Déblocage de l'iPhone : John McAfee s'apprête à manger une chaussure

Si l'on se fie à sa récente interview à *Russia Today*, John McAfee n'a jamais été aussi prêt de machouiller une chaussure devant des caméras de télévision qu'aujourd'hui. Petit rappel des faits : récemment, le fondateur de l'éditeur d'antivirus a expliqué être en mesure, avec l'aide de hackers de sa connaissance, d'accéder aux données de l'iPhone que détient le FBI, et pour lequel le bureau fédéral demande l'assistance d'Apple. Une affaire qui a vu les deux parties s'opposer bruyamment et qui est désormais entre les mains du Congrès des Etats-Unis.

Sans avoir été sollicité, John McAfee a offert gratuitement son assistance dans cette affaire, et entend fournir un accès aux données d'un iPhone d'un des auteurs de la tuerie de San Bernardino. Et le candidat à la présidentielle américaine (sous les couleurs du parti libertarien) d'ajouter : « *Je mangerai ma chaussure sur le show de Neil Cavuto si nous ne pouvons pas casser ce chiffrement.* » Le milliardaire s'est laissé 3 semaines, à lui et à son équipe, pour y parvenir et a affirmé dans un premier temps vouloir s'appuyer sur des techniques d'ingénierie sociale.

Pour McAfee, 2 ingénieurs et 30 minutes !

Au-delà de cette première affirmation étonnante – l'ingénierie sociale a peu de chance de fonctionner si ses cibles sont prévenues par avance ! -, les déclarations du fantasque homme d'affaires à la chaîne *Russia Today* montrent qu'il ne semble pas prêt de trouver la bonne méthode pour casser les sécurités de l'iPhone (rappelons que les données du terminal sont chiffrées et que leur accès dépend de la saisie d'un code secret, Apple ayant limité à 10 les tentatives successives pour éviter les attaques par force brute).

Selon John McAfee, pour accéder aux données de l'iPhone, il suffit d'un ingénieur hardware et d'un ingénieur logiciel. « L*'ingénieur hardware copie le jeu d'instructions, soit iOS et les applications, et la mémoire. Puis, vous faites tourner un programme appelé désassembleur, qui prend tous les zéros et uns et les transforme en instructions lisibles. Puis, le programmeur s'assoit et lit ce résultat à la recherche du premier accès au clavier, parce que c'est la première chose que vous faites quand vous ouvrez votre terminal. Puis vous lisez les instructions sur l'endroit où le code secret est stocké en mémoire. C'est aussi simple que cela. Et cela demande une demi-heure* », décrit en substance John McAfee, pour qui cette technique fonctionnerait avec tout ordinateur.

Code PIN stocké en mémoire : une fable

L'histoire serait belle, si elle n'était totalement farfelue. Sans même parler des exagérations qu'elle comporte, toute la démonstration de McAfee repose sur le fait que le code PIN du terminal serait stocké en clair quelque part dans la mémoire de l'iPhone, et que iOS compare cette valeur au code entré par l'utilisateur. Sauf que l'iPhone n'a – pour des raisons évidentes – pas été conçu de cette manière.

Dans un document assez complet sur la sécurité de ses smartphones, Apple explique ainsi que le code PIN de l'utilisateur est combiné à un identifiant matériel unique pour générer la clef de chiffrement de l'iPhone. Le code PIN n'est donc pas stocké en mémoire (que ce soit dans la Ram ou dans la mémoire flash), tout simplement parce que le mécanisme imaginé par les ingénieurs d'Apple n'en a pas l'utilité. Si le code PIN entré pour accéder au terminal est faux, la clef générée en combinant ce sésame avec l'identifiant matériel ne fonctionnera pas et les fichiers chiffrés le resteront. A l'inverse, le bon code PIN va permettre de créer la bonne clef, donc de déchiffrer les fichiers. Le système vérifie donc que le sésame est valide en tentant de l'utiliser, et non en le comparant à une valeur stockée quelque part.

Laser et acide : le seul espoir ?

La technique est d'ailleurs des plus classiques ; elle est par exemple également employée par Windows BitLocker et TrueCrypt. Signalons que si les OS classiques – comme Windows, Linux ou OS X – stockent bien les codes d'accès de leurs utilisateurs sur la machine, ceux-ci sont transformés par une fonction mathématique avant leur écriture. Une opération évidemment non réversible. Pour vérifier la validité d'un sésame, l'OS opère la même transformation et compare son résultat à la valeur stockée. Même sur un ordinateur 'classique', la technique décrite par McAfee ne fonctionnerait donc pas, en tout cas pas aussi simplement qu'il la décrit.

Comme le signale *Ars Technica*, le meilleur espoir de décoder l'iPhone de San Bernardino consiste à utiliser une technique combinant recours à l'acide et aux lasers pour tenter d'accéder à l'identifiant matériel unique de ce terminal. Pour ensuite le combiner avec les codes PIN possibles pour reconstituer la clef de chiffrement idoine. Une technique coûteuse et hautement risquée, car l'accès physique au processeur qu'elle implique peut tout aussi bien se traduire par la destruction du terminal. Et la perte de toutes les données qu'il renferme.

A lire aussi :

Contre le FBI, les experts en chiffrement soutiennent (presque tous) Apple

Arrêté, John McAfee demande l'asile politique au Guatemala