Vault 7-WikiLeaks y Wannacrypt0r

Ingeniería de Servidores

Doble Grado en Ingeniería Informática y Matemáticas
ETSIIT, Universidad de Granada

Resumen

Hasta ahora, toda nuestra interacción con los computadores y programas ha venido determinada únicamente por el mero hecho de la funcionalidad. Hemos basado nuestros sistemas de comunicación como Internet únicamente en el aspecto funcional, sin tener la precaución suficiente en temas de privacidad, vulnerabilidades y seguridad informática en general. Este punto puede provocar que nuestros servicios web, servicios de almacenamiento de ficheros o aplicaciones profesionales fallen, liberen información confidencial y con ello expongan a nuestra empresa.
WikiLeaks ha puesto a disposición de todos una serie de vulnerabilidades y herramientas que han sido supuestamente empleadas por agencias de inteligencia como la CIA, el FBI y la NSA. Entre estas vulnerabilidades ha destacado recientemente un fallo de seguridad del protocolo SMB que ha infectado numerosos equipos con un ransomware llamado Wannacrypt0r. Este fallo ha tenido a muchas empresas en una situación difícil, entre ellas podemos mencionar a Telefónica, Renault o a Iberdrola.

1. Releases Vault 7

1.1. Scribbles

El 28 de Abril de 2017 tuvo lugar la publicación de la release 'Scribbles' [29]. Estos documentos liberados por WikiLeaks hacen referencia a un proyecto de la CIA sobre marcas de agua en documentos. Este procedimiento indica cómo insertar 'Web beacon tags' dentro de un documento. Estas etiquetas son consideradas por la EFF como un bug que provoca un fallo de seguridad hacia el usuario. Estas etiquetas pueden camuflarse, incluso aparecer invisibles dentro de los documentos por lo que pasarían inadvertidas ante los usuarios. Las etiquetas tienen la función de monitorizar quién está leyendo un documento [31].
Según WikiLeaks y la documentación del proyecto Scribbles ha sido útil sobre todo en las versiones de Microsoft Office 97-2016. Este fallo de seguridad afectaría a los documentos creados con esta suite ofimática, por contra no se garantiza el funcionamiento bajo documentos OpenOffice o LibreOffice ya que estos procesadores de texto podrían revelas las etiquetas al usuario y así poder evitarlas.
Cabe además destacar que este procedimiento se conoce desde el 1 de marzo de 2016 y no se pretendía liberar hasta (como mínimo) 2066.

1.2. Weeping Angel

Weeping Angel fue publicada el 21 de Abril de 2017. Esta release trata sobre la herramienta con el mismo nombre que disponía la CIA [30]. Esta herramienta estaba diseñada para la serie F de las televisiones inteligentes de Samsung. Esta herramienta es una extensión de otra herramienta diseñada en un inicio por el MI5/BTSS tras compartir estos equipos de inteligencia sus conocimientos con la CIA.
La herramienta hace uso de un conjunto de vulnerabilidades y puertas traseras para emplear remotamente los elementos hardware de las televisiones para espiar a los usuarios. Entre otras cosas algunas televisiones de la serie F disponen de micrófono, elemento usado por Weeping Angel para realizar escuchas.

1.3. Hive

HIVE [27] fue publicada el 14 de abril de 2017. Se trata de toda una infraestructura malware back-end con una interfaz de acceso público HTTPS usada por la CIA para transferir información de ciertas máquinas a la CIA y recibir comandos de sus operadores para ejecutar tareas específicas en dichas máquinas. HIVE es utilizado a través de múltiples softwares maliciosos y operaciones de la CIA. La interfaz pública HTTPS utiliza zonas poco sospechosas para así ocultar su presencia. Tiene dos funciones principales: monitorización de los usuarios y shell interactiva.

Se puede encontrar una descripción de esta infraestructura back-end en [2], donde se dice que para servidores C&C (Command and Control), se configuran dominios específicos y direcciones IP para cada objetivo. Estos dominios parece que son registrados por los atacantes, pero en realidad se usan servicios de privacidad para ocultar su identidad real. Las IPs provienen de compañías que ofertan VPS o servicios de webhosting. El malware se comunica con los servidores C&C a través de HTTPS usando un protocolo de criptografía para impedir la identificación de las comunicaciones.

1.4. Grasshopper

El 7 de abril de 2017, WikiLeaks publicó la release Grasshopper [26], una plataforma usada para confeccionar la parte maliciosa del malware para sistemas operativos Windows.
Grasshopper se nutre de múltiples módulos que pueden ser usados por los operadores de la CIA como bloques para construir un implante personalizado que se comportará de forma diferente, por ejemplo manteniendo persistencia en un computador, dependiendo de qué particularidades o capacidades sean seleccionadas en el proceso de construcción. Adicionalmente, Grasshopper ofrece un lenguaje muy flexible para definir reglas usadas para supervisar el dispositivo objetivo, de forma que el payload solo se instala si el objetivo tiene la configuración correcta, por ejemplo, si el computador ejecuta una versión de Windows específica, o si tiene un antivirus en concreto.
Grasshopper ofrece herramientas usando ciertos mecanismos de persistencia y modificados a través de extensiones. Uno de los mecanismos de persistencia utilizados por la CIA es 'Stolen Goods', cuyos componentes fueron tomados del

malware Carberp, un rootkit ruso, confirmando el supuesto reciclado de malware encontrado por la CIA. 'El código fuente de Carberp fue publicado en Internet y no ofrece dificultades para robar cualquiera de sus componentes'.

1.5. Marble Framework

El 31 de marzo de 2017, WikiLeaks revela Marble [28]; 676 líneas de código fuente del Framework Marble, perteneciente a la CIA. Marble se usa para obstaculizar el trabajo de los investigadores forenses y las compañías antivirus y así evitar atribuir virus, troyanos y ataques a la CIA.

Marble lleva a cabo ésto escondiendo fragmentos de texto usados en los malwares de la CIA. Además, el código fuente muestra que Marble no solo tiene pruebas de ejemplo en inglés, también tiene en chino, ruso, coreano o árabe.

1.6. Dark Matter

EL 23 de Marzo de 2017, WikiLeaks revelaba 'Dark Matter' [25], que contiene documentación sobre ciertos proyectos de la CIA para infectar el firmware de los computadores Mac de Apple (dicha infección persiste aún reinstalando el sistema). Estos documentos explican los técnicas usadas por la CIA para ganar 'persistencia' en los dispositivos Apple, incluyendo Macs y iPhones y demostrando su uso de malware en EFI/UEFI y firmware.

A parte de otros, estos documentos revelan que se trata de un mecanismo para ejecutar código en los dispositivos periféricos mientras que el portátil Mac, o el PC, se está iniciando, permitiendo al atacante iniciar su software malicioso por ejemplo desde un USB aunque la contraseña del firmware esté activa.

'DarkSeaSkies' es un implante que persiste en el firmware EFI del MacBook Air de Apple. Este malware contiene a DarkMatter, realizando inyecciones o implantes en el espacio de EFI, kernel y del usuario.

2. Obtención de información de Wikileaks

Actualmente podemos obtener mucha información acerca de Vault 7 y las releases que se han hecho hasta la fecha. Cabe destacar que conforme van pasando los días se van publicando nuevas releases y archivos con vulnerabilidades.
Para empezar podemos leer la nota de prensa que publicó WikiLeaks con motivo de la revelación de Vault 7 [32]. En esta nota de prensa se explica con carácter general el motivo de la liberación del contenido de Vault 7 y qué contiene. Así mismo podemos encontrar en esa página un breve análisis, ejemplos y un apartado de preguntas frecuentes. Este apartado sirve como introducción al repositorio de documentos.
También disponemos de las subsecciones que hemos resumido con anterioridad. Cada subsección tiene su propia página que nos resume qué podemos encontrar y qué vulnerabilidad o ataque liberan en esa release. También disponemos, a parte de los resúmenes, de los documentos que conforman, explican y escenifican la vulnerabilidad o ataque que protagoniza la release [35]. Dentro de estos

documentos podemos encontrar guías de usuario, explicaciones extensas del fallo e incluso ejemplos de los ataques.
Estas secciones explicadas anteriormente conforman las vulnerabilidades más grandes y representativas pero disponemos aún de un repositorio más grande que contiene el resto de información de Vault 7. Este repositorio está formado por los ataques y fallos descubiertos por la comunidad y que han sido dados a WikiLeaks. Estos fallos pueden contener más o menos información pero al menos se nos informa de en qué consiste dicha vulnerabilidad. Además contiene más información sobre las releases principales de Vault 7 [33].
Cabe mencionar al menos que para subir un fichero a WikiLeaks necesitaremos Tor. En su página web disponemos de una opción llamada 'Submit' que nos redirigirá a una página web que nos indica que debemos usar Tor y nos proporciona un enlace Onion [34]. Si abrimos este enlace en el Tor-Browser nos dará un formulario que podemos rellenar indicando el material que tenemos así como diferentes cuestiones que permiten identificar la información y comprobar su veracidad [36].

3. Obtención de información de Wannacrypt0r

En el caso de Wannacry, al estar muy reciente el hecho, hemos tenido que hacer una investigación del malware y su funcionamiento por nuestra cuenta. Hemos querido investigar varios factores como el funcionamiento, cómo podemos desactivarlo con las herramientas que existen actualmente en desarrollo y qué información podemos obtener en sí del fichero ejecutable.
En primer lugar tuvimos que obtener una muestra del malware fiable. Nuestra muestra fue obtenida de un Gist en GitHub que contenía información del malware [6]. Comprobamos mediante una plataforma fiable como Virus Total que el código MD5 de la muestra que habíamos obtenido estaba catalogado como Wannacry en su base de datos.
Tras esto ya podemos empezar a trabajar con el malware. Para cerciorarnos de que nuestras máquinas no sufrían daños ni se veían afectadas por el malware decidimos probar el ransomware en una máquina virtual con Windows 7, ya que esta ha sido la plataforma más afectada y se especula que se desarrolló pensando en la misma. Por motivos de seguridad deshabilitamos cualquier adaptador de red de la máquina virtual ya que esto podía hacer que infectásemos equipos Windows dentro de la misma red que aún no tuvieran el parche. Al tener los adaptadores de red desactivados también evitamos que el malware se desactive al comprobar su KillSwitch (Ver 4.5). Así mismo por precaución debemos eliminar cualquier carpeta compartida que hayamos creado, sacar cualquier disco virtual que hayamos introducido y deshabilitar el portapapeles compartido y la función de arrastrar y soltar. Gracias a toda la configuración podemos estar seguros de que contendremos el malware dentro de la máquina virtual y no infectará ni encriptará nuestro sistema. Somos conscientes de que utilizar una máquina virtual podría haber llevado a problemas ya que no funciona como un 'sandbox', de todos modos y tras realizar varias pruebas hemos concluido que el malware no explota ninguna vulnerabilidad que le permita infectar la máquina anfitriona desde la máquina virtual.
Una vez establecidos todos los patrones de seguridad hemos querido obtener las cadenas embebidas dentro del fichero ejecutable. Para ello hemos creado

por seguridad una nueva máquina virtual con una distribución GNU/Linux con configuración idéntica a la máquina anterior. De este modo nos ahorramos trabajar con el malware en nuestra máquina e infectarla por error. Dentro de esta máquina virtual hemos ejecutado el comando 'strings' sobre nuestra muestra. De aquí hemos obtenido información como el KillSwitch, las plataformas sobre las que funciona y varios nombres de librerías que emplea.
Para deducir el funcionamiento de Wannacry lo hemos probado en la máquina con Windows 7 que describimos anteriormente. Gracias a esto hemos podido observar 'in situ' los ficheros que se crean, el mensaje de alerta del ransomware y la manera en que encripta los archivos (Ver 4.2)
Para desactivarlo hemos probado varias herramientas citadas en el apartado 4.5. Hemos podido concluir que las herramientas que actualmente están desarrolladas no funcionan de manera estable y los ficheros pueden no ser recuperados. Entre las herramientas probadas hemos podido ver que la que mejor resultado nos otorga es un script realizado en PowerShell por la empresa Eleven Paths [7].

4. Wannacry

4.1. Definición de ransomware

Podemos definir el ransomware como un tipo de malware que secuestra la máquina del usuario afectado con diversas técnicas pidiendo un rescate para poder recuperarla [14]. Los ransomware modernos y los más comunes suelen encriptar el ordenador o dispositivo consiguiendo con ello que los datos no estén disponibles para el propietario.
Para poder recuperar la máquina se utilizan diversos métodos pero por regla general se emplean métodos de pago que no puedan ser rastreados como los Bitcoins [3]. Gracias a esto los atacantes reciben dinero a través de operaciones monetarias a una cuenta anónima siendo las operaciones no rastreables.
Con esto se produce una extorsión hacia el usuario, ya que normalmente si no se paga antes de un periodo establecido los archivos son borrados. Esto produce pérdidas de información no sólo a particulares sino a grandes empresas y PYMES. Este tipo de ataque representa un problema cuando no se tienen mecanismos de copia de seguridad para prevenir pérdidas de información. Actualmente este es uno de los tipos de malware más común teniendo numerosos ejemplos como Reveton, CryptoLocker, CryptoWall o Wannacry [5].

4.2. Funcionamiento de Wannacrypt0r

Dado que WannaCrypt es un ransomware, su funcionamiento está basado en la encriptación o cifrado del sistema de archivos del terminal infectado, o parte de él, de forma que el usuario es incapaz de acceder a su información (dando lugar a la extorsión, chantaje o rescate). Para conseguirlo, los desarrolladores del malware han aunado los dos tipos de cifrado que existen, simétrico y asimétrico, dando lugar a lo que se conoce como cifrado mixto, aprovechando los puntos fuertes de ambos cifrados y solapando sus debilidades. En el caso del cifrado simétrico, el proceso de cifrado es muy rápido pero la clave que desencripta supone un problema, ya que debe mantenerse a buen recaudo para que el malware

surta efecto y no es fácil. Por el contrario, el cifrado asimétrico, con el paradigma clave pública-privada solventa los problemas con la clave, pero la encriptación es muy lenta (debido a los algoritmos matemáticos necesarios para generar claves tan beneficiosas).

El procedimiento seguido por WannaCrypt es el siguiente: el software, al ejecutarse, comienza a encriptar con cifrado simétrico los archivos de las carpetas (Temp, por ejemplo, no es cifrada). Las claves de ese cifrado simétrico son, a su vez, cifradas con cifrado asimétrico, de forma que se genera una clave pública que encripta y una privada que desencripta. Esa clave privada es enviada a un servidor, totalmente desconocido para el usuario, que guarda la clave. En la práctica, la hace desaparecer. Si el computador infectado no estuviera conectado a la red, la clave privada permanece en el mismo.

Hemos comprobado, con nuestros experimentos sobre máquinas virtuales, que no se encriptan todos los archivos ni todas las carpetas. Además, aquellos que sí son encriptados son movidos a otros directorios del sistema de archivos, generando así un caos sin precedentes.

En [1] se puede ver la explicación de estos procedimientos por parte de un profesor de la Universidad de Nottingham

4.3. Plataformas afectadas y tipos de contagio

Este ataque ha sido programado y planificado para atacar máquinas ejecutando los sistemas operativos de Microsoft, tanto en sus versiones de escritorio como en sus versiones de servidor [4]. Entre las versiones afectadas encontramos: Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows 10, Windows Server 2012 R2, Windows Server 2016, Windows XP, Windows 8.
La versión más problemática de la lista es Windows 7 que aún siendo una versión ya antigua de Windows tiene actualmente el 48.5 % de cuota de mercado [13], lo que hace que la mayoría de las personas que han sido infectadas con Wannacry estuvieran ejecutando Windows 7.
Al igual que la mayoría de ransomware se instala en la máquina afectada a través de correos electrónicos con ficheros maliciosos. Estos ficheros pueden ser hojas de cálculo con programas embebidos, archivos PDF o directamente ficheros ejecutables. En este proceso se aprovechan vulnerabilidades o puertas traseras que permitan a los atacantes introducir su malware en los formatos mencionados anteriormente [15].
Tras esta infección inicial los atacantes utilizan una vulnerabilidad conocida del protocolo SMB para continuar la infección dentro de la red local [10]. Este protocolo se utiliza para compartir ficheros entre máquinas Windows dentro de la misma red [9]. La vulnerabilidad permite ejecutar código remoto en otra máquina de la misma red pudiendo de esta manera los atacantes ejecutar el binario de Wannacrypt0r en el resto de máquinas de la red para infectarlos a todos.

4.4. Expansión del virus a través de SMB

Tal y como se cita en [22], los ransomware no se suelen extender rápidamente. Amenazas como WannaCrypt utilizan normalmente emails como vector del ataque, dejando a los usuarios la descarga y ejecución de los archivos maliciosos (de forma camuflada). Sin embargo, en este caso, los desarrolladores del malware usaron el código del exploit de la vulnerabilidad SMB 'Eternal Blue', (SMBv1, que permite a atacantes remotos ejecutar código a través de paquetes). Esta vulnerabilidad fue resuelta en el boletín de seguridad de Microsoft 'MS17-010' ([23]), publicada el 14 de marzo de 2017.

El código usado por WannaCrypt fue diseñado para trabajar con todos los sistemas operativos Windows, aprovechándose de que la mayoría de ellos han permanecido vulnerables al fallo de SMB. Cabe destacar que no todos los sistemas operativos han sufrido el ataque con la misma virulencia, ya que por ejemplo Windows 10 dispone de un sistema forzoso de actualizaciones a menos que sea desactivado por el usuario. Esto ha hecho que dicha versión se haya parcheado mucho antes y con mayor efectividad.
No se han encontrado pruebas concluyentes sobre cuál fue el primer detonante del malware, pero existen dos escenarios posibles:

- A través de emails diseñados para que los usuarios ejecutaran el malware y activan el contagio con el exploit SMB.
- Contagio a través del exploit SMB cuando un computador sin parche de seguridad está conectado a otras máquinas infectadas.

4.5. Killswitch, situación actual de Wannnacry

En la programación del malware Wannacrypt0r se pensó en el momento en que se requiriera parar el ransomware completamente y con ello desactivarlo. Este procedimiento ha sido llamado por algunos expertos como 'KillSwitch'.
El malware, al ejecutarse en la máquina atacada, lo primero que realiza es comprobar un dominio que en un principio no se encontraba registrado. Este dominio puede ser extraído de diferentes maneras del binario. Para poder extraer la información en este caso podemos utilizar herramientas como 'string', 'pestr' o incluso Wireshark. Con las dos primeras herramientas podemos obtener cadenas de texto que se encuentran directamente en el fichero ejecutable. Al hacer esto podemos observar una única referencia web en texto plano que resultó ser el llamado 'KillSwitch'. El otro modo de obtener dicha dirección es con un sniffing de la red para ver con qué dominios y servidores se comunica el malware.
Este proceso fue realizado por un forense informático que también dirige un blog famoso sobre malware [11]. Tras darse cuenta de la existencia de este dominio introducido dentro del binario lo registró para ver si ocurría algo y con ello paró la extensión de Wannacry [12].
Actualmente el malware continúa expandiéndose pero no con su versión original que ya ha sido desactivada. Se están realizando copias de dicho ransomware eliminando el KillSwitch y realizando variantes, incluso pidiendo más dinero [16]. Así mismo ya disponemos de información obtenida del malware [6] y de ciertas herramientas en desarrollo para revertir el proceso de encriptado como

la desarrollada por Eleven Paths(Telefónica) [7] o por usuarios anónimos de GitHub [8].

4.6. Relación con Wikileaks y beneficios obtenidos

Las reacciones de Microsoft sobre WannaCrypt no se hicieron esperar. La compañía hizo una petición a todos los gobiernos del mundo para ver el ciberataque global como una 'llamada de atención', como así asegura la nota de prensa de la agencia EFE en [24]. En palabras de Brad Smith, presidente y asesor legal de Microsoft, 'Hemos visto aparecer en WikiLeaks vulnerabilidades almacenadas por la CIA, y ahora estas vulnerabilidad robada a la NSA ha afectado a clientes en todo el mundo'. De aquí podemos extraer que WikiLeaks filtró dicho fallo de seguridad y los atacantes la usaron para así confeccionar su malware.
En [17] se pueden encontrar las posibles cuentas de Bitcoins que los secuestradores establecieron para cobrar los rescates ([19],[18],[21],[20]). En ellas se muestra que han podido cobrar alrededor de 139,85063858 BTC, lo que hace un total de 280590,94€

5. Conclusiones

Como hemos podido comprobar a lo largo de este trabajo la seguridad informática afecta tanto a usuarios como a servidores y empresas. Este hecho hace que debamos establecer reglamentos internos de seguridad, políticas de seguridad y prevenir las infecciones en nuestros entornos de trabajo y personal.
En el caso de los servidores y las empresas debemos de mantener copias de seguridad con periodicidad que nos permitan recuperar el flujo de trabajo y la información de manera rápida ante un ataque o un fallo. Asimismo debemos formar a nuestro personal de cualquier ámbito para saber qué archivos se pueden abrir con un ordenador de la empresa y cómo deben operar con los archivos que quieran abrir. Esto puede incluir usar por ejemplo versiones de programas para leer documentos que sepamos que son menos propensas a fallos de seguridad.
Estas políticas de seguridad podrían haber prevenido a muchas empresas de perder su información por culpa del ransomware tratado a lo largo de este trabajo. En el caso de haber sido infectado hubiera sido tan sencillo recuperarse del ataque como cargar la copia de seguridad disponible y continuar con el ritmo de trabajo. Esto puede hacernos perder alguna información, pero siempre es preferible esto antes que perder todo lo recopilado hasta el momento.
De igual manera los protocolos de seguridad podrían haber prevenido a muchas empresas de infectarse con este malware. Los empleados deben estar formados y comprender los riesgos que puede conllevar abrir un email de una persona desconocida en nuestro puesto de trabajo o ejecutar y abrir ficheros que no hemos comprobado. Una política de seguridad clara es que no se deben ejecutar ficheros que se hayan recibido a través de correo electrónico de usuarios no confiables.
Por lo tanto podemos concluir que la seguridad informática es un campo de la empresa y el entorno laboral que no debemos dejar de lado. Las prevenciones en estos entornos son clave y van a conducir a la larga a un entorno de trabajo más seguro y estable.

Referencias

[1] https://www.youtube.com/watch?v=pLluFxHrc30&t=712s year =.

[2] https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7, Consultado el 10 de mayo de 2017.

[3] https://bitcoin.org/es/bitcoin-para-personas, Consultado el 20 de Mayo de 2017.

[4] https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/, Consultado el 20 de Mayo de 2017.

[5] https://es.wikipedia.org/wiki/Ransomware#Tipos_de_ransomware, Consultado el 20 de Mayo de 2017.

[6] https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168, Consultado el 20 de Mayo de 2017.

[7] https://github.com/ElevenPaths/Telefonica-WannaCry-FileRestorer, Consultado el 20 de Mayo de 2017.

[8] https://github.com/gentilkiwi/wanakiwi/releases, Consultado el 20 de Mayo de 2017.

[9] https://msdn.microsoft.com/es-es/library/windows/desktop/aa365233(v=vs.85).aspx, Consultado el 20 de Mayo de 2017.

[10] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx, Consultado el 20 de Mayo de 2017.

[11] https://www.malwaretech.com/, Consultado el 20 de Mayo de 2017.

[12] https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html, Consultado el 20 de Mayo de 2017.

[13] https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0, Consultado el 20 de Mayo de 2017.

[14] https://www.trendmicro.com/vinfo/us/security/definition/ransomware, Consultado el 20 de Mayo de 2017.

[15] http://www.elladodelmal.com/2017/05/el-ataque-del-ransomware-wannacry.html, Consultado el 20 de Mayo de 2017.

[16] http://www.lavanguardia.com/tecnologia/20170515/422588908726/wannacry-virus-variantes-infeccion-telefonica-nhs-nsa-windows.html, Consultado el 20 de Mayo de 2017.

[17] http://blog.elhacker.net/2017/05/ataque-masivo-de-ransomware-en-europa-rusia-wana-cryp
html, Consultado el 26 de mayo de 2017.

[18] https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn, Consultado el 26 de mayo de 2017.

[19] https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw, Consultado el 26 de mayo de 2017.

[20] https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94, Consultado el 26 de mayo de 2017.

[21] https://blockchain.info/es/address/1BANTZQqhs6HtMXSZyE2uzud5TJQMDEK3m, Consultado el 26 de mayo de 2017.

[22] https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/, Consultado el 26 de mayo de 2017.

[23] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx, Consultado el 26 de mayo de 2017.

[24] http://www.lavozdegalicia.es/noticia/tecnologia/2017/05/15/virus-wanna-cry-uso-herramienta-informatica-robada-nsa-estadounidense/00031494848110394179682.htm, Consultado el 26 de mayo de 2017.

[25] https://wikileaks.org/vault7/#Dark%20Matter, Consultado el 30 de Abril de 2017.

[26] https://wikileaks.org/vault7/#Grasshopper, Consultado el 30 de Abril de 2017.

[27] https://wikileaks.org/vault7/#Hive, Consultado el 30 de Abril de 2017.

[28] https://wikileaks.org/vault7/#Marble%20Framework, Consultado el 30 de Abril de 2017.

[29] https://wikileaks.org/vault7/#Scribbles, Consultado el 30 de Abril de 2017.

[30] https://wikileaks.org/vault7/#Weeping%20Angel, Consultado el 30 de Abril de 2017.

[31] https://w2.eff.org/Privacy/Marketing/web_bug.html, Consultado el 8 de Mayo de 2017.

[32] https://wikileaks.org/ciav7p1/index.html#PRESS, Consultado el 8 de Mayo de 2017.

[33] https://wikileaks.org/ciav7p1/cms/index.html, Consultado el 9 de Mayo de 2017.

[34] https://wikileaks.org/ciav7p1/cms/index.html#submit, Consultado el 9 de Mayo de 2017.

[35] https://wikileaks.org/vault7/document/, Consultado el 9 de Mayo de 2017.

[36] http://wlupld3ptjvsgwqw.onion/wlupload.en.html, Consultado el 9 de Mayo de 2017.