Buenas Prácticas
CCN-CERT BP-04/16

Ransomware

Marzo de 2017

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2017.03.23 20:19:50 +01'00'

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas del Sector Público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. INTRODUCCIÓN

Hoy en día, una de cada catorce descargas en Internet contiene una muestra de código dañino y dentro del amplio mundo de estos códigos dañinos o malware, el ransomware es una de las variantes más frecuentes, tanto en entornos corporativos como en entornos domésticos.

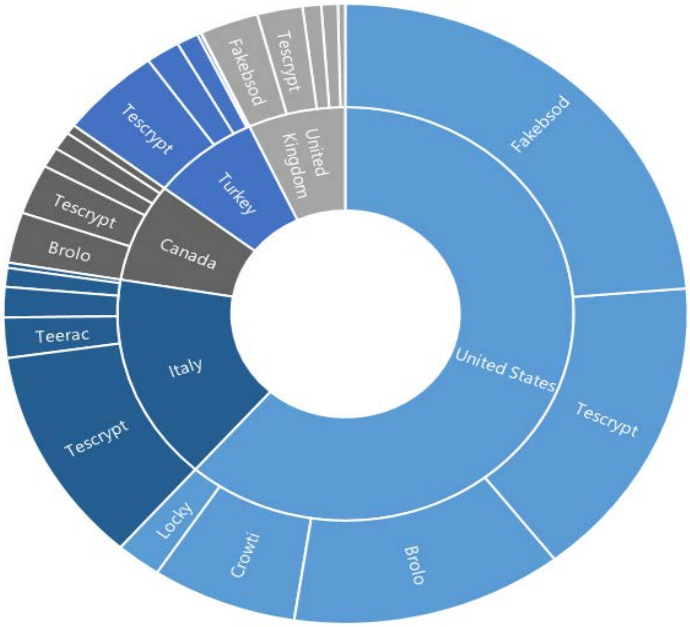


Figura 1.- Infecciones de Ransomware más significativas por países (2015-2016).

El objetivo de este tipo de código dañino es cifrar el mayor número posible de ficheros almacenados en la máquina de la víctima haciéndolo de tal manera que el usuario no se percate de lo que está sucediendo hasta que el sistema se encuentre comprometido. Una vez que ha terminado el proceso del secuestro de la información,

se informa de ello al usuario dándole instrucciones para el pago de un rescate (*ransom*, del inglés) a cambio de la recuperación de sus ficheros.

El comprometimiento del sistema se plasma generalmente en un nuevo fichero de texto que aparece en cada uno de los directorios cifrados, bien en forma de un llamativo fondo de escritorio con una nota de rescate o en una ventana persistente en la que se dan las instrucciones y los enlaces a seguir para realizar el correspondiente pago.

Figura 2.- Ejemplo de sistema infectado.

En casi todos los casos de ransomware, es común solicitar un pago no trazable para la recuperación de los ficheros. Este pago suele hacerse en criptomonedas[1] (***cryptocurrency***) como es el caso de **Bitcoin**[2].

Para evitar ser identificado, el secuestrador recibe el dinero del rescate a través de redes con un alto grado de anonimato, como puede ser el caso de la **red Tor**[3] (***The Onion Routing***). De esta forma, los cibercriminales consiguen no dejar rastro resultando casi imposible su localización.

En cuanto a los vectores de infección utilizados por este tipo de código dañino para comprometer los equipos de sus víctimas, hay que prestar especial atención a la navegación web y al empleo de correos electrónicos. De hecho, el Phishing[4] representa más de una cuarta parte del total de las infecciones por ransomware.

La razón de ser de esta guía de buenas prácticas es facilitar información, herramientas y procedimientos que permitan, en la medida de lo posible, evitar la infección por ransomware, recuperar los ficheros si hubiera fallado lo anterior y, en cualquier caso,

[1] Ver https://es.wikipedia.org/wiki/Criptomoneda
[2] Ver https://es.wikipedia.org/wiki/Bitcoin
[3] Ver https://es.wikipedia.org/wiki/Tor_(red_de_anonimato)
[4] El Phishing consiste en engañar al usuario haciéndole creer que se encuentra ante una página web o mensaje de correo electrónico legítimo con el objetivo de que, a través de él, entregue sus datos o se descargue algún tipo de software que, al final, resulta ser malicioso. Ver https://es.wikipedia.org/wiki/Phishing

crear un entorno suficientemente seguro para evitar futuras infecciones o minimizar los daños ocasionados por las mismas.

Frente a los ataques informáticos es necesario actuar, al menos, en cuatro (4) fases distintas: la prevención, la detección, la respuesta y la remediación del ataque. En esta guía se expondrán medidas que son aplicables a dichas fases.

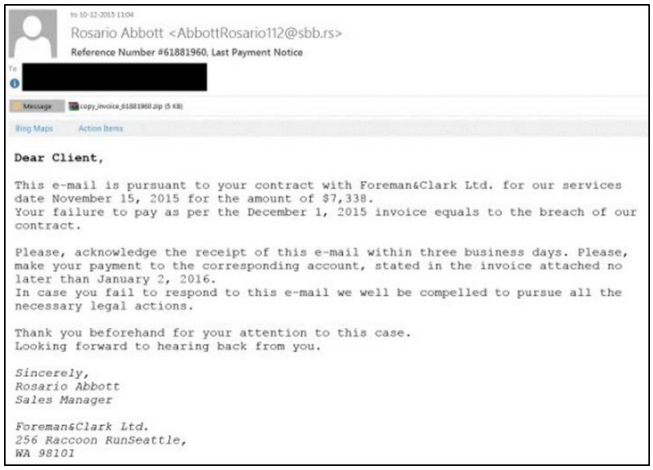
3. VECTORES DE INFECCIÓN

Para prevenir las infecciones, lo más conveniente es conocer el medio de entrada del malware, así como sus mecanismos de propagación. Sin embargo, en el mundo del código dañino, tras una infección no siempre es posible determinar con exactitud cual ha sido el origen o las causas de la infección.

Los mecanismos y posibilidades para que la infección se produzca son variados siendo importante conocer los vectores de infección más comunes. En algunos casos, el malware puede permanecer latente en el sistema durante cierto tiempo y manifestarse a raíz de una acción concreta o determinación de una fecha específica, lo cual hace difícil esclarecer con exactitud el momento de la infección.

3.1 Phishing mediante correo electrónico

Uno de los mecanismos de infección más frecuentes entre los distintos tipos de ransomware ha sido el correo electrónico, utilizando un mensaje aparentemente inocuo y legítimo.


Rosario Abbott <AbbottRosario112@sbb.rs>
Reference Number #61881960. Last Payment Notice

Dear Client,

This e-mail is pursuant to your contract with Foreman&Clark Ltd. for our services date November 15, 2015 for the amount of $7,338.
Your failure to pay as per the December 1, 2015 invoice equals to the breach of our contract.

Please, acknowledge the receipt of this e-mail within three business days. Please, make your payment to the corresponding account, stated in the invoice attached no later than January 2, 2016.
In case you fail to respond to this e-mail we well be compelled to pursue all the necessary legal actions.

Thank you beforehand for your attention to this case.
Looking forward to hearing back from you.

Sincerely,
Rosario Abbott
Sales Manager

Foreman&Clark Ltd.
256 Raccoon RunSeattle,
WA 98101

Figura 3.- Correo fraudulento empleado por TeslaCrypt.

Dentro del Phishing se pueden distinguir dos (2) formas de infección típicas, ya sea mediante el enlace a una página fraudulenta que oculta el código dañino en una aparente aplicación legítima o mediante un fichero especialmente manipulado que aparece adjunto al mensaje de correo.

3.1.1 Mediante enlace web

Este tipo de infección consiste en dirigir a la víctima hacia un sitio web que puede ser legítimo pero que los cibercriminales han alterado previamente "*troyanizado*" o que

puede ser una copia prácticamente idéntica, que resulta indistinguible de la versión legítima.

En ambos casos, la víctima invoca consciente o inconscientemente la descarga de una aplicación ejecutable, en principio no sospechosa, tras la cual se oculta el código dañino.

3.1.2 Mediante fichero adjunto

En este caso, el propio mensaje de correo electrónico lleva consigo un fichero semánticamente relacionado con el texto del mensaje y que bajo alguna excusa (falso informe bancario, formularios, imágenes, curriculum vitae, etc.) invita y consigue que la víctima lo abra, operación que desencadena la ejecución del código dañino.

Para obtener más información de como prevenir estas formas de infección, se aconseja consultar el informe BP-02-16 Buenas Prácticas en Correo Electrónico.

3.2 Navegación web

Este es el método de infección cuya popularidad está más en alza en los últimos tiempos. Consiste en aprovechar las vulnerabilidades de algunos componentes del navegador y los servidores que ofrecen las páginas web.

Los responsables de las campañas de ransomware, se encargan previamente de hacerse con el control de esos servidores y comprometer las páginas que ofrecen, incluyendo en ellas contenido dañino que explota las debilidades del navegador. De este modo, provocan que el navegador del usuario termine descargándose código binario que inmediatamente se ejecuta, iniciando el proceso de infección.

Para evitar este tipo de infecciones lo único que se puede hacer es utilizar la versión más actualizada del navegador y de sus extensiones. En principio, es recomendable tener bloqueados todos aquellos componentes que no sean estrictamente necesarios. Algunos de los *plugins* más utilizados son Flash Player, Java y Silverlight.

Uno de los principales problemas de los *plugins* es que aumentan significativamente la exposición a determinado tipo de ataques durante la navegación web. Algunos de estos *plugins* contienen un gran número de vulnerabilidades críticas que permiten a los atacantes ejecutar código en el equipo de la víctima.

Tan sólo hace falta que el usuario haga clic o navegue hasta una página dañina para que su equipo sea comprometido (sin necesidad siquiera de descargar o interactuar con la página en cuestión). La mayor parte de los navegadores permiten habilitar o deshabilitar los componentes instalados. Puede ser una buena opción, la de activar *plugins* de forma temporal como Flash y Java de manera controlada por el usuario.

Así mismo, conviene recurrir a complementos específicos para bloquear la apertura de pop-ups[5], iframes, ejecución de código JavaScript y anuncios (Ads). Todos esos mecanismos pueden ser utilizados para obligar al navegador a cargar páginas que pueden estar comprometidas o sirven para ejecutar código dañino.

Para obtener más información sobre como prevenir estas formas de infección, se aconseja consultar el informe BP-06-16 Buenas Prácticas en Navegadores Web.

[5] Ver http://es.ccm.net/faq/9996-bloquear-ventanas-emergentes-de-publicidad-pop-ups

4. DESINFECCIÓN

4.1 Identificar el Ransomware

Utilizando el servicio **NoMoreRansom**[6] se puede identificar a qué familia pertenece el código dañino que ha infectado el equipo y ha cifrado sus ficheros. Una vez conocida la identidad del malware, se puede intentar corregir el contratiempo que ha causado.

En este caso, la identificación del atacante se puede hacer facilitando un fichero cifrado por el mismo o enviando el fichero en el que se especifican las instrucciones de rescate. Ambos elementos son suficientemente esclarecedores como para saber si se trata de un atacante ya conocido.

4.2 Pasos a seguir después de la infección

En el caso de que se logre detectar la infección, lo primero que hay que hacer es **desconectar el equipo de la red**. La finalidad de este proceder es:

- Evitar que la acción de cifrado alcance al contenido alojado en las unidades de red accesibles desde el equipo infectado.
- Que el código dañino pueda contactar con su servidor de mando y control.

Dado que el cifrado precisa de la capacidad de cálculo del equipo infectado para su acción, por lo general, también es recomendable apagar el equipo.

Analizar que procesos se están ejecutando en el ordenador no suele ayudar en gran medida a diagnosticar lo que está pasando ya que, en la mayoría de los casos, el ransomware suele estar camuflado bajo la apariencia de un proceso legítimo como, por ejemplo, "*explorer.exe*". En caso de identificar el proceso que está accediendo masivamente al disco, hay que actuar sobre el mismo finalizándolo.[7]

Para ayudar a identificar el proceso malicioso, se puede usar la herramienta **Monitor de Recursos** de Windows. Para acceder a ella, basta con ejecutar "*resmon*" (tecla Windows + r).

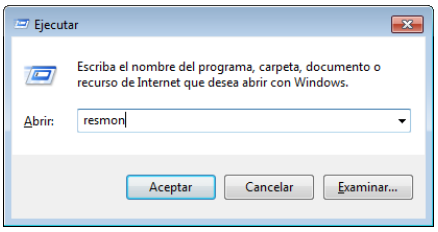


Figura 4.- Ventana del comando "ejecutar".

Dado que la operación de cifrado de los ficheros requiere tiempo de CPU y acceso a disco, estas características pueden utilizarse para identificar el proceso o aplicación que está realizando el ataque. La forma de hacerlo es fijarse en lo siguiente:

1) **Procesos de aplicaciones que realmente no se estén ejecutando**: si se observa que en la lista de procesos aparece uno con el nombre de una aplicación como, por ejemplo, "*notepad.exe*" o "*calc.exe*", y dicha aplicación realmente no está abierta, es muy probable que se trate de un proceso dañino disfrazado de aplicación inocua.

[6] Ver https://www.nomoreransom.org/
[7] Cerrar procesos con el Administrador de tareas, ver https://support.microsoft.com/es-es/kb/2499971

2) **Identificar procesos repetidos con diferente PID**[8]: si aparecen varias veces procesos con el mismo nombre, estos pueden ser identificados mediante su PID. Todos esos procesos deben depender de un proceso original y ser parte de su árbol de procesos. En el caso de que haya alguno fuera de ese árbol, probablemente se trate de un proceso dañino.

3) **Procesos con una gran cantidad de ficheros abiertos o con un excesivo uso de la CPU o del disco**: el proceso de cifrado es costoso en cuanto al consumo de recursos, por lo que el proceso atacante usará una gran cantidad de los mismos, sobre todo CPU y acceso a disco.

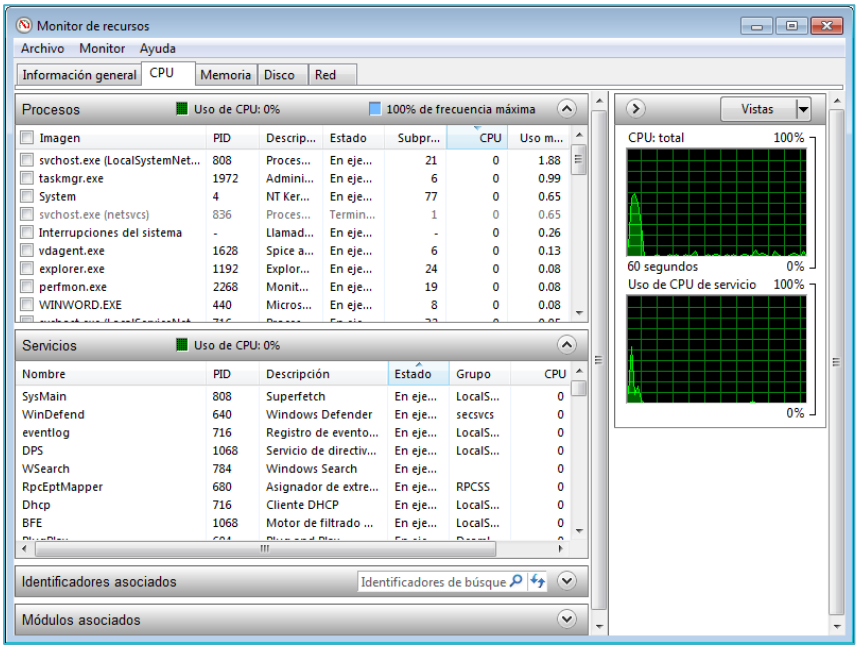


Figura 5.- Imagen del monitor de recursos en Windows 7.

4.3 Aspectos a tener en cuenta

4.3.1 El tiempo

Algunas variedades de ransomware utilizan el tiempo transcurrido después de la infección como un factor de presión para forzar el pago del rescate por parte de la víctima.

Lo más recomendable es utilizar ese margen de tiempo para ponerse en contacto con expertos y autoridades relacionadas con la ciberseguridad para obtener la mayor cantidad posible de información sobre casos de infecciones similares y consejos sobre como actuar en dichos casos.

4.3.2 Eliminación del código dañino

Por lo general, el objetivo principal del ransomware no es conseguir su persistencia en el equipo infectado, ya que la misma solicitud del rescate pone de manifiesto su presencia.

[8] PID, "Process ID": es un numero identificativo que es único y que representa a cada proceso en ejecución. Ver https://en.wikipedia.org/wiki/Process_identifier

Por esta razón, en la mayoría de los casos, su eliminación puede ser sencilla y suele haber herramientas de desinfección especialmente desarrolladas para tal fin y a disposición de las víctimas para que puedan eliminar el código dañino del dispositivo atacado.

4.3.3 Recuperación de ficheros

Una vez identificado el espécimen de ransomware que ha infectado el equipo, se pueden consultar sitios en Internet en los que se indica si, en ese momento, es posible o no la recuperación (descifrado) de los ficheros secuestrados.

Si tal recuperación es posible es gracias a herramientas desarrolladas por organizaciones tan variadas como Kaspersky[9], Intel Security, McAfee, Panda Security, Sophos, HitMan, compañías anti-malware, distintos centros de respuesta conocidos como CERT[10], equipos de investigación como **NoMoreRansom**[11], Fuerzas y Cuerpos de Seguridad del Estado nacionales e internacionales, foros especializados como **bleepingcomputer**[12] e investigadores y analistas de seguridad que liberan las claves maestras de forma pública y altruista, entre otros muchos.

Existe una utilidad, frecuentemente actualizada, que recopila información sobre todas las familias de ransomware conocidas (herramientas de recuperación, fechas de aparición, etc.). Se recomienda consultarla si se ha sido víctima de una infección con el fin de conocer toda la información disponible sobre el ataque y, si fuera necesario, conseguir una herramienta de recuperación. Esta herramienta se puede encontrar en el siguiente enlace:

https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml

4.4 Mitigar los efectos de la infección

Mitigar los efectos de la infección debe entenderse como aquellas acciones que le permitan a la víctima reducir los efectos de la infección, en este caso en el número de ficheros cifrados o que le permitan recuperarse de forma total o parcial de la infección.

Una vez se ha sufrido una infección y los ficheros han sido cifrados, éstos se pueden recuperar por distintos medios:

- Obtener una herramienta especifica de descifrado (enlace Apartado 4.3.3).
- Restaurar el sistema y recuperar los ficheros cifrados.

Para dicha restauración, existen varias soluciones:

- En el caso de que en el equipo infectado se esté utilizando el sistema operativo Windows 7, o anteriores, se dispone de la opción preventiva de activar y utilizar las denominadas **Shadow Copies**.[13]
- En los sistemas Windows posteriores a la versión 7, existe la posibilidad de utilizar la opción **File History**.[14]

[9] Ver http://www.kaspersky.es/
[10] Ver https://en.wikipedia.org/wiki/CERT_Coordination_Center
[11] Ver https://www.nomoreransom.org/index.html
[12] Ver http://www.bleepingcomputer.com/
[13] Ver https://en.wikipedia.org/wiki/Shadow_Copy
[14] Ver https://support.microsoft.com/en-us/help/17128/windows-8-file-history

- Para cualquier tipo de sistema operativo e infraestructura, siempre es posible utilizar herramientas de **backup**.

5. BUENAS PRÁCTICAS

A continuación, se señalan las principales medidas para prevenir, detectar y/o mitigar parcialmente la acción de un ransomware:

1. **Mantener copias de seguridad periódicas de todos los datos importantes.** Es necesario mantener dichas copias aisladas y sin conectividad con otros sistemas, evitando así el acceso desde equipos infectados.
2. **Mantener el sistema actualizado con los últimos parches de seguridad,** tanto para el sistema operativo como para el software que hubiere instalado**.**
3. Mantener una primera línea de defensa con las **últimas firmas de *código dañino* (antivirus),** además de disponer de una **correcta configuración de los cortafuegos** a nivel de aplicación (basado en listas blancas de aplicaciones permitidas)**.**
4. **Disponer de sistemas *antispam* a nivel de correo electrónico** y establecer un nivel de filtrado alto, de esta manera se reduce las posibilidades de infección a través de campañas masivas de ransomware por correo electrónico.
5. **Establecer políticas seguridad en el sistema para impedir la ejecución de ficheros desde directorios comúnmente utilizados por el ransomware** (App Data, Local App Data, etc.). Herramientas como *AppLocker*, Cryptoprevent o CryptoLocker Prevention Kit permiten crear fácilmente dichas políticas.
6. **Bloquear el tráfico relacionado con dominios y servidores C2 mediante un IDS/IPS**, evitando así la comunicación entre el código dañino y el servidor de mando y control.
7. **Establecer una defensa en profundidad empleando herramientas como EMET**, una solución que permite mitigar *exploits* (incluidos *0-days*).
8. **No utilizar cuentas con privilegios de administrador**, reduciendo el potencial impacto de la acción de un ransomware**.**
9. **Mantener listas de control de acceso para las unidades mapeadas en red.** En caso de infección, el cifrado se producirá en todas las unidades de red mapeadas en el equipo víctima. Restringiendo los privilegios de escritura en red se mitigará parcialmente el impacto
10. Se recomienda el empleo de **bloqueadores de Javascript para el navegador**, como por ejemplo "**Privacy Manager**", que impide la ejecución de todos aquellos *scripts* que puedan suponer un daño para nuestro equipo. De este modo reduciremos las opciones de infección desde la web (*Web Exploit Kits*).
11. **Mostrar extensiones para tipos de fichero conocidos**, con el fin de identificar posibles archivos ejecutables que pudieren hacerse pasar por otro tipo de fichero.
12. Adicionalmente, se recomienda la instalación de la herramienta "**Anti Ransom**", que tratará de bloquear el proceso de cifrado de un ransomware (monitorizando "*honey files*"). Además, esta aplicación realizará un volcado de la memoria del código dañino en el momento de su ejecución, en el que con suerte se puede hallar la clave de cifrado que estuviera empleándose.

13. Finalmente, **el empleo de máquinas virtuales evitará en un alto porcentaje de casos la infección por ransomware**. Debido a las técnicas *anti-debug* y anti-virtualización comúnmente presentes en este tipo de código dañino, se ha demostrado que en un entorno virtualizado su acción no llega a materializarse.

5.1 Concienciación

Uno de los factores críticos en las infecciones por ransomware es la dimensión humana. En la mayoría de los casos, los atacantes utilizan la denominada Ingeniería Social para engañar a sus víctimas y llevar a cabo sus ataques. Un buen ejemplo de ello son los casos de Phishing ya mencionados como principal vector de infección.

Por ello, un paso de vital importancia en la defensa de todos los sistemas frente a infecciones y ataques es que todos los usuarios estén alerta y adecuadamente informados sobre las técnicas más utilizadas por los cibercriminales y ofrecer un conjunto de pautas para reducir la superficie de ataque de dichas acciones dañinas.

Con la concienciación del componente humano se puede reducir en gran medida el riesgo asociado a la entrada de correos, documentos y cualquier otro tipo de descargas dentro del sistema. Describir la facilidad con la que muchos de estos ataques son realizados es uno de mejores métodos para concienciar al usuario sobre las consecuencias que puede acarrear hacer un mal uso de los recursos del sistema.

5.2 Shadow copies

5.2.1 Sistemas Operativos Windows anteriores a Windows 8

En los sistemas operativos que van desde Windows XP a Windows 7, ambos inclusive, está disponible una tecnología denominada **Shadow Copies**, que permite al usuario realizar, manualmente o de forma automática, copias de los ficheros almacenados en el equipo incluso aunque estén en uso. Estas copias se hacen con el fin de poder restaurarlos más tarde si algún contratiempo lo hace necesario.

Se trata de una medida preventiva fácil de implementar y no necesita software adicional para ello. Sin embargo, no es una solución válida frente a todos los tipos de ransomware; por ejemplo, "*CryLocker*" y "*CryptoWall*" son dos ejemplos que explícitamente eliminan estos ficheros de restauración.

Pero puede ser de utilidad en el caso de una infección por un ransomware que no altere las **Shadow Copies**. Las mismas, se activan del siguiente modo:

1) Desde **Inicio**, se abre el **Panel de control**.
2) Se accede a **Sistema**.
3) Dentro de Sistema, se accede a la sección **Protección del sistema**.
4) En el apartado **Configuración de la protección**, se seleccionan las unidades de las que se desea hacer las *Shadow Copies*.
5) Por último, se selecciona **Crear**.

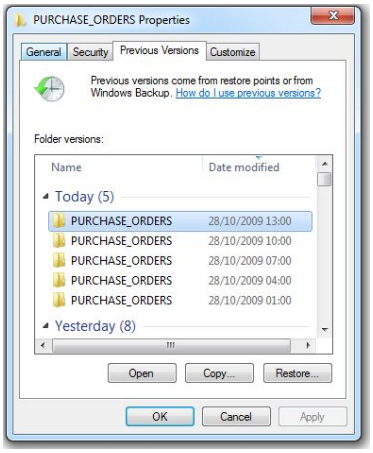


Figura 6.- Shadow Copies en Windows 7.

En aquellos casos en los que la infección no haya afectado a las *Shadow Copies*, el efecto de la infección se puede combatir restaurando esas copias en un equipo previamente desinfectado y sin trazas del código dañino. Para ello, hay que seguir las siguientes instrucciones:

1) Desde el menú **Protección del Sistema** (siguiendo los pasos 1, 2 y 3 de su creación), se elige la opción **Restaurar Sistema**.
2) A continuación, se selecciona el punto de restauración al cual se quiere volver.
3) Se confirma y se espera a la finalización del proceso de restauración.

Para más información sobre el uso de las *Shadow Copies*, se puede consultar el artículo de Microsoft sobre este servicio:

https://technet.microsoft.com/en-us/library/ee923636(v=ws.10).aspx

5.2.2 Sistemas Operativos Windows 8 o posteriores

A partir de Windows 8, la funcionalidad que permite hacer distintas copias de los ficheros se denomina **File History** y consiste en el almacenamiento de las copias de seguridad **en un medio extraíble**[15], lo que supone una gran diferencia con respecto a esa misma funcionalidad en versiones previas de los sistemas operativos Windows. Además de ello, también es posible habilitar las *Shadow Copies* mencionadas anteriormente.

Antes de utilizar *File History* es necesario elegir donde se van a hacer las copias de seguridad. Para ello se puede seleccionar un **medio extraíble** como puede ser un disco externo o una memoria USB conectada al equipo, o incluso un disco accesible en la misma red local a la que está conectado el equipo.

Es necesario tener en cuenta que *File History* **solo copia** los ficheros guardados en las carpetas de Documentos, Música, Imágenes, Videos y carpetas del escritorio, así como los ficheros almacenados en *OneDrive* para su acceso off-line en el equipo.

5.3 Backup Genérico

La medida más efectiva contra el ransomware es disponer siempre de varias copias de respaldo de todos los ficheros importantes. De hecho, la extorsión sólo se da cuando el ransomware atacante ha conseguido cifrar **ficheros que son únicos e irrecuperables** y

[15] Ver http://www.howtogeek.com/74623/how-to-use-the-new-file-history-feature-in-windows-8/

no queda más remedio que pagar el rescate si se quieren recuperar. Es esencial disponer de al menos una **copia de seguridad** de todos los ficheros importantes, de modo que se pueda recurrir a esa copia de respaldo cuando haga falta recuperarlos.

Las políticas de respaldo recomiendan tener siempre tres (3) copias actualizadas, completas, depositadas en tres (3) sitios diferentes y geográficamente distantes, además de estar almacenadas en dos (2) tipos de soporte distintos y, sobre todo, **estar todos ellos fuera de la red**. Por ejemplo, una posibilidad, aunque no sea la mejor, sería utilizar simultáneamente el propio equipo (1), un servicio de almacenamiento en la nube (2) y un medio extraíble (3).

En las copias de seguridad hay que proteger tanto la **integridad** como la **confidencialidad** de las mismas, por lo que se recomienda **cifrarlas y firmarlas criptográficamente**, sobre todo si van a almacenarse en la nube.

A continuación, se mencionan una serie de aplicaciones de código libre que permiten realizar copias de seguridad/respaldo de forma eficiente.

- **Amanda**[16]. Es una herramienta multiplataforma (Windows, Linux, macOS) que permite hacer copias en discos magnéticos, cintas, dispositivos ópticos (DVD) y en sistemas de almacenamiento en la nube.
- **BackupPC**[17]. Es una herramienta disponible para Windows y Linux que permite hacer copias de seguridad de grandes cantidades de datos, empleando para ello la compresión de ficheros para reducir el tamaño de la información a guardar, reduciendo costes.
- **Bacula**[18]**.** Es una de las suites más empleadas en el ámbito empresarial para la realización de copias de seguridad. Está disponible para entornos Windows, Linux y macOS.
- **FreeFileSync**[19]. Es una herramienta de sincronización de carpetas que permite la realización de copias de seguridad tanto de equipos locales como de unidades en red. Entre sus funcionalidades más útiles hay que resaltar la automatización de tareas, la confección de detallados informes de error y la posibilidad de utilizar nombres de ruta largos. Está disponible para Linux, Windows y macOS.
- **UrBackup**[20]. Esta herramienta permite la realización de copias de seguridad en segundo plano, mientras se trabaja, de forma que no interfiere con la labor que esté desarrollando el usuario. Es una herramienta rápida y eficaz, a la vez que permite realizar copias de seguridad por Internet. Disponible para Windows y Linux.

5.4 Bloqueo de macros

Desde la llegada de la suite MS Office 2007, los documentos que terminan en *.docx*, *.xlsx* y *.pptx* no contienen macros[21], sólo lo hacen aquellos que terminan en *.m*. En las versiones de MS Office 2016[22], las macros están deshabilitadas por defecto siendo lo más recomendable trabajar en un entorno donde no sea necesario el uso de macros.

[16] Ver http://www.amanda.org/
[17] Ver http://backuppc.sourceforge.net/
[18] Ver http://blog.bacula.org/
[19] Ver http://www.freefilesync.org/
[20] Ver http://www.urbackup.org/
[21] Ver https://es.wikipedia.org/wiki/Macro
[22] Ver https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

Para asegurarse de que las macros están desactivadas[23], se puede proceder del siguiente modo:

1) Seleccionar en la pestaña **Archivo** (MS Office 2013-2010) o en el botón de Microsoft Office (MS Office 2007).
2) Seleccionar en **Opciones** (MS Office 2013-2010), Opciones de Excel/Word/... (MS Office 2007).
3) Seleccionar en **Centro de Confianza** y a continuación seleccionar **Configuración del Centro de confianza**.
4) Seleccionar **Configuración de macros**.
5) Seleccionar "**Deshabilitar todas las macros sin notificación**".
6) Aceptar.
7) Salir del programa y reiniciar para verificar la configuración elegida.

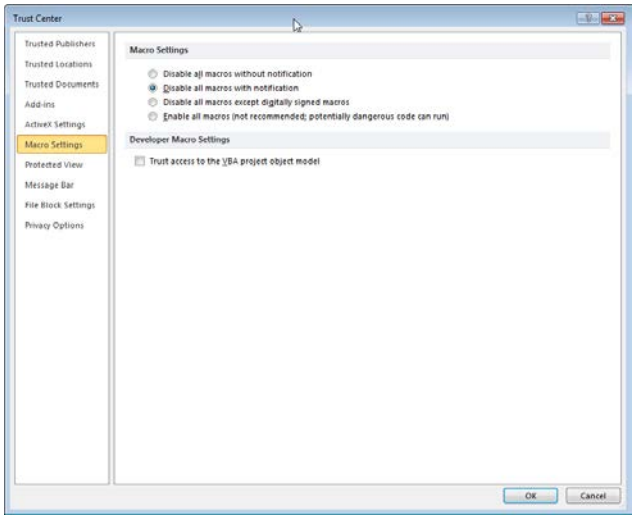


Figura 7.- Bloqueo de Macros en Microsoft Office.

En el caso de que se requiera la ejecución de código VBA (macros), se recomienda elegir la opción "**Deshabilitar todas las macros con notificación**" para poder examinar su comportamiento a priori utilizando herramientas como **OfficeMalScanner**. Si es preciso operar con macros, lo mejor opción es "**Deshabilitar todas las macros excepto las firmadas digitalmente**".

En Internet hay servicios que permiten analizar el contenido de cualquier fichero[24], pero también existen otros que están especializados en el análisis de macros dañinas que pudieran venir con documentos de tipo PDF, Word, Excel y PowerPoint. En cualquier caso, hay que tener en cuenta que al analizar el fichero se pierde el control exclusivo del mismo por lo que deberá tenerse en consideración que **se ha hecho público**.

Algunos de esos servicios son los siguientes:

- General (http://www.document-analyzer.net/).

[23] Ver https://support.office.com/es-es/article/Habilitar-o-deshabilitar-macros-en-documentos-de-Office-7b4fdd2e-174f-47e2-9611-9efe4f860b12

[24] Por ejemplo ver https://www.virustotal.com/es/

- Doc (https://malwaretracker.com/doc.php).
- PDF (https://malwaretracker.com/pdf.php).

5.5 Correcta configuración de cuentas de usuario y sus permisos.

Cualquier sistema operativo multiusuario, y Windows es uno de ellos, tiene que seguir una política de permisos lo más restrictiva posible, de forma que los usuarios tengan acceso única y exclusivamente a aquellos recursos y funcionalidades que les sean necesarios para su trabajo.

A este proceder se le conoce como "***de mínimo privilegio***" y es el que debería aplicarse en todos los escenarios. Una correcta implementación de la política de permisos puede evitar que un usuario sea capaz de infectar a toda una red si el ransomware se propaga.

A continuación, se muestra una serie de direcciones con instrucciones para poder gestionar correctamente los permisos de usuario en máquinas con diferentes versiones del sistema operativo Windows:

- Windows 7.

  http://www.welivesecurity.com/la-es/2015/05/22/como-administrar-permisos-usuarios-grupos-usuarios-windows-7/
- Windows 10.

  https://channel9.msdn.com/Blogs/MVP-LATAM/Administra-tus-cuentas-de-usuario-en-Windows-10

5.6 Honeypots[25] o Sistemas Trampa.

Una de las fases de todo proceso defensivo frente a un ataque es la detección del mismo. En general, cuanto antes se sepa que el sistema está siendo atacado, antes se podrá reaccionar deteniéndolo o mitigando sus efectos.

Una de las formas de detectar las infecciones por ransomware es instalar en la maquina un sistema trampa o honeypot, que actúa como señuelo que delata la presencia del código dañino.

La medida consiste en crear una carpeta con ficheros variados que resulten atractivos al código dañino, pero que no sean los que utilizan los usuarios de esa máquina. Las acciones sobre esa carpeta se monitorizan en tiempo real de tal forma que cuando el ransomware acceda a ellos para cifrarlos, se detecta su presencia y es detenido.

Una limitación de esta medida es que no detecta lo que pueda haber hecho el código dañino hasta que acceda a los ficheros señuelo y cifrado parte del sistema. Dado que el contenido de la carpeta no representará un porcentaje significativo de la totalidad de los ficheros, su sensibilidad a la hora de detectar el ataque puede no ser alta. Un ejemplo de herramienta de este tipo se puede encontrar en:

http://www.security-projects.com/?Anti_Ransom

Si se detecta una infección, el programa muestra una alerta indicando que proceso está modificando alguno de los archivos cebo y ofrecerá la opción de terminar ese proceso o dejar que continúe.

[25] Ver https://es.wikipedia.org/wiki/Honeypot

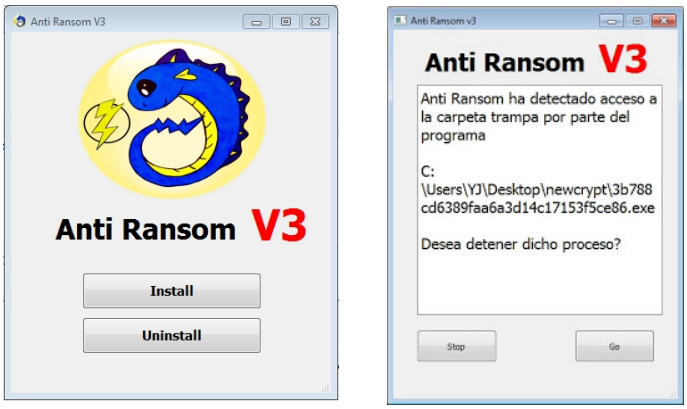


Figura 8.- Programa Anti-Ransom.

5.7 Navegación segura

Uno de los métodos de infección más utilizados por el ransomware es la explotación de vulnerabilidades en los navegadores web. Para ello se recurre a los **exploit kits**[26], que son programas diseñados para explotar vulnerabilidades conocidas en las aplicaciones con el fin de conseguir el control total sobre el sistema atacado.

Sin embargo, éste no es el único método de infección que está relacionado con los navegadores web, también se puede emplear el Phishing o cualquier otro método que termine con la ejecución de código dañino en el equipo víctima (memorias USB de propaganda, regaladas o encontradas, Apps de moda, servicios web, etc.).

Para protegerse de este tipo de ataques, la recomendación básica es mantener actualizado tanto el navegador web como las extensiones o complementos instalados en el mismo. De ese modo, al navegador se le habrán aplicado todas las correcciones conocidas y con ello se estará disminuyendo el número y extensión de los puntos débiles que puede emplear el atacante (superficie de exposición).

Además, se recomienda hacer uso de extensiones o complementos del navegador web cuyo fin sea aumentar la seguridad de los mismos. Unas extensiones recomendadas son las que bloquean la apertura de ventanas emergentes, como es el caso de **AdBlock**[27] (Google Chrome y Mozilla Firefox) que evitaría la carga de páginas no solicitadas por el usuario o que son conocidas por ser dañinas.

También se recomienda utilizar extensiones para protegerse contra Phishing (que están incluidas en los navegadores principales) y otras amenazas, como puede ser la extensión **Avast Online Security** para Google Chrome.

En caso de utilizar otros navegadores que no permitan este tipo de extensiones, como es el caso de Internet Explorer, se pueden emplear herramientas como el filtro **SmartScreen**, que indica si la página a la que se está accediendo es legítima o pretende suplantar la identidad de otra. Para activar ese filtro se selecciona la pestaña **Seguridad → Filtro SmartScreen → Activar el filtro.**

[26] Ver https://en.wikipedia.org/wiki/Exploit_kit
[27] Ver https://getadblock.com/

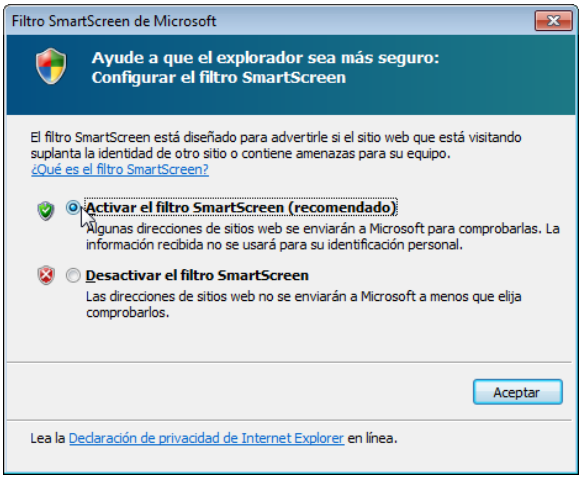


Figura 9.- Bloqueo de Macros en Microsoft Office.

Una medida más drástica, pero muy eficaz, es la desactivación de la ejecución de **JavaScript**[28], permitiéndose sólo en sitios web de confianza. La ejecución de este tipo de código es peligrosa porque puede permitir la ejecución automática de código malicioso que descargue y ejecute el ransomware en la máquina.

La desactivación de JavaScript se puede conseguir en la configuración del propio navegador web o mediante el uso de extensiones como **NoScript** (FireFox) y **ScriptSafe** (Chrome).

Esta medida, eficaz en la prevención de ejecución de código malicioso, es la más intrusiva para el usuario y puede dar problemas con algunos de sus sitios web habituales, haciendo que estos no se muestren como deberían o que no se incluyan algunas funcionalidades.

Entre estas funcionalidades se encuentran algunos *plugins*, la visualización de datos, presentaciones web, buscadores y elementos gráficos en general. La desactivación de JavaScript, por tanto, da un aspecto mucho más plano de la web.

5.8 Extensiones conocidas de los archivos

El camuflaje es una técnica de engaño muy utilizada por el malware en general y por el Phishing en particular. La idea es ocultar un archivo ejecutable, bajo la apariencia de otro no ejecutable y aparentemente inocuo.

Para comodidad del usuario, en los sistemas operativos actuales las extensiones de archivo más comunes son omitidas del nombre del fichero y su icono es elegido de modo que sea el más representativo para ese tipo de archivo.

Este comportamiento puede utilizarse para engañar al usuario haciéndole creer que un fichero es otra cosa distinta a la que realmente es; por ejemplo, un proceso ejecutable podría simular ser una imagen al llevar un nombre terminado en *.jpg*, pero realmente ser un fichero con la terminación *.jpg.exe* que es algo completamente distinto.

Al tener activada la opción de ocultar las extensiones conocidas, el usuario no verá que se trata de un ejecutable y no de una imagen.

[28] Ver https://es.wikipedia.org/wiki/JavaScript

Para mostrar las extensiones ocultas hay que acceder a las opciones de carpeta del explorador de Windows. La forma más sencilla es desde la barra de herramientas de cualquier ventana del explorador, eligiendo la opción de **Opciones de carpeta** bajo el menú **Vista**. Una vez en las opciones de carpeta, en la sección de Vista debe desactivarse la opción de **Ocultar extensiones para archivos conocidos.**

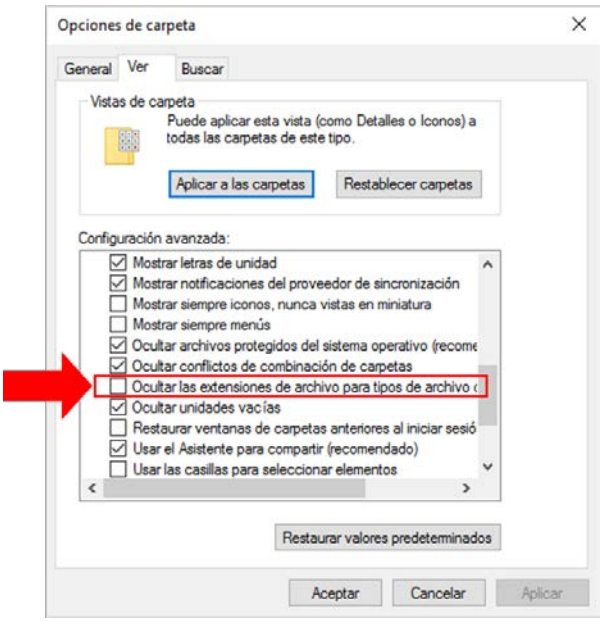


Figura 10.- Opción de no ocultar extensiones conocidas.

Otra forma de abusar de este comportamiento es la creación de accesos directos cuyo icono es modificado para hacer creer al usuario que es un tipo de archivo conocido. La forma de distinguir un fichero de un acceso directo es tan sencilla como observar la esquina inferior izquierda del icono, que en caso de ser un acceso directo mostrará un indicador en forma de flecha y no deberá utilizarse a menos que se confíe en su procedencia.

5.9 EMET

Con el ánimo de mitigar los efectos del malware en sus sistemas operativos, Microsoft ha desarrollado *Enhanced Mitigation Experience Toolkit*, o EMET. Se trata de una herramienta de seguridad puesta a libre disposición de los usuarios.

EMET proporciona una interfaz de usuario que le ayuda a configurar las características relacionadas con la seguridad del sistema operativo Windows. Se puede utilizar como una capa extra de seguridad entre los cortafuegos personales y el software antivirus.

5.9.1 Manual de instalación

Para poder instalar EMET, quizás haya que instalar en primer lugar *.NET Framework*. Si es preciso y no se sabe cómo hacerlo, es recomendable consultar el siguiente enlace:

https://msdn.microsoft.com/es-es/library/5a4x27ek(v=vs.110).aspx

Una vez *.NET Framework* está descargado e instalado, se procede descargar la herramienta EMET del siguiente enlace:

https://www.microsoft.com/en-us/download/details.aspx?id=53354

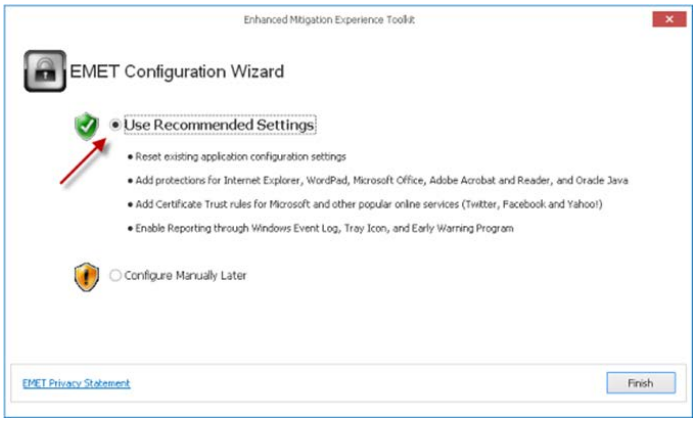


Figura 11.- Instalación de la herramienta EMET.

Se recomienda elegir la opción "***Use Recommended Settings***" para simplificar la configuración de EMET. Es preciso indicar que la instalación de EMET puede provocar ciertas interferencias con algunas aplicaciones, y que la velocidad del equipo puede verse reducida si el número de programas a controlar por esa herramienta es excesivo.

Si se desea obtener más información sobre cómo poder añadir o quitar programas específicos de la lista de vigilancia de la aplicación EMET, se recomienda entrar en la página:

http://articulos.softonic.com/como-proteger-windows-con-emet

Usuarios más avanzados pueden encontrar más detalles en:

https://www.trustedsec.com/november-2014/emet-5-1-installation-guide/

5.10 AppLocker

Applocker[29] es una aplicación introducida en Windows Server 2008 R2 y Windows 7 que amplía sus características de control de aplicaciones y las políticas de ejecución restringida.

Esta herramienta se utiliza para crear reglas basadas en los atributos de los archivos (nombre, firma digital, etc.) a fin de controlar el acceso al software instalado en el equipo. Ese control permite, entre muchas opciones, bloquear el acceso a un programa o a un servicio determinado.

En el siguiente enlace se encuentra información detallada sobre *Applocker*:

https://technet.microsoft.com/es-es/library/mt431725(v=vs.85).aspx6

5.11 Recuperación de los ficheros mediante el almacenamiento en la nube

Desde hace algún tiempo, es muy común el uso de **servicios de sincronización de ficheros**[30] o de almacenamiento en la nube[31].

Cuando se tiene sincronizado el contenido de una carpeta local con otra en la nube, ambas ubicaciones tienen los mismos ficheros. Si en un equipo local se sufre el ataque de un agente de ransomware, las copias locales serán cifradas y, posteriormente, el

[29] Ver https://msdn.microsoft.com/es-es/library/ee424367(v=ws.11).aspx
[30] Ver https://en.wikipedia.org/wiki/File_synchronization
[31] Ver https://en.wikipedia.org/wiki/Cloud_storage

sistema de sincronización copiara en la nube esos mismos ficheros borrando los anteriores, de modo que las copias en la nube también terminarán cifradas.

Sin embargo, el borrado de ficheros es una acción aparente en muchos de estos servicios de almacenamiento en la nube ya que realmente se trata de un sistema de ficheros con control de versiones[32].

En estos sistemas, los ficheros borrados no se borran realmente, sino que quedan almacenados como una versión anterior que sigue siendo accesible para el administrador del servicio en la nube.

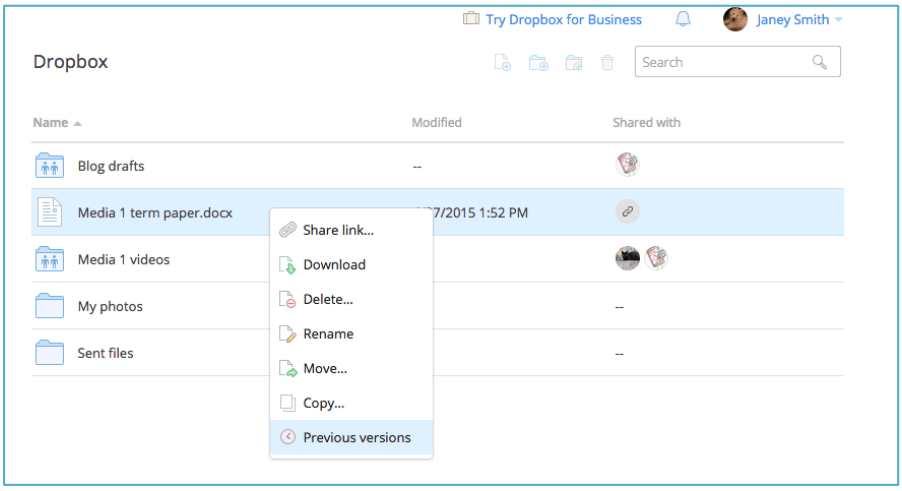


Figura 12.- Control de versiones en Dropbox.

En esos casos, y según sea la política del proveedor de servicios, a veces es posible eliminar de la nube las versiones cifradas (secuestradas) y recuperar versiones anteriores de esos mismos archivos.

Tanto **Dropbox**[33] como **Google Drive**[34] ofrecen posibilidades en este sentido, por lo que siempre hay que considerar la posibilidad de restaurar lo que se tenía sincronizado en la nube. Obviamente, la operación de restauración debe hacerse una vez se haya limpiado completamente el equipo afectado.

5.12 Cuando todo parece perdido.

Una vez que el sistema ha sido infectado y que el ransomware haya conseguido cifrar todo el sistema de ficheros accesible, puede darse el caso de que consultando foros especializados no haya antídoto que permita recuperar la información. En ese caso, **no conviene proceder al borrado de los ficheros afectados**.

El hecho de que en ese momento no exista una herramienta que permita el descifrado de los ficheros secuestrados, no significa que no pueda existir en un futuro próximo. En ese caso, es mejor no destruir la única copia que hay de nuestros ficheros, aunque esta copia esté cifrada con una clave que, en ese momento, no esté disponible.

Lo más recomendable es:

1) Copiar todos los ficheros cifrados en una unidad externa vacía.

[32] Ver https://en.wikipedia.org/wiki/Versioning_file_system
[33] Ver https://www.dropbox.com/help/11
[34] Ver https://support.google.com/docs/answer/190843?hl=es

2) Limpiar y desinfectar el equipo infectado.

3) Poner a buen recaudo una copia de seguridad de los ficheros cifrados hasta que se conozca alguna forma de recuperar esos ficheros.

6. CONCLUSIÓN

A la hora de dotar de seguridad a un sistema informático es necesario aplicar todas las medidas disponibles y, a ser posible, organizadas en capas para dificultar el éxito de cualquier ataque.

Así mismo, una rápida detección de la infección puede permitir detenerla, limitando el número de ficheros afectados. En ese momento se procede a la completa limpieza del equipo afectado y se intenta la recuperación de los ficheros que han sido afectados.

Dado que el verdadero riesgo del ransomware es que secuestren **la única copia disponible de un fichero**, toda la resiliencia del sistema depende de que se mantengan **copias de seguridad** adecuadamente **actualizadas**, **cifradas** y **firmadas**, fuera del alcance (**off-line**) de nuestro equipo.

Disponer de una adecuada copia de seguridad de los ficheros importantes convierte el ataque de ransomware en una molestia en lugar de ser un desastre.

Por último, para estar al día de las medidas de seguridad contra el ransomware, se recomienda la lectura del Informe de Amenazas CCN-CERT IA-03/17.

7. DECÁLOGO

1	Informar y concienciar a todos los usuarios de los riesgos y amenazas que supone el Ransomware, de modo que su estado de consciencia, alerta y formación disminuyan la posibilidad de infección.
2	Mantener un sistema de copias de seguridad/respaldo actualizado, tanto de los sistemas locales como de las ubicaciones distantes. A ser posible deben mantenerse al menos dos (2) copias de seguridad en diferentes localizaciones y desconectadas del Sistema.
3	Deshabilitar las macros en los documentos de Microsoft Office y otras aplicaciones similares.
4	Deshabilitar Windows Script Host para evitar la ejecución de scripts en el Sistema. Para ello se pueden seguir los pasos descritos en el siguiente enlace de Microsoft: https://technet.microsoft.com/es-es/library/ee198684.aspx
5	Seguir las recomendaciones publicadas sobre protección del correo electrónico. (Ver Guía CCN-CERT BP-02/16)
6	Complementar el antivirus y cortafuegos personal con programas como *AppLocker* (bloqueo de ejecución de programas) y EMET (detección y bloqueo de técnicas de exploit).
7	Mantener una conducta de navegación segura, empleando herramientas y extensiones de navegador web completamente actualizadas que ayuden a prevenir ejecuciones no autorizadas de código en el navegador web. (Ver Guía CCN-CERT BP-06/16)

8	Activar la visualización de las extensiones de los ficheros para evitar ejecución de código dañino camuflado como fichero legítimo no ejecutable.
9	Configurar el UAC (User Access Control) de Windows de la forma más restrictiva posible, pidiendo siempre confirmación para la ejecución de aquellos procesos que requieran altos privilegios.
10	Mantener el sistema operativo y todas las soluciones de seguridad actualizadas, así como cortafuegos personal habilitado.