GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN-CERT centro criptológico nacional

CCN-CERT IA-11/18

Medidas de seguridad contra ransomware

Mayo 2018

Edita:

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA DEL GOBIERNO
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

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
2018.06.04 01:11:54 +02'00'

Fecha de Edición: junio de 2018

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

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, 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. PRÓLOGO

La historia del Ransomware ha cambiado y evolucionado mucho en estos últimos años. Ha sido el tipo de código dañino más destructivo en la última década. Ha pasado de afectar a equipos personales, a ser una amenaza para grandes empresas e incluso infraestructuras vitales (como hospitales, bancos, compañías estatales energéticas…) de diferentes países: en Ucrania se produjo un ataque al Banco Central; en Reino Unido, 16 hospitales cerraron en mayo del 2017; y España se vio afectada con el caso de WannaCry. [Ref.83]

Según los rasgos y características de las campañas principales que han acontecido, este apartado pretende ofrecer una visión de qué es un Ransomware, los cambios adoptados, su evolución, los nuevos objetivos de los ciberdelincuentes que los diseñan, qué estrategias y métodos de infección han usado a lo largo del tiempo (y cómo han variado) y, en definitiva, cuál ha sido la trayectoria del Ransomware.

Tal y como se describe en la Guía de Seguridad (CCN-STIC-401)[1]: El ransomware es un código dañino para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado. El caso índice puede datarse en los años 80 (PC Cyborg), donde este tipo de virus se distribuía por “disquetes”. Sin embargo, es a partir del 2011 cuando las infecciones cobran relevancia y se empieza a consolidar hasta llegar a lo que hoy se conoce como Ransomware.

Aunque los primeros ataques se centraban en determinados países de Europa del Este, en los últimos años la proliferación de Ransomware ha ido en aumento como consecuencia directa de las grandes sumas de dinero que obtienen los atacantes, extendiéndose así por toda Europa, Estados Unidos, Canadá, y prácticamente todo el globo.

Durante este periodo (2011-2016) el método de infección más empleado fue el envío de correos electrónicos fraudulentos, los cuales contenían el código dañino como fichero adjunto. Actualmente, muchas empresas se han preocupado de formar a sus empleados y hacerles conocer este tipo de prácticas, por lo que actualmente los cibercriminales buscan la **no interacción del usuario.** Según Kaspersky Security Bulletin 2016 ([Ref.-55]) se ha producido un descenso del 50% en el número de correos electrónicos que contienen Ransomware, cobrando importancia otras vías de infección como los ataques por RDP (Remote Desktop Protocol). Ejemplo de ello son los ataques causados por la variante *Dharma,* que mediante fuerza bruta a estos servicios conseguía acceso a los equipos y una vez dentro trataba de realizar la infección del

[1]https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

mismo mediante diversos payloads[2], o por otros protocolos como el SMB en los ataques de WannaCry.

A diferencia de otros tipos de virus informáticos, cuyo objetivo es extraer información, el propósito del ransomware es obtener dinero de manera rápida y directa. Se utilizan técnicas cada vez más sofisticadas y complejas de criptografía, con el fin de hacer irrecuperables los archivos cifrados, puesto que los ciberdelincuentes piden una suma de dinero a cambio de los ficheros.

Esta cantidad de dinero que se pide como rescate ha ido en aumento en los últimos años. En 2014 se estimaba un promedio de 373$ por equipo infectado, en 2015 de 294$, pero en 2016 la media se situaba en 1077$ dólares según Symantec (2017). La forma de pago se ha visto prácticamente inalterada, y se usa la moneda virtual Bitcoin por su anonimidad. Al igual que la cantidad de dinero exigido ha aumentado, también lo ha hecho la propagación de este tipo de código dañino. En 2011-2012 se produjo en España el primer caso con cierta repercusión: el Virus de la Policía, donde en el mejor de los casos se producía un bloqueo del sistema (mediante un mensaje a pantalla completa en el que podrá visualizarse el texto de extorsión), pero no un cifrado de los documentos. Existieron más variantes de este virus, pero todos ellos parecieron estar destinados a ordenadores personales y sin mucha propagación, contenidos en del país que atacaban.

En los últimos años, sin embargo, las acciones dañinas de este tipo de código han evolucionado dando lugar a una nueva generación de Ransomware denominada "file encryptors", cuyo principal objetivo es cifrar la gran mayoría de documentos del equipo. La complejidad de dicho cifrado variará en función del tipo de Ransomware. Algunos implementan determinados algoritmos de cifrado en el propio código (Blowfish, AES, TEA, RSA, etc.), mientras que otros se apoyarán en herramientas de terceros (por ejemplo, herramientas como LockDir, GPG, WinRAR, etc.).

Los ataques que tienen como objetivo a grandes empresas y estructuras de un país se interesan en infectar el máximo número posible de máquinas. Por ello, se puede hablar de propagación global con casos como el de WannaCry en 2017, donde se produjeron 400.000 ataques en 150 países diferentes. La extensión de este tipo de malware, así como el crecimiento de variantes, se debe también en parte a lo que se conoce como RaaS (Ransomware as a Service), un servicio por el cual los cibercriminales facilitan la creación de Ransomware a cualquier persona que lo desee a cambio de un porcentaje de las ganancias que su campaña pudiera ganar. Según

[2]En español, carga útil. De forma genérica, hace referencia al contenido relevante de una transferencia, al conjunto de datos transmitidos que es en realidad el mensaje esperado, sin cabeceras ni metadatos. En malware, esta carga útil se refiere a la parte del virus informático que se encarga propiamente de las acciones dañinas.

Kaspersky Security Bulletin 2016, los ataques relacionados con Ransomware se triplicaron en 2016 respecto a 2015.

Figura 1.Period of Ransomware's Attack. Fuente: Kaspersky Security Bulletin 2016 [Ref.-55]

A raíz de estos hechos, el presente informe tiene por objeto dar a conocer determinadas pautas y recomendaciones de seguridad que ayuden a los responsables de seguridad a prevenir y gestionar incidentes derivados de un proceso de infección por parte de determinados tipos de ransomware. El informe describe aspectos técnicos de algunas de las muestras de ransomware más activas actualmente. Asimismo, se indicará el método de desinfección de cada espécimen y, para aquellos casos en los que sea posible, se especificarán también los pasos necesarios para recuperar los ficheros afectados.

Para profundizar en mayor detalle sobre la evolución de este tipo de código dañino se recomienda la lectura de los siguientes informes:

- **"Ransomware: A Growing Menace"**, Symantec [Ref.-2].
- **"Ransomware: Next-Generation Fake Antivirus"**, Sophos [Ref.-3].

3. VÍAS DE INFECCIÓN

Las vías de infección utilizadas por los diversos tipos de ransomware no se diferencian respecto al resto de categorías de código dañino. Siguiendo una serie de pautas básicas de seguridad podrían prevenirse prácticamente la mayoría de infecciones de este tipo de código dañino. A continuación se describen algunos de los métodos de infección más utilizados:

- Uso de mensajes de *Spam/phishing.* A pesar de que otros métodos de infección están cobrando cada vez más relevancia, el uso de correos electrónicos como medio de propagación sigue siendo el más utilizado. El uso de mensajes de *spam* o de *phishing* unido a la ingeniería social, para que el usuario ejecute determinado fichero adjunto o bien acceda a determinada URL, será una de las técnicas más habituales para conseguir ejecutar código dañino en el equipo del usuario. Por ejemplo, multitud de víctimas de **TorrentLocker** en Reino Unido, resultaron infectadas como consecuencia de una página de *phishing* que

simulaba un determinado servicio de seguimiento de paquetes legítimo (*Royal Mail package-tracking*). Una vez el usuario introducía el *captcha* correspondiente, descargaba un ".zip" con el binario dañino. Si el usuario ejecutaba dicho binario, resultaba infectado con TorrentLocker. Además, la página fraudulenta de *Royal Mail* sólo sería visible para visitantes de Reino Unido. Este es sólo un ejemplo de las múltiples estrategias que pueden adoptar los atacantes para tratar de engañar a los usuarios.

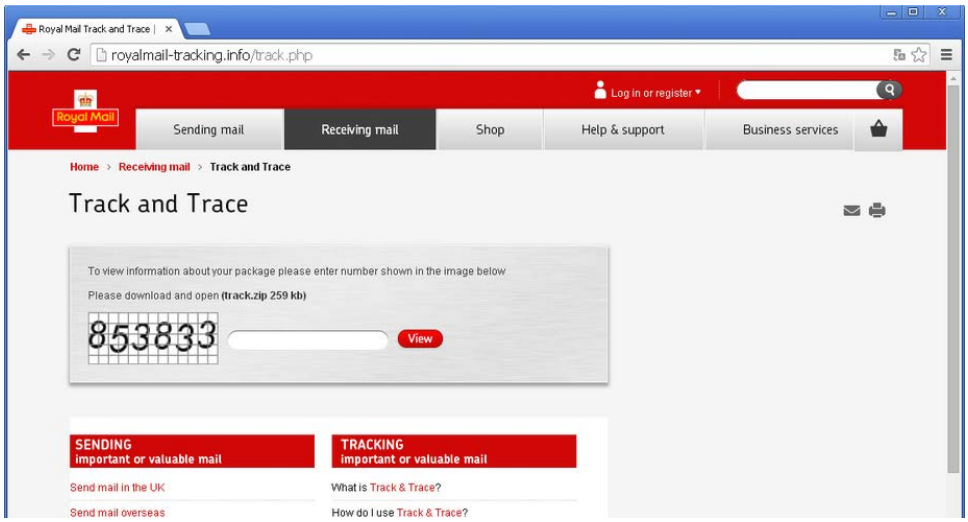


Figura 2. Phishing Royal Mail (TorrentLocker). Fuente: Welivesecurity

En otros casos, menos elaborados, los mensajes de correo contienen directamente como adjunto el propio fichero dañino. La siguiente captura se corresponde con cierta campaña de spam en la que se utiliza el Ransomware Troj/Ransom-JO. El cuerpo del correo contiene información de lo que parece un ticket recientemente comprado por el usuario.

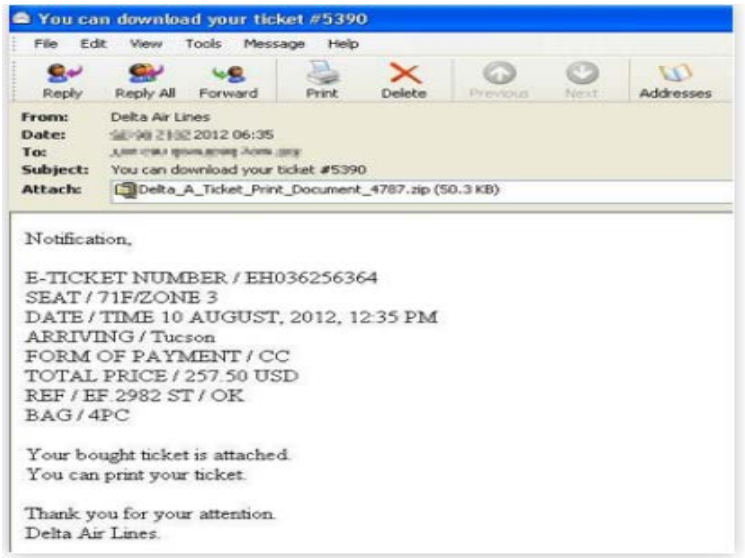


Figura 3. Troj/Ransom-JO. Fuente: Sophos

- *Web Exploit Kits* [3] que se aprovechan de vulnerabilidades en el navegador o en los *plugins*[4] instalados (*drive-by downloads: descargas realizadas automáticamente sin el conocimiento del usuario)*. En estos casos, cuando el usuario navega en cierto sitio web comprometido, un *iframe*[5] redirecciona el navegador a un segundo sitio dañino en el que se encuentra instalado un "*Web Exploit Kit*", que tratará de explotar alguna vulnerabilidad del navegador o de alguno de sus *plugins*. Generalmente, este tipo de *frameworks* suele apoyarse en librerías javascript, como por ejemplo **PluginDetect,** para obtener las versiones de los *plugins* utilizados y ejecutar así el *exploit*[6] correspondiente. Uno de los métodos de distribución de CryptoWall fue el Infinity Exploit Kit (también conocido como Redkit V2). Cada vez más *exploit* kits disponen de un ransomware en su sistema de distribución.

- Por medio de otro código dañino. Un sistema infectado por especímenes como Citadel, Zeus, etc., puede utilizarse para descargar y ejecutar el ransomware. Por ejemplo, una de las vías de infección de CryptoWall en los últimos meses se ha realizado mediante el *downloader* **Upatre** procedente de la *botnet* de *spam* **Cutwail**.

- Servicios RDP (*Remote Desktop Protocol*) con contraseñas predecibles o vulnerables a ataques por diccionario. Los atacantes suelen utilizar herramientas automatizadas que escanean equipos de forma masiva en busca de servicios como Terminal Server. Posteriormente, intentarán acceder al mismo mediante cuentas y contraseñas comúnmente utilizadas: admin, Administrator, backup, console, Guest, sales, etc.

- A través de anuncios señuelo o *banners*.

- Métodos que dependen cada vez menos de la iteración del usuario: Mediante la ingeniería social, los cibercriminales difunden (en la mayoría de los casos) documentos de ofimática en los que se muestra un contenido ilegible. Se pide habilitar las macros para leer el contenido del mensaje, lo cual es una trampa para poder ejecutar código en la máquina donde se abre el documento.

[3] *Web Exploit Kit*: código dañino que automatiza la explotación de vulnerabilidades en el navegador web.
[4] Un *plugin* es una extensión que complementa la funcionalidad de un software.
[5] Por *iframe* se conoce un tipo de elemento HTML que permite insertar o incrustar un documento HTML dentro de otro documento HTML.
[6] Un *exploit* es un programa que explota o aprovecha una vulnerabilidad de un sistema informático en beneficio propio.

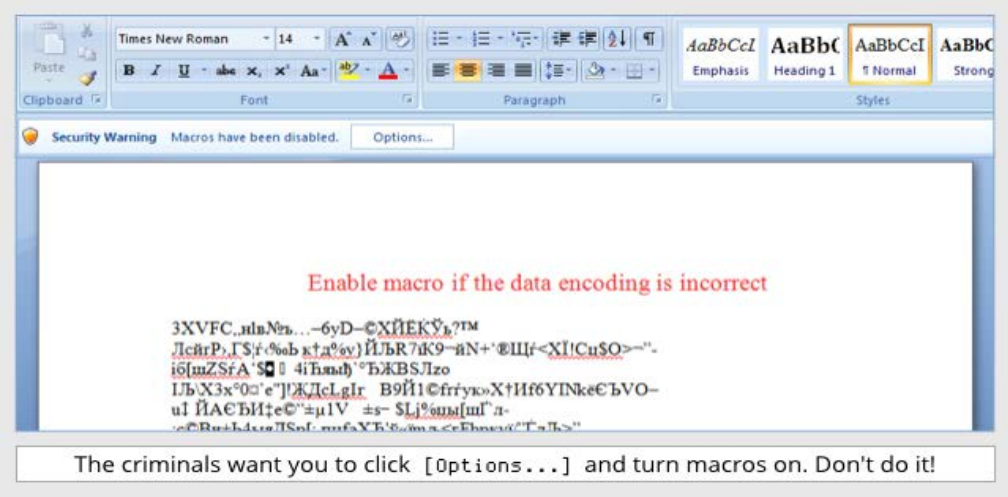


Figura 4. Ejemplo de documento dañino.

Este método requería la interacción del usuario pero, desde finales de 2017 hasta hoy en día, se observa cada vez con más frecuencia cómo van surgiendo "nuevos" métodos automáticos (realmente ya conocidos pero no usados masivamente), que no necesitan del factor engaño. Alguno de estos métodos puede observarse en la ejecución de código arbitrario con la sola apertura de un documento de Microsoft Word7, donde no es siquiera necesaria la habilitación de macros o que una persona dé permisos [Ref.-55] [Ref.-63] [Ref.-64].

Este tipo de métodos suele ser trasparente y difícil de detectar. A su vez, existen diversos CVE −Common Vulnerabilities and Exposures, siglas CVE, es una lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único−, relacionados con métodos utilizados para saltarse la necesidad de interacción entre el usuario y la UAC (Control de cuentas). Algunos de estos CVE son CVE-2010-43988, CVE-2011-00459 o CVE-2017-021310. Más información en las referencias [Ref.-76] y [Ref.-77].

[7] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-064
[8] https://www.cvedetails.com/cve/CVE-2010-4398/
[9] https://www.cvedetails.com/cve/CVE-2011-0045/
[10] https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0213

4. MEDIDAS PREVENTIVAS

4.1 Listado de medidas preventivas

En la siguiente lista se resumen las principales medidas que se han de adoptar, en orden de prioridad, para prevenir, detectar y/o mitigar parcialmente la acción de un *ransomware*:

1. **Mantener copias de seguridad periódicas (*backups*) 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 *firewall*** a nivel de aplicación (basado en *whitelisting* de aplicaciones permitidas)**.**
4. **Disponer de sistemas *antispam* a nivel de correo electrónico**, y establecer un nivel de filtrado alto, de esta manera reduciremos las posibilidades de infección a través de campañas masivas de *ransomware* por mail.
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*) y que será descontinuada en 2018. Existe una guía para su correcta configuración, denominada Guía de Seguridad de las TIC CCN-STIC 950 “Recomendaciones de empleo de la herramienta EMET” [Ref.78]. Se propone, como alternativa, utilizar las herramientas que Windows 10 provee por defecto.
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 *dump* de la memoria del *código dañino* en el momento de su ejecución, en el que con suerte se hallará la clave de cifrado simétrico 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.

4.2 Principales medidas preventivas

Para reducir las posibilidades de infección por parte de este tipo de código dañino se recomienda seguir las siguientes pautas de seguridad:

- Mantener copias de seguridad periódicas de todos los datos importantes. Existe la “norma” del 3-2-1, que determina que se deberían realizar al menos tres copias de seguridad de los datos, dos de las cuales deberán estar en soportes diferentes (por ejemplo, un DVD o un disco duro externo, un USB o incluso en la nube) y una última en formato físico en un lugar distinto a donde se almacenan las dos primeras, evitando así posibles catástrofes como incendios, robos, etc. Es importante que las copias de seguridad no sean accesibles desde la red de la organización (o, si no es posible, que al menos dos de las tres copias no sean accesibles).

  Esto último se debe a que algunos Ransomware como **CryptoLocker** tienen capacidad para listar y recorrer las unidades montadas en el equipo. De esta forma, si un USB conectado al sistema infectado se emplea para guardar copias de seguridad, corre el riesgo de ser infectado también. Dichas acciones dañinas afectarían también a aplicaciones como Dropbox y similares, las cuales utilizan unidades de almacenamiento locales. Desde Windows es posible programar

copias de seguridad periódicas de forma sencilla desde la opción **"Copias de Seguridad y Restauración"** *(Panel de Control -> Sistema y Seguridad -> Hacer una copia de seguridad del equipo).*

- **Utilizar VPN** (*Virtual Private Networking*) como método de acceso remoto a determinados servicios. Parte de las infecciones por Ransomware se producen a través de servicios de escritorio remoto. En concreto, se ha detectado el uso de RDP para propagar variantes como Shade, Apocalypse, Dharma o SamSam.
- **Los atacantes emplean herramientas y scripts con diccionarios** de palabras para tratar de obtener credenciales válidas de usuarios. En el caso de Dharma, por ejemplo, una vez consigue acceso al equipo, mediante el portapapeles o las unidades de almacenamiento compartidas, descargaba diferente *payloads* en la máquina con los que trataba de infectarla.

  Por ello, y para reducir al máximo el éxito de este tipo de ataques, se propone:

  1. Deshabilitar el portapapeles y unidades de almacenamiento compartidas en los equipos con acceso remoto disponible desde fuera. En el caso de Windows Server 2008:
  2. En la máquina que actúa como servidor, haga clic en Inicio.
  3. Seleccione Herramientas Administrativas y, a continuación, seleccione configuración de host de sesión de escritorio remoto.
  4. Debajo de la sección Conexiones, haga clic derecho en el nombre de la conexión y haga clic en Propiedades.
  5. En la ventana de Propiedades, seleccione la pestaña Configuración del cliente
  6. En Redirección, tiene la posibilidad de habilitar o deshabilitar los recursos. En este caso en concreto deshabilite "No aceptar redirección al portapapeles" y "No admitir redirección de las unidades"

- **Mantener el Sistema Operativo actualizado**. Como se ha comentado, el acceso por RDP es el primer paso, pero la infección se consigue con el aprovechamiento de alguna vulnerabilidad existente en el equipo. Es por ello que se recomienda tener las actualizaciones automáticas activadas.
- Si es totalmente necesario que el equipo sea accesible desde Internet:
  - **Use contraseñas seguras**. La obtención de la combinación de usuario y clave para poder acceder al sistema se realiza mediante fuerza bruta, es decir, probando todas las posibles combinaciones de caracteres. También se puede llevar a cabo mediante ataque por diccionario, esto

es, comprobando los usuarios y contraseñas más habituales (admin:1234, admin:admin…). Otro tipo de ataque puede producirse mediante el uso de diccionarios, archivos que contienen usuarios y contraseñas comúnmente usados. Para combatir este tipo de ataque no se deben usar las credenciales por defecto. Han de ser cambiadas, y además ser de una longitud considerablemente larga, que incluyan mayúsculas, minúsculas, números e incluso símbolos. Una página que puede servir para consultar la robustez de la contraseña elegida y obtener una estimación del tiempo que se necesita para obtenerla por fuerza bruta y/o diccionario es http://password-checker.online-domain-tools.com/. **En caso de usar este servicio o similares, escoger finalmente una contraseña similar y no la final.**

- **No utilizar el usuario Administrador** para acceder remotamente. Una configuración correcta de los usuarios y los permisos de estos es esencial. En la mayoría de los casos, una cuenta con menos privilegios que la de Administrador será suficiente para realizar la mayoría de tareas en el equipo remoto.
- **Utilizar puertos no predeterminados**. La mayoría de cibercriminales utilizan herramientas que escanean los puertos que RDP usa por defecto para encontrar estos servicios y atacarlos. Una medida para poder evitar ser escaneado por las herramientas más básicas es cambiar el puerto que viene preconfigurado por uno de su elección.
- **Usar políticas White Lists**. Mediante la correcta configuración del Firewall puede configurar lo que se conocen como “listas blancas”. Solo los equipos (IP's) que se encuentren en dichas listas, podrán hacer uso del servicio. Puede complementarse con Black Lists, listas negras, para una mayor seguridad.
- **Establecer un máximo de intentos de acceso**. Con esta medida se reducen los ataques de fuerza bruta/por diccionario.

- Con la ayuda del **visor de eventos de Windows** se pueden identificar IP’s sospechosas, pues todos los eventos relacionados con el acceso por RDP quedan registrados con el ID 1149. La información incluye la cuenta que se ha usado (y posiblemente usurpada) y la IP. A continuación, se muestra cómo desde el Firewall de Windows (Versión 10, aunque es similar para versiones anteriores) pueden crearse listas de acceso permitidos (White List) o listas de bloqueo (Black List):

  1. En primer lugar, hacer clic en el icono inferior izquierdo con el logo de Windows (Inicio) y escribir “Windows Defender Firewall” y hacer clic en Windows Defender Firewall con seguridad avanzada.

2. Acto seguido, sobre Reglas de Entrada se debe presionar el botón derecho del ratón y seleccionar “Nueva regla…”

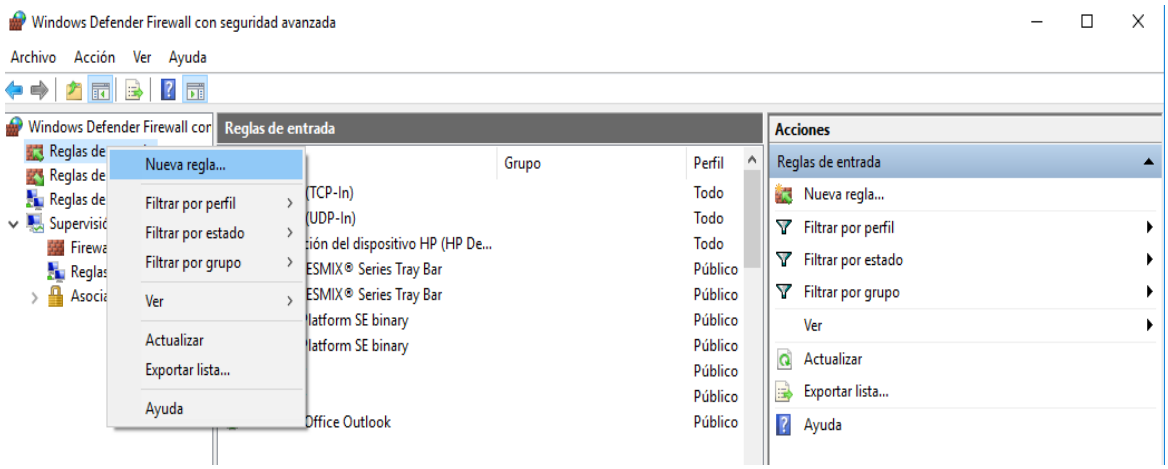


Figura 5. Creación de reglas en el Firewall de Windows.

3. En la nueva ventana que aparece, escoger la opción “Personalizada” y se presiona Siguiente. En la próxima ventana, se deberá seleccionar la opción “Todos los programas”

4. La configuración del paso posterior debe ser la siguiente:

   - Tipo de protocolo: TCP
   - Número de protocolo: 6 (por defecto).
   - Puerto local: Puertos específicos, en concreto el 3389.
   - Puerto remoto: Todos los puertos.

El puerto 3389 es el usado por defecto por el servicio RDP. En caso de que sus sistemas usen un puerto personalizado, será necesario sustituir el 3389 de la imagen por dicho puerto. También es recomendable en este paso añadir el puerto 445, que es el puerto por defecto del servicio SMB, el cual también está siendo atacado por Ransomware (WannaCry, NotPetya).

5. En el siguiente paso, se decide si se implementará una lista de IP’s permitidas (White List) o una lista de IP’s bloqueadas (Black List)

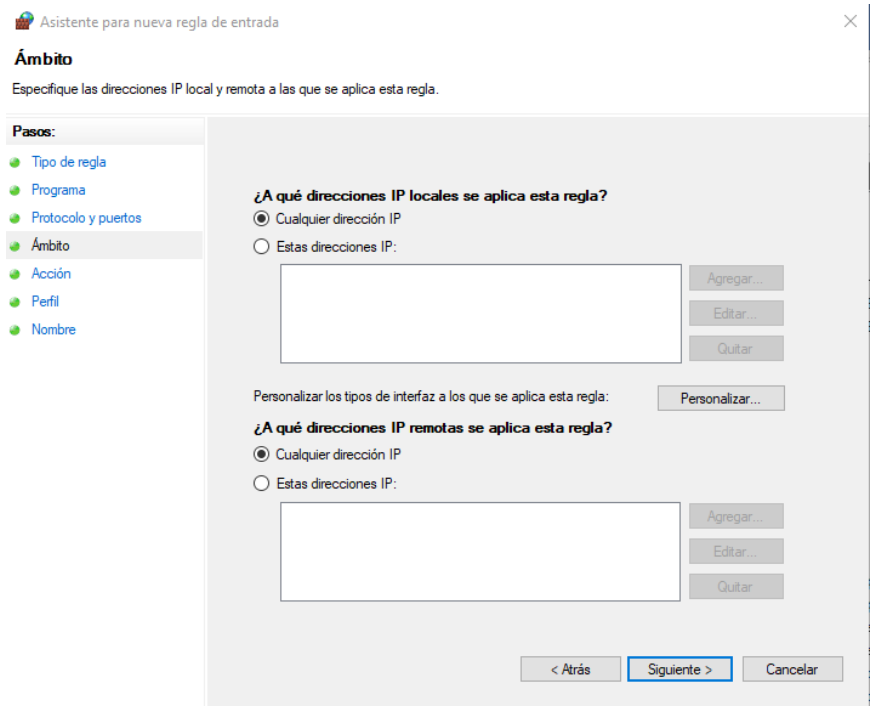


Figura 6. Elección de IP's a permitir (i).

En general, las listas de acceso permitido son más seguras, ya que el atacante solo podría tratar de acceder al servicio si usara alguna de las IP's listadas. Sin embargo, si se programa una serie de IP's bloqueadas,' y se incluye la dirección del atacante, a este le bastaría simplemente con cambiar su IP, lo cual es mucho más sencillo. Se va a suponer por tanto que se va a establecer una lista de accesos permitidos. La primera opción no debe ser cambiada, y a la segunda pregunta ("¿A qué direcciones IP remotas se aplica esta regla?") se selecciona "Estas direcciones IP".

6. Acto seguido, haga clic en Agregar y se le presentará la próxima ventana donde se deberá especificar qué IP's son las que deben tener acceso al recurso. Finalmente, se hace clic en Siguiente y se selecciona "Permitir la conexión".

7. Se avanza hasta la última ventana, en la que se nombra la regla, se hace clic en finalizar y quedaría configurado el Firewall para bloquear cualquier IP que trate de acceder al servicio RDP diferente a las establecidas.

Para comprobar rápidamente la configuración del Firewall se puede realizar un rápido escaneo de nuestra IP para examinar que puertos están abiertos y accesibles desde fuera. Una herramienta para esto es: http://www.shieldcheck.com/, que realiza un escaneo de los puertos más comunes.

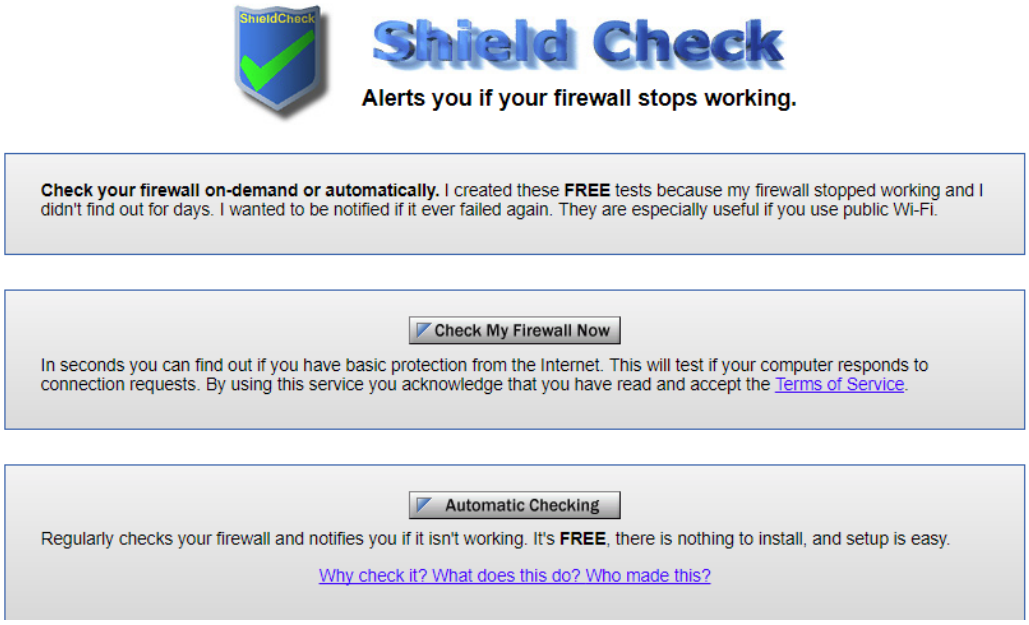


Figura 7. ShieldCheck. Herramienta de escaneo de puertos online.

- Para prevenir infecciones desde páginas dañinas que emplean Web Exploit Kits, así como ficheros ofimáticos dañinos que puedan llegar al equipo por medio de correo electrónico, redes sociales, etc., se recomienda mantener el software correctamente actualizado. Algunas de las principales vías de infección en ataques de este tipo suelen ser el navegador, versiones antiguas de Java, Flash o Adobe Acrobat.
- Además de disponer de software correctamente actualizado, es recomendable utilizar **soluciones que permitan mitigar *exploits***. Herramientas como **EMET** [11][Ref.-5] permiten aplicar determinadas medidas de seguridad tales como DEP, EAF, ASLR, SEHOP, NPA[12], etc., de forma personalizada a los procesos que se deseen, para prevenir la ejecución de código dañino (incluidos 0-days[13]). Se recomienda que herramientas como el navegador así como aquellas utilizadas para abrir ficheros ofimáticos (Microsoft Office, Adobe Reader, etc.) se encuentren protegidos por EMET (consultar guía de uso CCN-STIC 950 [Ref.78]) o herramientas similares. Este tipo de aplicaciones no deben verse como una alternativa al antivirus, sino como una herramienta adicional más de protección.

[11] EMET (abreviatura de *Enhance Mitigation Experience Toolkit*) es una utilidad gratuita de Microsoft que permite configurar a bajo nivel multitud de aspectos de seguridad de un sistema.
[12] DEP, EAF, ASLR, SEHOP, NPA: conjunto de características de seguridad incluidas en la mayoría de sistemas operativos modernos que permiten mitigar exploits.
[13] Los llamados *exploits* de día-cero (*zero-day)* son aquellos que todavía no se han publicado y, por tanto, no disponen de soluciones de seguridad que eviten la vulnerabilidad

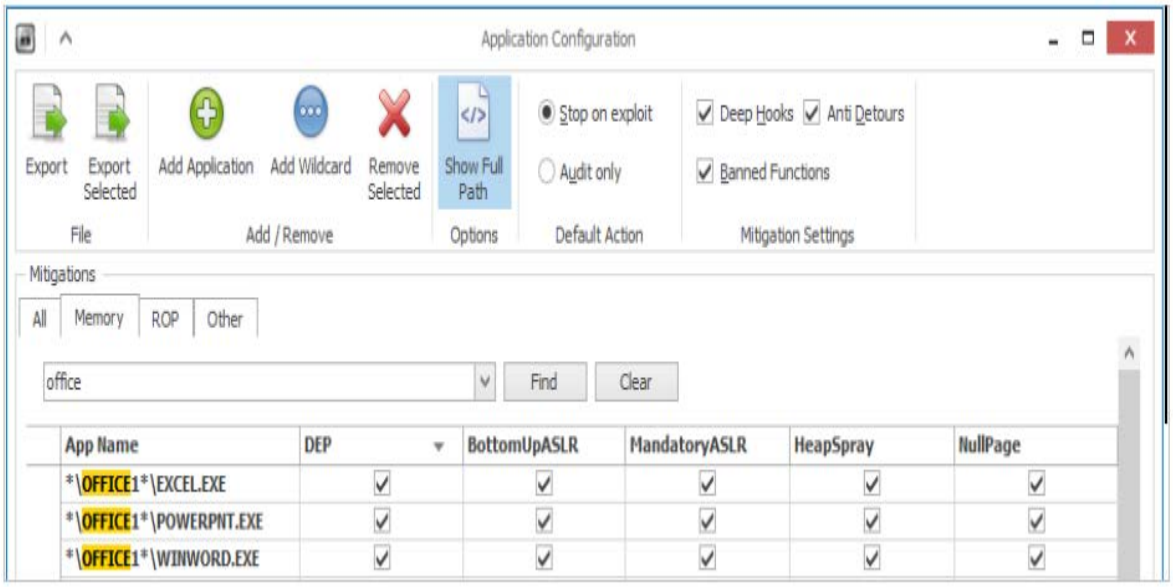


Figura 8. EMET

- Valorar el **uso de aplicaciones de lista blanca (W*hite Listing*)**. Este tipo de aplicaciones [Ref-.6] están diseñadas para proteger el sistema operativo contra programas no autorizados y dañinos. Su objetivo es garantizar que sólo los programas explícitamente autorizados puedan ser ejecutados, impidiendo la ejecución de todos los demás. La implementación de este tipo de sistemas se consigue utilizando una combinación de software encargado de identificar y permitir la ejecución de los programas aprobados con el uso de listas de control de acceso, mediante las cuales se impide la modificación de dichas restricciones. Por ejemplo, **AppLocker** [Ref.-7] es un conjunto de políticas presentes en Windows 7 que permiten establecer múltiples niveles de cumplimiento y establecer listas blancas de ejecución. Existen diversas alternativas de terceros que permiten también implementar listas blancas, por ejemplo **Bit9 Parity Suite** [Ref.-8], **McAfee Application Control** [Ref.-9], **Lumension Application Control** [Ref.-10], etc.
- En Windows 10, a través del Centro de Seguridad Windows Defender, se ha añadido la funcionalidad **"Acceso controlado a carpetas"**[14], que permite establecer un control sobre las aplicaciones que pueden modificar una serie de directorios protegidos. De este modo, las carpetas que se establezcan como carpetas protegidas no se verán modificadas por software no autorizado, evitando así el cifrado por parte de un ransomware.

[14] https://support.microsoft.com/es-es/help/4046851/windows-10-controlled-folder-access-windows-defender-security-center

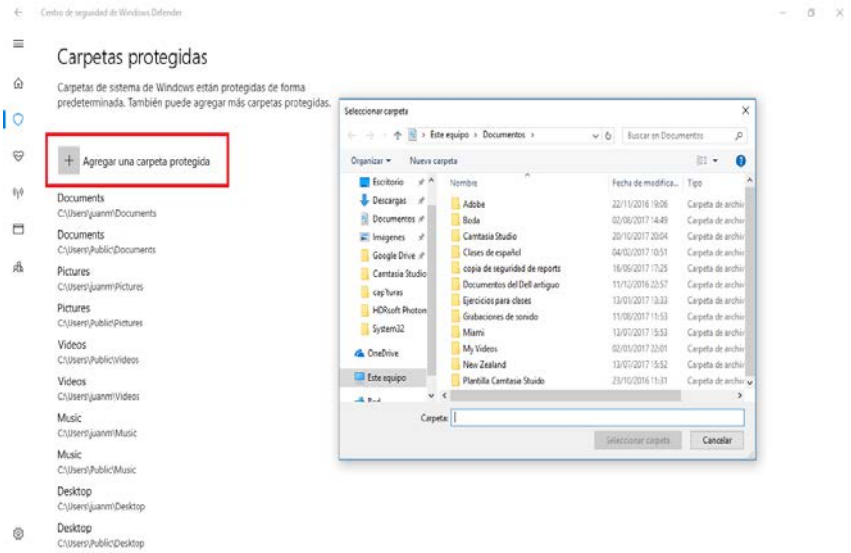


Figura 9. Carpetas protegidas en Windows 10.

- Considérense herramientas como **CryptoLocker Prevention Kit** [Ref.-11], las cuales permiten crear políticas de grupo para impedir la ejecución de ficheros desde directorios como App Data, Local App Data o directorios temporales (comúnmente utilizados por gran variedad de ransomware).
- Otro software similar con una instalación más intuitiva y sin necesidad de utilizar el **Group Policy Editor** (disponible en las versiones Professional, Ultimate y Enterprise de Windows) es **CryptoPrevent**. Esta herramienta [Ref.-12] permite configurar determinadas reglas objeto de directiva de grupo en el registro para bloquear la ejecución de determinados tipos de ficheros (.exe, .pif, .com, etc.), ubicados en ciertas localizaciones del sistema. La herramienta permite también crear listas blancas de aplicaciones confiables, generar alertas vía email, etc. Aunque la herramienta presenta una interfaz sencilla de configuración, es posible parametrizar opciones más concretas por medio de su vista avanzada (imagen de la derecha). Este tipo de herramientas ayudarán a prevenir una gran variedad de ransomware (incluidos algunos tan dañinos como CryptoLocker).

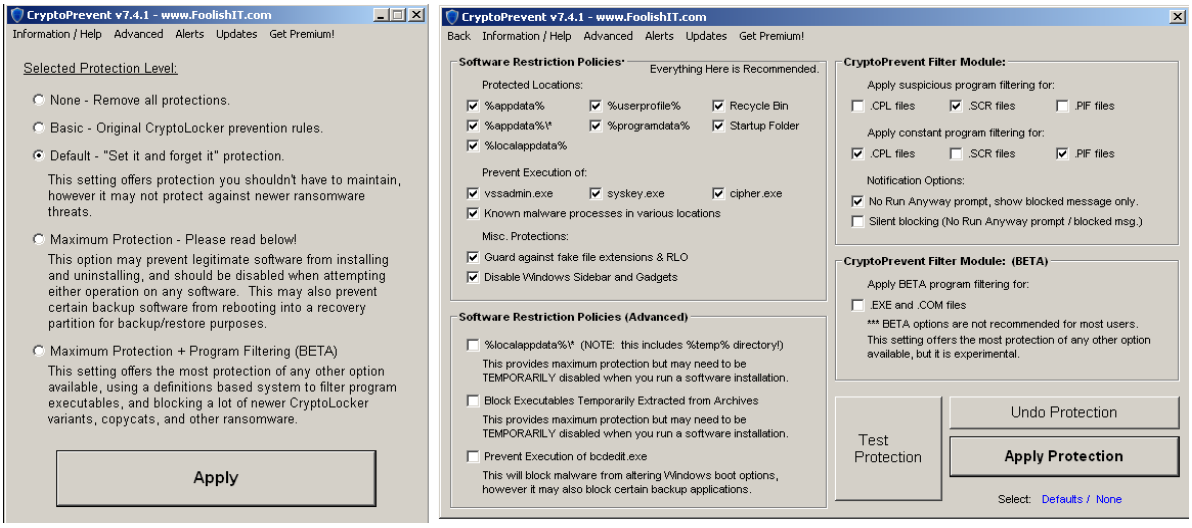


Figura 10. CryptoPrevent

- Si en lugar de utilizar las herramientas previamente descritas se desea añadir políticas de forma manual en la "Directiva de Seguridad Local", deberán llevarse a cabo los siguientes pasos.

  1. Dentro de las directivas de restricción de software, hay que pulsar el botón derecho sobre la categoría "**Reglas adicionales**" y posteriormente se elegirá la opción "**Regla de nueva ruta de acceso**". En la siguiente imagen se muestra una regla para impedir la ejecución de ficheros ".exe" desde la ruta %AppData%, la cual es frecuentemente utilizada por diversos tipos de ransomware para volcar sus binarios. Únicamente es necesario especificar la ruta de acceso y el nivel de seguridad "**No permitido**".

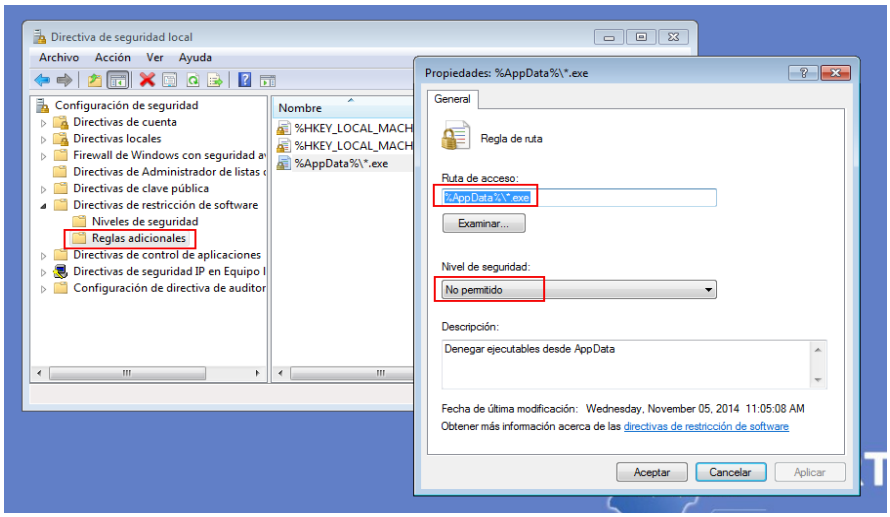


Figura 11. Directiva de seguridad local

2. Tras instalar la política, si se intenta ejecutar un binario desde dicha ruta se generará la siguiente alerta, además del evento correspondiente.

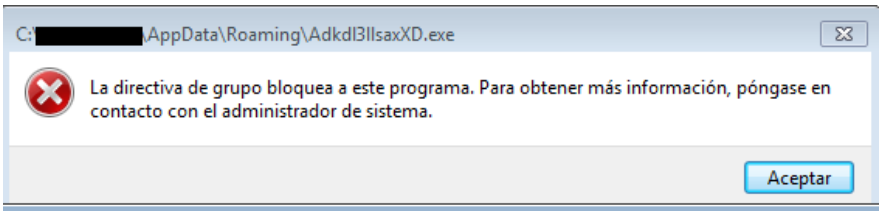


Figura 12. Alerta: Bloqueo programa

Considérense otras rutas como %UserProfile%\Local Settings, %UserProfile%\Local Settings\Temp\, etc., para denegar la ejecución de binarios. Muchos tipos de código dañino, no solo ransomware, son descargados y ejecutados desde estos directorios.

- Se recomienda **mostrar las extensiones para tipos de ficheros conocidos**. Algunos Ransomware como CryptoLocker o CryptoTorrent utilizan ficheros dañinos con doble extensión (.PDF.EXE) para ocultar su verdadera naturaleza. Si el sistema no muestra la extensión principal del fichero puede hacer creer al usuario que se trata de un fichero ofimático en lugar de un ejecutable.

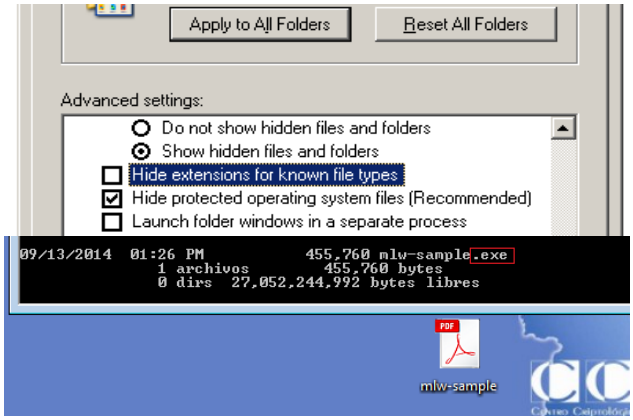


Figura 13. Mostrar extensiones de ficheros conocidos

- Es fundamental **educar a los usuarios** en aspectos de ingeniería social. Gran parte de las infecciones provienen a través de mensajes de correo electrónico que tratan de incitar al usuario a abrir una determinada página o ejecutar cierto fichero. Existen multitud de soluciones de seguridad que ayudan a prevenir este tipo de ataques por medio, por ejemplo, de mail scanners que permiten analizar las URL de los correos electrónicos y determinar la peligrosidad de las mismas. Sin embargo, dichas soluciones no son infalibles. Por ejemplo, la variante CryptoLocker.F utilizaba como vía de infección un correo electrónico con ciertos enlaces a páginas dañinas. Cuando se abre uno de estos enlaces se muestra un captcha al usuario para poder visualizar el contenido de la página.

De esta forma, se asegura que es el usuario y no una solución de seguridad la que alcanza la página. Educar a los usuarios sobre los métodos utilizados por los atacantes será la manera más eficaz para prevenir infecciones.

- No utilizar cuentas con permisos de administrador a no ser que sea estrictamente necesario. La ejecución de cierto código dañino, bajo una cuenta de administrador, permite llevar a cabo todo tipo de acciones dañinas en el sistema. Considérese el uso de cuentas limitadas para la gran mayoría de usuarios.
- Utilizar un s**istema antivirus correctamente actualizado y un firewall de aplicación** en el sistema operativo con reglas de filtrado restrictivas. Dichas contramedidas servirán como refuerzo adicional a otros sistemas de protección basados en red tales como IDS/IPS, etc. Cabe destacar que diversas aplicaciones AV disponen de módulos y funcionalidades específicas para tratar de prevenir las acciones dañinas de los ransomware como, por ejemplo, el **Advanced Memory Scanner** [Ref.-13] de ESET, el módulo System Watcher [Ref.-14] de Kaspersky o la tecnología **CryptoGuard** [Ref.-15] de HitmanPro.Alert. La siguiente captura se corresponde con este último software. CryptoGuard basa su funcionamiento en la monitorización del sistema de ficheros, bloqueando procesos que generen cualquier tipo de comportamiento anómalo sobre el mismo. Dicha solución es bastante efectiva para mitigar ataques como los llevados a cabo por CryptoLocker, Dorifel, etc.

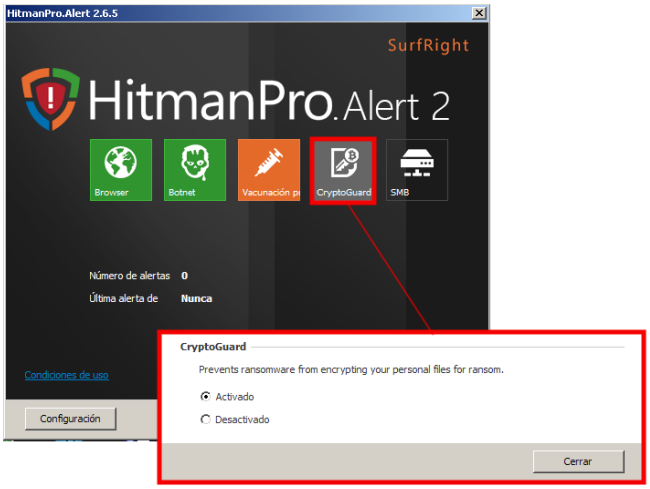


Figura 14. HitmanPro.Alert (CryptoGuard)

La herramienta "**Anti Ransom**" [Ref.-42] es una alternativa para mitigar parcial o totalmente el impacto producido por una infección de ransomware. El funcionamiento de esta aplicación es sencillo:

1. Se crean "*honeyfiles*" (ficheros susceptibles de ser cifrados por ransomware) y se ubican en carpetas del usuario (Mis Documentos, C:\Documents and Settings\, etc.).

2. Se monitoriza si alguno de los "honeyfiles" es alterado.

3. Detecta el proceso que está modificando el "honeyfile" en cuestión.

4. Vuelca la memoria del proceso en busca de la clave de cifrado que estaba empleando para cifrar el fichero.

5. Mata el proceso correspondiente al ransomware.

Se trata de una utilidad que, en el peor de los casos, será capaz de parar el proceso de cifrado del ransomware, lo cual mitiga parcialmente el impacto. Y, en algunos casos, encuentra la clave de cifrado que estaba usando el ransomware, con la cual es posible descifrar los ficheros que hubieran sido cifrados.

5. MEDIDAS REACTIVAS

5.1 Procedimiento general

En el momento en que se produce una infección por ransomware se comenzarán a cifrar los ficheros del equipo y los mapeados en las unidades conectadas, tanto dispositivos físicos (USB's, discos duros externos, etc.) como unidades de red.

En la gran mayoría de situaciones se es consciente de la infección cuando el ransomware ha finalizado su ejecución y todos los ficheros se han cifrado. Sin embargo, existe la posibilidad de que éste aún no haya terminado su ejecución, permitiendo en el mejor de los escenarios recuperar la clave de cifrado o evitar que más ficheros sean cifrados.

Se recomienda seguir los siguientes pasos generales en el momento de la detección de un ransomware:

1. **Desconectar las unidades de red**, esto supone "tirar del cable" de red (o desactivar las interfaces inalámbricas). De este modo se podría llegar a evitar el cifrado de ficheros en unidades de red accesibles, en el caso de que el ransomware aún no hubiera finalizado su ejecución.

Figura 15. Desconexión de unidades de red

2. **Comprobar si el proceso dañino aún sigue ejecutándose**. Esta tarea no es sencilla en muchos casos ya que el proceso dañino podría haberse inyectado en otro legítimo o simplemente podría haber finalizado su ejecución.

   Sin embargo, en caso de identificarse el proceso en cuestión (usando herramientas como Process Explorer de Sysinternals), desde el Administrador de Tareas de Windows (Taskmanager) se realizará un dump (volcado de la memoria) del proceso dañino. Para ello, hay que hacer clic derecho sobre el proceso y seleccionar la opción "Crear archivo de volcado" (se guardará en %TMP%). Una vez volcado el fichero hay que guardarlo a buen recaudo en un sistema aislado.

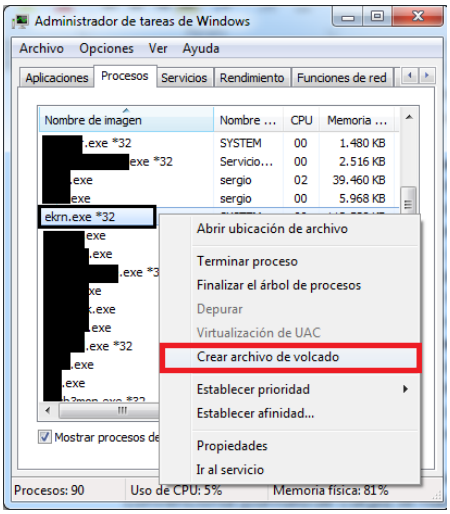


Figura 16. Realización de volcado de memoria de un proceso

3. **Finalizar la ejecución del proceso dañino.** Para ello existen dos alternativas:
   I. En caso de haberse identificado el proceso simplemente bastará con parar su ejecución desde el Administrador de Tareas de Windows: clic derecho sobre el proceso y seleccionar la opción "Finalizar el árbol de procesos".

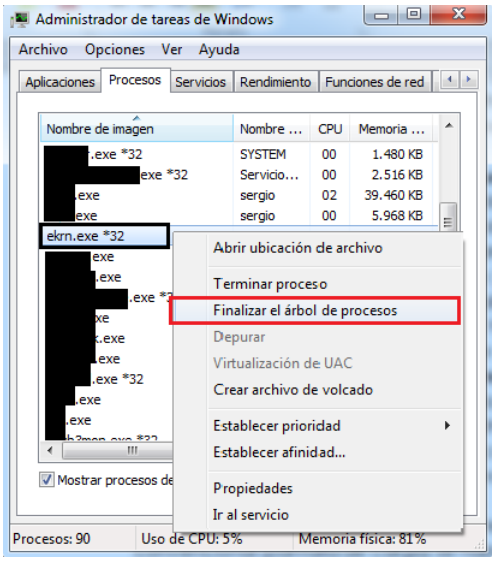


Figura 17. Finalización del proceso

II. Si no se ha podido identificar el proceso, se recomienda apagar el equipo de manera manual e inmediata.

4. **Arrancar el equipo en Modo Seguro**. Antes de que arranque Windows de manera convencional (pantalla de carga) se habrá de pulsar la tecla F8 para acceder al menú de arranque avanzado, desde el que se seleccionará iniciar desde "Modo Seguro". De este modo evitaremos que el ransomware vuelva a arrancar de nuevo en caso de que éste fuera persistente.

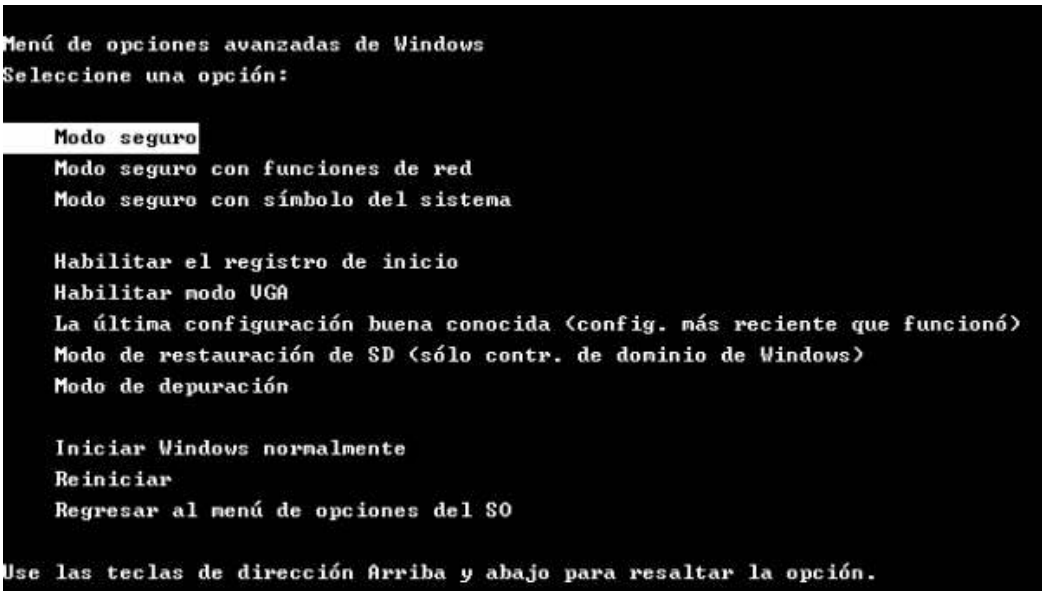


Figura 18. Inicio en modo seguro

5. **Realizar una copia de seguridad del equipo**. Esta copia contendrá todos los ficheros cifrados y no cifrados, y deberá realizarse en un dispositivo de almacenamiento externo aislado de la red. En caso de que no pudieran descifrarse los ficheros es importante conservarlos, ya que en un futuro puede que se rompa el cifrado o se liberen las claves del C&C.

Figura 19. Realización de backup

6. **Comunicar el incidente de seguridad al equipo/persona competente** (CCN-CERT por ejemplo). La información que ha de adjuntarse en la incidencia está reflejada en el apartado "Comunicación del Incidente".
7. **Valorar el escenario.** Para determinar si es posible recuperar los ficheros cifrados, se seguirán los pasos descritos en el apartado de "Valoración de Escenarios".

5.2 Comunicación del incidente

Las preguntas a las que hemos de dar respuesta tras una infección por ransomware, y que serán de utilidad para el equipo de seguridad que gestione la incidencia, son las siguientes:

- ✓ ***¿Disponen de copia de seguridad de los datos cifrados?*** → En caso de disponer de un *backup* de los datos afectados por el ransomware se deberá realizar una copia de seguridad de los ficheros cifrados (por si el proceso de restauración fallara). Posteriormente se desinfectará el/los equipo/s afectado/s, y finalmente se restaurarán los datos originales.

- ✓ ***¿La infección se encuentra en uno o en varios equipos?*** → Es importante determinar cuáles son los equipos afectados. En cada uno de ellos será necesario llevar a cabo las acciones descritas en el quinto apartado, "Medidas Reactivas".

- ✓ ***¿Se han cifrado las unidades de red (si las hubiera mapeadas)?*** → En muchos casos los activos más importantes se encuentran en unidades de red, por lo que se debe determinar si el ransomware ha accedido a los mismos. En cualquier caso hay que "tirar del cable de red" tan pronto como se sea consciente de la infección.

- ✓ ***¿Se han cifrado todos los formatos de ficheros? ¿Cuáles?*** → Responder a esta pregunta ayudará en algunos casos a determinar la familia de ransomware.

- ✓ ***¿Qué mensaje de rescate se muestra al usuario?*** → Una vez finaliza su ejecución, el ransomware mostrará, o depositará en el equipo, las instrucciones para "rescatar" los ficheros cifrados. Es importante adjuntar en el incidente esta información ya que también ayudará a identificar el espécimen de ransomware.

- ✓ ***¿Cómo se produjo la infección (adjunto en correo electrónico, etc.)?*** → En algunos casos será posible obtener la muestra del binario causante de la infección. Este fichero permitirá al equipo de seguridad determinar qué ransomware concreto ha producido la infección y si es, o no, posible la recuperación de los ficheros.

- ✓ ***¿Han llevado a cabo alguna medida para desinfectar el/los equipo/s afectado/s?*** → Si se ha realizado la copia de seguridad del equipo desde el modo seguro se puede proceder a la desinfección del mismo. Sin embargo, es importante esperar la respuesta del equipo de seguridad, ya que en ciertas circunstancias será posible recuperar las claves de cifrado empleadas utilizando o utilizando el "Shadow Volume Copy".

Además de dar respuesta a las preguntas anteriores, toda la información adicional que pueda ser considerada de interés habrá de adjuntarse en la incidencia (muestras de ficheros cifrados y originales con distintas extensiones y tamaños, volcado de memoria del ransomware, etc.).

5.3 Valoración de escenarios

Tras la realización de los pasos descritos en el quinto apartado, "Medidas Reactivas" es necesario realizar una valoración del impacto producido por el ransomware, de modo que en última instancia se pueda intentar la recuperación de los ficheros cifrados.

A continuación se listan los escenarios posibles, partiendo del más favorable al más desfavorable:

- ❖ **ESCENARIO Nº1: Se dispone de backup completo del equipo afectado.** En este escenario se procedería a desinfectar el equipo afectado para posteriormente restaurar la copia de seguridad.

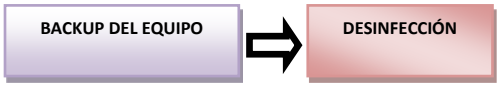
- ❖ **ESCENARIO Nº2: Existe una herramienta que permite el descifrado.** Si existen herramientas públicas para restaurar los ficheros cifrados por un espécimen concreto de ransomware se hará uso de las mismas.

Desafortunadamente, sólo unas pocas variantes de ransomware son descifrables, o bien porque se han obtenido todas las claves de cifrado tras la intervención del servidor C&C, o porque existe una vulnerabilidad conocida en el código dañino que permite el descifrado de los ficheros. Consultar el séptimo apartado, "Descifrado de ransomware".

- **ESCENARIO Nº3: Se dispone de Shadow Volume Copy.** Bastaría con restaurar las copias de seguridad que realiza Windows automáticamente de los ficheros, utilizando Shadow Explorer, por ejemplo. En muchos casos el ransomware imposibilitará esta acción. Para más información consultar el apartado número seis, "Restauración de ficheros".

- **ESCENARIO Nº4: Se pueden recuperar los ficheros utilizando software forense.** En ocasiones algunos programas forenses son capaces de recuperar algunos ficheros originales borrados por el ransomware.

- **ESCENARIO Nº5: Conservar los ficheros cifrados a buen recaudo**, ya que es posible que en el futuro éstos puedan ser descifrados con una herramienta específica.



Efectuar el pago por el rescate del equipo no garantiza que los atacantes envíen la utilidad y/o contraseña de descifrado, sólo premia su campaña y les motiva a seguir distribuyendo masivamente este tipo de código dañino.

Según Symantec 2017, uno de cada cinco negocios no consiguió recuperar sus archivos tras realizar el pago. Por ello, **no se recomienda en ningún caso efectuar el pago.**

6. RESTAURACIÓN DE FICHEROS

Una vez se han seguido las "Medidas Reactivas" recomendadas y se ha "Comunicado el Incidente" al equipo de seguridad competente, se intentarán recuperar los ficheros cifrados utilizando los métodos que se describen a continuación.

6.1 Shadow Volume Copy

El servicio *Shadow Copy* de Windows, también conocido como **Volume Snapshot Service (VSS),** permite hacer copias automáticas periódicas de los datos almacenados en recursos compartidos, así como unidades del equipo (sobre sistemas de ficheros NTFS). Para ello el VSS crea copias ocultas de los cambios que experimentan bloques de datos del sistema de ficheros, permitiendo así recuperar información individual (por ejemplo ficheros) en el caso de pérdida o borrado accidental. Para más información técnica sobre este sistema se recomienda la lectura "*Volume Shadow Copy"* desde la página de Microsoft [Ref.-16].

A diferencia del sistema implementado en Windows XP (restauración del sistema), el VSS mantiene *snapshots* de volúmenes del sistema; por ejemplo, de toda la unidad C. De esta forma, se protegerían no sólo los ficheros del sistema sino todos los datos contenidos en dicha unidad, incluyendo los documentos de los usuarios, ficheros de programas, etc.

Si se cuenta con un sistema operativo Windows Vista o superior, en el caso de ser víctima de un ransomware del cual sea prácticamente imposible recuperar los ficheros originales −por ejemplo, debido al sistema de cifrado utilizado−, es recomendable considerar el uso de VSS para tratar de recuperar una copia previa de los ficheros afectados (siempre y cuando la unidad VSS no se haya visto afectada). Para proceder a recuperar los ficheros de cierto directorio, únicamente es necesario acceder a las propiedades del mismo y posteriormente dirigirse a la pestaña "**Versiones Anteriores**". Desde esta pestaña será posible visualizar y restaurar cada una de las copias creadas por VSS sobre dicho directorio. Téngase en cuenta que el *backup* más reciente puede no coincidir (al tratarse de una versión más antigua) con la última versión del fichero original antes de verse afectado por el ransomware.

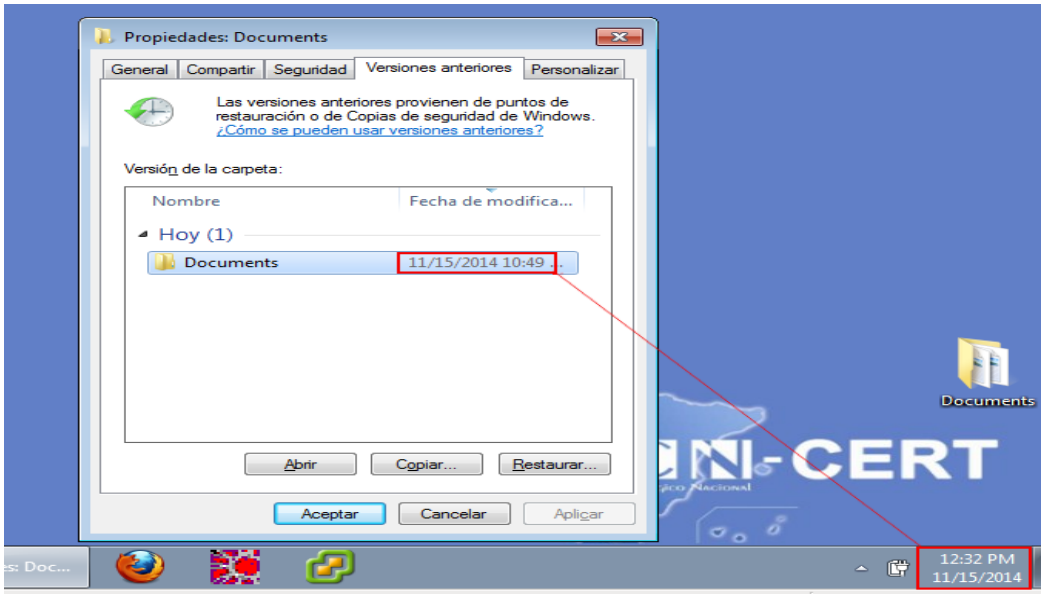


Figura 20. Restauración de ficheros (VSS)

Otra alternativa para restaurar una copia creada por el VSS de los documentos es utilizar el software **Shadow Explorer** [Ref.-17]. Dicho programa presenta una interfaz muy sencilla desde la que se podrá visualizar y restaurar cada una de las copias creadas por el VSS. En la siguiente captura se ha seleccionado el *backup* más reciente, previo a la infección de cierto ransomware. Posteriormente, tras hacer botón derecho sobre el directorio seleccionado, se ha elegido la opción **"Export".**

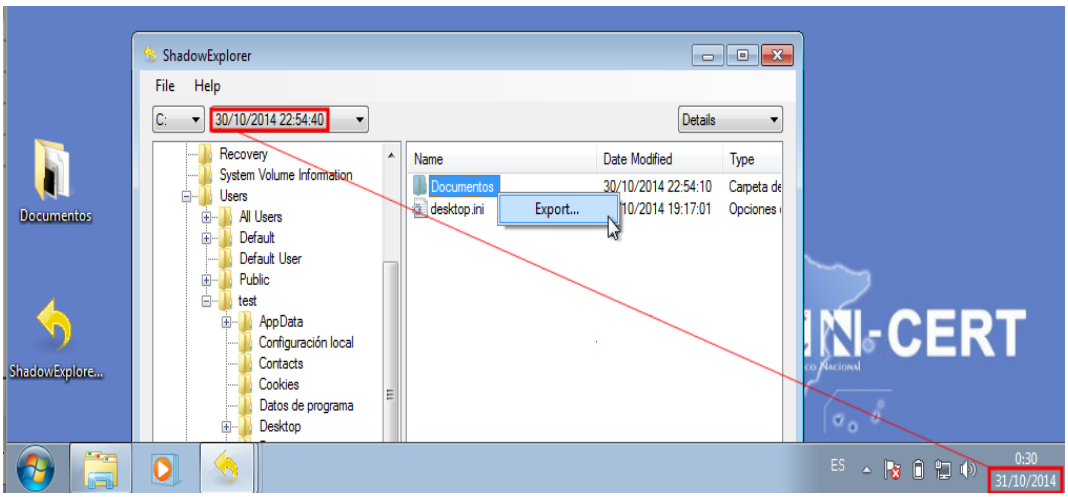


Figura 21. Shadow Explorer

Cabe destacar que los *ransomware* más recientes, conscientes de este mecanismo para recuperar ficheros, implementan funcionalidades para desactivar el VSS y eliminar los puntos de restauración.

6.2 Restauración de ficheros en Dropbox

Es importante destacar que, en el caso de utilizar el cliente de Dropbox para sincronizar determinado directorio con la unidad de almacenamiento en la nube proporcionada por dicho servicio, el mismo es igualmente susceptible de ser infectado por un código dañino de tipo ransomware. Esto significa que un espécimen podría recorrer la unidad montada de Dropbox y cifrar todos sus ficheros. Posteriormente, estos ficheros se sincronizarían con la unidad de almacenamiento online, quedando de esta forma cifrado tanto en local como en la cuenta de Dropbox.

En este caso, Dropbox también permite restaurar una copia de cierto fichero a una versión anterior. Únicamente hay que hacer botón derecho sobre el fichero que se desea restaurar y posteriormente elegir la opción "Versiones anteriores", desde donde se podrá elegir cada uno de los *backups* realizados sobre dicho fichero.

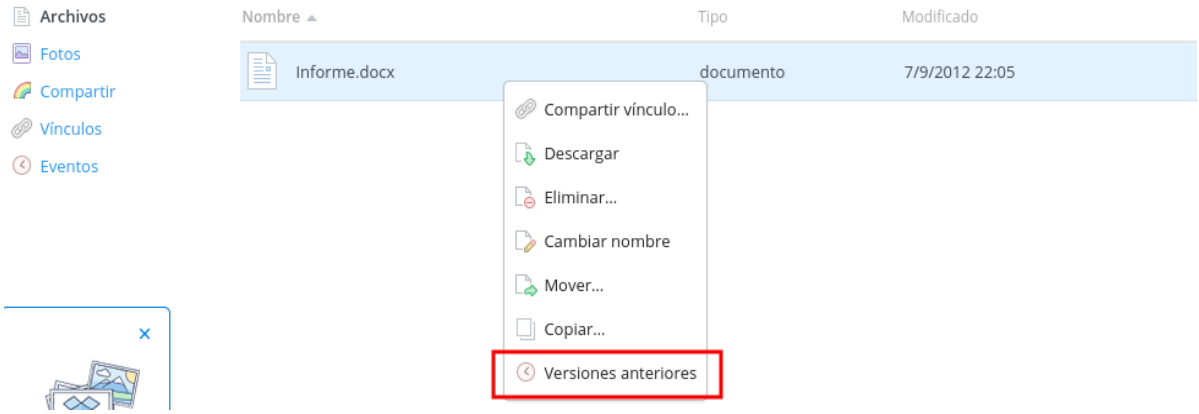


Figura 22. Restauración de ficheros (Dropbox)

Si se gestiona un gran volumen de ficheros en Dropbox, dicho proceso puede resultar un poco engorroso, ya que no existe la opción de restaurar un directorio al completo. En estos casos puede automatizarse el proceso apoyándose en scripts de terceros. Por ejemplo, mediante el script en Python **dropbox-restore** [Ref.-18] es posible especificar el directorio que se desea restaurar así como la fecha de *backup* de cada uno de sus ficheros. Téngase en cuenta que si un fichero no existe en la fecha especificada, el mismo será eliminado. Para utilizar el script es necesario disponer de la API Dropbox para Python. En el siguiente ejemplo se ha hecho uso del gestor de paquetes PIP para su instalación.

```
root@ccn-lab:~/dropbox-restore# python get-pip.py
Requirement already up-to-date: pip in /usr/local/lib/python2.7/dist-packages
Cleaning up...
root@ccn-lab:~/dropbox-restore# pip install dropbox
Downloading/unpacking dropbox
  Downloading dropbox-2.2.0.zip (691kB): 691kB downloaded
  Running setup.py (path:/tmp/pip_build_root/dropbox/setup.py) egg_info for package dropbox

Downloading/unpacking urllib3 (from dropbox)
  Downloading urllib3-1.9.1.tar.gz (171kB): 171kB downloaded
  Running setup.py (path:/tmp/pip_build_root/urllib3/setup.py) egg_info for package urllib3

    warning: no previously-included files matching '*' found under directory 'docs/_build'
Installing collected packages: dropbox, urllib3
  Running setup.py install for dropbox

  Running setup.py install for urllib3

    warning: no previously-included files matching '*' found under directory 'docs/_build'
Successfully installed dropbox urllib3
Cleaning up...
root@ccn-lab:~/dropbox-restore#
```

Figura 23. Dropbox restore script

Posteriormente, para utilizar el *script* únicamente es necesario especificar el directorio así como la fecha de restauración (formato AAAA-MM-DD). Fíjese que el directorio indicado debe ser relativo al directorio utilizado para montar la unidad de Dropbox (en el ejemplo, */root/Dropbox).*

```
root@ccn-lab:~/Dropbox# python2.7 restore.py Documentos-Backup/ 2014-11-01
1. Go to: https://www.dropbox.com/1/oauth2/authorize?response_type=code&client_id=[redacted]
2. Click "Allow" (you might have to log in first)
3. Copy the authorization code.
Enter the authorization code here: MYKcVG2TmSQAAAAAAAAD05EUIgqZBsqVd
Restoring folder: Documentos-Backup/
/Documentos-Backup/Cuentas 2014 (1).pdf SKIP
/Documentos-Backup/Cuentas 2014-ab.pdf SKIP
/Documentos-Backup/Cuentas 2014.pdf SKIP
/Documentos-Backup/Informe.docx SKIP
```

Figura 24. Dropbox restore script

6.3 Restauración de ficheros en Google Drive

Al igual que Dropbox, Google Drive también es susceptible de ser infectado por un código dañino de tipo ransomware. Esto significa que un espécimen podría recorrer la unidad montada de Google Drive y cifrar todos sus ficheros. Posteriormente, estos ficheros se sincronizarían con la unidad de almacenamiento online, quedando de esta forma cifrado tanto en local como en la cuenta de Google Drive.

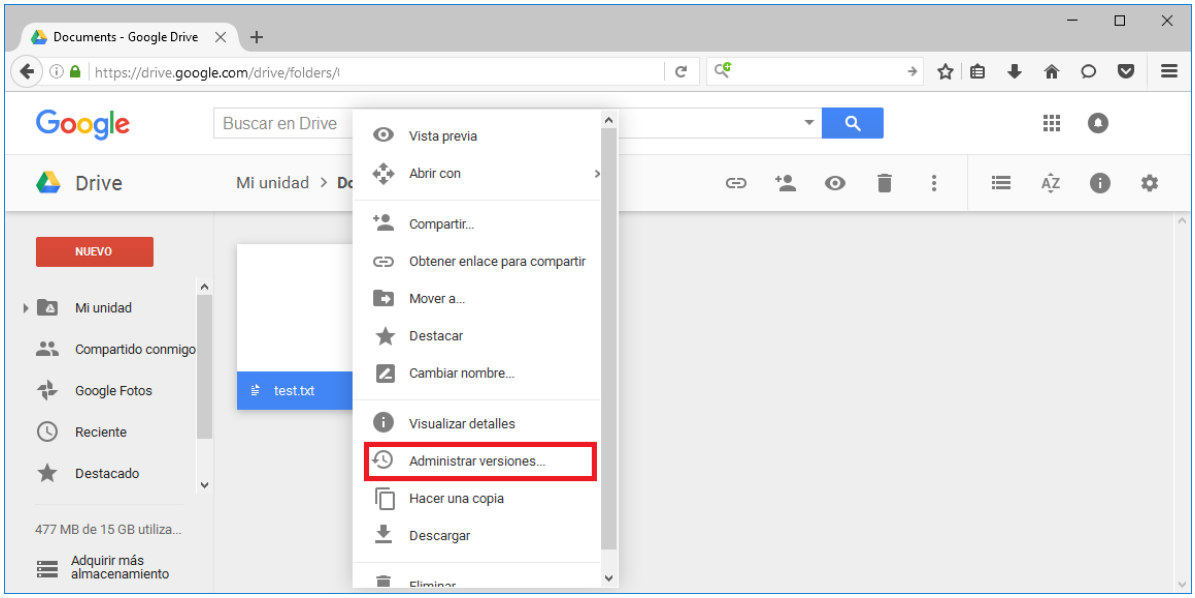


Figura 25. Restauración de ficheros (Google Drive)

En este caso, Google Drive también permite restaurar una copia de cierto fichero a una versión anterior. Únicamente hay que hacer botón derecho sobre el fichero que se desea restaurar y posteriormente elegir la opción "Versiones anteriores", desde donde se podrá elegir cada uno de los *backups* realizados sobre dicho fichero.

Al igual que con Dropbox, si se gestiona un gran volumen de ficheros, dicho proceso puede resultar un poco engorroso, ya que no existe la opción de restaurar un directorio al completo. Puede automatizarse el proceso apoyándose en scripts de terceros. Por ejemplo, mediante una API php: **GoogleDriveRestore** [Ref.-19] es posible especificar el directorio que se desea restaurar así como la fecha de *backup* de cada uno de sus ficheros.

7. PRINCIPALES CAMPAÑAS DE RANSOMWARE EN ESPAÑA

Según los datos extraídos entre octubre del 2016 y abril de 2017 por Sophos ([Ref. 79]), España ocupaba el octavo puesto a nivel europeo en la lista de países con mayor incidencia de ataques de ransomware. Dos variantes fueron las protagonistas: Cerber y Locky, la primera con un 50% de la actividad y la segunda, con un 25%. Sin embargo, no han sido las únicas campañas en los últimos dos años, y en esta sección se ofrecerá un pequeño resumen de sus características para, posteriormente, ofrecer una lista de las herramientas que se conocen a día de hoy para tratar de recuperar los ficheros de un sistema afectado.

7.1 Cerber

Cerber fue durante 2016 y principios de 2017 una de las principales variantes de Ransomware distribuida. A finales de diciembre y principios de enero, fue causante del 25% de toda la actividad global de este tipo de virus y se estima que reportaba alrededor de 2,3 millones de dólares a sus creadores al año.

Además, fue uno de los primeros en ofrecer RaaS (Ransomware as a service). Cualquiera podía disponer de su pequeña versión de Cerber y unirse a la distribución de este tipo de código dañino a cambio de un 40% de los beneficios.

	Cerber v1,v2,v3	Cerber v4	Cerber v5	Cerber SFX	Cerber v6
Tipo de fichero	EXE	EXE	EXE	SFX (Loader) VBS, DLL	EXE
Excepciones (Cerber no se ejecuta si detecta ciertos componentes en el sistema)	Dependiendo del lenguaje de la máquina en la versión 1 y 3 y presencia de antivirus en la versión 2	Dependiendo del lenguaje de la máquina	Dependiendo del lenguaje de la máquina	Presencia de antivirus, máquinas virtuales o Sandbox, y lenguaje de la maquina	Dependiendo del lenguaje de la máquina
Rutina Anti-Antivirus	Ninguna	Ninguna	Ninguna	Ninguna	Ficheros de software de antivirus y firewall bloqueados por el firewall de Windows.
Rutina Anti-sandbox	Ninguna	Ninguna	Ninguna	VM and Sandbox (	VM and Sandbox
Borrado de las copias de seguridad.	Si (vsadmin, WMIC, BCDEdit)*	Yes (WMIC)*	Si (WMIC)* Removed in v5.02	Depende de las variantes de la versión.	Depende de las variantes de la versión.
Lista de exclusiones (Directorios y ficheros no cifrados por Cerber)	Directorios en concreto y ciertas extensiones de ficheros.	Directorios en concreto y ciertas extensiones de ficheros.	Directorios en concreto y ciertas extensiones de ficheros, así como Directorios de antivirus y firewalls.	Directorios en concreto y ciertas extensiones de ficheros, así como Directorios de antivirus y firewalls.	Directorios en concreto y ciertas extensiones de ficheros.

Se conocen seis versiones de Cerber, cada una más sofisticada que la anterior como se puede observar en la tabla anterior. En la última versión, ya se detectaba si el equipo disponía de Firewall, Antivirus o si se estaba ejecutando en un entorno virtual.

Aunque se propagaba por Exploit Kits, lo más común era que lo hiciera mediante correo electrónico. Las últimas versiones de Cerber distribuían un archivo JS (JavaScript) que en la mayoría de los casos ejecutaba un Script de PowerShell embebido para posteriormente realizar el cifrado de los archivos del equipo.

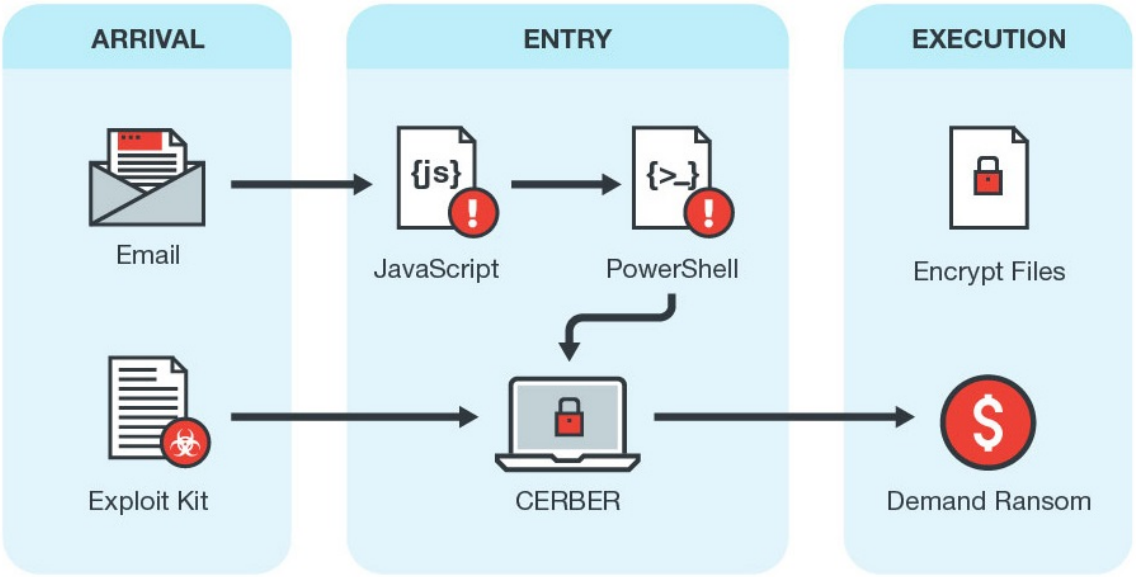


Figura 26. Proceso de Infección Cerber 6 [Ref.-57]

Una característica de Cerber era que disponía de un modo offline, es decir, era capaz de ejecutarse y realizar todo el proceso de cifrado sin conectarse a un servidor de mando y control (C2).

Para más información sobre el proceso de cifrado y algunas otras características de esta variante de Ransomware consultar el documento CCN-CERT ID-21-16-Cerber.

7.2 Locky

Según Kaspersky, los países más afectados por Locky son Francia, Italia, Alemania, Estados Unidos y España. En total se estima que pudo haber afectado a 114 países. Su distribución comenzó en febrero de 2016 y, al igual que la mayoría de Ransomware, usaba el correo electrónico como medio de infección.

Son once las versiones conocidas de esta familia de Ransomware:

.locky	Feb-16
.zepto	Jun-16
.odin	Sep-16
.shit	Oct-16
.thor	Oct-16
.aesir	Nov-16
.zzzzz	Nov-16
.osiris	Dec-16
.loptr	May-17
.diablo6	Aug-17
.lukitus	Aug-17

Figura 27. Historia de las variantes existentes de Locky

Con las diferentes versiones se iba modificando también el archivo dañino que se distribuía, desde un documento Word que pedía al usuario que activara las Macros para poder ver un supuesto mensaje, pasando por el uso de Exploit Kits, hasta que en las últimas versiones se usaba un archivo JavaScript que se encargaba de descargar Locky posteriormente.

Locky usaba una combinación de RSA y AES para asegurar un buen cifrado de los ficheros. A día de hoy, no existe herramienta de descifrado. De hecho, se considera uno de los Ransomware más sólido en cuanto a programación y método de cifrado se refiere. Más información en el documento: Informe Código Dañino CCN-CERT ID-09/16 Ransom.Locky [Ref.-73]

7.3 WannaCry

Quizás, el más conocido dada la atención que recibió de los medios informativos por su virulencia. El primer ataque se produjo el 12 de mayo de 2017, en Asia.

A pesar de que existiera un parche por parte de Microsoft que solventaba la vulnerabilidad de la que WannaCry, se aprovechaba para extenderse. Fue una de las campañas de más rápida propagación: en apenas un día se reportaron 230.000 equipos infectados, de los cuales un 98% tenían Windows 7 como Sistema Operativo.

En España, las infecciones llegaron a 1200, afectando a infraestructuras tan importantes como telecomunicaciones y energía. Sin embargo, a pesar de las masivas infecciones, menos de un 1% pagó el rescate.

WannaCry se aprovechó de la vulnerabilidad conocida como EternalBlue, un exploit que afectaba al protocolo SMB, escaneando tanto la red interna como la externa en busca de equipos no actualizados, donde acto seguido desplegaba una variante del payload conocido como Doublepulsar. También hacia uso de las sesiones

activas de RDP para suplantar a sus usuarios y detectaba la presencia de software específico para tratar de frenas ataques de Ransomware (en concreto, antiransomware).

Un investigador de UK (MalwareTech) descubrió en las primeras versiones de WannaCry la existencia de un Kill Switch, es decir, un mecanismo por el cual la expansión del Ransomware pudo ser mitigada. Antes de comenzar la infección, WannaCry realizaba un ping (una manera de comprobar si una página/dominio existe y está operativa) a un dominio en concreto compuesto de caracteres aleatorios. Si el dominio existía, la infección se detenía. Bastó con comprar el dominio. Alguno de estos dominios son:

a. iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
b. ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
c. iuqerfsodp9ifjaposdfjhgosurijfaewrwergweb.com
d. iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com
e. ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com

Sin embargo, como el propio investigador advirtió, era cuestión de tiempo que sacaran nuevas versiones sin esta característica.

Utiliza los algoritmos RSA-2048 y AES-128 y actualmente no existe herramienta para el descifrado de los archivos, pero sí existen herramientas para prever la infección. El CCN-CERT desarrolló una herramienta (vacuna) para evitar la infección de WannaCry 2.0, NoMoreCry, la cual puede descargarse en aquí.

En el siguiente enlace, se puede encontrar un manual para la configuración e instalación de la herramienta en su formato instalador (.msi) así como ficheros .txt que explican cómo funciona. Para más información, consultar el informe que el CCN-CERT redactó sobre WannaCry [Ref.80]

7.4 NOTPetya

Apareció el 27 de junio de 2017 por primera vez en Ucrania, como una supuesta actualización de un software relacionado con la gestión de impuestos, ampliamente empleado por su administración pública (MeDoc).

Hasta el día de hoy, se trata del Ransomware más virulento. Se habla de 5000 sistemas afectados en menos de 10 minutos [Ref.-75], de entre los cuales se listan entidades financieras, de transporte, energía e incluso organizaciones relacionadas con la salud. . Aunque NotPetya comparta algunas características con Petya, los investigadores no supieron confirmar al 100% que se tratara de una variante o de

siquiera una creación de los mismos autores, y de ahí su nombre. NotPetya es más sofisticado, mucho más robusto.

Al igual que WannaCry, se aprovecha del exploit EternalBlue para propagarse a través de SMB. A posteriori, NotPetya trata de expandirse realizando lo que se conoce como movimiento lateral, tratando de explotar los siguientes caminos:

f. PsExec

g. WMI – Windows Management Instrumentation

h. EternalBlue

i. EternalRomance (Otro exploit para el protocolo SMB)

j. Extraer contraseñas del equipo para infectar otros.

k. Las dos primeras herramientas son programas legítimos de Microsoft, por lo que su uso no hace saltar ninguna alarma.

Según los análisis que se han realizado, NotPetya cifra los archivos de un equipo con AES-128 y genera un ID. Sin embargo, no existen evidencias para afirmar la relación entre la clave de cifrado y el ID generado, por lo que sería posible que los ficheros no pudieran ser recuperados incluso tras el pago, lo que indica que podría tratarse de una campaña destructiva.

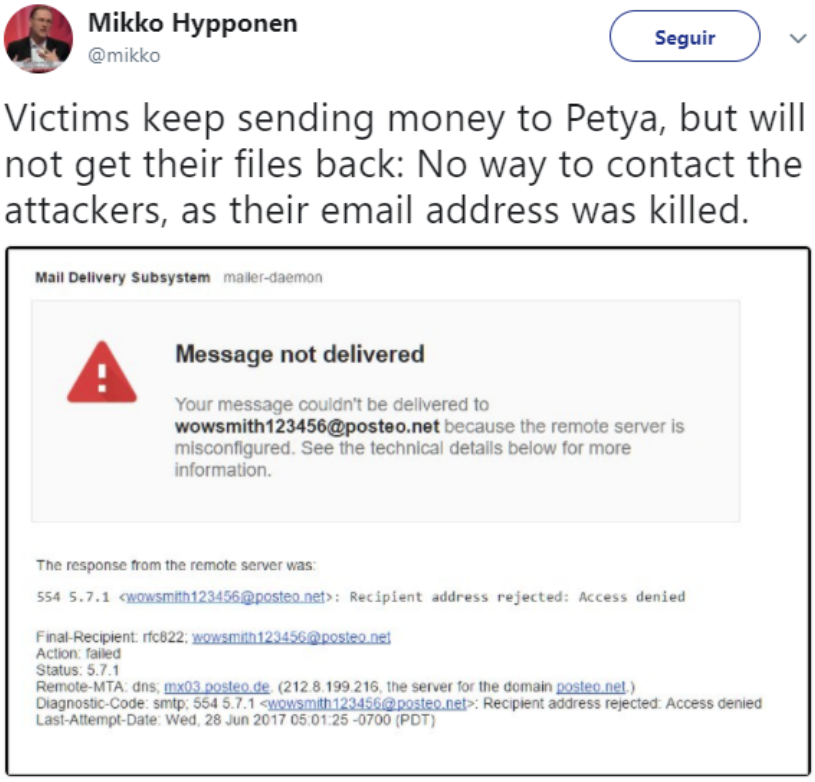


Figura 28. Mikko Hypponen (experto en seguridad informática) advirtiendo de los riesgos que conlleva enviar el dinero pedido.

No existe una herramienta para el descifrado automático de los ficheros. De forma teórica, la recuperación de estos, cuanto menos es costosa, pero no imposible (al menos en un caso ideal-teórico). Más información, aquí:

https://www.crowdstrike.com/blog/full-decryption-systems-encrypted-petya-notpetya/

7.5 Crysis/Dharma

Dharma es una de las tantas extensiones/versiones que ha usado el Ransomware Crysis a lo largo de su existencia, entre las cuales se encuentra también .cesar, .unión, .dharma, .wallet, .zzzzz, .arena, .cezar, .java y .write.

Según ESET, esta familia de malware, descubierta el 9 de junio de 2016[15], se ha encontrado en 123 países, aunque el 60% de las infecciones se concentran en 10, siendo España el número dos. **[Ref.-90]**

Es uno de los ransomware que utiliza la fuerza bruta contra servicios RDP, que se encuentran expuestos al exterior para propagarse. Según Trendmicro, en enero de 2017, Crysis duplicó el número de ataques por fuerza bruta. Crysis no es el único que se aprovecha de este servicio; Shade, Apocalypse, SamSam, Bucbi, DMA Locker, LockCrypt [Ref.- 61] o Smrss32 son otros ejemplos de códigos dañinos que tratan de propagarse usando este medio. Esto hecho refleja la clara tendencia de los cibercriminales por emplear nuevos métodos de infección, que requieran cada vez menos de la interacción del usuario.

Las versiones .java y .write son las últimas campañas. En concreto, una nueva oleada de Phishing fue lanzada en febrero de 2018 para propagar la primera. A día de hoy existen diversas herramientas para recuperar los ficheros, como la herramienta RakhniDecryptor de Kaspersky o ESETCrysisDecryptor, de ESET[16].

Lamentablemente, no funciona con todas las variantes de Dharma/Crysis (a día de hoy no se conoce un método para descifrar los ficheros para los sistemas afectados por la versión .java o .write).

[15] https://www.symantec.com/security_response/writeup.jsp?docid=2016-060920-2315-99

[16]https://download.eset.com/com/eset/tools/decryptors/crysis/latest/esetcrysisdecryptor.exe.

8. DESCIFRADO DE RANSOMWARE

8.1 Tabla resumen

En la siguiente tabla se muestra un resumen de las posibilidades de recuperación de los datos cifrados dependiendo del tipo de ransomware que haya producido la infección, las familias mostradas son las que han tenido más impacto en España:

RANSOMWARE	POSIBILIDAD DE RECUPERACIÓN DE LOS DATOS	
BANDARCHOR	Dependiendo de la muestra y su similitud con el Ransomware llamado RAKHNI se puede intentar usar la herramienta de descifrado realizada por Kaspersky. En caso de que la muestra no tenga similitud, solo a partir de backup.	○
BAT_CRYPTOR	A partir de backup.	✗
CERBER	A partir de backup. En las versiones 1 y 2 mediante herramienta de Check Point.	✗
CRITONY (variante del CTB-LOCKER)	A partir de backup.	✗
CRYPTEAR	Al ser una prueba de concepto y tener su código fuente, su autor publicó una herramienta de descifrado en el mismo repositorio del código.	✓
CRYPTODEFENSE (2ª versión de CRYPTOWALL)	Mediante herramienta de Emsisoft.	✓
CRYPTOFORTRESS	A partir de backup.	✗
CRYPTOGRAPHIC LOCKER	Mediante herramientas forenses de recuperación de ficheros.	○
CRYPTOLOCKER	Consultar en www.decryptcryptolocker.com	○
CTB-LOCKER / CRITONI	A partir de backup.	○
CRYPTOWALL	A partir de backup. En la tercera versión a través de herramientas de recuperación de archivos. La cuarta y quinta versión sólo si se puede obtener la clave RSA.	✗
CRYPTXXX	Mediante herramienta de Kaspersky.	?
DMALOCKER	Para las dos primeras versiones se puede usar la herramienta de Emsisoft. En el caso de las dos últimas versiones solo se puede a partir de backups.	○
LOCKY	Comprobar mediante herramienta de Emsisoft Autolocky.	○
PETYA	En la primera versión se puede utilizar la herramienta realizada por bleepingcomputer, en el caso de la segunda se ha publicado la clave privada de descifrado.	✓
MISCHA	Se ha publicado la clave privada de descifrado.	✓
SATANA	Solo a partir de backup. El sector de arranque no se recupera.	✗
TESLACRYPT	Mediante la herramienta de descifrado realizada por ESET.	✓
TORRENTLOCKER	Mediante herramienta TorrentUnlocker de BleepingComputer. La última versión no puede ser descifrada (desde mayo 2016 aproximadamente).	○
ZEROLOCKER	Mediante herramienta UnlockZeroLocker de Vínsula.	✓
JAZZ	Mediante herramienta RakhniDecryptor de Kaspersky Labs.	✓
WANNACRY	Solo a partir de backup. Existe herramienta de prevención del CCN, NoMoreCry.	○
CRYSIS	Consultar herramienta RakhniDecryptor de Kaspersky Labs. Solo algunas variantes.	○
NONPetya	Actualmente no existe una solución automatizada, y la solución manual es costosa.	○

✓ Sí existe solución ○ Existe solución parcial ✗ No existe solución

8.2 Identificación del ransomware

Para proceder al posible descifrado de los archivos es importante conocer el tipo de familia de ransomware que los ha cifrado. Hay diversas páginas donde averiguar la familia de ransomware partiendo de un fichero de muestra, pero las más efectivas y recomendables son;

- nomoreransom.org (https://www.nomoreransom.or/crypto-sheriff.php)
- IDRansomware (https://id-ransomware.malwarehunterteam.com)

En estas páginas se pueden subir los ficheros cifrados y las notas de rescate. De este modo, y a través del tipo de encriptación y método de rescate, se logra saber qué tipo de familia es la que ha infectado.

8.3 Herramientas de descifrado

En ciertos casos, es posible descifrar los ficheros cifrados por un espécimen concreto de ransomware. Las herramientas que permiten el descifrado y restauración de los ficheros pueden aprovechar:

- Debilidades en el algoritmo de cifrado empleado por el ransomware
- Recuperación de la clave a través de la información contenida o generada por el binario (ficheros temporales, claves de registro, etc.)
- En ocasiones, mediante la colaboración policial e internacional, es posible tomar el control de los servidores de C&C, de los cuales se pueden extraer las claves empleadas en los procesos de cifrado.

A continuación se listan algunas de las herramientas y utilidades online existentes, que permiten el descifrado de ciertos especímenes de ransomware ordenadas por familia:

Ransomware	Herramienta	Web
AlcatrazLocker	Herramienta Avast	https://files.avast.com/files/decryptor/avast_decryptor_alcatrazlocker.exe
Apocalypse	Herramienta Avast	https://files.avast.com/files/decryptor/avast_decryptor_apocalypse.exe
Bad Block	Herramienta Avast	https://files.avast.com/files/decryptor/avast_decryptor_badblock.exe
Bandarchor	Herramienta Kaspersky	https://support.kaspersky.com/sp/viruses/disinfection/10556
Bart	Herramienta Avast	https://files.avast.com/files/decryptor/avast_decryptor_bart.exe
Cryptodefense	Herramienta Emsisoft	https://decrypter.emsisoft.com/cryptodefense
Cryptolocker	-	http://www.decryptcryptolocker.com
CryptXXX v3	Herramienta Kaspersky	https://support.kaspersky.com/mx/8547

Ransomware	Herramienta	Web
Crysis	-	https://files.avast.com/files/decryptor/avast_decryptor_crysis.exe
DMAlocker	Herramienta Emsisoft	https://decrypter.emsisoft.com/dmalocker
Globe	Herramienta Avast	https://files.avast.com/files/decryptor/avast_decryptor_globe.exe
JigSaw	Herramienta Avast	https://files.avast.com/files/decryptor/avast_decryptor_jigsaw.exe
Legion	Herramienta AVG	http://files-download.avg.com/util/avgrem/avg_decryptor_Legion.exe
Locky	Herramienta Emsisoft	https://decrypter.emsisoft.com/autolocky
Petya	Herramienta Bleepingcomputer	http://download.bleepingcomputer.com/fabian-wosar/Petyaextractor.zip
SFZLocker		https://www.avg.com/es-es/ransomware-decryption-tools#szflocker
Teslacrypt	Herramienta Eset	https://download.eset.com/special/ESETTeslaCryptDecryptor.exe
Torrentlocker	Herramienta Bleepingcomputer	http://download.bleepingcomputer.com/Nathan/TorrentUnlocker.exe
Zerolocker	Herramienta Vinsula	http://vinsula.com/security-tools/unlock-zerolocker/

Además de estos enlaces, se puede consultar:

- Enlace a la solución de Trendmicro, para combatir un amplio abanico de variedades de ransomware (incluyendo algunas no tan conocidas) https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor
- Una herramienta de parte de Emsisoft, que combate la infección de diversas familias de Ransomware, también menos conocidas y algunas no incluidas en las herramientas anteriores listadas https://decrypter.emsisoft.com/
- En caso de que la variante que ha infectado el equipo no se encontrara listada en ninguna de las herramientas anteriores, se puede probar suerte con el buscador que ofrece barkly: https://www.barkly.com/ransomware-recovery-decryption-tools-search

Es importante repetir que, aun no existiendo herramientas de descifrado, se aconseja no pagar. He aquí algunos ejemplos y noticias de muestra que, además de no ofrecer una herramienta para desinfectar y recuperar sus archivos, guardan los datos de la tarjeta de crédito empleada (Ransomware: MindLost) o páginas TOR (las más comunes para realizar el pago) que roban los pagos que se realizan. [Ref.-65] [Ref.-66]

9. REFERENCIAS

[Ref.-1] Wikipedia: Ransomware

http://en.wikipedia.org/wiki/Ransomware

[Ref.-2] Ransomware: A Growing Menace

http://www.symantec.com/connect/blogs/ransomware-growing-menace

[Ref.-3] Ransomware: Next-Generation Fake Antivirus

http://www.sophos.com/es-es/why-sophos/our-people/technical-papers/ransomware-next-generation-fake-antivirus.aspx

[Ref.-4] Remote Desktop (RDP) Hacking 101: I can see your desktop from here

http://www.welivesecurity.com/2013/09/16/remote-desktop-rdp-hacking-101-i-can-see-your-desktop-from-here/

[Ref.-5] Kit de herramientas de Experiencia de mitigación mejorada

http://support.microsoft.com/kb/2458544/es

[Ref.-6] Application whitelisting explained

http://www.asd.gov.au/publications/csocprotect/Application_Whitelisting.pdf

[Ref.-7] Windows 7 AppLocker Executive Overview

http://msdn.microsoft.com/en-us/library/dd548340(v=ws.10).aspx

[Ref.-8] The Bit9 Security Platform

https://www.bit9.com/solutions/security-platform

[Ref.-9] McAfee Application Control

http://www.mcafee.com/in/products/application-control.aspx

[Ref.-10] Lumension: Application Control

https://www.lumension.com/application-control-software.aspx

[Ref.-11] CryptoLocker Toolkit

http://www.thirdtier.net/2013/10/cryptolocker-prevention-kit

[Ref.-12] Foolishit: CryptoPrevent

https://www.foolishit.com/vb6-projects/cryptoprevent/

[Ref.-13] Eset: Advanced Memory Scanner

http://www.eset.com/int/about/technology/

[Ref.-14] Kaspersky Cryptomalware Countermeasures Subsystem

http://media.kaspersky.com/pdf/Kaspersky_Lab_Whitepaper_Cryptoprotection_final_ENG.pdf

[Ref.-15] CryptoGuard: Prevents your files from being taken hostage!

http://www.surfright.nl/en/cryptoguard

[Ref.-16] Microsoft: Volume Shadow Copy Service

http://technet.microsoft.com/en-us/library/ee923636.aspx

[Ref.-17] Shadow Explorer

http://www.shadowexplorer.com/downloads.html

[Ref.-18] Dropbox-Restore (Github)

https://github.com/clark800/dropbox-restore

[Ref.-19] GoogleDriveRestore (Github)

https://github.com/ryancastle/d1e22981275c9971c81f

[Ref.-20] KernelMode: CryptoLocker (Trojan:Win32/Crilock.A)

http://www.kernelmode.info/forum/viewtopic.php?f=16&t=2945

[Ref.-21] CryptoLocker Ransomware Information Guide and FAQ

http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

[Ref.-22] Operation Tovar, taking a swipe at CryptoLocker and Gameover Zeus

https://www.404techsupport.com/2014/05/mcafee-writes-about-operation-tovar-taking-a-swipe-at-cryptolocker-and-gameover-zeus/

[Ref.-23] Bleepingcomupter: Cryptolocker Hijack program

http://www.bleepingcomputer.com/forums/t/506924/cryptolocker-hijack-program/page-207#entry3441321

[Ref.-24] WeliveSecurity: Cryptolocker 2.0 – new version, or copycat?

http://www.welivesecurity.com/2013/12/19/cryptolocker-2-0-new-version-or-copycat/

[Ref.-25] CryptoWall Ransomware Built With RC4 Bricks

http://blogs.mcafee.com/mcafee-labs/cryptowall-ransomware-built-with-rc4-bricks

[Ref.-26] CryptoWall and DECRYPT_INSTRUCTION Ransomware Information Guide and FAQ

http://www.bleepingcomputer.com/virus-removal/cryptowall-ransomware-information

[Ref.-27] CryptoWall Encrypted File Recovery and Analysis

http://www.wyattroersma.com/?p=108

[Ref.-28] ForensicsWiki: Tools: Data Recovery

http://www.forensicswiki.org/wiki/Tools:Data_Recovery

[Ref.-29] CryptoDefense: The Ransomware Games have begun

http://labs.bromium.com/2014/05/27/cryptodefense-the-ransomware-games-have-begun/

[Ref.-30] CryptoDefense: The story of insecure ransomware keys and self-serving bloggers

http://blog.emsisoft.com/2014/04/04/cryptodefense-the-story-of-insecure-ransomware-keys-and-self-serving-bloggers/

[Ref.-31] Emsisoft: Decrypt CryptoDefense Tool

http://tmp.emsisoft.com/fw/decrypt_cryptodefense.zip

[Ref.-32] CryptoDefense and How_Decrypt Ransomware Information Guide and FAQ

http://www.bleepingcomputer.com/virus-removal/cryptodefense-ransomware-information

[Ref.-33] TorrentLocker Unlocked

http://digital-forensics.sans.org/blog/2014/09/09/torrentlocker-unlocked

[Ref.-34] Bleepingcomputer: TorrentLocker Ransomware Cracked and Decrypter has been made

http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made

[Ref.-35] TorrentLocker – New Variant with New Encryption Observed in the Wild

http://www.isightpartners.com/2014/09/torrentlocker-new-variant-observed-wild

[Ref.-36] KernelMode: Cryptographic Locker

http://www.kernelmode.info/forum/viewtopic.php?f=16&t=3466

[Ref.-37] Symantec: Russian ransomware author takes the easy route

http://www.symantec.com/connect/blogs/russian-ransomware-author-takes-easy-route

[Ref.-38] Avast: Self-propagating ransomware written in Windows batch hits Russian-speaking countries

http://blog.avast.com/2014/08/27/self-propagating-ransomware-written-in-windows-batch-hits-russian-speaking-countries/

[Ref.-39] "Crypto Ransomware" CTB-Locker (Critroni.A) on the rise

http://malware.dontneedcoffee.com/2014/07/ctb-locker.html

[Ref.-40] Elliptic curve cryptography + Tor + Bitcoin

http://securelist.com/analysis/publications/64608/a-new-generation-of-ransomware/

[Ref.-41] Introduction to the ZeroLocker ransomware

http://stopmalvertising.com/malware-reports/introduction-to-the-zerolocker-ransomware.html

[Ref.-42] Vínsula: Unlock ZeroLocker

http://vinsula.com/security-tools/unlock-zerolocker

[Ref.-43] Anti-Ransom Tool

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

[Ref.-44] Cryptowall 3.0 Analysis

http://blogs.cisco.com/security/talos/cryptowall-3-0

[Ref.-45] TOR vs I2P

http://thehackerway.com/2012/02/08/preservando-el-anonimato-y-extendiendo-su-uso-comparacion-de-redes-anonimas-y-conclusiones-finales-parte-xxxxii/

[Ref.-46] TOR vs I2P

http://www.bleepingcomputer.com/forums/t/563859/new-ctb-locker-campaign-underway-increased-ransom-timer-and-localization-changes/

[Ref.-47] Cryptofortress Analysis ESET

http://www.welivesecurity.com/2015/03/09/cryptofortress-mimics-torrentlocker-different-ransomware/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+eset%2Fblog+%28ESET+Blog%3A+We+Live+Security%29

[Ref.-48] Cryptofortress Deep Analysis lexsi-leblog

http://www.lexsi.com/securityhub/cryptofortress

[Ref.-49] WIN32/REVETON

https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Win32%2fReveton#tab_2

[Ref.-50] Teslacrypt/Alphacrypt Analysis

http://www.bleepingcomputer.com/forums/t/574900/teslacrypt-ransomware-changes-its-name-to-alpha-crypt/

[Ref.-51] Alphacrypt Analysis

http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information

[Ref.-52] Android Locker Fortinet

https://blog.fortinet.com/post/locker-an-android-ransomware-full-of-surprises

[Ref.-53] Teslacrypt 3.0 Analysis Securelist

https://securelist.com/blog/research/71371/teslacrypt-2-0-disguised-as-cryptowall/

[Ref.-54] Teslacrypt 3.0 – Información técnica

http://www.isightpartners.com/2015/09/teslacrypt-2-0-cyber-crime-malware-behavior-capabilities-and-communications/

[Ref.-55] Kaspersky Security Bulletin 2016

https://securelist.com/76757/kaspersky-security-bulletin-2016-story-of-the-year/

[Ref.-56] Multi-Stage Word Attack Infects Users Without Using Macros

https://www.bleepingcomputer.com/news/security/multi-stage-word-attack-infects-users-without-using-macros/

[Ref.-57] Cerber Version 6 Shows How Far the Ransomware Has come.

https://blog.trendmicro.com/trendlabs-security-intelligence/cerber-ransomware-evolution/

[Ref.-58] How to Block Ports 445 & 3389

https://www.backup-utility.com/anti-ransomware/how-to-block-port-445-in-windows-3889.html

[Ref.-59] Articulo acerca de la efectividad del Firewall de Windows frente a WannaCry

https://www.computerworld.com/article/3197421/networking/the-windows-firewall-is-the-overlooked-defense-against-wannacry-and-adylkuzz.html

[Ref.-60] Ransomware statistics 2017

https://blog.barkly.com/ransomware-statistics-2017

[Ref.-61] LockCrypt Uses RDP

https://www.bleepingcomputer.com/news/security/lockcrypt-1btc-variant-installed-over-hacked-remote-desktop-services/

[Ref.-62] NonPetya and Saturn – February 2018

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-16th-2018-notpetya-and-saturn/

[Ref.-63] Rapid Ransomware Being Spread Using Fake IRS Malspam

https://www.bleepingcomputer.com/news/security/rapid-ransomware-being-spread-using-fake-irs-malspam/

[Ref.-64] Ransomware can use Office OLE objects to bypass CFA

https://www.bleepingcomputer.com/news/security/researcher-bypasses-windows-controlled-folder-access-anti-ransomware-protection/

[Ref.-65] Sites Stealing Ransom Payments & GandCrab

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-2nd-2018-tor-sites-stealing-ransom-payments-and-gandcrab/

[Ref.-66] MindLost Ransomware Is a Piece of Junk That Wants to Collect Credit Card Details

https://www.bleepingcomputer.com/news/security/mindlost-ransomware-is-a-piece-of-junk-that-wants-to-collect-credit-card-details/

[Ref.-67] 10 of the Most Significant Ransomware Attacks of 2017

https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/10-significant-ransomware-attacks-2017/

[Ref.-68] Internet Security Threat Report ISTR July 2017 Contents Executive summary and Key findings Ransomware: An overview A new breed of threat: WannaCry and Petya Businesses in the crosshairs Affecting the bottom line: Impact of ransomware How ransomware is spread Major ransomware threats Protection and best practices Ransomware 2017 An ISTR Special Report

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf

[Ref.-69] ZLAB Malware Analysis Report: NotPetya

https://csecybsec.com/download/zlab/NotPetya-report.pdf

[Ref.-70] Alert (TA17-181A) Petya Ransomware

https://www.us-cert.gov/ncas/alerts/TA17-181A

[Ref.-71] NotPetya: Timeline of a Ransomworm

https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/

[Ref.-72] Full Decryption of Systems Encrypted by Petya/NotPetya

https://www.crowdstrike.com/blog/full-decryption-systems-encrypted-petya-notpetya/

[Ref.-73] CCN-CERT ID-09/16 Ransom.Locky

https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-publicos/1513-ccn-cert-id-09-16-ransom-locky.html?path=informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-publicos

[Ref.-74] Locky ransomware returns to the game with two new flavors.

https://blog.malwarebytes.com/cybercrime/2017/08/locky-ransomware-returns-to-the-game-with-two-new-flavors/

[Ref.-75] De Wannacry a Petya: cómo un 'ransomware' ha paralizado (otra vez) el mundo

https://www.elconfidencial.com/tecnologia/2017-06-28/petya-ransomware-ciberataque-wannacry_1406044/

[Ref.-76] PowerPoint File Armed with CVE-2017-0199 and UAC Bypass

https://www.fortinet.com/blog/threat-research/powerpoint-file-armed-with-cve-2017-0199-and-uac-bypass.html

[Ref.-77] De Wannacry a Petya: cómo un 'ransomware' ha paralizado (otra vez) el mundo

https://www.bleepingcomputer.com/news/security/windows-10-uac-bypass-uses-backup-and-restore-utility/

[Ref.-78] Guía de Seguridad de las TIC CCN-STIC 950. RECOMENDACIONES DE EMPLEO DE LA HERRAMIENTA EMET

https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2154-ccn-stic-950-recomendaciones-de-empleo-de-la-herramienta-emet-1/file.html

[Ref.-79] España se encuentra en el Top 10 de países europeos con mayor actividad de ransomware

https://news.sophos.com/es-es/2017/06/20/espana-se-encuentra-top-10-paises-europeos-mayor-actividad-ransomware/

[Ref.-80] Informe Código Dañino CCN-CERT ID-17/17

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2169-ccn-cert-id-17-17-codigo-danino-wannacry-1/file.html

[Ref.-81] The top 10 worst ransomware attacks of 2017, so far

https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/

[Ref.-82] Must-Know Ransomware Statistics 2017

https://blog.barkly.com/ransomware-statistics-2017

[Ref.-83] Un potente ciberataque afecta a grandes empresas de todo el mundo

https://elpais.com/internacional/2017/06/27/actualidad/1498568187_011218.html

[Ref.-84] ISTR Ransomware 2017

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf

[Ref.-85] WannaCry Ransomware Statistics: The Numbers Behind the Outbreak

https://blog.barkly.com/wannacry-ransomware-statistics-2017

[Ref.-86] I Cerber Ransomware: Everything You Need to Know

https://blog.barkly.com/cerber-ransomware-statistics-2017

[Ref.-87] ZLAB Malware Analysis Report: NotPetya

https://csecybsec.com/download/zlab/NotPetya-report.pdf

[Ref.-88] Alert (TA17-181A) Petya Ransomware

https://www.us-cert.gov/ncas/alerts/TA17-181A

[Ref.-89] Full Decryption of Systems Encrypted by Petya/NotPetya

https://www.crowdstrike.com/blog/full-decryption-systems-encrypted-petya-notpetya/

[Ref.-90] Nueva herramienta de descifrado para el ransomware Crysis

https://www.welivesecurity.com/la-es/2016/11/24/herramienta-descifrado-ransomware-crysis/