Laser et acide pour déchiffrer un iPhone, mais avec des risques

Pendant que la bataille entre Apple et le FBI bat son plein, chacun prend position pour les uns ou pour les autres. Dernier en date Bill Gates supporte le FBI dans sa démarche d'avoir accès illimité au téléphone, un iPhone 5C, d'un des responsables de l'attentat perpétré à San Bernardino. Mais un autre son de cloche se fait entendre parmi les spécialistes de la sécurité, notamment Edward Snowden.

Le célèbre lanceur d'alertes et les experts estiment que le FBI a d'autres moyens pour accéder aux informations sur l'iPhone du criminel. Dans un article d'ABCnews, ils parlent notamment d'une technique dite « de-capping chip » ou décapsulage de puce. Cette méthode demande doigtée et patience pour réussir.

Un décapage à l'acide

Andrew Zonenberg, chercheur senior chez IOActive, en a donné le vade-mecum. En premier lieu, il faut extraire le composant où se situe la puce de l'iPhone. Cette puce est encapsulée dans une gangue de polymère. Pour l'éliminer, l'expert utilise de l'acide. Une fois dégagé, il faut percer très soigneusement avec un faisceau d'ion pour atteindre le cœur de la puce. Une fois ce travail réalisé qui peut prendre du temps et de l'argent, le spécialiste place des petites sondes à certains endroits pour récupérer bit après bit l'UID (l'unique ID de l'iPhone).

A travers ces sondes, il est possible de récupérer des données chiffrées et aussi l'algorithme de création de clé de cryptage de l'utilisateur. Avec l'ensemble de ces informations et l'usage de la force brute (sans limitation des 10 essais), il serait donc possible d'exhumer les dernières conversations contenues dans le smartphone d'Apple.

Plus précis avec le laser infrarouge

Un travail long, fastidieux, mais surtout risqué. En utilisant de l'acide, on s'expose à détruire la puce de l'iPhone et la rendre inutilisable à jamais. Un investissement et un risque trop importants constate Dmitry Nedospasov, un spécialiste de la sécurité basé à Berlin. Pour lui, il existe une méthode un peu moins risquée et moins onéreuses pour accéder à la puce.

Il utilise un laser infrarouge, comme un foret capable de percer et d'accèder à la puce et aux informations UID. Ce procédé a déjà été utilisé en 2010 par Chris Tarnovsky, un hacker qui a réussi à craquer le microcontrôleur d'une Xbox 360. Le hic est qu'il avait utilisé un microscope électronique coûtant 250 000 dollars.

Du temps, de l'argent, on comprend que le FBI est plutôt misé sur le rapport de force avec Apple sur le terrain judiciaire. La firme de Cupertino a demandé au gouvernement la création d'un comité d'experts indépendants pour se pencher sur le sujet et fixer un cadre plus clair.

A lire aussi :

John McAfee veut aider le FBI à déchiffrer l'iPhone
Chiffrement : Apple refuse d'aider le FBI à casser la sécurité de l'iPhone

Crédit Photo : Easy Touch Images-Shutterstock