Comment contourner un iPad verrouillé dans iCloud ?

C'est pour se sortir d'un mauvais pas qu'un chercheur en sécurité indien a trouvé comment contourner l'écran de verrouillage d'un iPad. Comme il l'explique, la tablette qu'il venait d'acheter sur eBay avait été verrouillée par le précédent utilisateur avec la fonction Localiser mon iPhone (Find My iPhone). Laquelle exige de saisir l'identifiant et le mot de passe enregistré dans iCloud pour débloquer l'appareil à son démarrage. Une mesure de sécurité qui prévient les risques d'accès au contenu du terminal lorsque celui-ci est perdu ou volé.

Planter le verrou d'iCloud

Hermanth Joseph, expert en sécurité pour Slash Secure, n'explique pas s'il a tenté ou non de contacter le vendeur pour qu'il désactive de son côté le verrouillage (ce qui laisse penser qu'il s'agissait d'un appareil volé) et a préféré trouver un moyen de contourner les mesures de sécurité d'iOS, en version 10.1 dans le cas présent. *« Le verrou d'iCloud est une couche logiciel de sorte que si je peux le planter, il m'ouvrira l'écran d'accueil*, reporte-t-il sur son blog. *Alors, comment je peux le planter ? »*

Pour y parvenir, le chercheur habitué à remonter des vulnérabilités critiques auprès de Google, Microsoft, Yahoo ou encore Twitter, a choisi de se connecter à partir d'un nouveau réseau Wifi que celui choisi initialement lors du démarrage de la machine pour se connecter à iCloud. Il a ensuite sélectionné le mode WPA2 Enterprise comme protocole de chiffrement. Ce qui ouvre la saisie sans limite de caractères dans les champs nom, utilisateur et mot de passe qui s'affichent alors. *« Parfait pour créer un débordement de mémoire tampon »*, s'est réjouit l'expert en sécurité.

La Smart Cover déverrouilleur

Il s'est donc entêté à saturer la saisie des champs jusqu'à ce que l'iPad se bloque. A partir de là (et après plusieurs tentatives de redémarrage), il a utilisé le Smart Cover pour mettre en veille la tablette. Après 25 secondes d'attente, la tentative de connexion Wifi s'est éteinte avec pour résultat d'afficher l'écran d'accueil du système sans demander les identifiants de déverrouillage enregistrés dans Find My iPhone. Ou comment Hermanth Joseph a contourné la sécurité d'iOS.

Le chercheur précise avoir signalé la vulnérabilité à Apple le 4 novembre dernier. Après avoir demandé des éléments de démonstration supplémentaires, la firme de Cupertino a déclaré qu'elle apportera les correctifs nécessaires si elle considère la trouvaille du chercheur comme une véritable faille. Laquelle serait toujours présente sur iOS 10.1.1 selon la démonstration en vidéo qu'a faite Benjamin Kunz Mejri, chercheur allemand pour Vulnerability Lab de son état. Ce qui devrait d'autant plus pousser Apple à corriger au plus vite une vulnérabilité désormais publique.

Lire également

[iOS et OS X, un piratage par de simples images]
[iOS 10 réduit l'autonomie des iPhone à néant]
[Fuites de données : les apps iOS plus percées que celles d'Android]

crédit photo © www.BillionPhotos.com – shutterstock