Cellebrite, le hacker d'iPhone se fait pirater

Il y a un air de Hacking Team qui flotte sur Cellebrite. Comme son homologue italien, la société israélienne spécialisée dans le hacking des terminaux mobiles s'est fait pirater des données. Le site *Motherboard* rapporte avoir obtenu 900 Go de données liées à Cellebrite comprenant des informations sur les clients, des bases de données et plusieurs documents techniques des solutions de la firme.

Ces données sont issues en partie de serveurs liés au site web de Cellebrite. Le cache comprend des noms d'utilisateurs et des mots de passe pour se connecter aux bases de données de Cellebrite liées au nom de domaine my.cellebrite. Cette partie du site est utilisée par les clients pour notamment accéder aux nouvelles versions des logiciels. Les adresses mail ont été vérifiées par *Motherboard* en essayant de créer des comptes sur le portail client de Cellebrite. Dans la majorité des cas, les mails étaient déjà utilisés.

De même, l'archive intègre des fichiers contenant des preuves suites à des saisies de téléphones. Pour mémoire, Cellebrite est connue pour son produit phare, un *universal forensic extraction device* (UFED), un outil vendu à la police et aux gouvernements qui permet aux enquêteurs d'extraire les données d'un grand nombre de téléphones portables. La société avait été mise en lumière lors de l'affaire du déblocage de l'iPhone 5C d'un des tueurs de San Bernardino.

Intrusion sur un serveur externe

Face à cette annonce, Cellebrite a reconnu avoir eu « *récemment un accès non autorisé à un serveur web externe* ». Et d'ajouter dans un communiqué que « *une enquête est menée pour déterminer l'étendue du vol. Le serveur concerné comprenait une sauvegarde de la base de données de my.cellebrite, le système de gestion des licences des clients de la société. Il y a quelques temps, la société a migré sur un nouveau système de compte utilisateur. Aujourd'hui, on sait que les informations accessibles étaient des données basiques de contacts d'utilisateurs souhaitant recevoir des alertes sur les produits Cellebrite et des mots de passe hachés de clients qui n'avaient pas basculé sur le nouveau système* ». La firme israélienne conseille aux clients de changer leur mot de passe.

Le ou les pirates revendiquant ce vol de données ont expliqué à *Motherboard* que leurs motivations étaient politiques, en accusant le renforcement des lois sur la surveillance.

A lire aussi :

Déblocage de l'iPhone : le FBI a payé des hackers

Le FBI se transforme en casseur d'iPhone

crédit photo © andriano.cz – shutterstock