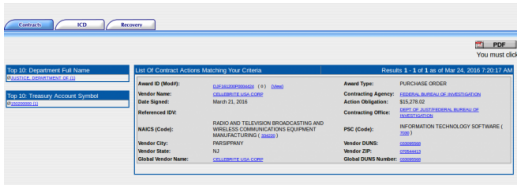
iPhone chiffré : une boîte israélienne à la rescousse du FBI ?



iPhone chiffré : une boîte israélienne à la rescousse du FBI ?

Lundi 21 mars, le FBI a pris tout le monde de court en annonçant avoir trouvé une solution pour accéder aux données stockées sur l'iPhone chiffré de l'un des co-auteurs de la tuerie de San Bernardino, Syed Farook.
Après avoir aboyé partout que seul Apple pouvait débloquer la situation, l'administration américaine a en effet affirmé avoir reçu l'aide d'un mystérieux « tiers », annulant ainsi une confrontation prévue le lendemain même devant une cour de Californie.
En attendant le compte-rendu de cette méthode, que la justice attend d'ici le 5 avril, la presse spécialisée spécule sur l'identité de l'auxiliaire-mystère. Et avance un nom : Cellebrite.

Maître du « digital forensics »

Pour Yedioth Ahronoth (en hébreu), qui cite des sources anonymes, cela ne fait même aucun doute : c'est bien cette boîte israélienne qui a aidé le FBI.
Vidéo promotionnelle d'une solution de Cellebrite, permettant de débloquer un iPhone
Si les deux intéressés se sont refusés à tout commentaire, les spécialistes de l'informatique et du renseignement estiment l'information probable.
Il faut dire que cette firme, établie depuis 1999, est l'une des rares à maîtriser l'art du « digital forensic » dans la téléphonie mobile et le GPS.
Soit la dissection des appareils numériques, dans le cadre notamment d'enquêtes.
Le chercheur David Billard, sollicité en tant qu'expert dans des affaires de ce genre et rattaché à la cour d'appel de Chambéry, détaille :
« Le digital forensic consiste à récupérer les preuves, ou éléments de preuve, dans des appareils numériques. […]
Par exemple, extraire des vidéos d'un ordinateur dans le cadre d'une enquête sur un viol, retrouver des SMS effacés d'un téléphone portable dans le but de confirmer, ou infirmer, une complicité, etc… »

Analyse des appareils brûlés, écrasés, chiffrés…

*Or en la matière, l'inventaire de Cellebrite est fourni. **Promet de venir à bout** de matériel protégé par un mot de passe, « écrasé, cassé, brûlé ou endommagé par l'eau ». Et, plus intéressant en l'espèce :*
« d'analyser des formats d'application de données et des méthodes de chiffrement complexe et inconnu. »
*Le FBI semble d'ailleurs parfaitement conscient de ces compétences puisque l'agence a noué de nombreux contrats avec Cellebrite, relève le journaliste américain **John Paczkowski**, qui est allé fouiller dans les bases de données publiques de l'administration. A chaque fois, il est question d'acquisition de matériel de télécommunication, sans fil, relatif à l'informatique, par le ministère de la justice américain (le DOJ).*

*L'accord conclu entre Cellebrite et le FBI, le 21 mars 2016 – **DPSD / gouvernement américaine***
*En tout, 2 millions de dollars auraient ainsi été dépensés depuis 2012, **écrit Motherboard**. Qui relève un autre détail intéressant : **le 21 mars 2016**, soit le jour de l'annonce-surprise du FBI, un accord de 15 000 dollars a justement été signé avec Cellebrite.*

Cellebrite déjà sollicité… sans succès

Avant même que le journal israélien pointe explicitement vers Cellebrite, son nom revenait de toute façon déjà dans les articles sur la saga opposant le FBI à Apple.
*L'expert des appareils d'Apple Jonathan Zdziarski **prévenait déjà en septembre 2014** : malgré les précautions louables de la marque, les derniers systèmes d'exploitation de l'iPhone ne sont pas totalement inviolables. Et Cellebrite faisait selon lui parti des rares entreprises capables de fournir des solutions commerciales pour accéder aux données du téléphone.*
*Il ne pouvait être plus proche de la vérité : dans une déclaration remise à la cour appelée à trancher le contentieux entre Apple et le FBI, un ingénieur de l'agence explique avoir déjà eu recours aux services de cette entreprise ! Sans succès… jusque là, **rapporte le New York Times** ce jeudi.*

Nombreux faits d'armes

*Par le passé aussi, Cellebrite s'est démarqué par quelques faits d'armes évocateurs. Début 2016, c'était pour **avoir aidé la police néerlandaise** à lire les messages chiffrés et supprimés d'un Blackberry.*
*Huit ans auparavant, l'association américaine en défense des libertés civiles, l'ACLU, **se lançait dans une procédure** contre la police du Michigan, accusée d'utiliser illégalement les outils de Cellebrite pour fouiller dans les téléphones des suspects.*
*Au nom du Freedom of Information Act (le FOIA), l'organisation **a demandé la publication** de compte-rendus sur l'utilisation de cette solution technique. La police a rétorqué que cette publication lui coûtait des centaines de milliers de dollars et, à notre connaissance, l'ACLU n'a toujours rien reçu… [Lire la suite]*

Réagissez à cet article

Source : *iPhone chiffré : une boîte israélienne à la rescousse du FBI ? – Rue89 – L'Obs*