CCN-CERT

BP/04

Ransomware

INFORME DE BUENAS PRÁCTICAS

MAYO **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEDE-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.05.27 13:46:58 +02'00

Centro Criptológico Nacional, 2018

Fecha de edición: mayo de 2021

Índice

Índice

1. Sobre CCN-CERT, CERT gubernamental nacional

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación 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.

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, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la **información clasificada** (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del **Sector Público** es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de **operadores críticos del sector público** la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. Introducción

La familia de código dañino conocida como ransomware ha sido la amenaza más concurrente y dañina, con una gran evolución en los últimos años.

Aproximadamente en 2012, se encontraban las primeras variantes cuyo principal objetivo era bloquear el equipo infectado. Años más tarde, el ransomware evolucionó hasta lo que se conoce hoy en día como "cifradores" de archivos. El escenario empeoró en 2015-2016 cuando proliferaron los RaaS (Ransomware as a Service), servicios que ofrecían los cibercriminales para poder diseñar este tipo de malware de manera sencilla a cambio de un porcentaje de las potenciales ganancias que pudiera tener la campaña.

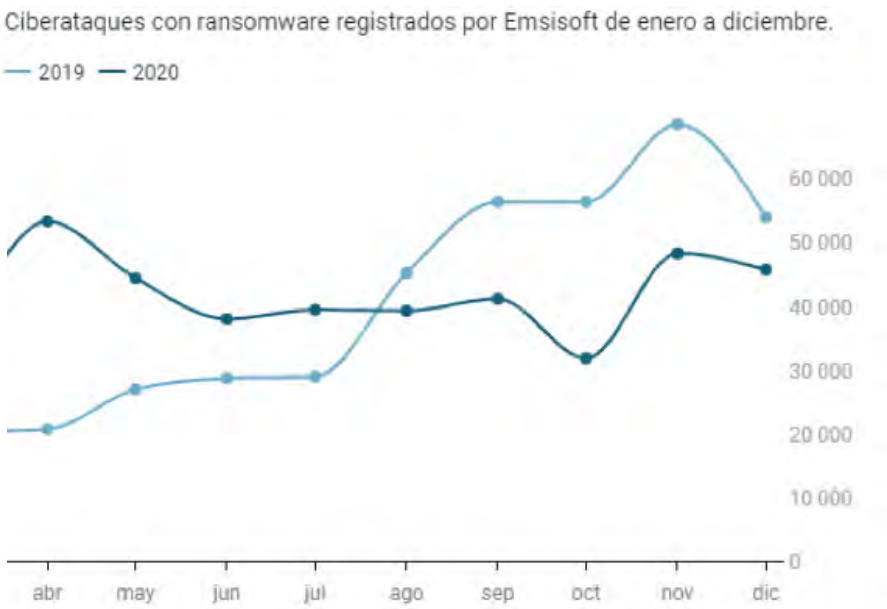
Durante el período de 2019 a 2020 se pudo observar un claro aumento en los ciberataques, cuando la pandemia comenzó a expandirse por todo el mundo y los gobiernos de diversos países decretaron confinamientos.

Según Emsisoft[1], el número total de ataques por ransomware creció un 12,39 % en 2020 respecto al año anterior. En enero de 2020 los incidentes relacionados con ransomware crecieron un 59,84% con respecto al mismo mes del año anterior. En febrero los ataques con este tipo de código crecieron un 137,17%. Pero no es hasta abril cuando se registra el crecimiento récord: de un 156,55%. A partir de mayo el crecimiento se suaviza. Ese mes pasa a crecer un 64,36% con respecto al mismo mes de mayo del año anterior, y en verano la diferencia osciló en torno a un 30%. El segundo semestre del año 2020 registró menos incidentes que durante el mismo período de 2019.

En noviembre de 2020 se registraron aproximadamente 25 grupos de ransomware diferentes en actividad.

El número total de ataques por ransomware creció un 12,39 % en 2020 respecto al año anterior

1. https://www.businessinsider.es/grafico-ensena-como-pandemia-ha-disparado-ciberataques-834287.



[Figura 1] Ciberataques con ransomware registrados por Emisoft

Informes como el que realizó Cognyte[2] aseguran que las tres familias de ransomware con mayor actividad durante 2020 a nivel global fueron Ryuk, Maze y REvil/Sodinokibi.

Además, según otro informe realizado por Palo Alto Networks[3] los ciberdelincuentes que operan los ataques con ransomware recaudaron más que nunca en ese mismo año.

En los ciberataques por ransomware, los ciberdelincuentes[4] atacan utilizando un código dañino que cifra datos y sistemas informáticos, para, posteriormente, exigir un rescate después a sus víctimas si estas quieren recobrar la normalidad. Cabe destacar que los criminales cargan contra objetivos cada vez más vulnerables, como organizaciones sanitarias, y han desarrollado estrategias más agresivas que fuerzan a pagar esos rescates.

En los ciberataques por ransomware, los ciberdelincuentes atacan utilizando un código dañino que cifra datos y sistemas informáticos, para, posteriormente, exigir un rescate después a sus víctimas si estas quieren recobrar la normalidad

2. Ver: https://www.cognyte.com/blog/what-you-need-to-know-about-the-top-4-global-ransomware-vulnerabilities-and-how-to-stay-protected/
3. Ver: https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/
4. Ver: https://www.businessinsider.es/pagos-rescate-ransomware-triplicaron-durante-pandemia-833859

Se ha mantenido invariante en todos estos años el método de pago, siendo utilizadas las criptomonedas (en la mayoría de los casos, Bitcoin) por su carácter anónimo.

En un mundo en el que la mayoría de las fuentes relacionadas con la seguridad informática prevén que este tipo de amenazas siga aumentando es importante saber cómo defenderse.

En esta guía se expondrán medidas que son aplicables a dichas fases.

Frente a los ataques informáticos es necesario actuar, al menos, en cuatro fases distintas:

1. **Prevención**
2. **Detección**
3. **Respuesta**
4. **Remediación del ataque**

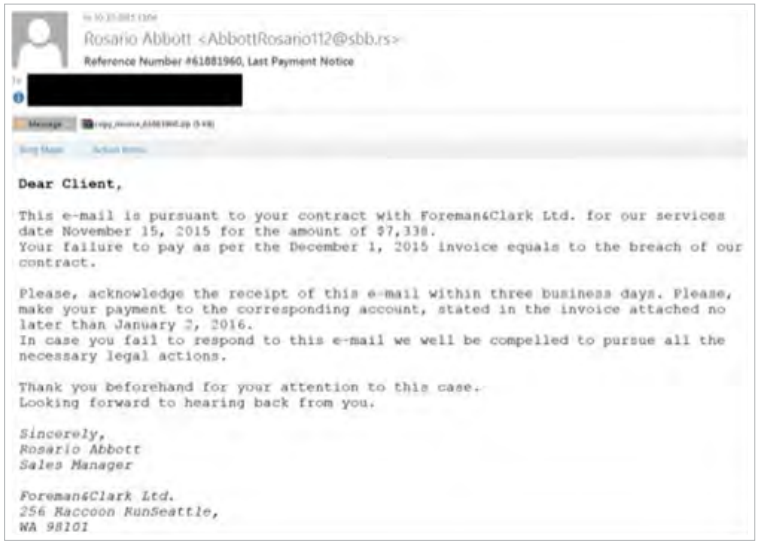
3. Vectores de infección

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

Los mecanismos y posibilidades para que la infección se produzca son variados, siendo importante conocer los vectores más comunes. En algunos casos, el código dañino 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

Aunque en descenso (para el caso del ransomware), la utilización de correos electrónicos fraudulentos (phishing) sigue estando muy presente en el día a día.


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 3, 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

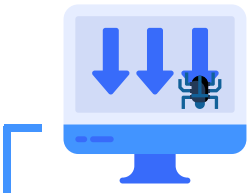
Foreman&Clark Ltd.
256 Raccoon RunSeattle,
WA 98101

[Figura 2] Correo fraudulento empleado por TeslaCrypt

Este tipo de correos se apoya en la llamada ingeniería social (la manipulación de las personas con el objetivo de que estas realicen una serie de tareas al gusto del manipulador) para conseguir que el usuario ejecute un archivo aparentemente inofensivo.

Dentro del phishing se pueden distinguir dos 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.

Formas de infección típicas del phishin



Mediante enlace web

Mediante fichero adjunto

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

En ambos casos, la víctima descarga o ejecuta (de forma consciente o inconsciente) una aplicación que, aunque en principio no parece sospechosa, oculta el código dañino.

3.3 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 cómo prevenir estas formas de infección, se aconseja consultar el informe BP-02-16 Buenas Prácticas en Correo Electrónico.

3.4 Navegación web. Web Exploit Kits

También se pueden encontrar lo que se denominan Web Exploit Kits: una vía de infección más sutil y transparente que se aprovecha de alguna vulnerabilidad conocida del navegador o de algún plugin instalado para poder ejecutar código dañino.

La transparencia de este método recae en que los responsables de las campañas de ransomware se encargan previamente de hacerse con el control de servidores legítimos para 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.

Web Exploit Kits: vía de infección más sutil y transparente que se aprovecha de alguna vulnerabilidad conocida del navegador o de algún plugin instalado para poder ejecutar código dañino

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.

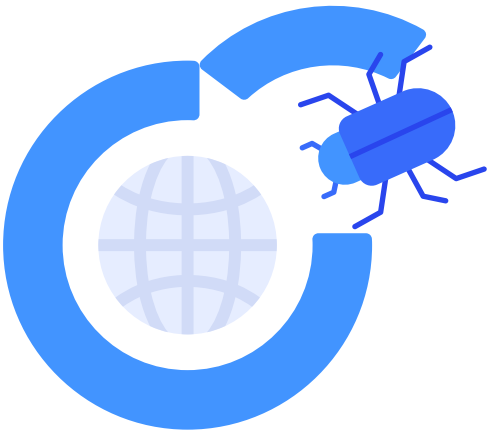
Uno de los principales problemas de los plugins es que aumentan significativamente la exposición a determinado tipo de ataques durante la navegación web. Algunos de estos plugins contienen un gran número de vulnerabilidades críticas que permiten a los atacantes ejecutar código en el equipo de la víctima.

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. Activar plugins, como Flash y Java, de forma temporal y de manera controlada por el usuario puede ser una buena opción.

Asimismo, 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 para ejecutar código dañino.

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

Para evitar este tipo de infecciones lo único que se puede hacer es utilizar la versión más actualizada del navegador y de sus extensiones



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

3.5 Ataques por RDP

Conscientes del cambio de escenario por la pandemia de la COVID 19, que ha obligado a los empleados a realizar gran parte de su trabajo a través del acceso remoto, los ciberdelincuentes –sobre todo los operadores de ransomware– intentan explotar las nuevas oportunidades para aumentar sus ganancias[6].

El RDP se ha convertido en un vector de ataque muy popular en los últimos años, especialmente entre los operadores de ransomware, que utilizan este protocolo para ganar acceso a los equipos de la infraestructura y posteriormente propagarse.

Los atacantes, mediante herramientas automatizadas, buscan equipos que tengan expuesto este servicio a Internet. A continuación, mediante un ataque por fuerza bruta (esto es, probando todas las combinaciones alfanuméricas posibles) o por ataques de diccionario (archivos de gran tamaño compuestos por los usuarios y contraseñas más habituales y usadas en Internet) tratan de conseguir acceso al equipo.

Por esta razón, resulta de vital importancia asegurarse de que las combinaciones de usuario y contraseña que se usan para acceder a los servicios sean robustas.

El RDP se ha convertido en un vector de ataque muy popular en los últimos años, especialmente entre los operadores de ransomware

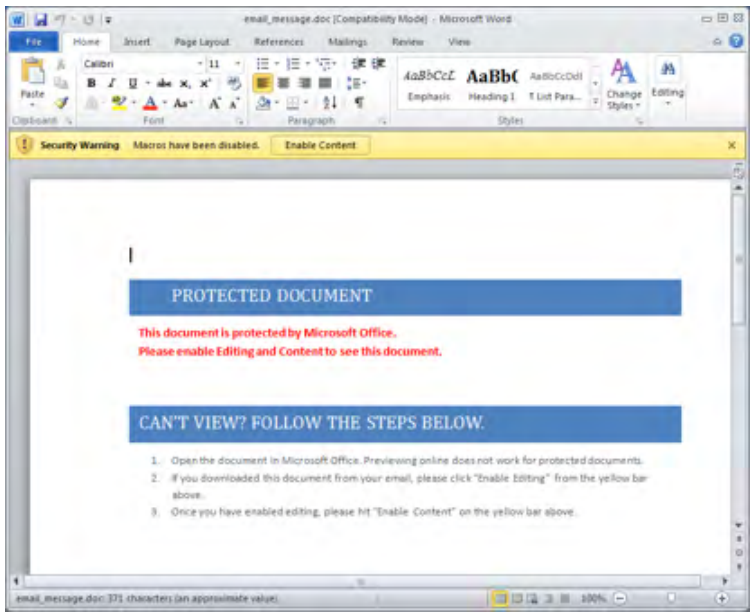
6. https://www.welivesecurity.com/la-es/2020/06/29/crecieron-ataques-fuerza-bruta-dirigidos-rdp-durante-pandemia/

3.6 Ataques sin interacción del usuario

Frente a un escenario donde cada vez más usuarios son aleccionados sobre los ataques informáticos y los métodos más frecuentes de infección (en definitiva, más concienciados con la seguridad informática), los creadores de malware (de forma generalizada) adaptan sus métodos con el propósito de extender sus ejecutables dañinos lo máximo posible.

Esta evolución se ha podido contemplar en la distribución de documentos de ofimática dañinos, cuyo contenido a primera vista parece ilegible o protegido. Se advierte que, para ser capaz de leer el documento, es necesario activar las macros, tras lo cual el código dañino se ejecuta.

[Figura 3] Ejemplo de documento dañino supuestamente protegido



Sin embargo, desde finales de 2017 se empezaron a utilizar métodos donde la ingeniería social ya no era necesaria, dado que la interacción del usuario se elimina. Un ejemplo es el uso de exploits (programas que se aprovechan de una inseguridad para poder ejecutar código arbitrario) en los propios documentos ofimáticos que se ejecutan con la simple apertura del mismo, sin necesidad de activar macros. Este tipo de ataques son muy peligrosos ya que la necesidad de interacción es nula, pues no suelen mostrar ninguna alerta o ventana, lo que dificulta la tarea de determinar cuándo se realizó la infección.

3.7 Por medio de otro malware

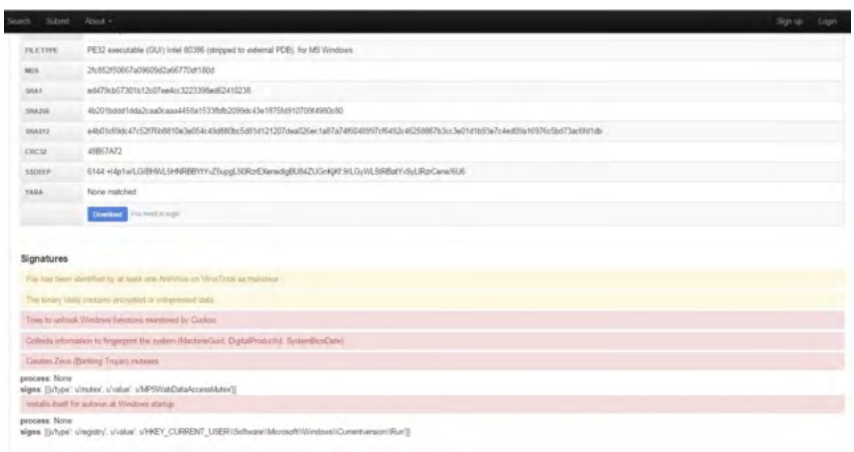
Es bastante común que la vía de entrada de software dañino al equipo se produzca mediante otro malware que ha sido previamente instalado

Casos como estos pueden darse, por ejemplo, con la familia de virus conocidas como troyanos, que conceden el control total del sistema al atacante, downloaders ("descargadores") cuyo único cometido es descargar más malware o backdoors, es decir, puertas traseras que se dejan abiertas en el ordenador infectado con el objetivo de tener una entrada directa en el futuro.

A su vez, es muy común que los programas destinados al *pirateo* de software comercial estén infectados. En un primer momento, puede parecer que dichos programas realizan correctamente su función, pero es en estos casos donde podría no detectarse el malware acoplado, pues el software logra efectivamente funcionar y paralelamente infectar el sistema.

Para este tipo de casos se necesita un análisis más exhaustivo del fichero. Existen servicios web que analizan un documento sospechoso con diversos antivirus de manera gratuita, tales como http://www.novirusthanks.org/.

Del mismo modo y para un examen aún más profundo, es posible utilizar el servicio de https://malwr.com/ cuya tecnología implementa una Sandbox con Cuckoo (máquina virtual) donde la muestra es ejecutada y analizada al detalle (archivos creados, registros modificados, conexiones, llamadas al sistema, capturas de pantalla…), para ofrecer unos resultados mucho más completos y minuciosos.



[Figura 4]
Ejemplo de análisis realizado por "*malwr*"

4. Desinfección

4.1 Primeros pasos

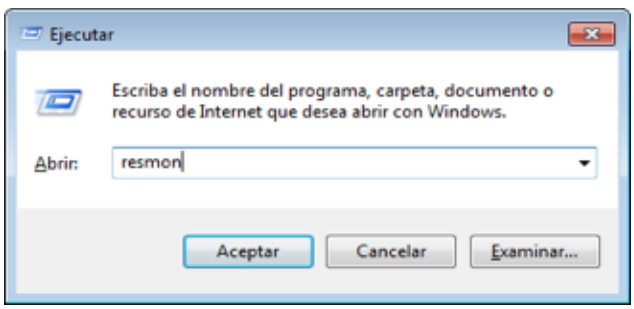
Lo primero que hay que hacer si se detecta una infección es desconectar el equipo de la red, dado que, por lo general, el cifrado precisa de la capacidad de cálculo del equipo infectado para su acción. Este procedimiento tiene distintas finalidades:

- **Evitar que la acción de cifrado alcance al contenido alojado en las unidades de red accesibles desde el equipo infectado.**

- **Eludir que el código dañino pueda contactar con su servidor de mando y control.**

Analizar qué 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 dañino, se puede usar la herramienta Monitor de Recursos de Windows. Para acceder a ella, basta con ejecutar "resmon" (tecla Windows + r).



[Figura 5]
Ventana del comando "ejecutar"

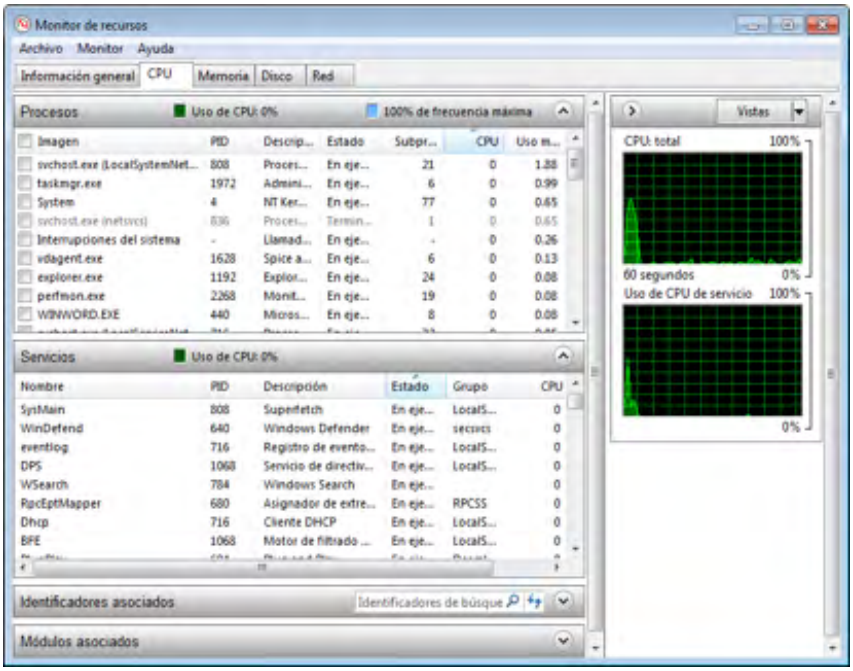
7. Cerrar procesos con el Administrador de tareas, ver https://support.microsoft.com/es-es/kb/2499971

Debido a que la operación de cifrado de los ficheros requiere tiempo de CPU y acceso al disco, estas características pueden utilizarse para identificar el proceso o aplicación que está realizando el ataque. Para ello, se debe prestar atención en lo siguiente:

- **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.

- **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 uno 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.

- **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 6]
Imagen del monitor de recursos en Windows 7

8. PID, "Process ID": es un numero identificativo que es único y que representa a cada proceso en ejecución. Ver https://www.computerhope.com/jargon/p/pid.htm

4.2 Identificar el ransomware

Es importante conocer qué variante de ransomware ha infectado los equipos afectados, y para ello se puede utilizar alguno de estos servicios: **NoMoreRansom** o **IDRansomware**.

En estas páginas web se pueden subir los ficheros e identificar a qué familia pertenece el código dañino que ha infectado el equipo y ha cifrado sus ficheros. En este caso, la identificación del atacante se puede hacer facilitando un fichero cifrado 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.

Conocer qué familia ha atacado los sistemas permite realizar una búsqueda sobre los detalles y comportamiento de dicho código dañino, pudiendo obtener información valiosa (como conocer si existe o no una herramienta de descifrado y recuperación de ficheros).

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 y obtener así la mayor cantidad posible de información sobre casos de infecciones similares y consejos sobre cómo 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.

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 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, se debe 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.

9. Ver http://www.kaspersky.es/
10. Ver https://searchdatacenter.techtarget.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia#
11. Ver https://www.nomoreransom.org/index.html
12. Ver http://www.bleepingcomputer.com/

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, de manera que se pueda conocer 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

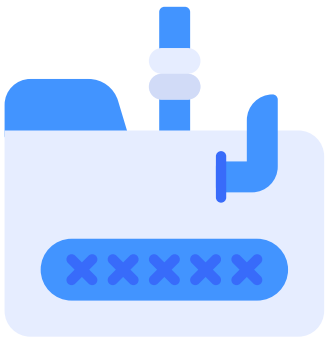
Además, es imprescindible revisar el documento titulado "CCN-CERT IA-11-18 Medidas Seguridad Ransomware", en el cual se enumeran muchos más recursos para facilitar la recuperación de ficheros, entre otros:

- http://files-download.avg.com/util/avgrem/avg_decryptor_Legion.exe
- https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor
- https://www.mcafee.com/us/downloads/free-tools/index.aspx
- https://decrypter.emsisoft.com/

Es importante mencionar que, en el caso de que no existieran herramientas de descifrado, no se aconseja realizar el pago, pues esto solo sirve de incentivo para que los ciberdelincuentes sigan creando campañas de ransomware.

Asimismo, el pago del rescate no asegura la recuperación de los ficheros. Existen campañas que no solo ofrecen herramientas de descifrado real, sino que también guardan los datos de la tarjeta de crédito empleada. También se han detectado paginas TOR fraudulentas (enlaces anónimos donde se realiza normalmente el pago de estos rescates). Según Symantec 2017, uno de cada cinco negocios no consiguió recuperar sus archivos tras realizar el pago.

El pago del rescate no asegura la recuperación de los ficheros



4.4 Mitigar los efectos de la infección

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

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

- Mediante una herramienta especifica de descifrado (Apartado 4.3.3).
- A través de la restauración del sistema, que permite 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].
- Para cualquier tipo de sistema operativo e infraestructura siempre es posible utilizar herramientas de backup.

13. Ver https://www.welivesecurity.com/la-es/2017/09/26/shadow-copies-backup-windows-ransomware/
14. Ver https://support.microsoft.com/en-us/help/17128/windows-8-file-history

5. Buenas prácticas

A continuación, se señalan las principales medidas para prevenir, detectar 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. **Políticas BYOD (Bring Your Own Device).** Cada vez es más habitual que las empresas adopten este tipo de política, que permite al trabajador usar sus dispositivos electrónicos como medio de trabajo dentro de la organización. Estos aparatos son un potencial vector de infección y es por ello por lo que es imprescindible definir unas reglas de seguridad.

4. **Contraseñas seguras**. Como se ha mencionado, el ataque a servicios visibles desde Internet con credenciales de acceso débiles (contraseñas inseguras) es un procedimiento que se vuelve cada vez más asiduo.

5. **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).

6. **Disponer de sistemas antispam a nivel de correo electrónico** y establecer un nivel de filtrado alto. De esta manera, se reducen las posibilidades de infección a través de campañas masivas de ransomware por correo electrónico.

7. **Establecer políticas de 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.

8. **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.

9. **No utilizar cuentas con privilegios de administrador**, lo que permite reducir el potencial impacto de la acción de un ransomware.

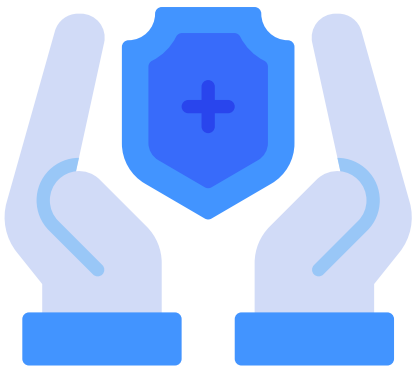
10. **Mantener listas de control de acceso** para las unidades mapeadas en red. En caso de infección, el cifrado se producirá en todas las unidades de red mapeadas en el equipo víctima. Restringiendo los privilegios de escritura en red se mitigará parcialmente el impacto

11. 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 se reducen las opciones de infección desde la web (Web Exploit Kits).

12. **Mostrar extensiones para tipos de fichero conocidos**, con el fin de identificar posibles archivos ejecutables que pudieren hacerse pasar por otro tipo de fichero.

13. 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.

14. 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.



6. Concienciación

La seguridad de una organización recae, en gran parte y de un modo u otro, en los usuarios. Que estos sean conscientes de las amenazas del mundo digital es una tarea imprescindible que se ha de acometer.

Es de suma importancia que las personas que trabajen con equipos informáticos conozcan las diferentes técnicas que utilizan los ciberdelincuentes para perpetrar en los sistemas informáticos, sean capaces de detectarlas y evitarlas para poder reducir así el número de infecciones.

Como se ha detallado, muchas de las estrategias que usan los atacantes requieren del factor humano, en concreto del uso de ingeniería social, como por ejemplo en el caso de correos fraudulentos (phishing) o a la hora de activar las macros en un documento ofimático infectado. Por ello, la concienciación de los usuarios reduce en gran medida el riesgo de ataques.

Asimismo, se ha podido observar cómo los cibercriminales se han percatado de la creciente formación de estos y como resultado han empleado métodos en los que la interacción de las personas no es necesaria.

Esto es muestra de que el mundo de la seguridad informática está siempre en movimiento, y por esta razón resulta necesario que el entrenamiento del personal de una corporación sea continuo en el tiempo y con cierta frecuencia para mantenerse al tanto de las nuevas amenazas que emergen día tras día.

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.

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

7. Shadow copies

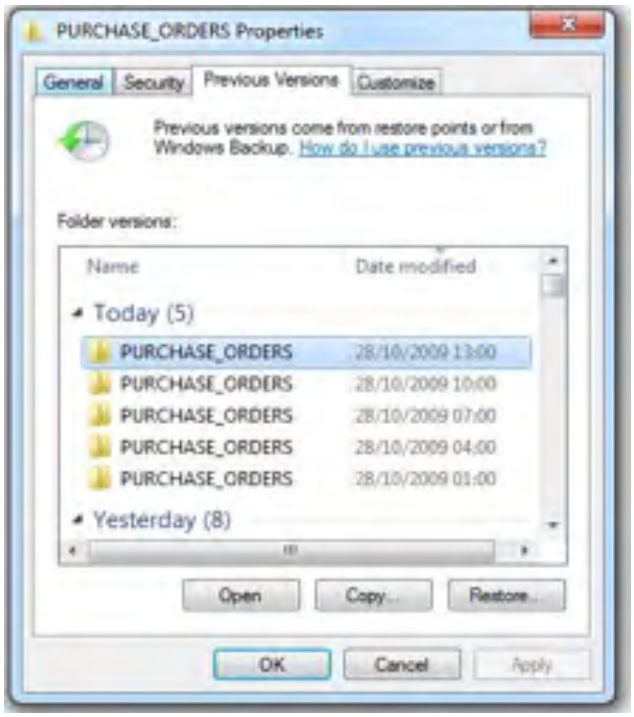
7.1 Sistemas operativos Windows anteriores a Windows 8

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, 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" explícitamente eliminan estos ficheros de restauración. No obstante, 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:

La tecnología Shadow Copies permite al usuario realizar, manualmente o de forma automática, copias de los ficheros almacenados en el equipo, aunque estén en uso

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 7] 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:

- Desde el menú **Protección del Sistema** (siguiendo los pasos 1, 2 y 3 de su creación), se elige la opción **Restaurar Sistema**.
- A continuación, se selecciona el **punto de restauración** al cual se quiere **volver**.
- 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[15] sobre este servicio.

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

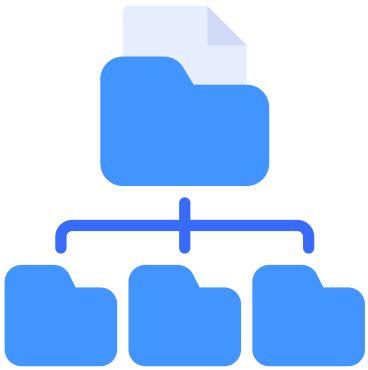
7.2 Sistemas operativos Windows 8 o posteriores

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**[16], 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 dónde 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 ***One Drive*** para su acceso off-line en el equipo.

File History permite hacer distintas copias de los ficheros, almacenando las copias de seguridad en un medio extraíble



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

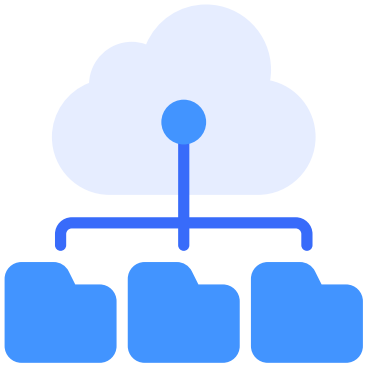
7.3 Backup genérico

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 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 copias actualizadas, completas, depositadas en tres sitios diferentes y geográficamente distantes, además de estar almacenadas en dos 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, un servicio de almacenamiento en la nube y un medio extraíble.

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

> **La medida más efectiva contra el ransomware es disponer siempre de varias copias de respaldo de todos los ficheros importantes**



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

- **Amanda**[17]. 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**[18]. 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**[19]. 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**[20]. 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**[21]**.** 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.

17. Ver http://www.amanda.org/
18. Ver https://backuppc.github.io/backuppc/
19. Ver http://blog.bacula.org/
20. Ver http://www.freefilesync.org/
21. Ver http://www.urbackup.org/

7.4 Bloqueo de macros

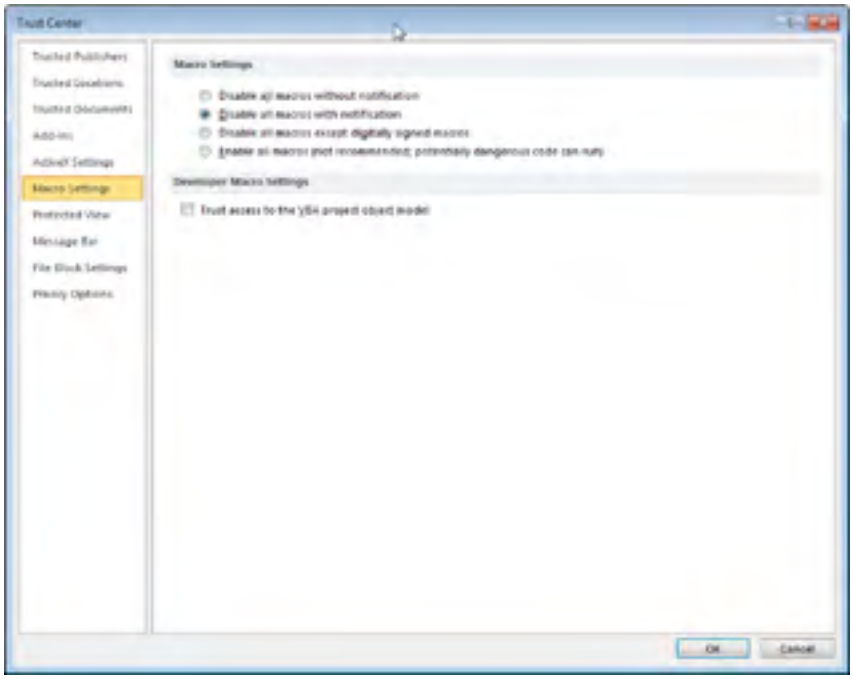
Desde la llegada de la suite MS Office 2007, los documentos que terminan en *.docx*, *.xlsx* y *.pptx* no contienen macros[22], solo lo hacen aquellos que terminan en ".m". En las versiones de MS Office 2016[23], las macros están deshabilitadas por defecto. Lo más recomendable es trabajar en un entorno donde no sea necesario el uso de macros.

Para asegurarse de que las macros están desactivadas[24], 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.

22. Ver https://support.microsoft.com/es-es/office/inicio-r%C3%A1pido-crear-una-macro-741130ca-080d-49f5-9471-1e5fb3d581a8
23. Ver https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/
24. Ver https://support.office.com/es-es/article/Habilitar-o-deshabilitar-macros-en-documentos-de-Office-7b4fdd2e-174f-47e2-9611-9efe4f860b12

[Figura 8]
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, la mejor opción es **"Deshabilitar todas las macros excepto las firmadas digitalmente"**.

En Internet hay servicios que permiten analizar el contenido de cualquier fichero[25], pero también existen otros que están especializados en el análisis de macros dañinas incluidas en 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/).
- **Doc** (https://malwaretracker.com/doc.php).
- **PDF** (https://malwaretracker.com/pdf.php).

25. Por ejemplo, ver https://www.virustotal.com/es/

7.5 Correcta configuración de cuentas de usuario y sus permisos

Cualquier sistema operativo multiusuario (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

7.6 Honeypots o sistemas trampa

Una de las fases de todo proceso defensivo frente a un ataque es la detección de este. 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[26], 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 las acciones del código dañino hasta que accede 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 qué proceso está modificando alguno de los archivos cebo y ofrecerá la opción de terminar ese proceso o dejar que continúe.

[Figura 9] Programa Anti-Ransom

26. Ver https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/

7.7 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**[27], 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, este 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 estos. Las extensiones recomendadas son las que bloquean la apertura de ventanas emergentes, como es el caso de **AdBlock**[28] (Google Chrome y Mozilla Firefox), que evitaría la carga de páginas no solicitadas por el usuario o que son conocidas por ser dañinas. Como complemento, para evitar la aparición de ventanas emergentes, se puede añadir el plugin **PopUp Blocker**.

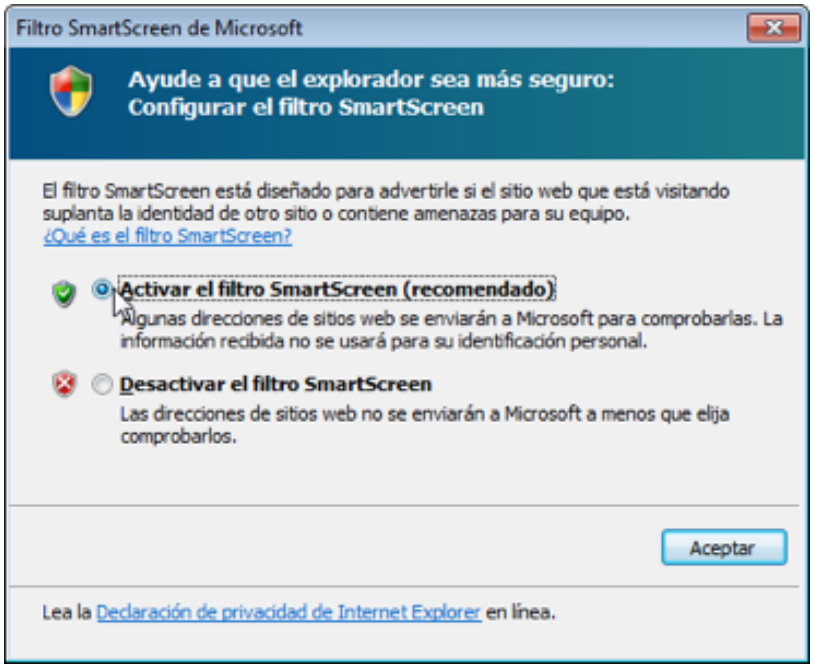
También se recomienda utilizar extensiones para protegerse contra phishing (que están incluidas en los navegadores principales) y otras amenazas, como puede ser la extensión **Avast Online Security** para Google Chrome.

Uno de los métodos de infección más utilizados por el ransomware es la explotación de vulnerabilidades en los navegadores web, recurriendo a los exploit kits

27. Ver https://www.eset.com/bo/empresas/compania/kit-de-exploits-que-son-y-como-protegerse-de-ellos/
28. Ver https://getadblock.com/

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** à **Filtro SmartScreen** à **Activar el filtro**.

[Figura 10]
Bloqueo de Macros en Microsoft Office



Una medida más drástica, pero muy eficaz, es la desactivación de la ejecución de **JavaScript**[29], permitiendo su activación solo en sitios web de confianza. La ejecución de este tipo de código es peligrosa porque puede permitir la activación automática de código dañino 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 dañino, 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 eliminando 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.

29. Ver https://developer.mozilla.org/es/docs/Learn/JavaScript/First_steps/What_is_JavaScript

7.8 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.

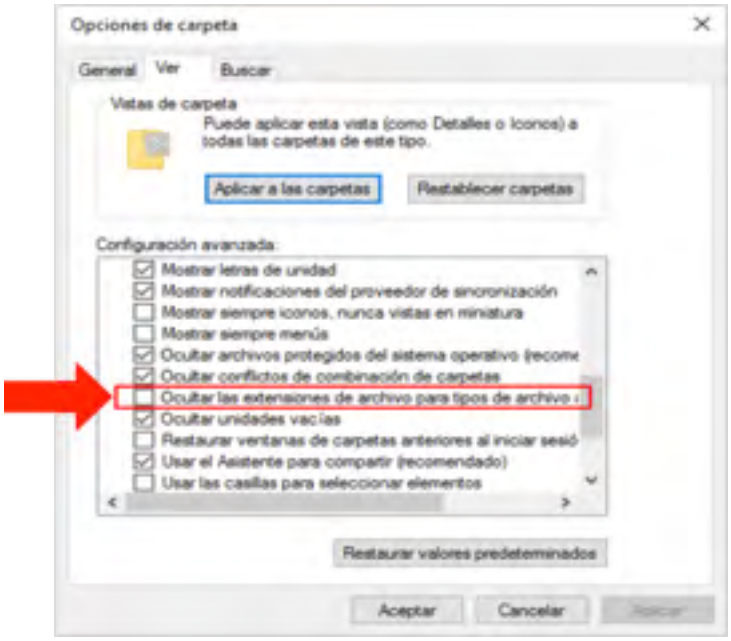
Este comportamiento puede utilizarse para engañar al usuario haciéndole creer que un fichero es otra cosa distinta a la que realmente es; por ejemplo, un proceso ejecutable podría simular ser una imagen al llevar un nombre terminado en *".jpg"*, pero realmente ser un fichero con la terminación *".jpg.exe"*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

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.**

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.

El camuflaje es una técnica de engaño muy utilizada por el malware en general y por el phishing en particular

[Figura 11]
Opción de no ocultar
extensiones conocidas



7.9 Applocker

AppLocker[30] 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.

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

30. Ver https://msdn.microsoft.com/es-es/library/ee424367(v=ws.11).aspx

7.10 Políticas BYOD

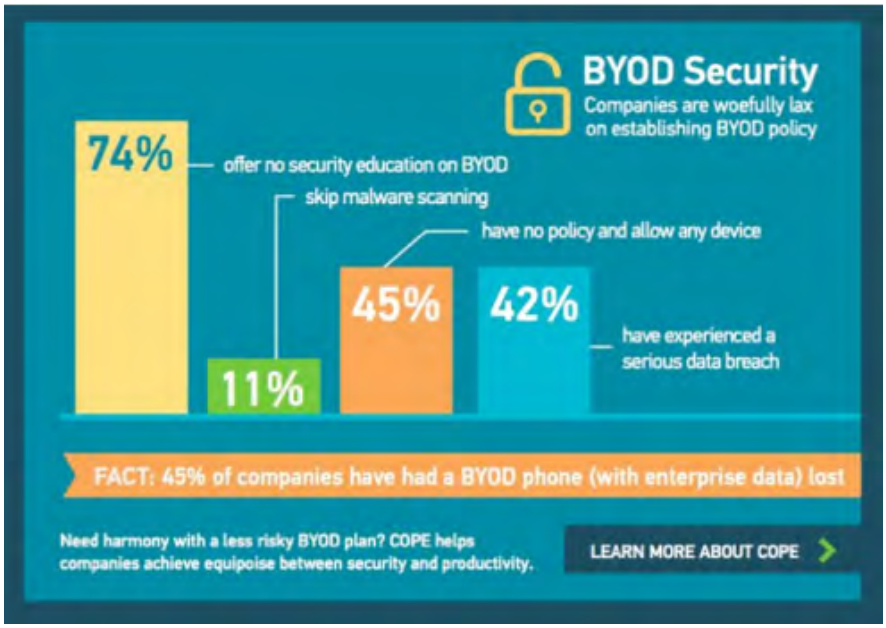
A medida que el BYOD se expande (hasta un 74 % de organizaciones llevan a cabo estas políticas o tienen planeado introducirlas en un futuro.), los empresarios o directores de las organizaciones deben asegurarse de que tanto sus empleados como la propia empresa está debidamente protegida ante los nuevos riesgos que se exponen.

Dichos riesgos pueden suponer:

- Pérdida de información del cliente o de la compañía.
- Accesos no autorizados a la red de la compañía.
- Infecciones de malware.

A medida que el BYOD se expande, los empresarios o directores de las organizaciones deben asegurarse de que tanto sus empleados como la propia empresa está debidamente protegida ante los nuevos riesgos que se exponen

[Figura 12] Estadística sobre políticas derivadas de la implementación de BYOD



Estas son algunas recomendaciones para mitigar lo máximo posible los riesgos:

1. Asegurarse de que los dispositivos no se desbloquean sin introducir un PIN, un patrón o una contraseña. Parece algo obvio, pero más de un 30 % de usuarios no configuran ninguna protección de acceso a su dispositivo al ser más aparatoso.
2. Monitorizar las conexiones que se realizan, especialmente en los puntos de acceso Wi-Fi, los cuales deben estar debidamente configurados y siempre con contraseña de acceso. También pueden implantarse otros controles, como control de acceso por listas blancas o filtrado MAC.
3. Copias de seguridad periódicas.
4. Es interesante tener disponibles servicios del tipo “Find my device”, como implementan muchos teléfonos inteligentes Android, los cuales pueden ser localizados (incluso sin tener el GPS activado) mediante la cuenta Google asociada, dando lugar incluso a poder borrar la información si es necesario.
5. Nunca deben guardarse datos relacionados con la empresa en dispositivos que se vayan a usar fuera de esta.
6. Disponer de antivirus específicos para dispositivos móviles o tabletas.
7. Existen muchas aplicaciones comerciales que se encargan de escanear el sistema en busca de códigos dañinos, así como también de ofrecer una capa extra de protección frente a las amenazas más comunes. Si bien disponer de un software de este estilo no nos garantiza la exención de ataques, esta es una medida indispensable.
8. Como ya se ha comentado, se deberá usar software que ofertan MDM, tales como Docker o Sandbox. El equipo de IT deberá valorar las diferentes posibilidades y examinarlas concienzudamente para apostar por la mejor opción.

Para más información, se puede consultar la guía sobre seguridad en Android del CCN Guía CCN-STIC 453C.

7.11 Contraseñas seguras

Como se ha mencionado, es importante tener unas credenciales de acceso robustos a los servicios desplegados por la organización. Es primordial también asegurarse de que nunca se utilicen usuarios y claves de acceso que ya vinieran configurados por defecto; es necesario reestablecerlos. A continuación, se proporcionan algunas claves para elegir una contraseña segura:

- **Utilizar una combinación de caracteres alfanuméricos: es imprescindible que las contraseñas no se limiten a una secuencia de letras o números exclusivamente.**
- **Usar contraseñas diferentes por cada servicio.**
- **Longitud no menor a 12 caracteres.**
- **Utilización de símbolos para dificultar la fuerza bruta, así como la alternancia de mayúsculas y minúsculas.**

En el mejor de los casos, la contraseña deberá ser **aleatoria**. Se puede comprobar la robustez de la secuencia elegida en servicios web como http://password-checker.online-domain-tools.com/ en el que se estimará cómo de complicado sería para un atacante adivinarla mediante fuerza bruta o ataques por diccionario (se recomienda usar una contraseña parecida y no la final).

Seguir estos pasos puede mitigar notablemente los ataques contra servicios como el ya mencionado RDP.

Es importante tener unas credenciales de acceso robustos a los servicios desplegados por la organización

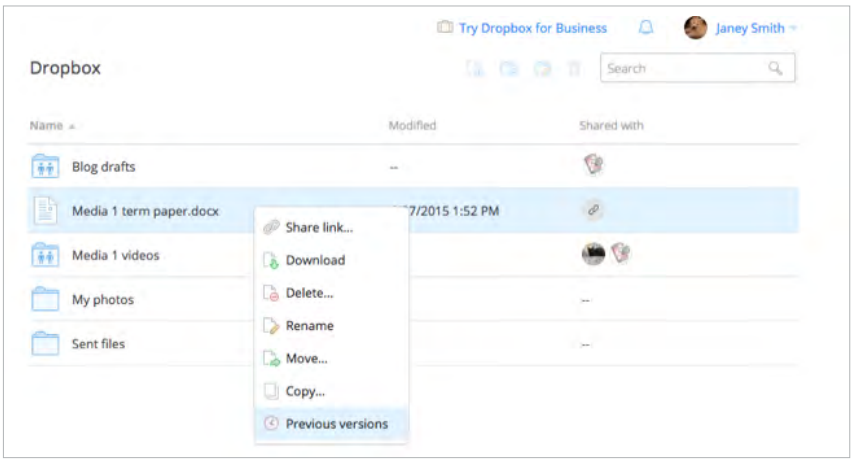
7.12 Recuperación de ficheros mediante almacenamiento en la nube

Desde hace algún tiempo, es muy común el uso de **servicios de sincronización de ficheros**[31] o de almacenamiento en la nube[32].

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 sistema de sincronización copiará 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[33].

[Figura 13]
Control de versiones en Dropbox



31. Ver https://support.microsoft.com/es-es/office/v%C3%ADdeo-%C2%BFqu%C3%A9-es-la-sincronizaci%C3%B3n-de-archivos-7b265f0e-2e36-478a-8857-7026b9ec831c
32. Ver https://azure.microsoft.com/es-es/overview/what-is-cloud-storage/
33. Ver https://www.techopedia.com/definition/1861/versioning-file-system

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.

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**[34] como **Google Drive**[35] 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.

7.13 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 exista de los ficheros, aunque esta 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.**
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.**

34. Ver https://www.dropbox.com/help/11
35. Ver https://support.google.com/docs/answer/190843?hl=es

8. Conclusión

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

Asimismo, 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 y se procede a intentar recuperar los ficheros que han sido afectados.

Dado que el verdadero riesgo del ransomware es que secuestre **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-11/18.

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

9. Decálogo básico de seguridad

Este decálogo de buenas prácticas pretende sentar las bases sobre las medidas de seguridad contra el ransomware.

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 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 actualizado 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 el cortafuegos personal habilitado. No usar usuarios y contraseñas por defecto.

CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


ccn-cert
centro criptológico nacional
CCN
centro criptológico nacional