# Vault 7 : votre smartphone et votre TV samsung sont-ils piratés par la CIA ?

écrit par Oncle Bob | 9 mars 2017

Vault 7 : Wikileaks révèle les instruments de contrôle de la CIA, capables de hacker les Iphones, les smartphones et les smart TV. La CIA, en coopération avec le MI5 britannique, a développé un programme: weeping angel (l'ange pleureur) qui empêche les tv Samsung de s'éteindre(tout en ayant l'air éteint), et agissant comme un micro, qui envoie les conversations effectuées à proximité de cette télé, par le biais d'Internet, à un serveur de la CIA. Ils est dit que les moyens, les instruments(tools) de la CIA sont même supérieurs à ceux de la NSA. Ce qui est étonnant, c'est que ces moyens n'ont apparemment pas été utilisés contre le terrorisme, étant donné les attentats.

Vault 7 dévoile aussi la possibilité qu'Obama et la CIA auraient pu assassiner le journaliste Michael Hastings. La CIA aurait travaillé en outre sur le moyen de prendre le contrôle des voitures et de provoquer des accidents(assassinat masqué). Wikileaks n'a révélé pour l'instant que moins d'un pour cent de Vault 7.

A lire en complément :

### Révélations Vault 7 de WikiLeaks : la CIA affirme avoir été au courant, et accuse des fournisseurs

Au lendemain de révélations sur les techniques de surveillance électronique de la CIA, des agents affirment qu'ils savaient que celles-ci auraient lieu. Ils soupçonnent des sociétés ayant collaboré avec la CIA d'être derrière ces fuites.

S'exprimant sous couvert d'anonymat, des hauts responsables du renseignement

américain ont confié à l'agence Reuters, le 8 mars, que la CIA était au courant de la fuite imminente de documents de l'agence de renseignent sur la surveillance électronique, publiés par WikiLeaks le 7 mars.

## Révélations Vault 7 sur la CIA : WikiLeaks précise que ce n'est qu'un début

Les fonctionnaires anonymes ont en outre confirmé que l'enquête interne des autorités se concentrait sur des fournisseurs extérieurs, qu'elles soupçonnent d'avoir confié les données confidentielles en question au site pro-transparence.

Les hauts responsables de la CIA ont également indiqué qu'ils considéraient comme authentiques les 8 761 documents de «Year Zero» – la première salve de données rendues publiques, parmi la masse d'informations que WikiLeaks a en sa possession, baptisée «Vault 7».

Le 8 mars toujours, le FBI a annoncé avoir lancé une enquête criminelle fédérale visant le site de Julian Assange, en coordination avec la CIA.

**Lire aussi** : Espionnage de la campagne présidentielle française de 2012 : Wikileaks publie des ordres de la CIA

La CIA en mesure de prendre le contrôle des Smartphones, selon les documents fuités

Les documents du lot Year Zero indiquent que la CIA a développé un code informatique, le code «24 zero day», qui lui permettrait de prendre le contrôle des smartphones fonctionnant avec le système d'exploitation d'Apple, iOS, et celui de Google, Android. La CIA serait également en mesure d'infiltrer d'autres types d'appareils électroniques, tels que des téléviseurs connectés, selon ces documents.

«Cette collection extraordinaire, qui représente plusieurs centaines de millions de lignes de codes, dévoile à son détenteur la totalité de la capacité de piratage informatique de la CIA», a commenté Devin Nunes, président la commission du Renseignement à la Chambre des représentants américaine, à la découverte des révélations de WikiLeaks.

Le site de Julian Assange entend certainement publier au compte-goutte les documents de son stock, comme il l'avait fait avec les mails du directeur de campagne d'Hillary Clinton, lors de l'élection présidentielle américaine de 2016. Avec Year Zero, WikiLeaks assure avoir dévoilé moins d'1% seulement de Vault 7…

https://francais.rt.com/international/34998-revelations-vault-7-wikileaks-cia-ete-au-courant

## Qu'est-ce que Vault 7 ?

Vault 7 est un nom de code, choisi par l'organisation Wikileaks. Il est utilisé pour désigner la publication colossale d'une série de documents secrets appartenants à la CIA, principale agence de renseignement américaine. Vault 7 est ce qu'on appelle une série : chaque publication sera donc une étape de celle-ci. La première publication de cette série se nomme *Year Zero* et contient déjà plus de 8 000 documents.

Ces derniers fonctionnent comme un effet d'annonce pour l'organisation qui espère pouvoir ainsi attirer l'attention des médias et des citoyens sur une base de données qui s'étoffera avec le temps. *Year Zero* n'est pas une série de documents choisis aléatoirement, c'est une sélection faite par Wikileaks qui permet de comprendre, selon l'organisation, que la CIA est activement investie dans le piratage de citoyens et entreprises du monde entier.

Selon Assange, mais cette affirmation ne peut, par essence, être prouvée, l'ensemble de Vault 7 constituerait l'intégralité de l'armement informatique de l'agence. Dans *Year Zero,* aucune arme n'est dévoilée par Wikileaks, qui préfère garder les logiciels malveillants dans l'ombre, le temps qu'ils soient *déminés*.

> *RELEASE: Vault 7 Part 1 "Year Zero": Inside the CIA's global hacking force https://t.co/h5wzfrReyy pic.twitter.com/N2lxyHH9jp*
>
> *— WikiLeaks (@wikileaks) 7 mars 2017*

### DE COMBIEN DE DOCUMENTS PARLE-T-ON ?

Pour le moment, seulement de 8 761 fichiers et documents. C'est *Year Zero*. À l'avenir, Vault 7 devra, toujours selon l'organisation, devenir le plus important leak jamais réalisé par Wikileaks, soit plus que l'intégralité des révélations faites par Snowden.

**QUELS SONT LES SMARTPHONES ET GADGETS CIBLÉS PAR LA CIA ?**

La première parution, *Year Zero*, semble accréditer la thèse d'un développement actif de nombreuses armes informatiques à l'intérieur même de l'agence américaine. Afin de rattraper son retard face à la NSA, la CIA aurait en effet, à l'instar d'un FSB russe, employé de nombreux ingénieurs et hackers pour développer de multiples virus, malwares et autres logiciels malveillants.

De fait, chacun de ces logiciels est une arme qui possède une cible. Si l'on en croit l'organisation – il faudra évidemment que chacun des documents soit analysé –, l'arsenal exhaustif de la CIA pourrait attaquer aussi bien une voiture connectée, un serveur Linux, un smartphone iOS, une tablette Android etc. En réalité, en regardant les différents logiciels dévoilés dans *Year Zero*, presque toutes les manipulations possibles, du phishing au malware, ont été travaillées et essayées par la CIA.

En somme, il est difficile de faire une liste exhaustive des cibles préférées de l'agence. Même si certains exemples devraient accaparer l'attention de toute la presse, notamment les iPhone que l'on découvre probablement plus vulnérables que ne le dit Cupertino, et bien sûr le cas des TV Samsung qui une fois contaminées seraient en mesure de se transformer en micro de salon, toujours selon Wikileaks.

Nous ne reprendrons pas ces premières analyses réalisées par l'organisation en tant qu'information : ce sont pour le moment, seulement des interprétations faites par une organisation. Un recoupement de l'information est nécessaire.

**QUE PEUT CRAINDRE UN CITOYEN ?**

Dire qu'il n'y a aucun risque serait autant un mensonge que dire que le risque présenté par ces documents est inexistant. Pour comprendre de quoi il en retourne, il faut se plonger dans la définition de l'espionnage informatique et essayer de distinguer espionnage ciblé et espionnage de masse. Vault 7, à première vue, est de l'espionnage ciblé : cela signifie que la CIA n'espionne pas de larges groupes d'innocents pour trouver un coupable, mais cherche à connaître les activités d'un suspect.

Le problème est plus philosophique : en exploitant des failles sans informer les constructeurs et les développeurs de logiciels, la CIA laisse des ouvertures dangereuses dans des logiciels qui pourraient être utilisées de manière différente

par des personnes malintentionnées. En plus, elle participe à la propagation des *armes numériques*, qui ont pour caractéristique principale de n'être jamais à court de munition.

Nous avons consacré un article détaillé à cette question complexe.

**JE LIS QUE LA CIA ESPIONNE MA TV SAMSUNG. EST-CE VRAI ?**

Le fait que la CIA ait développé en interne un outil pour accéder aux données d'un téléviseur Samsung ne veut pas dire qu'elle surveille tous les téléviseurs Samsung connectés du monde. En plus, le processus décrit dans les premiers documents de Wikileaks montrent qu'un agent a besoin d'un accès physique à un téléviseur pour installer les malwares à l'aide d'une clef USB.

Vous trouverez notre article complet sur ce sujet à cette adresse.

**EST-CE QUE CES INFORMATIONS SONT VÉRIFIÉES ?**

Oui par Wikileaks, mais pas par le reste du monde. Actuellement, de nombreuses rédactions, experts et divers citoyens sont en train de se plonger dans la première salve de Vault 7. Une fois que ce travail sera réalisé et que le recoupement de l'information sera possible, alors là, nous pourrons parler d'informations vérifiées.

**POURQUOI EST-CE IMPORTANT DE NUANCER À CE POINT LES PREMIÈRES ANALYSES DE WIKILEAKS ?**

Car l'organisation Wikileaks est une organisation humaine, avec ses problèmes et ses qualités. De fait, son interprétation doit être confrontée à la réalité et nous ne pouvons, en tant que journalistes, nous en tenir à une analyse réalisée à huis clos.

Les citoyens et hackers sont également invités à consulter les documents, et faire également un travail de vérification. C'est naturel et normal. Il n'y a qu'ainsi que Vault 7 pourra être traité convenablement et compris dans son ensemble. Par exemple, Edward Snowden lui-même est en ce moment en train de vérifier les dires de l'organisation. Il a d'ailleurs déjà pu pointer une erreur de lecture faite par Wikileaks.

Wikileaks : « ***Vault7*** *confirme que la CIA peut effectivement dévérouiller le chiffrement de Signal, Telegram, Whatsapp et Confide.*

E. Snowden : *Cela voudrait dire que la CIA a pu pirater ces applications et/ou leur chiffrement. C'est incorrect. Les documents montrent que ce sont directement iOS et Android qui ont été piratés. C'est un plus gros problème encore.*

***Je continue de travailler sur les publications, mais ce que Wikileaks a est sincèrement un gros dossier. Cela semble authentique.* »**

**EST-CE QUE LES TV SAMSUNG SANS MICRO PEUVENT NOUS ENTENDRE ?**

Un téléviseur, comme n'importe quel objet disposant d'une carte son, d'un équipement sonore et de sucroit de haut-parleurs, peut servir de micro même s'il n'en dispose pas. En tant qu'interface entre l'électricité et l'air, une membrane de haut-parleur sur un téléviseur peut être utilisée comme un micro. Pour mieux comprendre ce fonctionnement, nous vous invitons à lire notre article sur un cas d'écouteurs transformés en micro par des experts en cyber-sécurité.

**EN TANT QU'UTILISATEUR D'ANDROID, À QUEL POINT SUIS-JE VULNÉRABLE ?**

Il est connu de tous, même parfois exagérément, qu'Android n'est pas un système d'exploitation très sécurisé. Néanmoins, une fois cela dit, concernant la CIA et les armes dévoilées par Wikileaks, il est encore tôt pour mesurer le risque réel d'un smartphone à l'autre. Selon les premières analyses, iOS comme Android seraient touchés par les armes directement, et pas seulement par des applications tierces malveillantes installées par-dessus les OS. De fait, face à une telle menace, difficile de dire qui est le plus vulnérable.

http://www.numerama.com/politique/238694-vault-7-toutes-les-questions-comprendre-les-documents-devoiles-par-wikileaks.html