

Informe de Amenazas
CCN-CERT IA-01/16

MEDIDAS DE SEGURIDAD CONTRA RANSOMWARE

Agosto 2016



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
2016.08.10 15:25:43 +02'00'

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT 4

2. PRÓLOGO 5

3. VÍAS DE INFECCIÓN 7

4. MEDIDAS PREVENTIVAS 9

4.1 LISTADO DE MEDIDAS PREVENTIVAS 9

4.2 PRINCIPALES MEDIDAS PREVENTIVAS 10

5. MEDIDAS REACTIVAS 15

5.1 PROCEDIMIENTO GENERAL 15

5.2 COMUNICACIÓN DEL INCIDENTE 18

5.3 VALORACIÓN DE ESCENARIOS 18

6. RESTAURACIÓN DE FICHEROS 20

6.1 SHADOW VOLUME COPY 20

6.2 RESTAURACIÓN DE FICHEROS EN DROPBOX 21

6.3 RESTAURACION DE FICHEROS EN GOOGLE DRIVE 23

7. DESCIFRADO DE RANSOMWARE 24

7.1 TABLA RESUMEN 24

7.2 IDENTIFICACIÓN DEL RANSOMWARE 25

7.3 HERRAMIENTAS DE DESCIFRADO 25

8. REFERENCIAS 26

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. 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 Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. PRÓLOGO

Tal y como describe la Wikipedia [Ref.-1]: *"Un **ransomware** es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate"*.

Aunque inicialmente este tipo de código dañino estaba limitado a 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 reporta a los atacantes, extendiéndose así por toda Europa, Estados Unidos y Canadá.

A diferencia de otras categorías de código dañino cuyo objetivo es extraer información o utilizar los equipos como *bots* para diversos fines (*proxys*, ataques DOS, etc.), el ransomware tiene un único propósito: obtener dinero de forma inmediata. Para conseguir esto, el código dañino tratará de inducir miedo al usuario utilizando diversos elementos (*scareware*); por ejemplo, mediante avisos emitidos supuestamente por empresas o agencias de la ley que falsamente afirman que el sistema ha sido utilizado para actividades ilegales (por ejemplo: pornografía infantil, software ilegal, etc.). Dichos mensajes irán acompañados de un formulario en el que se exigirá al usuario que pague cierta suma de dinero a modo de sanción. El método de pago consistirá generalmente en sistemas de pago electrónico (Ukash, Paysafecard, MoneyPak, etc.), por medio de SMS *premium* o mediante Bitcoins.

En el mejor caso, el ransomware únicamente bloqueará el equipo del usuario impidiendo la ejecución de determinados programas, generalmente por medio de un *banner* a pantalla completa en el que podrá visualizarse el mensaje de extorsión. En algunos casos el contenido del mensaje será mostrado en el idioma correspondiente en base a la geo-localización de la máquina comprometida para dotar a éste de mayor credibilidad.

El conocido "virus de la policía", el cual tuvo cierta repercusión en España durante los años 2011 y 2012, es un ejemplo de este tipo de ransomware.

En los últimos años, sin embargo, las acciones dañinas de este tipo de código dañino han ido evolucionando dando lugar a una nueva generación de ransomware denominados "*file encryptors*", cuyo principal objetivo es cifrar la gran mayoría de documentos del equipo. En este caso, la principal herramienta de extorsión será el pago de cierta cantidad de dinero a cambio de la clave que permitirá recuperar (descifrar) los ficheros originales.

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.).

Las acciones ofensivas de ciertos tipos de ransomware pueden resultar muy dañinas. Por ejemplo, CryptoLocker emplea una combinación de cifrado simétrico y asimétrico para hacer realmente compleja la recuperación de los ficheros originales. Además, dichos ficheros son comúnmente sobrescritos en disco mediante ciertas herramientas de seguridad (por ejemplo, Microsoft SysInternals **SDelete**) para impedir su recuperación por técnicas

forenses. Asimismo, algunas variantes utilizan clientes de la red TOR[1] o I2P[2] para dificultar la trazabilidad de los servidores de control a los que se conectan los equipos infectados.

Como puede deducirse de dichas acciones, las consecuencias de un código dañino de estas características en un entorno corporativo pueden ser devastadoras. Además, dichas consecuencias pueden agravarse aún más si se cuenta con dispositivos de backup directamente conectados con el equipo infectado, ya que algunos tipos de ransomware comprueban cada una de las unidades montadas así como recursos compartidos de red para cifrar también su contenido.



Figura 1. Ejemplo ransomware

A raíz de estos hechos, el presente informe tiene por objetivo 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 describirá 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].

[1] TOR (abreviatura de *The Onion Router*) es un software diseñado para permitir el acceso anónimo a Internet. Aunque durante muchos años ha sido utilizado principalmente por expertos y aficionados, el uso de la red TOR se ha disparado en los últimos tiempos, debido principalmente a los problemas de privacidad de Internet. Correlativamente, TOR se ha convertido en una herramienta muy útil para aquellos que, por cualquier razón, legal o ilegal, no desean estar sometidos a vigilancia o no desean revelar información confidencial. CCN-CERT IA_09-15 Informe de Amenazas

[2] I2P (abreviatura de *Invisible Internet Project*) es un software que ofrece una capa de abstracción para comunicaciones entre ordenadores, permitiendo así la creación de herramientas y aplicaciones de red con un fuerte anonimato. Wikipedia.org

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.* Posiblemente este sea el vector de infección 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 (analizado en el punto 6) resultaron infectadas como consecuencia de una página de *phishing* que simulaba 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.

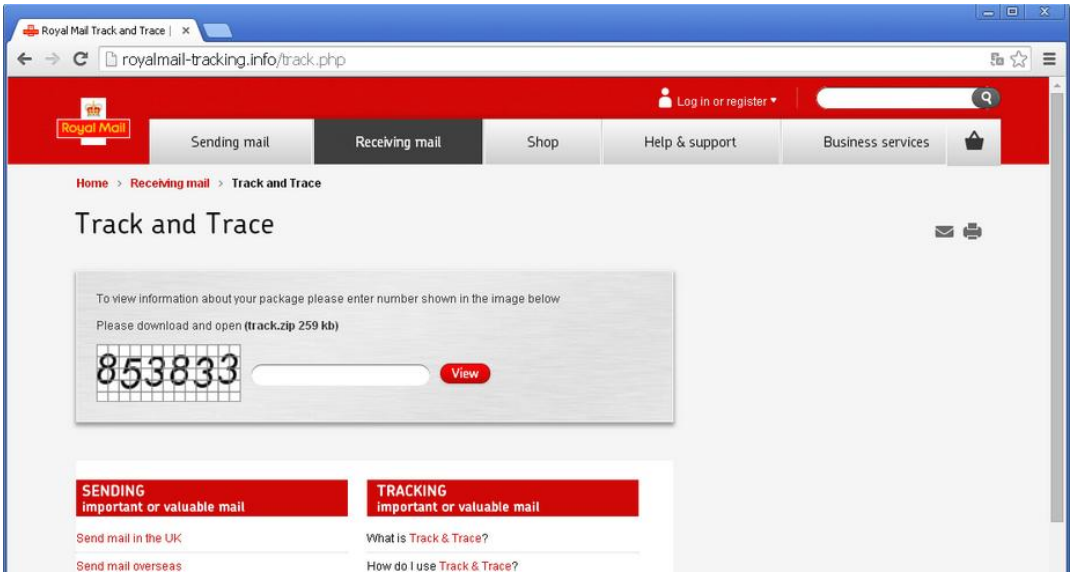


Figura 2. Phishing Royal Mail (TorrentLocker). Fuente: Welivesecurity

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.

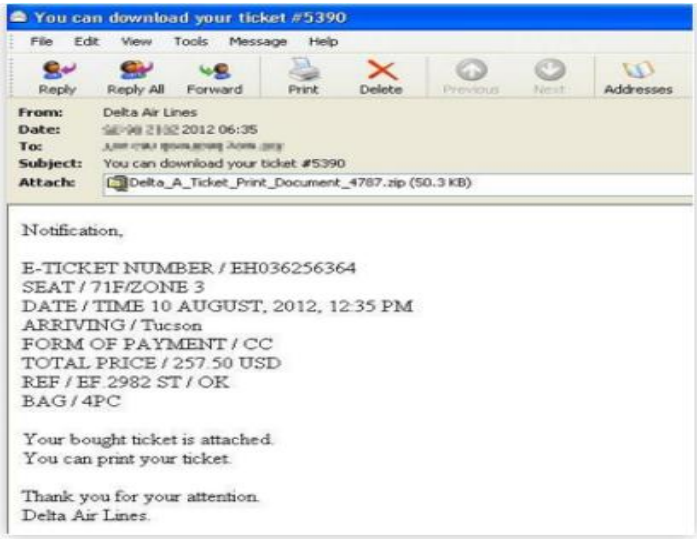


Figura 3. Troj/Ransom-JO. Fuente: Sophos

- *Web Exploit Kits* [3] que se aprovechan de vulnerabilidades en el navegador o en los *plugins*[4] instalados (*drive-by downloads*). En estos casos, cuando el usuario navega a 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. Por ejemplo, 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 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 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; por ejemplo, *banners* pornográficos.

[3] *Web Exploit Kit*: código dañino que automatiza la explotación de vulnerabilidades en el navegador web del usuario.

[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.

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*).
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 hallaremos 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. Dichas copias de seguridad **no deben ser accesibles directamente** desde el equipo de forma física (como por ejemplo, discos duros externos USB) o por medio de recursos compartidos en red. 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, servicios como RDP han sido ampliamente utilizados en los últimos años [Ref.-4] para tratar de infectar equipos con ransomware. Los atacantes emplean herramientas y scripts con diccionarios de palabras para tratar de obtener credenciales válidas de usuarios. En el caso de exponer este tipo de servicios al exterior, se recomienda utilizar contraseñas robustas y políticas *lock-out* que permitan establecer un número determinado de intentos de autenticación antes de bloquear la IP correspondiente. Del mismo modo, se recomienda establecer ACL (listas de control de acceso) para restringir el acceso a este tipo de servicios desde equipos de confianza.

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. El navegador, versiones antiguas de Java, Flash o Adobe Acrobat suelen ser algunas de las principales vías de infección en ataques de este tipo.

Además de disponer de software correctamente actualizado, es recomendable utilizar soluciones que permitan mitigar *exploits*. Herramientas como **EMET** [7][Ref.-5] permiten aplicar determinadas medidas de seguridad tales como DEP, EAF, ASLR, SEHOP, NPA[8], etc., de forma personalizada a los procesos que se deseen para prevenir la ejecución de código dañino (incluidos 0-days[9]). 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 o herramientas similares. Este tipo de aplicaciones no deben verse como una alternativa al antivirus, sino como una herramienta adicional más de protección.

[7] 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.

[8] DEP, EAF, ASLR, SEHOP, NPA: conjunto de características de seguridad incluidas en la mayoría de sistemas operativos modernos que permiten mitigar exploits.

[9] 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

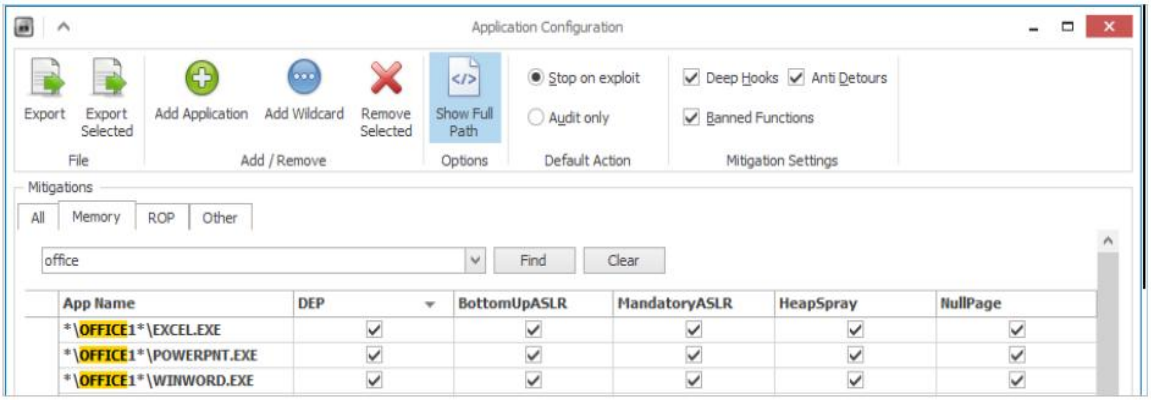


Figura 4. EMET

Valorar el uso de aplicaciones de lista blanca (*white 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.

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).

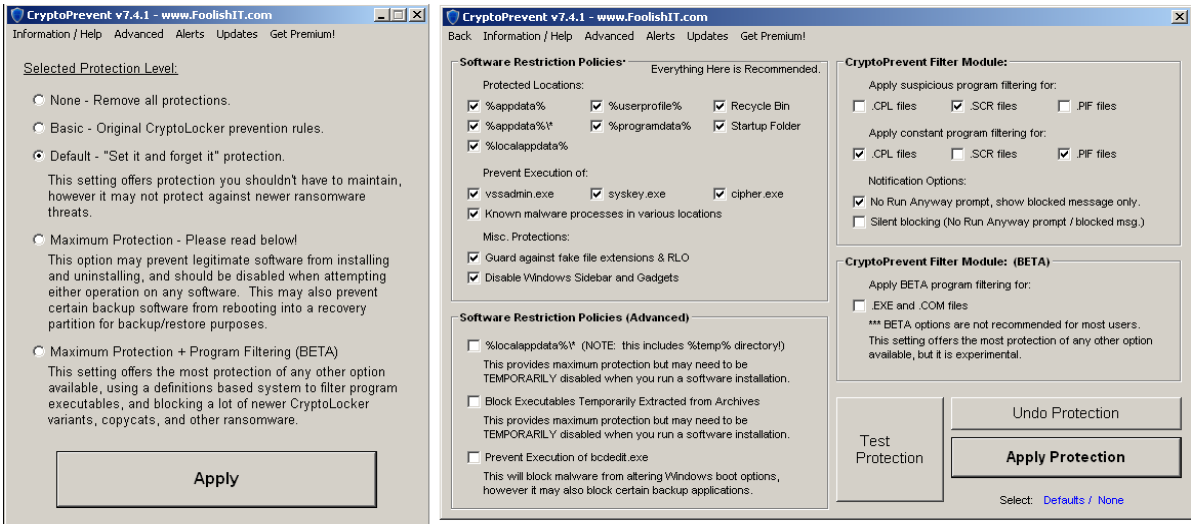


Figura 5. CryptoPrevent

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

- 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**".

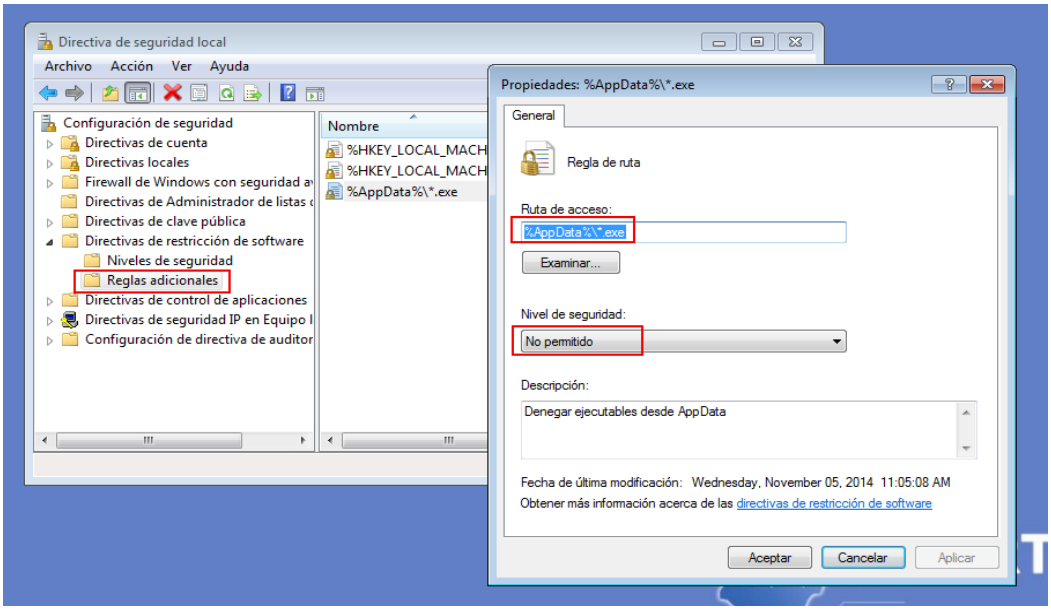


Figura 6. Directiva de seguridad local

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

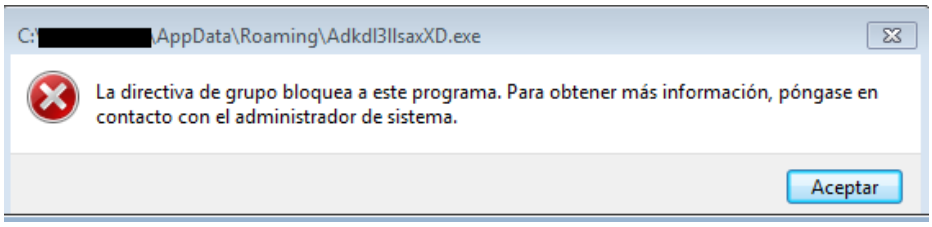


Figura 7. Alerta: Bloqueo programa

- Considérense otras rutas como *%UserProfile%\Local Settings*, *%UserProfile%\Local Settings\Temp*, etc., para denegar la ejecución de binarios. Muchos tipos de código dañino, no sólo 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.

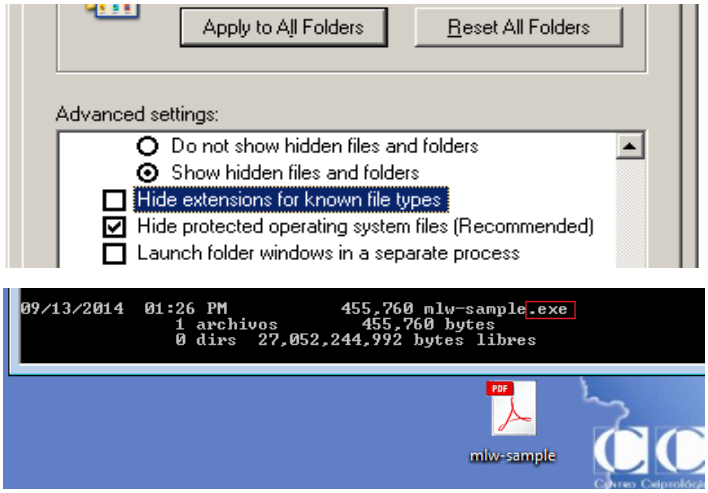


Figura 8. Mostrar extensiones de ficheros conocidos

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 sistema 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.

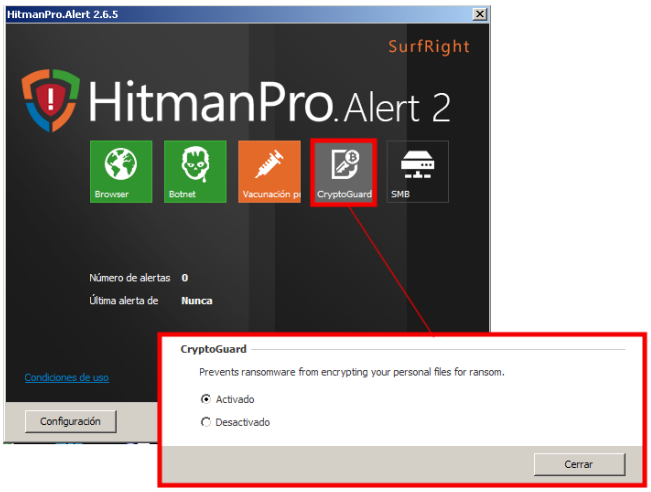


Figura 9. HitmanPro.Alert (CryptoGuard)

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, permitiéndonos 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 10. 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 click 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.

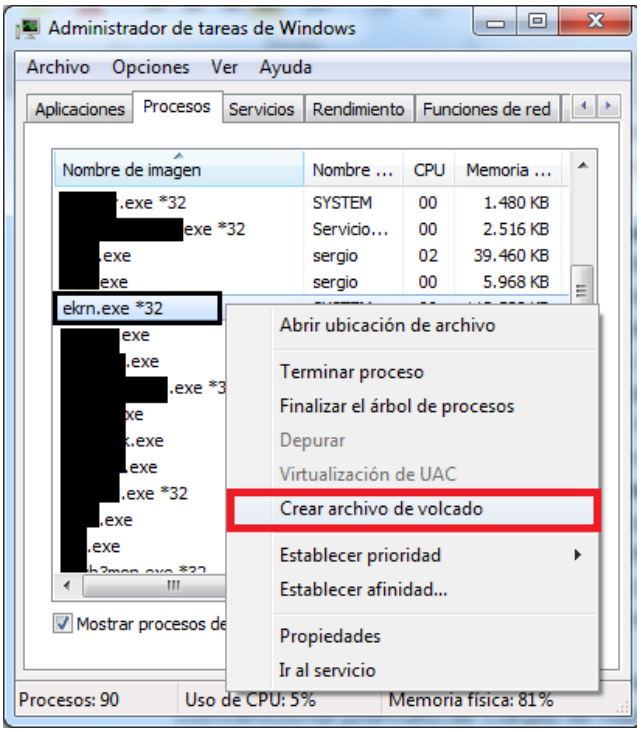


Figura 11. Realización de volcado de memoria de un proceso

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: click derecho sobre el proceso y seleccionar la opción "Finalizar el árbol de procesos".

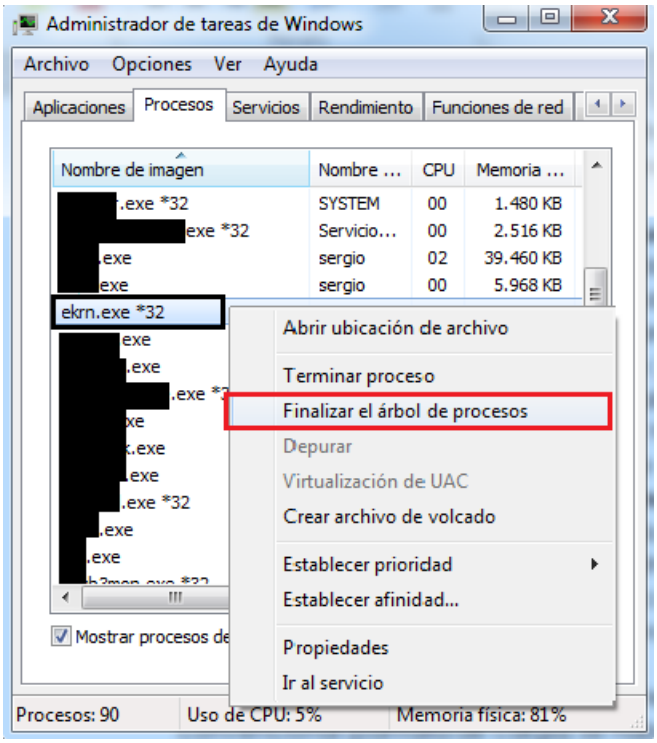


Figura 12. Finalización del proceso

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.

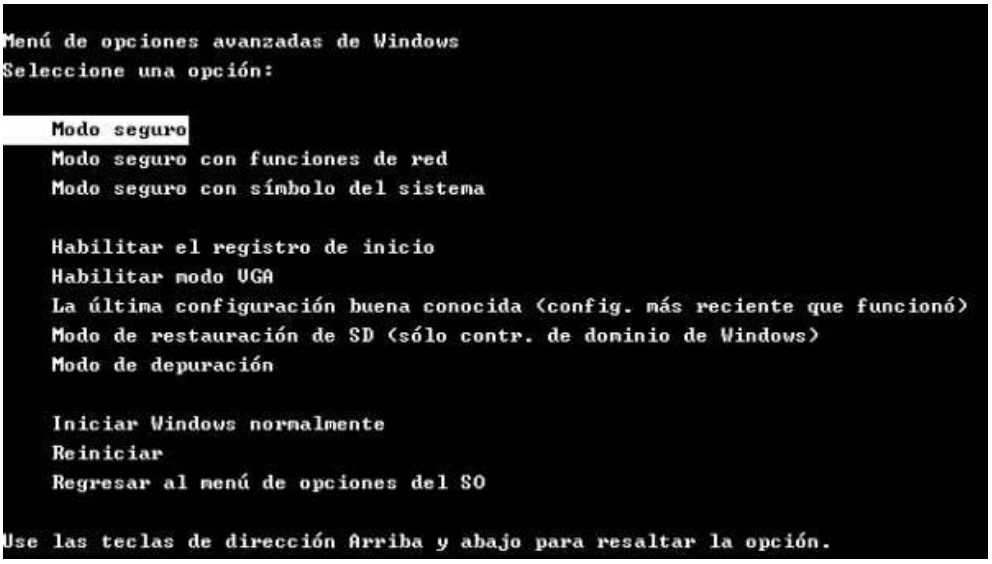


Figura 13. Inicio en modo seguro

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 pueda romper el cifrado o se liberen las claves del C&C.



Figura 14. 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 apartado 5 "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, hay que 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 nos 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 "Herramientas de Descifrado" 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 apartado 5 "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 apartado 7 "Descifrado de ransomware".



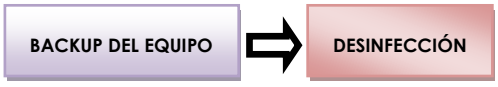
❖ **ESCENARIO Nº3: Se dispone de *Shadow Volume Copy***. Bastaría con restaurar las copias de seguridad que realiza Windows automáticamente de los ficheros, utilizando Shadow Explorer, por ejemplo. En muchos casos el ransomware imposibilitará esta acción. Para más información consultar el apartado 6 "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.

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 [Ref.-16] de Microsoft.

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.

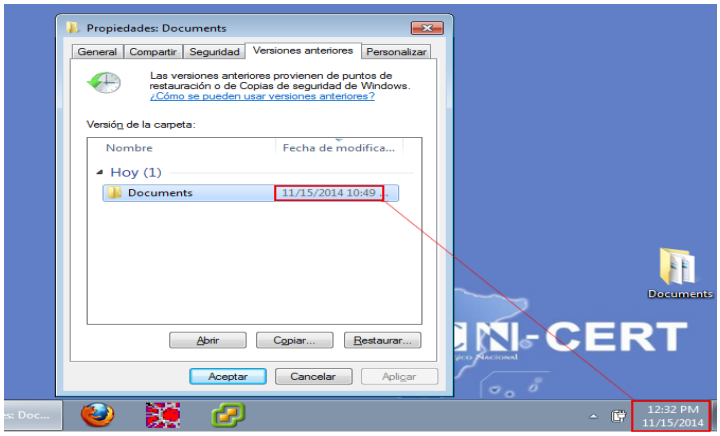


Figura 15. Restauración de ficheros (VSS)

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".**

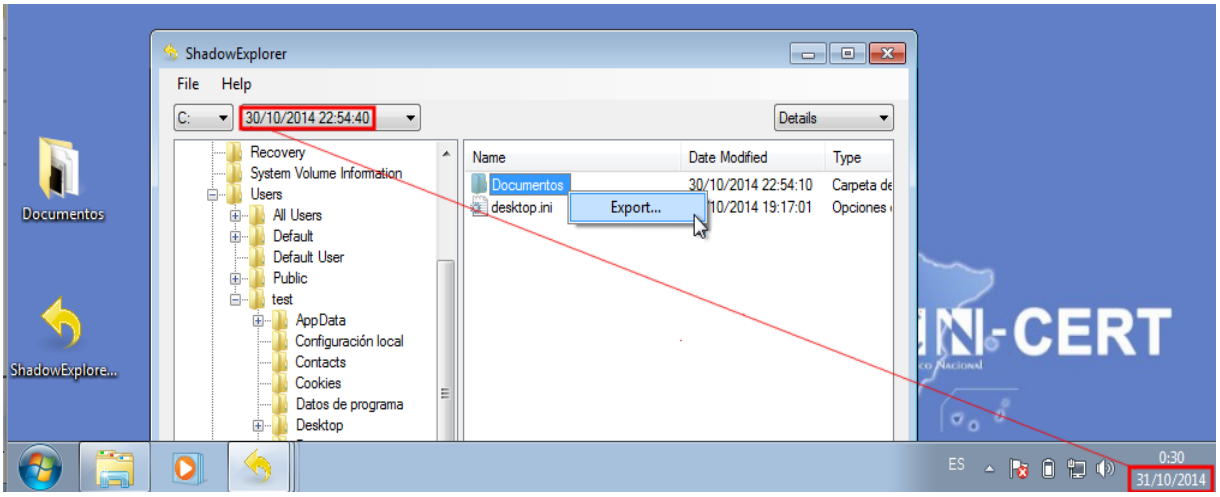


Figura 16. Shadow Explorer

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.

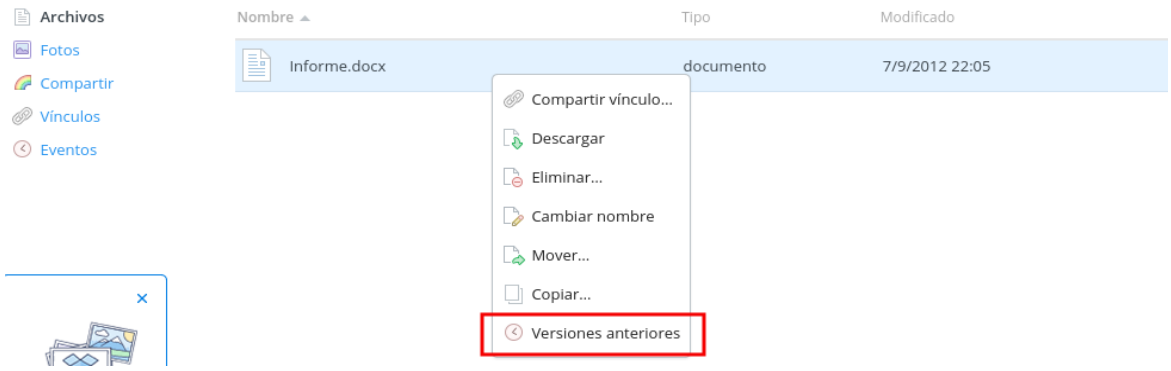


Figura 17. Restauración de ficheros (Dropbox)

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 18. 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 19. Dropbox *restore script*

6.3 RESTAURACION 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.

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.

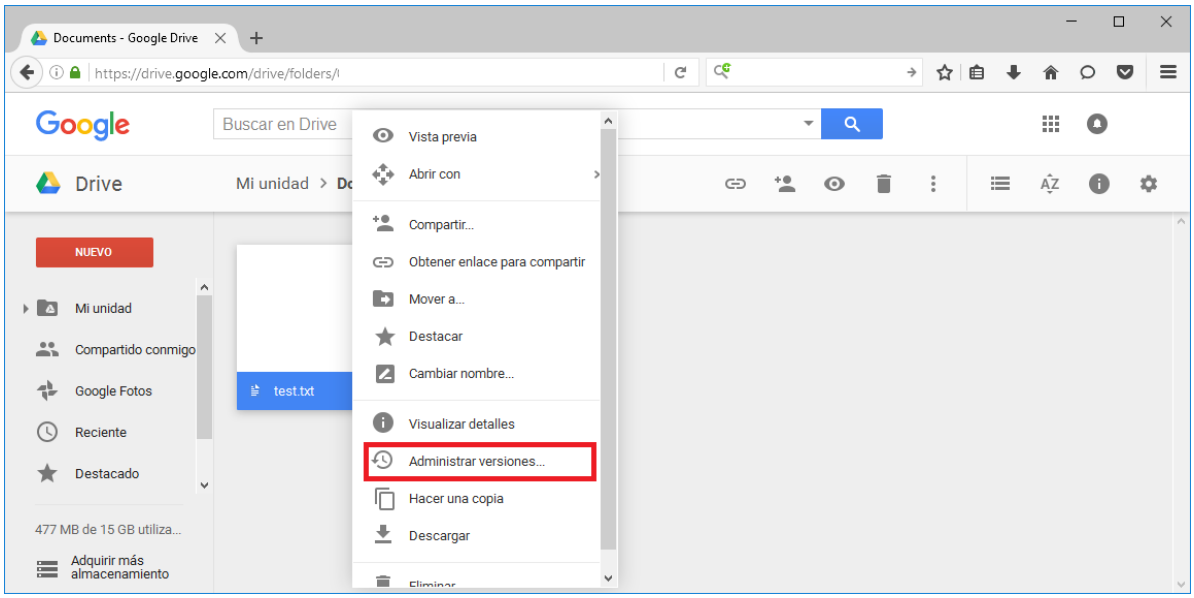


Figura 20. Restauración de ficheros (Google Drive)

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. DESCIFRADO DE RANSOMWARE

7.1 TABLA RESUMEN

En la siguiente tabla se muestra un pequeño 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 impacto en las Administraciones Públicas Españolas):

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.	✗
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.	✗
DMALOCKER	Para las dos primeras versiones se puede usar la herramienta creada por 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 a partir de backup.	○
MISCHA	A partir de backup.	✗
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.	✔

✔ Si existe solución ○ Existe solución parcial ✗ No existe solución

7.2 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 podemos subir los ficheros cifrados y las notas de rescate, de este modo y a través del tipo de encriptación y método de rescate, podremos saber qué tipo de familia es la que nos ha infectado.

7.3 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:

Bandarchor – herramienta kaspersky

Web: https://support.kaspersky.com/sp/viruses/disinfection/10556

Cryptodefense – herramienta emsisoft

Web: https://decrypter.emsisoft.com/cryptodefense

Cryptolocker

Web: http://www.decryptcryptolocker.com

DMAlocker – herramienta emsisoft

Web: https://decrypter.emsisoft.com/dmalocker

Locky – herramienta emsisoft

Web: https://decrypter.emsisoft.com/autolocky

Petya - herramienta bleepingcomputer

Web: http://download.bleepingcomputer.com/fabian-wosar/Petyaextractor.zip

Teslacrypt – herramienta eset

Web: https://download.eset.com/special/ESETTeslaCryptDecryptor.exe

Torrentlocker – herramienta bleepingcomputer

Web: http://download.bleepingcomputer.com/Nathan/TorrentUnlocker.exe

Zerolocker – herramienta vinsula

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

8. 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/