Vault 7 Wikileaks para Windows

Vladislav Stelmakh
UO257580@uniovi.es

Resumen
Este trabajo recoge y explica toda la información acerca de dicha colección de material confidencial documental de la CIA. Describiendo qué es, qué contiene, cómo y para qué fue creada, este análisis es imprescindible para el conocimiento de todo lo que nos oculta la CIA, todos sus trapos sucios, todo lo que no sabíamos hasta ahora y todo de lo que tendríamos que estar protegidos, prevenidos y en alerta, si no queremos sufrir posibles futuros ataques.

1. Introducción

La continua y rápida evolución de la tecnología y sobre todo de la informática, que trae consigo que todas nuestras tecnologías actuales se modernicen, conlleva también a la aparición de muchos nuevos problemas, siendo uno de los más importantes la aparición de un nuevo tipo de "ladrones" y nuevas técnicas de "robo", o mejor dicho, nuevos "criminales" con nuevas técnicas de poder llevar a cabo sus acometidas en el intento de obtener beneficios propios de manera ilegal. Si hoy en día vemos tanta seguridad en aplicaciones, programas, navegadores…, tantos antivirus y programas de protección de datos e información, es debido a que por otro lado existen miles y miles de softwares malignos (malware), y de personas que se dedican a realizar actos indebidos.

Por ello existe un grave problema, y es que no podemos ni debemos fiarnos de nadie hoy en día, debido a que cualquier persona, empresa… que pueda saber cualquier dato nuestro que sea confidencial, es directamente susceptible de ser un posible "delincuente", una posible vía de fuga de información que pueda comprometer nuestra seguridad y nuestros datos.

Es entonces, cuando surgen colecciones como Vault 7, que nos informan, nos ponen en alerta y nos dan a conocer información que nunca antes conocíamos, y hacen que podamos estar prevenidos y seguros.

2. Historia sobre Vault 7 e información importante sobre la CIA

Vault 7 es la mayor colección sustancial de documentos confidenciales de la Agencia Central de Inteligencia estadounidense (CIA) que se ha filtrado hasta el momento por el portal de filtraciones de WikiLeaks. Dichos documentos, que hablan sobre las supuestas técnicas de hacking de la CIA, para ejercer vigilancia electrónica y guerra informática, que constan de diversos malwares y armas cibernéticas capaces de afectar numerosos productos, comenzaron a ser lanzados el 7 de marzo de 2017 con el fin de que los desarrolladores fuesen capaces de analizarlas y proteger sus productos de ellas.

Haciendo uso de dichas armas de hackeo, la CIA era capaz de obtener información masiva desde cualquier SmartTV, Smartphone (Android o iPhone), de cualquier aplicación (WhatsApp, Telegram…), de afectar

ordenadores e incluso se han llegado a denunciar operaciones encubiertas de Europa, Medio Oriente y África realizadas desde el consulado estadounidense en la ciudad alemana de Frankfurt. La CIA ha llegado incluso a interferir en las elecciones presidenciales de Francia en 2012.
El rango de tiempo que abarca Vault 7, va desde los años 2013 hasta el 2016, y sus páginas están ordenadas de tal manera que, en cada nivel, aparecen primero las más antiguas.

Todo comenzó cuando se lanzó la primera parte de un total de siete entregas de filtraciones, denominada Año Cero (Year Zero), y que contenía un total de 8761 documentos privados de la CIA acerca de sus tareas de espionaje cibernético, obtenida recientemente y que abarca desde el año 2016.

WikiLeaks destaca que desde el 2001, la CIA ha ganado predominancia política y presupuestaria sobre la Agencia de Seguridad Nacional de los Estados Unidos (NSA).
La CIA prácticamente creó su propia Agencia de Seguridad Nacional, para replicar las capacidades de la NSA, la agencia rival. Su propia Agencia, contaba con más de 5000 usuarios registrados y había producido más de 1000 sistemas de hackeo, virus, troyanos y otros programas maliciosos.

Sello de la Agencia Central de Inteligencia (CIA)

Logotipo de WikiLeaks

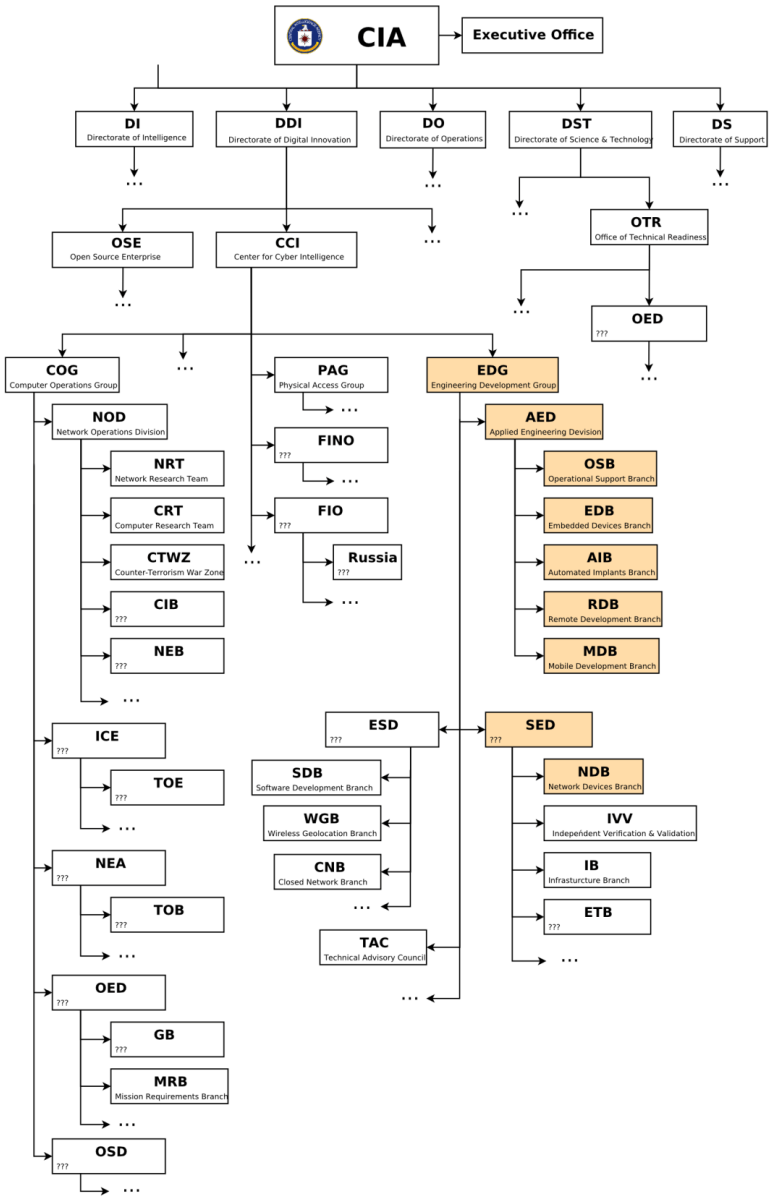
3. Fuente de información

Todos los documentos que se muestran en el Vault 7, son documentos que han sido robados, provenientes de una red de alta seguridad aislada, situada en Langley, Virginia, dentro del Centro de Ciberinteligencia de la CIA. Todas las fuentes, confían en que WikiLeaks no revelará información que pueda identificarles.

Según asegura WikiLeaks, la CIA ha perdido el control de la mayoría de su material de hackeo, incluyendo exploits, virus, troyanos, malware y toda la documentación relacionada, que habían ido a parar a 'hackers' privados y a 'exhackers' del anterior Gobierno, siendo uno de ellos quién tras haberse hecho con los documentos, tomó la decisión de compartirlos con la web de filtraciones.

4. Malware de la CIA y dispositivos pirateados

Las herramientas de hackeo y el malware de la CIA es desarrollado por el Engineering Development Group (EDG), un grupo de desarrollo de software del Centro de Inteligencia Cibernética (CCI), departamento perteneciente a la Dirección de Innovación Digital (DDI) de la CIA. El DDI es uno de los cinco mayores directorados de la CIA.



Según las filtraciones, la CIA se centraba en la creación de virus y malware usados para la obtención de información y pirateo de dispositivos como cualquier SmartTV, Smartphone (Androids y iPhones), sistemas operativos Windows, MacOS, Solaris y Linux, aplicaciones como WhatsApp, Signal, Telegram, Weibo, Confide y Cloackman…
Lo último de todo, ha sido el control remoto de los coches, la evasión de antivirus, la conversión de dispositivos electrónicos a micrófonos…

Herramientas de hacking a destacar:
CouchPotato, Weeping Angel, Athena, Grasshopper, Archimedes, Pandemic, ELSA, OutlawCoutry, BothanSpy y Gyrfalcon, Dumbo.

5. Cronología de Vault 7

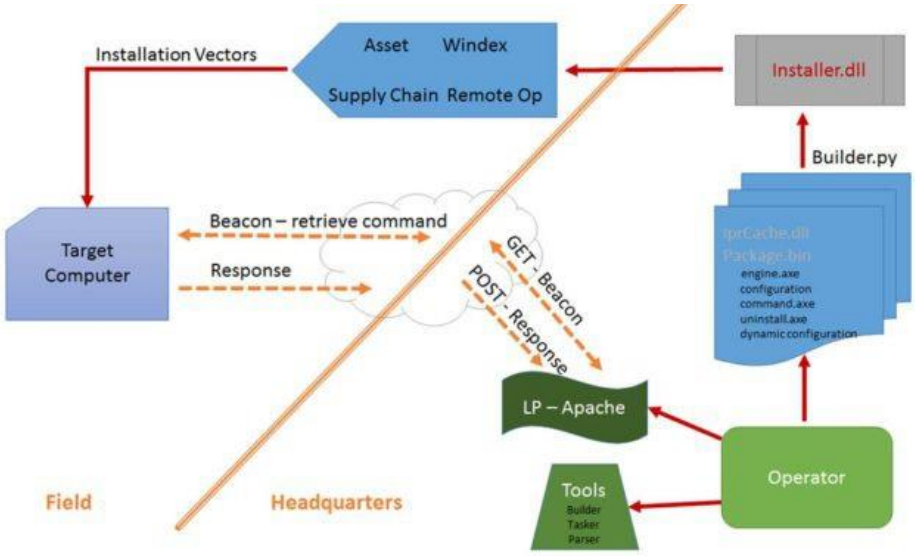
- ***7 de marzo:*** técnicas de espionaje de diversos dispositivos electrónicos.
- ***23 de marzo:*** técnicas para hackear dispositivos Apple (**Dark Matter**).
- ***31 de marzo:*** herramienta para ocultar hackeos (**Marble Framework**).
- ***7 de abril:*** documentos que describen una aplicación para crear malware para Windows (**Grasshopper**).
- ***14 de abril:*** guías de malware para controlar diversos dispositivos (**Hive**).
- ***21 de abril:*** herramienta de espionaje de televisores Samsung (**Weeping Angel**).
- ***28 de abril:*** información para el espionaje de documentos de Microsoft Office (**Scribbles**).
- ***5 de mayo:*** técnicas para hackear redes de área local LAN (**Archimedes**).
- ***12 de mayo:*** guías de usuario de dos malwares para sistemas operativos Windows (**AfterMidnight y Assassin**).
- ***19 de mayo:*** herramienta que permite el control remoto (**Athena**).
- ***1 de junio:*** herramienta para suplantación de código (**Pandemic**).
- ***15 de junio:*** herramienta para monitorear la actividad de internet (**Cherry Blossom**).
- ***22 de junio:*** documentos que describen varias herramientas de encuestas (**Brutal Kangaroo**).
- ***28 de junio:*** documentos sobre una herramienta de localización geográfica (**Elsa**).
- ***30 de junio:*** documentos de herramienta de redirección de tráfico en Linux (**OutlawCountry**).
- ***6 de julio:*** herramienta para interceptar y filtrar credenciales de SSH (**BothanSpy**).
- ***13 de julio:*** aplicación de Android de redireccionamiento de mensajería (**Highrise**).
- ***19 de julio:*** explorador tecnológico de análisis de ataques (**UCL / Raytheon**).

- ***3 de agosto:*** herramienta para suspender procesos mediante webcams y corrupción de video (**Dumbo**).
- ***10 de agosto:*** es une herramienta remota para la recopilación contra flujos de video (**CouchPotato**).
- ***24 de agosto:*** documentos que muestran operaciones contra servicios de enlace (**ExpressLane**).
- ***31 de agosto:*** herramienta de implantes en el sector de arranque (**Angelfire**).
- ***7 de septiembre:*** documentos sobre un sistema de control de misiles (**Protego**).

6. Vault 7 en Windows

Uno de los sistemas operativos más afectados ha sido Windows, para el que se habían creado diversos programas y herramientas para su infección y control. En este caso, los malwares pueden estar en dispositivos USB, CD, DVD, en áreas cubiertas en los discos o en sistemas para ocultar datos de imágenes. Además, realizan ataques contra las redes de Internet y sus servidores a través de la Network Devices Branch (Red del Sistema de Dispositivos) de la CIA. Entre estas herramientas destacan las siguientes:

- **Athena**
  Es una herramienta (spyware), que, una vez instalada, infecta el equipo y permite controlarlo de manera remota (configuración y control de tareas, así como la carga y descarga de código malicioso para realizar tareas específicas), con lo que se pueden realizar todo tipo de acciones. En este caso, la CIA enviaba todos los datos obtenidos de manera remota a un servidor propio. Manual de uso de Athena: https://wikileaks.org/vault7/document/Athena-v1_0-UserGuide/



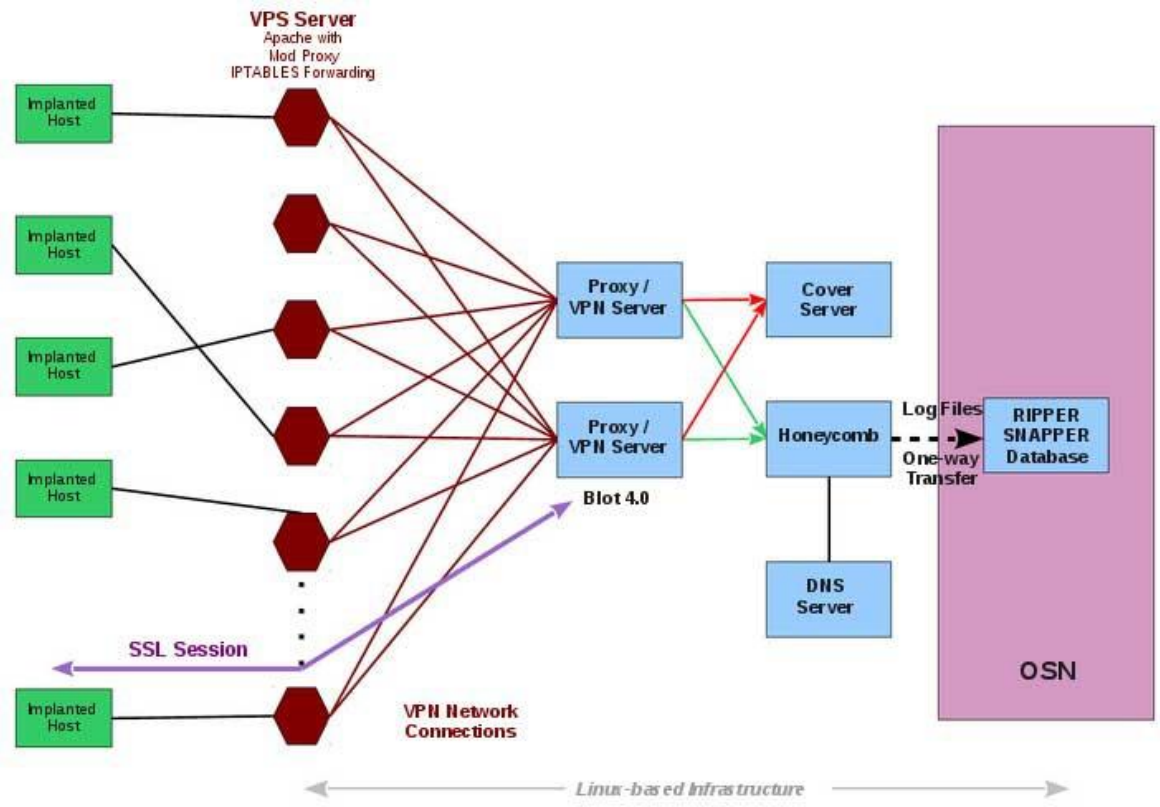
Demostración de us

- **Hive / Project Hive**

  Es un componente usado para controlar de manera remota el malware con el que la CIA infectaba ordenadores. Se envían una serie de comandos a ejecutar, y se recibía información robada, enviada desde dicho equipo.

  La herramienta estaba diseñada para ser indetectable**.** La comunicación se hacía a una página web pública falsa que a su vez daba lugar a una comunicación de varias capas a través de un VPN para evitar conocer el destino de la información. En el caso de que un usuario se topase por accidente con la página web de comunicación, su aspecto era el de una web normal y no daba pista a imaginar que pudiera ser de la CIA.

  Para evitar ser detectado por administradores de red, el malware usaba certificados digitales falsos. Entre ellos se incluía un certificado falso para el antivirus Kaspersky, que pretendía estar firmado por Thawte Premium Server CA. Es por ello, por lo que si un usuario o una empresa infectada por el malware analiza el código que sale de su ordenador o red, es fácil que atribuya los datos filtrados a entidades como Kaspersky en lugar de la CIA.



Funcionamiento

- **AngelFire**

  Es un malware que tiene la capacidad de cargar y ejecutar implantes personalizados que alteran el sector de arranque e instalan nuevos virus. Está formado por cinco componentes:

  1. ***Solartime:*** modifica el sector de arranque de Windows para ejecutar Wolfcreek cada vez que se inicia el sistema.
  2. ***Wolfcreek:*** driver del kernel cargado en el inicio del sistema y que sirve para cargar el resto de componentes una vez iniciado el sistema.
  3. ***Keystone:*** componente que mediante inyección de DLL ejecuta aplicaciones maliciosas directamente en memoria, sin que lleguen al disco duro.
  4. ***BadMFS:*** sistema de ficheros encubierto que se instala en espacio no particionado del disco duro de la víctima y almacena todos los drivers e implantes de Wolfcreek inicia.
  5. ***Windows Transitory File System:*** nuevo método para instalar AngelFire que permite al operador de la CIA crear ficheros temporales para tareas específicas en lugar de dejar dichos ficheros en el disco de la víctima.

- **Pandemic**

  Es una herramienta utilizada en ordenadores Windows que comparten archivos y programas dentro de una red local. Cuando el usuario descarga un archivo de ese ordenador infectado, Pandemic reemplaza el código del programa que se está descargando en tiempo real con una versión que incluye el troyano en su interior.

  Para ocultar su actividad, el archivo original en el servidor no es modificado en ningún momento, sino que se reemplaza en pleno tránsito de datos.

  A través de la ejecución del malware, se van infectando consecutivamente ordenadores en la red local.

  - For example: The targeted file is Pexplorer.exe, size 4.5 MB. The replacement file is NOTEPAD.exe, size 67 KB. If the remote user copies down pexplorer.exe to a local folder with that same file name, Windows will ask the user if they wish to overwrite/cancel the copy. When it does this, it will say that the size of the remote copy is 4.5 MB. However, after the operation is complete, the user will have only downloaded the replacement PE file of size 500 KB.

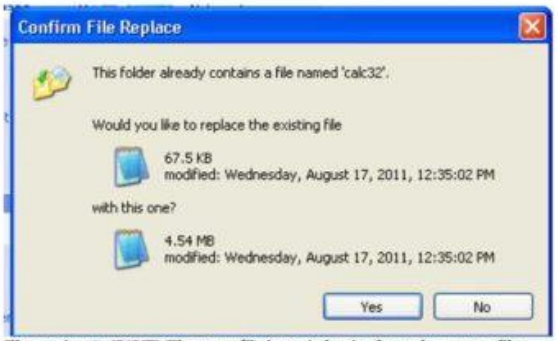


Illustration 1: (S//NF) The same file is copied twice from the remote file share to the user's local disk. As you can see, the file size Windows reports is vastly different, even if the user only gets the smaller replacement file

7. Conclusión

Estamos constantemente en peligro desde todos lados, no podemos fiarnos de nadie y tenemos que estar en todo momento precavidos y en alerta. Cualquier cosa que nos parezca extraña debemos evadirla y tenemos que tener mucho cuidado con lo que hacemos, donde lo hacemos, los datos que aportamos, la información que almacenamos, dónde la almacenamos es fundamental y cómo la protegemos.

Hoy en día, con la continua evolución y avances de la tecnología, nos exponemos cada vez más a atacantes del mundo "externo", y no solo a aquellos que pensábamos que eran los "malos", sino que ahora nos hemos dado cuenta que también a aquellos que "por fuera eran buenos" y que resultaron ser peores que los "malos".

En definitiva, todo esto está movido y apoyado por grandes empresas, agencias, política, ejército, grandes países y estados…, mayoritariamente por razones de negocio aunque también importantes razones personales.

8. Referencias

- https://www.mentealternativa.com/vault7-wikileaks/
- https://www.elperiodico.com/es/internacional/20170307/la-ultima-filtracion-de-wikileaks-en-claves-5882410
- https://wikileaks.org/ciav7p1/
- https://wikileaks.org/vault7/?
- https://actualidad.rt.com/actualidad/232744-vault-7-wikileaks-armas-ciberneticas-cia
- https://cybermedios.org/2017/03/22/filtraciones-de-la-cia-vault-7-todos-los-archivos-hasta-el-momento-2-gigas/
- https://es.wikipedia.org/wiki/Vault_7
- http://www.computing.es/seguridad/opinion/1097445002501/vault-7-files-tentaculos-del-ciberespionaje.1.html
- http://www.teinteresa.es/tecno/Vault-espionaje-CIA-revelado-WikiLeaks_0_1770422990.html
- https://resumen.cl/articulos/vault-7-las-herramientas-de-hackeo-de-la-cia-son-reveladas-por-wikileaks
- http://blog.smartekh.com/hackeo-cia
- https://nakedsecurity.sophos.com/es/2018/05/17/cias-vault-7-mega-leak-was-an-inside-job-claims-fbi/
- https://intereconomia.com/tecnologia/malware-la-cia-rastrea-la-localizacion-los-ordenadores-atacados-20170628-1646/
- https://www.csirtcv.gva.es/es/noticias/nuevo-framework-de-hackeo-de-la-cia-publicado-por-wikileaks-vault7.html
- https://www.adslzone.net/2017/05/19/athena-asi-puede-acceder-la-cia-casi-cualquier-pc-del-mundo-de-manera-remota/
- https://www.adslzone.net/2017/11/10/wikileaks-cia-malware-hive/
- https://computerhoy.com/noticias/software/cia-recibia-ayuda-empresas-crear-malware-segun-wikileaks-65353
- https://computerhoy.com/noticias/software/wikileaks-saca-luz-angelfire-otro-malware-cia-windows-67295
- https://www.adslzone.net/2017/06/02/pandemic-el-malware-de-la-cia-que-convierte-tu-pc-en-una-maquina-de-ataque/
- https://www.hackread.com/wikileaks-cia-windows-pandemic-malware/
- http://www.zonavirus.com/noticias/2017/pandemic-el-virus-creado-por-la-cia.asp