# Vault 7 : Wikileaks révèle comment la CIA peut pirater de nombreux appareils

Wikileaks a publié la première partie d'un gigantesque lot de documents, dont l'ensemble est nommé Vault 7. Ils montrent ainsi comment la CIA peut pénétrer dans certains appareils, qu'il s'agisse de TV connectées, de smartphones, d'ordinateurs ou mêmes de voitures.


Ce premier lot de milliers de documents est appelé par Wikileaks « Year Zero ». Il contient précisément 8 761 fichiers abordant les techniques utilisées par la CIA pour s'attaquer à certaines catégories de produits. Dans un monde post-Snowden, ce type de révélation n'étonnera guère.

## Les Smart TV de Samsung en première ligne

L'un des programmes les plus significatifs est Weeping Angel, une référence directe aux effrayants Anges Pleureurs de la série Doctor Who. Il concerne les téléviseurs connectés de Samsung et permet de les attaquer pour en prendre le contrôle. Ils peuvent être alors utilisés pour espionner les personnes autour, une méthode particulièrement efficace si les modèles sont équipés d'une webcam. Les conversations ainsi captées peuvent ensuite être transmises à l'agence.

Tous les modèles ne sont pas vulnérables, mais la série F8000 semble particulièrement concernée. Si les techniciens de la CIA parviennent cependant à entrer, ils peuvent récupérer l'historique de navigation ainsi que les identifiants Wi-Fi. L'activité malveillante de la TV peut par ailleurs être masquée en plongeant l'appareil dans un faux état de veille. Selon les documents de Wikileaks, l'outil a été développé conjointement avec le MI5 anglais en juin 2014.

Le cas de Weeping Angel ne surprendra pas. De nombreux articles – notamment dans nos colonnes – ont rappelé bien souvent que la sécurité des objets connectés laissait nettement à désirer. Le fait que la CIA puisse récupérer des identifiants et prendre le contrôle de webcams montre encore une fois que les constructeurs ont tout intérêt à se pencher sérieusement sur les protections de leurs produits.

## iPhone, appareils Android, tout y passe

La CIA ne s'en prend bien sûr pas qu'aux objets connectés. Sa Mobile Devices Branch dispose ainsi de programmes concernant aussi bien les iPhone que les smartphones Android. Le produit d'Apple semble particulièrement concerné, non à cause de sa part de marché (14,5 % selon les documents), mais par les catégories de personnes qui l'utilisent : diplomates, hommes politiques, et globalement une population de décideurs, y compris dans le monde professionnel.

Concernant Android, la CIA aurait en sa possession 24 failles 0-day exploitables via des attaques spécifiques, et toujours référencées comme valide en 2016. Ces brèches « armées » ont été développées en interne, ou obtenues ailleurs, notamment chez la NSA, le GCHQ ou depuis certaines sociétés privées, notamment celles opérant dans le marché gris (failles vendues au plus offrant, ou diffusées à certains clients payant une sorte d'abonnement).

Dans les deux cas – iOS et Android – la CIA disposerait de techniques capables de lui donner accès à de précieuses données avant même qu'elles soient chiffrées. L'agence serait en mesure notamment de récupérer des messages de plateformes telles que Signal, Telegram ou encore WhatsApp.

## Tout ce qui contient un système d'exploitation

Plus généralement, les documents indiquent que la CIA possède des attaques soigneusement préparées contre un très grand nombre de produits disposant d'un système d'exploitation, quel qu'il soit.

Windows, macOS et Linux peuvent ainsi passer au grill, de même que les équipements réseau tels que les routeurs. Les agents impliqués dans les attaques ont à leur disposition une véritable trousse à outils contenant notamment 24 fausses applications courantes, voire des jeux, comme VLC, Prezi, 2048 ou encore des antivirus tels que McAfee et Kaspersky. Même les machines protégées par un air gap – donc non reliées à un réseau ouvert – font l'objet de techniques particulières, impliquant du stockage externe, des partitions masquées ou encore des malwares cachés dans des images. Certains véhicules récents sont également dans le colimateur.

Sur une note séparée, on apprend également que le Center for Cyber Intelligence de la CIA possède une base dans le consulat américain de Francfort, pour couvrir les opérations en Europe, en Afrique et dans le Moyen-Orient. Interrogée sur l'ensemble de ces révélations, la CIA a simplement répondu qu'elle ne commentait jamais ce type de publication. De son côté, Edward Snowden a plongé dans les documents de Wikileaks, indiquant que tout semblait authentique.

## Les entreprises concernées calment le jeu

Le moins que l'on puisse dire au vu des détails fournis est que la situation a de quoi être anxiogène. Il n'y a cependant pas de quoi paniquer, en tout cas dans l'état actuel des révélations.

Les outils, failles et malwares abordés dans les documents ont en effet déjà plusieurs années. Les failles 0-day, donc découvertes et potentiellement exploitées avant même que l'éditeur concerné ne soit au courant, gardent leur pouvoir tant que les détails ne sont pas révélés. Or, plus le temps passe, plus les chances que les entreprises découvrent au moins certaines des vulnérabilités par d'autres moyens. C'est ce qui s'est produit en partie déjà cette nuit.

Un porte-parole d'Apple a ainsi indiqué à TechCrunch que la plupart des failles abordées avaient déjà été corrigées dans iOS. Cependant : « *Nous continuerons à travailler à la résolution rapide des vulnérabilités identifiées. Nous encourageons toujours les utilisateurs à télécharger le dernier iOS pour s'assurer qu'ils ont toujours les dernières mises à jour de sécurité* ». Un conseil d'ailleurs valable pour n'importe quel produit, quelle que soit la marque.

Samsung et Google n'ont pas encore réagi officiellement.

## Les applications de messagerie ne sont pas en tort

Du côté de Telegram, on communique également. L'éditeur explique qu'une application de messagerie est comme un château sur une montagne. Peu importe la résistance du château, si la montagne a un problème, il n'y aura pas de miracle. Comprendre : les problèmes pointés par Wikileaks concernent les systèmes d'exploitation, non les applications : « *Aucune application ne peut empêcher un clavier de savoir sur quelles touches vous appuyez. Aucune application ne peut cacher ce qui apparait sur l'écran depuis le système* ».

Telegram insiste : c'est aux constructeurs et éditeurs de réparer ces problèmes, les développeurs tiers n'y étant pour rien. La petite société se veut cependant rassurante, en rappelant que la CIA effectue des opérations ciblées et non une surveillance globale. Elle donne également quelques conseils de bon sens : ne pas utiliser d'appareil rooté ou jailbreaké à moins de savoir exactement ce que l'on fait, ne pas installer d'applications de sources inconnues, toujours être à jour, choisir un constructeur connu pour sa politique sérieuse de support…

Le point de vue est partagé par Ross Schulman, de l'Open Technology Institute. Il indique que les applications de messagerie n'ont rien à faire de plus, les problèmes abordés ne dépendant pas d'elles. Quel que soit le niveau de protection qu'elles offrent, les soucis se situent en amont, et elles ne peuvent pas empêcher les informations de fuiter avant qu'elles puissent faire quoi que ce soit.

Open Whisper Systems, éditeur du protocole Signal et de l'application du même nom, a lui aussi indiqué cette nuit qu'aucune des failles en possession de la CIA n'est de son ressort. Le protocole n'est donc pas directement ciblé, mettant au passage toutes les applications l'utilisant à « l'abri », notamment WhatsApp et Viber. Bien entendu, et encore une fois, si le système d'exploitation est compromis, ni le protocole, ni l'application ne pourront protéger l'utilisateur.

> The CIA/Wikileaks story today is about getting malware onto phones, none of the exploits are in Signal or break Signal Protocol encryption.
> 21:02 - 7 Mars 2017

## Privacy International : une situation prévisible

Privacy International n'est pour sa part pas surprise. L'ONG indique dans un communiqué qu'elle avertit depuis longtemps que les gouvernements disposent de ce type de capacité. Elle en appelle donc encore une fois les constructeurs à prendre leurs responsabilités et à travailler soigneusement la sécurité de leurs produits.

Rappelons qu'il ne s'agit que d'une première publication, Wikileaks promettant que d'autres vont suivre. L'organisation est également en possession d'une partie des malwares et autres fichiers que la CIA utilise dans ses programmes d'espionnage. Cependant, ces éléments ne seront dévoilés que plus tard, quand ils auront été désamorcés, supposément par leurs éditeurs respectifs. Un mouvement assez inhabituel de la part de Wikileaks.

Publiée le 08/03/2017 à 11:30

**Vincent Hermann**
Rédacteur/journaliste spécialisé dans le logiciel et en particulier les systèmes d'exploitation. Ne se déplace jamais sans son épée.