'Apple reste sereine. Elle se traduit notamment par **l'intégration de correctifs** lors des mises à jour d'iOS. La dernière mouture 8.1.1 n'échappe pas à cette règle en corrigeant la faille utilisée par le malware Wirelurker. Sur la partie surveillance gouvernementale, la firme de Cupertino s'est attirée les foudres du FBI en annonçant la mise en place d'un chiffrement des données par défaut des contenus des terminaux iOS. Une

annonce qualifiée de poudre aux yeux par certains spécialistes. Wirelurker et Masque sont finalement deux rappels à l'ordre pour Apple en matière de sécurité, surtout à un moment où la firme mène une offensive importante, avec l'appui d'IBM, pour promouvoir ses terminaux et ses applications en entreprise.

A lire aussi

Apple, champion de l'innovation depuis 10 ans
La puce A8X de l'iPad Air 2 d'Apple dévoile ses secrets
PHP, .Net, Java, iOS, Big Data : le salaire des développeurs en 2014 (Infographie)
Mobilité en entreprise : pourquoi iOS 8 gagne du terrain sur la concurrence (avis d'expert)

Crédit Photo: Denys Prykhodov-Shutterstock