Présentation de

Vault 7

Réalisé par Quentin Guardia
Master 1 Cybersécurité à l'Université de Paris
quentin.guardia@etu.u-paris.fr

Qu’est-ce que Vault 7 ?

Vault 7 est un ensemble de **documents confidentiels** appartenant à la Central Intelligence Agency (**CIA**), qui ont étaient publiés sur le site de **WikiLeaks**. Des milliers de documents ont donc été rendus publics le long de l’année **2017**.

Qu’est-ce que la CIA ?

Agence centrale de renseignement en Français, c’est l’une des plus célèbre **agence de renseignement** des États-Unis. Elle a officiellement pour but d’analyser les informations dans le monde pour assurer la sécurité du pays. Elle peut mener des opérations clandestines à l’étranger.

Qu’est-ce que WikiLeaks ?

Il s’agit d’une organisation fondée par le cybermilitant Julien Assange en 2006, qui bénéficie d’un fort pouvoir médiatique. Son but est de **faire connaître des documents (appelés leaks)**, souvent confidentiels, concernant **la guerre, l’espionnage** ou encore **la corruption**. Les milliers de documents rendus publics par WikiLeaks ont fait éclater de nombreux scandales à travers le monde.

D’où proviendrait la fuite ?

La fuite proviendrait du **Center for Cyber Intelligence**, qui est une unité spécialisée de la CIA. Faute de sécurité, les **plusieurs dizaines de téraoctets** de données ont été dérobés en 2016. Les documents volés datent alors de **2013 à 2016** et semblent authentiques.

Comment la fuite est devenue Vault 7 ?

Début février 2017, **WikiLeaks twitte énigmatiquement** des questions sur Vault 7, alors inconnu. Chaque question est accompagnée d'une image inexpliquée. Le 16 février, WikiLeaks publie les documents détaillant comment les élections présidentielles françaises de 2012 ont été surveillées par la CIA. Vault 7 est médiatisé dans la communauté informatique. Les premiers documents volés paraissent le 7 mars sous forme d'un projet, avant qu'une faille à la CIA ne soit déplorée.

Comment la fuite est devenue Vault 7 ?

Au total, **24 projets** ont été publiés jusqu'à septembre 2017. Certains éléments comme des codes source ou adresses IP ont été censurés par sécurité. La série de documents s'est faite connaître sur cette page de WikiLeaks :

https://wikileaks.org/ciav7p1/

Voici la version par projet :

https://wikileaks.org/vault7/

Que révèlent les documents apportés ?

Globalement, Vault 7 nous apprend que **la CIA sait pirater beaucoup de nos outils**. Voici quelques technologies concernées :

- Smartphones
- Systèmes d’exploitation
- Téléviseurs Samsung
- De nombreuses applications du quotidien

Que révèlent les documents apportés ?

- Des routeurs Cisco
- Du matériel informatique (hardware)
- Certains véhicules modernes
- Et bien d’autres technologies

Au vu de la **quantité gigantesque d’informations**, une infime partie des techniques de piratage seront décrites à la suite.

Les smartphones

Les vulnérabilités touchent aussi les géants **iOS et Android**.

Probablement beaucoup iOS car cet OS serait souvent utilisé par les personnes plus influentes.

Le système piraté peut observer l'écran ou accéder aux touches sur lesquelles l'utilisateur appuie. Ainsi, même lors de l'usage d'une application dont la connexion est sécurisée, les **données sont compromises**.

Les smartphones

L'espionnage est illustrable avec *HighRise*, une application Android installée inopinément qui permet à un espion d'intercepter les SMS entrant et sortant de l'appareil de la cible, en se comportant comme un proxy.

La Mobile Devices Branch (MDB) de la CIA travaille sur la **prise de contrôle** de smartphone à distance et sur le **vol d'informations** (SMS, caméra, localisation, micro, ...)

Failles relatives à Windows

Grasshoper est un ensemble d'outils (framework) qui vise à installer des malwares adaptés à la machine sur commande, tout en restant **invisible** aux yeux du système Windows.

Le programme *Scribbles* détecte des documents de Microsoft Office contenant de potentiels leaks, les marque et **espionne** l'utilisateur à l'ouverture des documents.

FAX DLL injection **détourne des fichiers** .dll (hijacking) afin de lancer un malware furtivement et durablement.

AfterMidnight se compose en partie d'un faux DLL et installe des malwares sur commande pour **contrôler l'ordinateur**.

On pourrait aborder *HIVE, JQJIMPROVISE, Athena* ou *Assassin*.

Failles relatives à Mac

Triton, Sonic Screwdriver, Achilles… Plusieurs programmes mettent en défaut **Apple**. C'est le cas de *DarkMatter*, *SeaPea* et *Nightskies* formant *DarkSeaSkies*. *DarkMatter* s'implante sur le système de démarrage EFI et **ne peut plus être supprimé**. Il installe *SeaPea* dans le kernel et *NighSkies* parmi les données utilisateur. Le rootkit *SeaPea* ne peut être supprimé qu'après formatage et lance *Nightskies* **en le masquant** des fichiers, connexions et/ou processus. *Nightskies* envoie des informations à la CIA grâce à internet comme une porte dérobée. Il s'installe sur l'iPhone au moment de la production.

Failles sous Linux

Aeris est lui un implant automatique agissant sur Mac comme Linux, et **tout OS basé sur POSIX**. Il fonctionne également comme une **porte dérobée** et peut implanter d'autres **malwares**. Il extrait les données des machines cibles grâce à une connexion sécurisée par TLS.

Gyrfalcon est un implant sous Linux visant **OpenSSH** en **capturant le trafic et identifiants**. Il stocke les données exfiltrées dans un fichier chiffré sur la machine cible. L'agent les récupère lors d'une session spéciale et les déchiffre. C'est donc un outil très puissant, qui nécessite cependant des privilèges pour être installé.

Les smartTV

L’Embedded Devices Branch (EDB) de la CIA travaille sur l’espionnage des appareils embarqués. L’exemple le plus célèbre est celui du « **Weeping Angel** », ou « Ange Pleureur » en français, en référence à 1984 de George Orwell. Grâce à un support USB, la CIA peut infecter des **télévisions connectées**. Au moment d’être éteintes, celles-ci restent invisiblement connectées, afin d’**écouter les conversations** avec le micro, ou même utiliser la potentielle caméra. Les données sont enregistrées ou directement envoyées sur des serveurs de la CIA via internet. On sait que Samsung a beaucoup était touché.

Les applications communes

De nombreuses applications en tout genre sont détournées (hijacking). On peut citer VLC, Firefox, Notepad ou 2048 et bien d'autres logiciels communs. Lorsqu'elles sont en cours d'exécution, les applications fonctionnent correctement. Cependant elles collectent **à l'insu de l'utilisateur**, les informations présentent sur le disque.

C'est aussi le cas de *Rain Maker*, qui usurpe un lancement de VLC pour collecter des données en les chiffrant sur la clé USB de l'espion.

Les routeurs Cisco

Vault 7 a fait savoir que **318 routeurs** d'une des plus emblématiques entreprises de réseaux étaient vulnérables. Plus précisément, il était possible pour un attaquant, quelle que soit la configuration du routeur, de redémarrer ce dernier ou d'**exécuter des commandes** à distance avec de hauts privilèges. Il était alors possible de **capturer les informations** qui y transitaient grâce à un système de redirection.

Le hardware

Le matériel peut également être source de vulnérabilités. Par exemple, sur un simple support USB ou bien avec *Hammer Drill*, qui est un malware invisible sur des CD ou DVD vierges. Il installe un **cheval de Troie** lors de la gravure du disque avec Néro, afin d'aussi toucher les systèmes isolés et protégés (air gapped). Puis *Hammer Drill* peut **récolter sur demande des données** du disque, journaliser l'ajout ou le retrait de CD ou DVD, etc.

Véhicules modernes

Sur certains **véhicules récents**, comme des voitures ou camions avec **système embarqué**, des failles exploitables ont été dévoilées par Vault 7. Il aurait ainsi était possible de **provoquer un accident** sans laisser de trace, rapporte WikiLeaks.

Et bien plus encore…

La CIA savait désactiver des caméras, leur micro ou enregistrement grâce à *Dumbo*. Certains serveurs pouvaient aussi être piratés, avec *HIVE* par exemple. De plus, la CIA était en capacité de changer l'empreinte des attaques pour ne pas se faire accuser. La listes des possibilités de la CIA était non-exhaustive. Ainsi, comme le laisse penser l'organigramme des branches par spécialité de la CIA, disponible sur le rapport de Vault 7, **d'innombrables systèmes sont vulnérables**, du hardware et/ou du software.

Pour résumer, quels étaient les principaux moyens d'action de la CIA ?

La CIA savait donc **écouter et contrôler** plusieurs technologies furtivement. L'écoute se fait par Listening Posts (LP) et le contrôle par Command and Control (C2). C'était souvent des **malwares** qui permettaient d'y arriver en lançant un exploit. Ils se basent sur des failles jamais détectées et donc insoupçonnées (faille zero days) et sont souvent sous forme d'implant. Ils peuvent être de plusieurs types : back door, trojan,... Et on la capacité d'être **difficilement détectables**, grâce au hijacking ou au masquage de leurs traces sur le système entre autres.

Pour résumer, quels étaient les principaux moyens d'action de la CIA ?

Lorsque plusieurs outils interagissent pour s'emparer d'un système, on parle de **framework**. Tout ceci peut s'implanter **physiquement**, par exemple par USB, ou bien **par réseau**. Et c'est par ces moyens que sont exfiltrées les informations. La difficulté de mise en place des différentes stratégies, notamment l'accès physique aux machines qui est souvent requis, fait que Vault 7 révèle des méthodes d'espionnage ciblé et non pas de masse comme celles de la NSA.

Sait-on tout ?

Il manque certains chaînons dans les arsenaux de la CIA. On ne sait par exemple pas avec quel malware fonctionne *HighRise* ou encore quels outils permettent à *Aeris* de cibler puis collecter les données. De plus certains logiciels ont du avoir de **nouvelles versions** depuis la publication de Vault 7. Ainsi, le grand public ne peut toujours pas savoir les quels de leurs outils sont vulnérables. Bien que les entreprises aient sécurisé les failles signalées par Vault 7.

Interrogations supplémentaires

- Pourquoi tant d'investissement dans l'espionnage ? Qui la CIA vise-t-elle et dans quel but ?
- Que nous cache-t-on de plus ? Qu'insinuaient les images des tweets de WikiLeaks précédant la parution de Vault 7 ?
- Ces failles ont-elles été créées ou ignorées volontairement ?
- La capacité de surveillance de la CIA est-elle plus importante que le colmatage des failles qu'elle détecte ?

Sources des images et références

Logo de WikiLeaks :
https://commons.wikimedia.org/wiki/File:Wikileaks_logo.svg

Logo de l'*Information Operations Center* de la CIA :
https://wikileaks.org/ciav7p1/logo.png

Caricature Big Brother :
https://commons.wikimedia.org/wiki/File:1984-Big-Brother.jpg

Références :
https://wikileaks.org/ciav7p1/
https://wikileaks.org/vault7/