Alerte : 6 millions d’iPhones victimes d’un Trojan qui exploite un bogue du DRM ?

Alerte : 6 millions d’iPhones victimes d’un Trojan qui exploite un bogue du DRM ?

D’après Palo Alto Networks, un nouveau malware baptisé AceDeceiver, a déjà infecté près de 6 millions d’appareils iOS non jailbreakés appartenant à des utilisateurs Chinois.

Comme ont pu le constater les chercheurs, ce trojan infecte les appareils mobiles via des ordinateurs Windows et exploite des erreurs commises par Apple dans le système de gestion des droits numériques (DRM). A l’heure actuelle, AceDeceiver circule uniquement sur le territoire chinois ; d’après Palo Alto, il s’agirait du premier malware capable d’infecter les gadgets d’Apple qui utilisent le système imparfait DRM FairPlay. Et il n’est pas nécessaire que l’appareil soit débridé pour garantir l’infection.

« D’abord, il y a eu XcodeGhost, puis ZergHelper, et maintenant AceDeceiver » a rappellé Ryan Olson, directeur des études sur les virus chez Palo Alto, alors qu’il commentait la dernière découverte aux journalistes de Threatpost. « Ils contribuent tous à l’érosion continue de la protection du magasin d’applications d’Apple ». D’après l’expert, AceDeceiver permet d’obtenir un accès « homme au milieu » à l’appareil iOS et de forcer l’utilisateur à communiquer son identifiant Apple aux attaquants.

Ce nouveau malware iOS se distingue de ses prédécesseurs par le fait qu’il n’utilise pas de certificats légitimes Apple pour s’introduire dans un appareil non débridé. Il opte pour la technique FairPlay Man-In-The-Middle, utilisée déjà depuis deux ans pour diffuser des applications pirates. D’après les conclusions de Palo Alto, le trojan AceDeceiver est le premier cas où ce genre de modification est utilisé pour installer des malwares sous iOS à l’insu de l’utilisateur.

L’analyse a démontré que les auteurs d’AceDeceiver ont préparé cette campagne malveillante pendant de nombreux mois. Au deuxième semestre de l’année dernière, ils ont réussi à introduire dans l’App Store trois versions différentes de l’application AceDeceiver avec une fonction d’économiseur d’écran. Cette opération s’imposait afin d’obtenir les codes d’autorisation d’Apple sollicités via iTunes. Par la suite, les individus malintentionnés ont exploité ces codes avec l’application Windows Aisi Helper spécialement développée à cette fin pour procéder à l’installation des malwares sur les appareils mobiles à l’insu de l’utilisateur.

Aisi Helper est vendu uniquement en Chine et se présente comme un outil pour iOS qui permet de créer des copies de sauvegarde, de restaurer le système, de débrider les appareils, d’administrer l’appareil et de le purger. Toutefois, dans ce cas l’existance d’un client de ce genre sur le poste de travail Windows simplifie également la tâche de l’attaquant car le malware peut être installé sur les appareils iOS lorsque ceux-ci sont connectés à l’ordinateur. AceDeceive réalise l’installation en substituant la poigné de main FairFlay par son propre serveur d’autorisation. Il s’agit d’une attaque FairPlay Man-In-The-Middle, appliquée pour la première fois en 2014.

AceDeceiver a été porté à l’attention d’Apple le mois dernier et la société a déjà retiré les trois faux économiseurs d’écran de son magasin d’applications. Palo Alto indique toutefois que l’attaque est toujours possible. « Tant que les attaquants disposent du code d’autorisation, ils ne doivent pas obligatoirement accéder à l’App Store pour diffuser ses applications » expliquent les chercheurs dans leur blog. Ryan Olson, de son côté, a confirmé aux journalistes que de telles utilisationsdétournées étaient possibles car les résultats de l’analyse réalisée par le mécanisme DRM d’Apple sont valides en dehors de l’écosystème iTunes.

Une fois installé sur un appareil iOS, AceDeceiver peut fonctionner comme un magasin d’applications alternatifs. Il fonctionne sous le contrôle des individus malintentionnés et offre un large choix de jeux et d’utilitaires. L’utilisateur est également invité à saisir son identifiant Apple et son mot de passe pour pouvoir accéder à toutes les fonctions de l’application pirate gratuite.

Ryan Olso explique qu’il est difficile d’éliminer les problèmes provoqués par AceDeceiver. Dans le cas de ZergHelper cité ci-dessus, Apple avait simplement supprimé le malware de son magasin. Le nouveau trojan se distingue par le fait qu’il compte sur un client Windows et utilise un code d’autorisation obtenu antérieurement, ainsi que des lacunes dans le projet FairPlay DRM.

Au moment de la publication de ce billet, Apple n’avait pas encore réagi aux questions de Threatpost…. [Lire la suite]

Réagissez à cet article

Source : *Un Trojan Exploite Un Bogue Du DRM Pour Charger Des Malwares Dans IOS – Securelist*