Seguridad de la información
Continuidad del negocio
Gobierno de TI

Documento Técnico: Procedimiento para evitar que un ransomware cifre los archivos en Windows

Versión 1.0

Junio 2016

Procedimiento para evitar que un ransomware cifre los archivos en Windows

El ransomware es un tipo de malware que emplea cifrado asimétrico para secuestrar la información de la víctima y solicitar un rescate. El cifrado asimétrico (clave pública) es una técnica criptográfica en la que se utilizan un par de claves para cifrar y descifrar un archivo. El delincuente genera de manera exclusiva el par de claves pública-privada para la víctima y almacena la clave privada para descifrar los archivos en su servidor. La víctima solamente podrá acceder a la clave privada tras el pago de un rescate al agresor, aunque tal y como se ha podido comprobar en campañas recientes de ransomware, esto no siempre sucede así. Sin acceso a la clave privada, resulta prácticamente imposible descifrar los archivos por los que se exige un rescate.

Evita el secuestro de tus datos

La mayoría de las campañas de ransomware empiezan por un mensaje de correo electrónico de phishing. Con el paso del tiempo, han ganado en sofisticación, y ahora muchas están específica y meticulosamente diseñadas en el idioma local de las víctimas a las que van dirigidas.

Ejemplos:

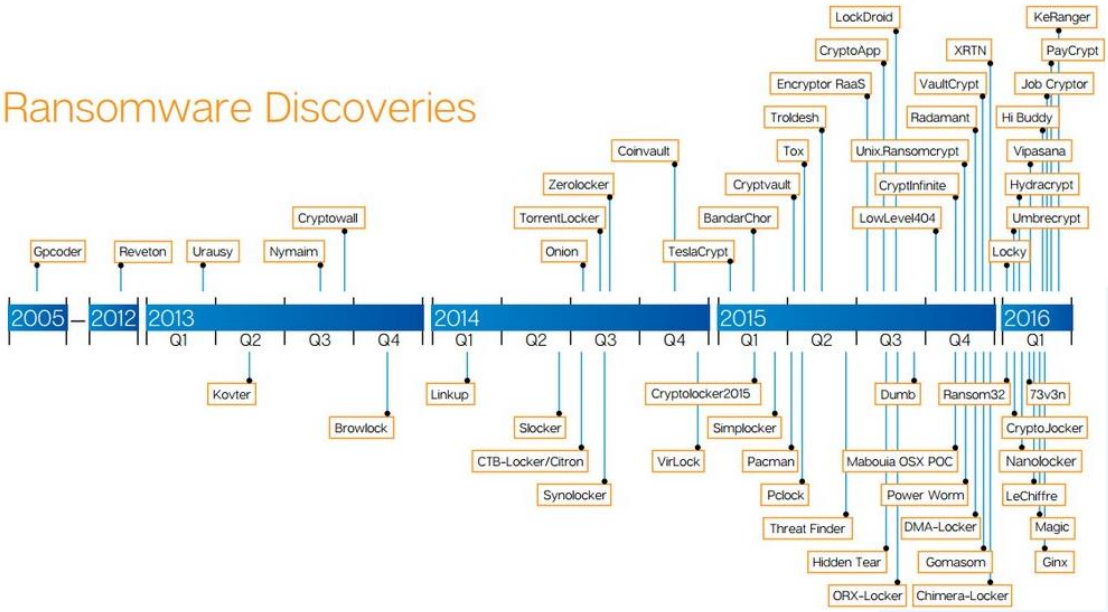
- AusPost y Office of State Revenue (Australia)
- Royal Mail (Inglaterra)
- DHL (Austria y Alemania)
- Česká pošta (República Checa)
- TTTNet (Turquía)
- SDA (Italia)
- Correos (España)

CryptoLocker, TorrentLocker, CryptoWall, CTB-Locker, ZeroLocker, TeslaCrypt, el sentido común es nuestro amigo. Correos no suele enviar email para avisarnos de la llegada de una carta certificada, suele ser el cartero quien nos deja un aviso en el buzón de nuestra casa. Si encontramos más de dos faltas gramaticales claras deberíamos empezar a sospechar.

Pero además al entrar a la supuesta página de Correos veremos en la barra de direcciones del navegador como el dominio no tiene nada que ver con Correos.es aunque en el e-mail y la página web aparezcan los logos de correos. Es un claro ejemplo de phishing (suplantación de identidad). Ya está bien de tomar el pelo a personas con menos conocimientos informáticos que no saben diferenciar entre una página real y una falsa.

¿Estas seguro del nombre de dominio? Estar seguro de que entran en el dominio correcto verificando el nombre de dominio. Muchas veces los atacantes utilizan nombres similares, que difieren en una letra y lo hacen esperando un error de escritura del usuario, como por ejemplo escribir Facebok en lugar de Facebook o bien utilizan subdominios muy largos.

Listado actualizado de Ransomware con sus extensiones



A continuación un listado de ransonware conocidos, el tipo de cifrado utilizado y la herramienta de descifrado (si la hay)

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

Name	Extensions	Extension Pattern	Ransom Note Filename(s)	Comment	Encryption Algorithm	Also known as	Decryptor	Info 1	Info 2	Screenshots
.CryptoHasYou.	.enc		YOUR_FILES_ARE_LOCKED.txt		AES(256)			http://www.nyxbone.co		https://www.google.c
777	.777	_[timestamp]_$[email]$.777 e.g. _-14-05-2016-11-59-36_$	read_this_file.txt		XOR	Sevleg	https://decrypter.emsis			
7ev3n	.R4A .R5A		FILES_BACK.txt			7ev3n-HONE$T	https://github.com/has	http://www.nyxbone.co		https://www.google.c
8lock8	.8lock8		READ_IT.txt	Based on HiddenTear	AES (256)		http://www.bleepingco			
Alpha Ransomware	.encrypt		Read Me (How Decrypt) !!!!.txt		AES(256)	AlphaLocker	http://download.bleepi	http://www.bleepingco		https://www.google.c
AutoLocky	.locky		info.txt info.html				https://decrypter.emsis			https://www.google.c
BadBlock			Help Decrypt.html				https://decrypter.emsis	http://www.nyxbone.co		http://www.nyxbone.c
Bandarchor		.id-[ID]_[EMAIL_ADDRESS]		Files might be partially encrypted	AES(256)	Rakhni		https://reaqta.com/201		https://www.google.c
BitCryptor	.clf			Has a GUI. CryptoGraphic Locker family. Newer CoinVault variant.			https://noransom.kasp			https://www.google.c
BlackShades Crypter	.Silent		Hacked_Read_me_to_decrypt_files.html YourID.txt		AES (256)	SilentShade		http://nyxbone.com/ma		
Blocatto	.blocatto			Based on HiddenTear	AES (256)		http://www.bleepingco			
Booyah				EXE was replaced to neutralize threat		Salam!				https://www.google.c
Brazilian	.lock		MENSAGEM.txt	Based on EDA2	AES(256)			http://www.nyxbone.co		http://www.nyxbone.c
BrLock					AES			https://www.proofpoint		https://www.google.c
Browlock				no local encryption, browser only						https://www.google.c
Bucbi				no file name change, no extension	GOST			http://researchcenter.p		https://www.google.c
BuyUnlockCode		(.*).encoded.([A-Z0-9]{9})	BUYUNLOCKCODE.txt	Does not delete Shadow Copies						https://www.google.c
Cerber	.cerber		# DECRYPT MY FILES #.html # DECRYPT MY FILES #.txt # DECRYPT MY FILES #.vbs		AES			https://blog.malwareby		https://www.google.c

Consejo básico de seguridad en Windows: Mostrar la extensión real de un archivo
Una extensión de nombre de archivo es un conjunto de caracteres que se agregan al final de un nombre de archivo para determinar qué programa debería abrirlo.

Para abrir Opciones de carpeta,
haga clic en el botón Inicio,
en Panel de control,
en Apariencia y personalización
y, por último, en Opciones de carpeta.
haga clic en la ficha Ver y, a continuación,
en Configuración avanzada, realice una de las acciones siguientes:

Para mostrar las extensiones de nombre de archivo, desactive la casilla Ocultar las extensiones de archivo para tipos de archivo conocidos y, a continuación, haga clic en Aceptar.

Desmarcar Ocultar las extensiones de archivo para tipos de archivo conocidos.

- Antes: .pdf
- Ahora mostrará: .pdf.exe

¿Cómo evitar o prevenir infección con CryptoWall o CryptoLocker?

1. Herramientas específicas Anti-ransomware (ver abajo)
2. Editor de directivas locales y de grupo (Group Policy Object, GPO)
3. Usando el dministrador de recursos del servidor de archivo en Windows 2012

Herramientas específicas de protección (Anti-Ransom)

- Anti-Ransomware de Malwarebytes (Basado en CryptoMonitor)
- HitmanPro
- CryptoPrevent (Básicamente aplica políticas de seguridad con GPO)
- Cryptostalker
- AntiRansom de SecurityByDefault.com
- AppLocker de Microsoft
- BDAntiRansomware de BitDefender
- PROTEIN – PROTEct your INformation (Powershell Anti-Ransomware)
- Cómo evitar infectarse con archivos JS adjuntos y ransomware
- Herramientas para detectar ransomware en Windows y Linux

Cryptostalker

Sean Williams, un desarrollador de San Francisco, creó un proyecto muy interesante llamado randumb que contenía un ejemplo al que bautizó como Cryptostalker y que, básicamente, monitoriza la creación o escritura de archivos en el sistema con datos aleatorios por medio de un análisis mediante frecuencia y asimetría (histograma). Si los archivos contienen datos aleatorios puede ser una señal de la actividad de un proceso de cifrado de un ransomware, por lo que la herramienta es ideal para alertar al usuario de forma temprana.

Además, recientemente ha sido portado a Go sustituyendo inotify por fsnotify de Google para las notificaciones. Funciona perfectamente en Linux y OSX aunque está pendiente probarlo más en Windows.

Su nuevo repositorio es: https://github.com/unixist/cryptostalker
Editor de directivas locales y de grupo (Group Policy Object, GPO)
Se pueden utilizar los grupos de Windows o el editor de directivas locales para crear directivas de restricción de software que bloquean los ejecutables que se inician cuando se encuentran en rutas específicas. Para obtener más información sobre cómo configurar directivas de restricción de software.

Las rutas de los archivos que han sido utilizados por esta infección son:

- C:\Users\\AppData\Local\.exe (Vista/7/8)
- C:\Users\\AppData\Local\.exe (Vista/7/8)
- C:\Documents and Settings\\Application Data\.exe (XP)
- C:\Documents and Settings\\Local Application Data\.exe (XP)
- %appdata%*.exe
- %appdata%**.exe
- %localappdata%*.exe
- %localappdata%**.exe

Con el fin de bloquear CryptoLocker podemos crear reglas para las rutas en las que no se permite la ejecución de archivos. Para crear estas directivas de restricción de software, añadiendo las políticas de forma manual usando el editor de directivas de seguridad local o el editor de directivas de grupo.

Nota: Si estás utilizando Windows Home o Windows Home Premium, no tendrás disponible el editor de directivas de seguridad local.
Con el fin de crear manualmente las directivas de restricción de software necesitas usar Windows Professional, Bussiness, Enterprise o Ultimate, o Windows Server. Si quieres establecer estas políticas para un determinado equipo puedes usar el editor de directivas de seguridad local. Si vas a aplicar estas políticas para todo un dominio, entonces necesitas utilizar el editor de directivas de grupo.

Para abrir el editor de directivas de seguridad local, haz click en el botón Inicio y escribe "Directiva de seguridad local", para después seleccionar el resultado de la búsqueda que aparece. Para abrir el editor de directivas de grupo, escribe "Directiva de grupo" en su lugar. En esta guía veremos el editor de directivas de seguridad local en los ejemplos.

Una vez la pantalla está abierta, expande Configuración de seguridad y, a continuación haz clic en la sección de directivas de restricción de Software. Si no ves nada en el panel de la derecha (como se muestra arriba), tendrás que añadir una nueva política. Para ello haz clic en el botón Acción y selecciona Nuevas políticas de restricción de Software. Esto habilitará la directiva para que aparezca el panel de la derecha. Después, debes hacer clic en la categoría Reglas adicionales, e ir al panel derecho, donde seleccionaremos Nueva regla de ruta… A continuación, agregamos una regla de ruta para cada uno de los elementos enumerados a continuación.

Si las directivas de restricción de software causan problemas al intentar ejecutar aplicaciones legítimas, mira esta sección sobre cómo habilitar aplicaciones específicas.

A continuación se presentan algunas reglas de ruta que se sugieren, no solo para bloquear las infecciones sin más, sino también para bloquear los archivos adjuntos que se ejecuten al abrir un cliente de correo electrónico.

Bloquear ejecutable CryptoLocker en %AppData%

- Ruta: %AppData%*.exe
- Security Level: Disallowed
- Descripción: Don't allow executables to run from %AppData%.Bloquear ejecutable CryptoLocker en %LocalAppData%
- Ruta usando Windows XP: %UserProfile%\Local Settings*.exe
- Ruta usando Windows Vista/7/8: %LocalAppData%*.exe
- Security Level: Disallowed
- Descripción: Don't allow executables to run from %AppData%.

Bloquear ejecutable Zbot en %AppData%

- Ruta: %AppData%**.exe
- Security Level: Disallowed
- Descripción: Don't allow executables to run from immediate subfolders of %AppData%.
- Block ejecutable Zbot en %LocalAppData%
- Ruta con Windows XP: %UserProfile%\Local Settings**.exe
- Ruta Windows Vista/7/8: %LocalAppData%**.exe
- Security Level: Disallowed

- Descripción: Don't allow executables to run from immediate subfolders of %AppData%.
- Bloquear ejecutables de un archivo adjunto abierto con WinRAR:
- Ruta en Windows XP: %UserProfile%\Local Settings\Temp\Rar**.exe
- Ruta en Windows Vista/7/8: %LocalAppData%\Temp\Rar**.exe
- Security Level: Disallowed
- Descripción: Block executables run from archive attachments opened with WinRAR.

Bloquear ejecutables de un archivo adjunto abierto con 7zip:

- Ruta en Windows XP: %UserProfile%\Local Settings\Temp\7z**.exe
- Ruta en Windows Vista/7/8: %LocalAppData%\Temp\7z**.exe
- Security Level: Disallowed
- Descripción: Block executables run from archive attachments opened with 7zip.
- Bloquear ejecutables de un archivo abierto con WinZip:
- Ruta en Windows XP: %UserProfile%\Local Settings\Temp\wz**.exe
- Ruta en Windows Vista/7/8: %LocalAppData%\Temp\wz**.exe
- Security Level: Disallowed
- Descripción: Block executables run from archive attachments opened with WinZip.
- Bloquear ejecutables de archivos adjuntos usando compresor de Windows:
- Ruta para Windows XP: %UserProfile%\Local Settings\Temp*.zip*.exe
- Ruta para Windows Vista/7/8: %LocalAppData%\Temp*.zip*.exe
- Security Level: Disallowed
- Descripción: Block executables run from archive attachments opened using Windows built-in Zip support.

Cómo protegerse contra Cryptolocker en Windows 2012

Vamos a implementar una solución basada en el Administrador de recursos del servidor de archivos *(File Server Resource Manager)*, conjunto de herramientas que permite administrar la cantidad y el tipo de datos almacenados en los servidores. Esta opción está disponible de manera gratuita en Windows Server 2012, añadiendo simplemente las características correspondientes dentro del servidor de archivos.

El Administrador de recursos del servidor de archivos es un conjunto de herramientas de Windows Server 2008 que permite a los administradores entender, controlar y administrar la cantidad y el tipo de datos almacenados en los servidores. Los administradores pueden utilizarlo para asignar cuotas a carpetas y volúmenes, realizar un filtrado activo de los archivos y generar informes de almacenamiento exhaustivos. Este conjunto de instrumentos avanzados no sólo permite al administrador supervisar los recursos de almacenamiento existentes, sino que además le ayuda a planear e implementar futuros cambios de directivas.

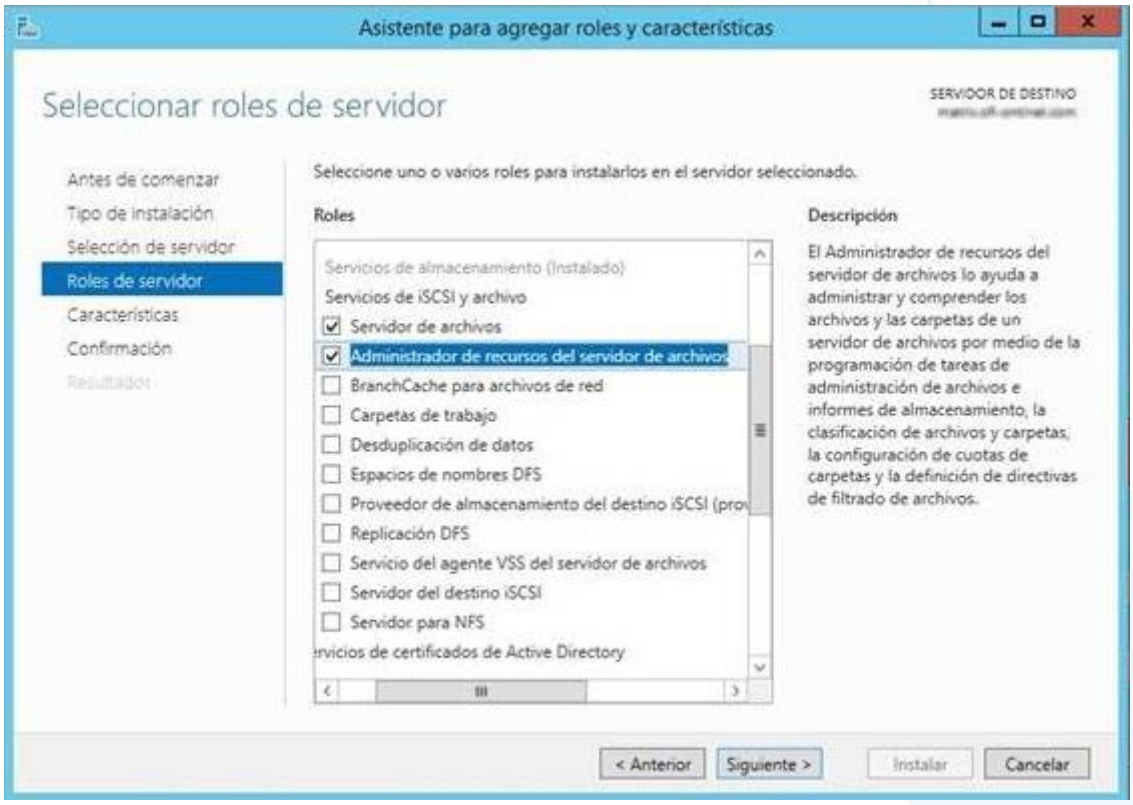
En el nodo Administración del filtrado de archivos del complemento MMC del Administrador de recursos del servidor de archivos, puede realizar las siguientes tareas:

- Crear filtros de archivos para controlar los tipos de archivos que los usuarios pueden guardar y generar notificaciones cuando los usuarios intenten guardar archivos no autorizados.
- Definir plantillas de filtrado de archivos que puedan aplicarse a nuevos volúmenes o carpetas y que pueden utilizarse en toda una organización.
- Crear excepciones de filtrado de archivos que amplíen la flexibilidad de las reglas de filtrado de archivos.

Por ejemplo, puede:

- Garantizar que no se almacenen archivos de música en las carpetas personales de un servidor y, al mismo tiempo, permitir el almacenamiento de tipos concretos de archivos multimedia que admitan la administración de derechos legales o que cumplan las directivas de la compañía. En el mismo escenario, puede que desee conceder a un vicepresidente de la compañía privilegios especiales para almacenar cualquier tipo de archivos en su carpeta personal.
- Implementar un proceso de filtrado para enviarle una notificación por correo electrónico cada vez que se almacene un archivo ejecutable en una carpeta compartida, que incluya información del usuario que almacenó el archivo y la ubicación exacta de éste, de modo que puedan tomarse las medidas preventivas pertinentes.

Cómo monitorizar archivos dentro de un servidor Windows 2012
Comenzaremos en la selección de roles de servidor, seleccionando el administrador de recursos:



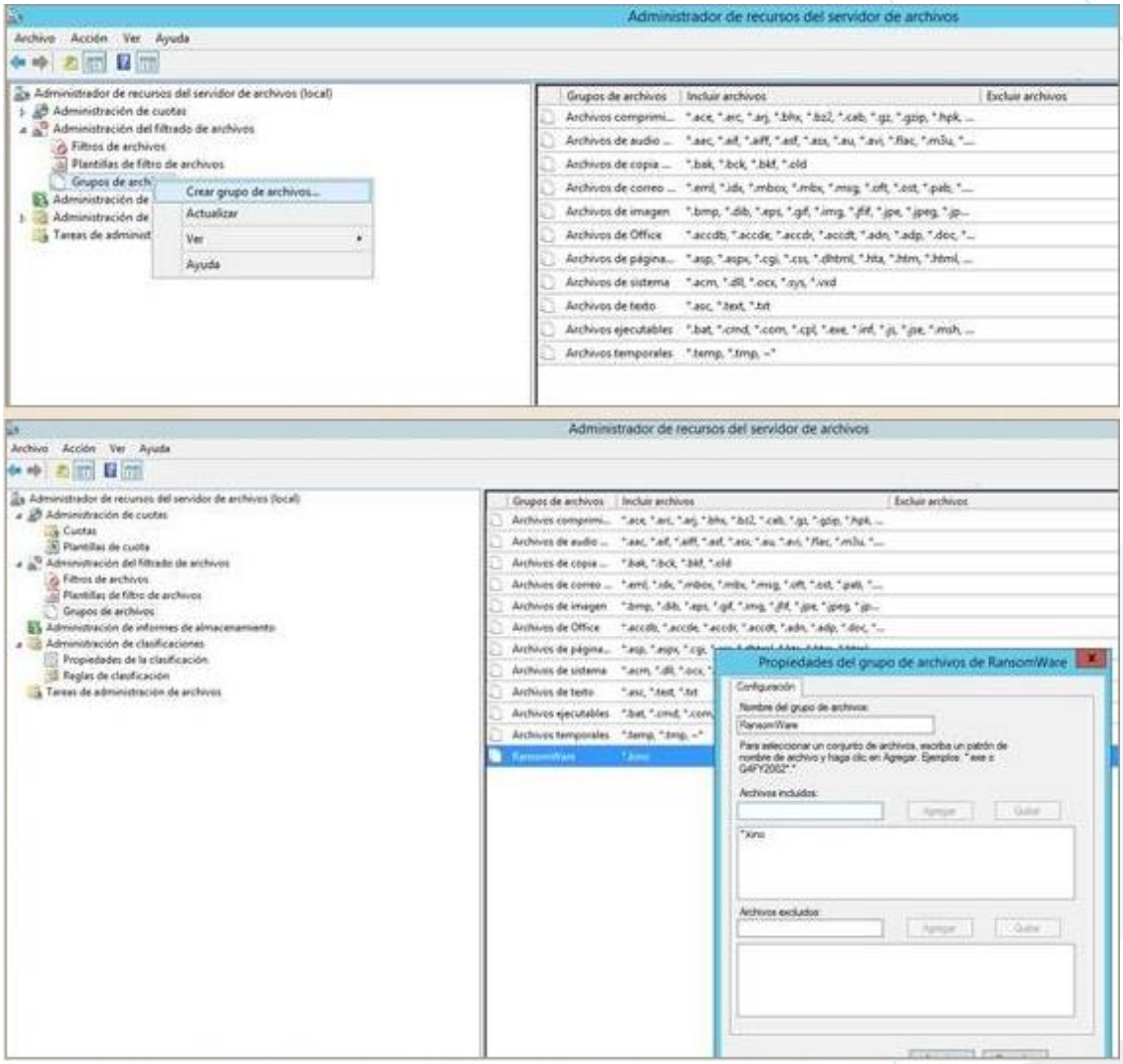
El concepto a desplegar es sencillo: monitorizar los archivos dentro del servidor. Para ello, introduciremos una serie de extensiones maliciosas empleadas por el malware para cifrar los archivos, poniendo un "señuelo" en esas carpetas para que en caso de infección, se detecte el proceso y se detenga.

Lo primero que debemos hacer es tener una lista de extensiones empleadas por el malware más o menos actualizadas.

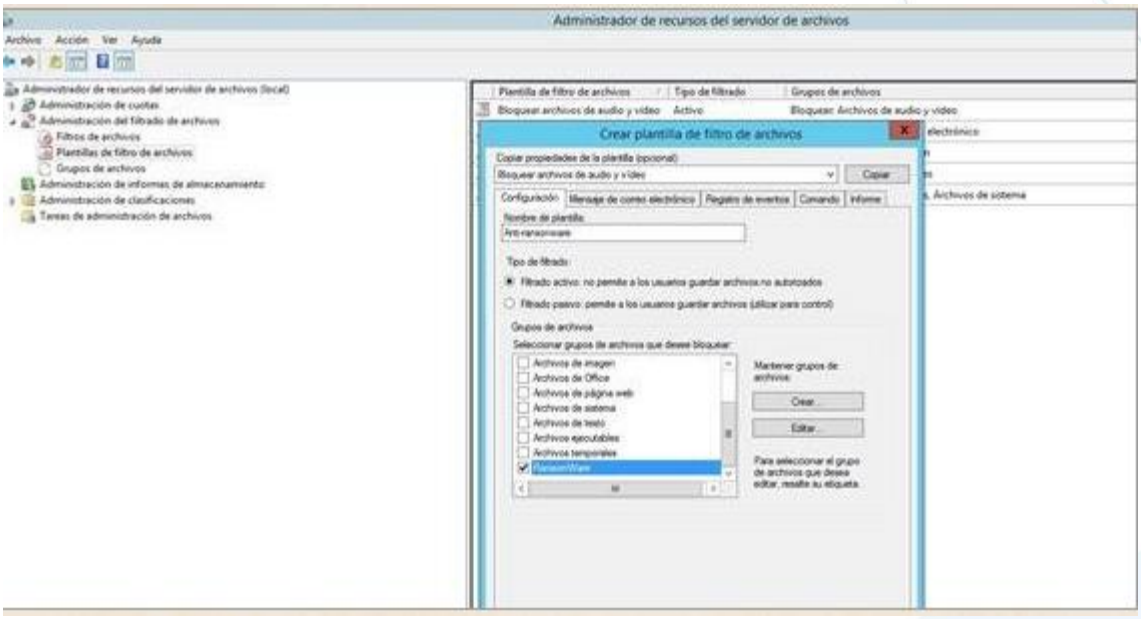
Pongamos como punto de partida este listado:

.*AES256, *.*cry, *.*crypto, *.*darkness, *.*enc*, *.*kb15, *.*kraken, *.*locked, *.*nochance, *.*oshit, *.*exx, *@gmail_com_*, *@india.com*, *cpyt*, *crypt*, *decipher*, *install_tor*.*, *keemail.me*, *qq_com*, *ukr.net*, *restore_fi*.*, *help_restore*.*, *how_to_recover*.*, *.ecc, *.exx, *.ezz, *.frtrss, *.vault, *want your files back.*, confirmation.key, enc_files.txt, last_chance.txt, message.txt, recovery_file.txt, recovery_key.txt, vault.hta, vault.key, vault.txt, *.aaa, *help_your_files*.

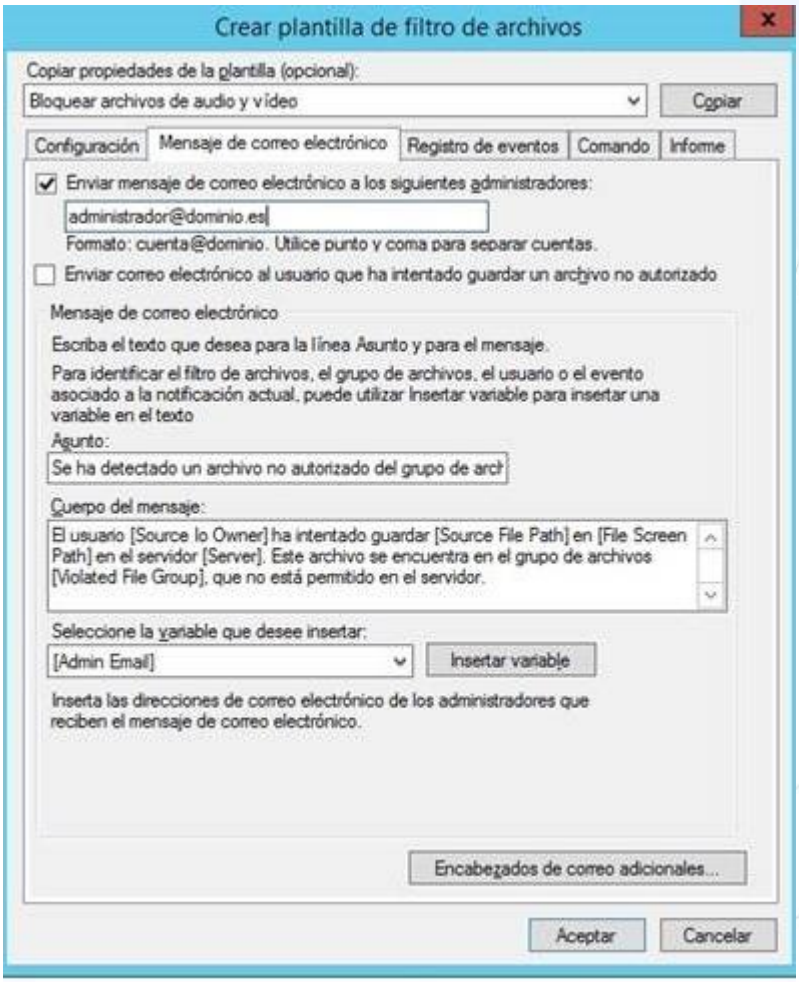
En el Administrador de recursos creamos un grupo de archivos que incluya este tipo de extensiones:



El siguiente paso es crear una plantilla de actuación, en la que definiremos el comportamiento deseado ante la detección de un archivo con la extensión mencionada:

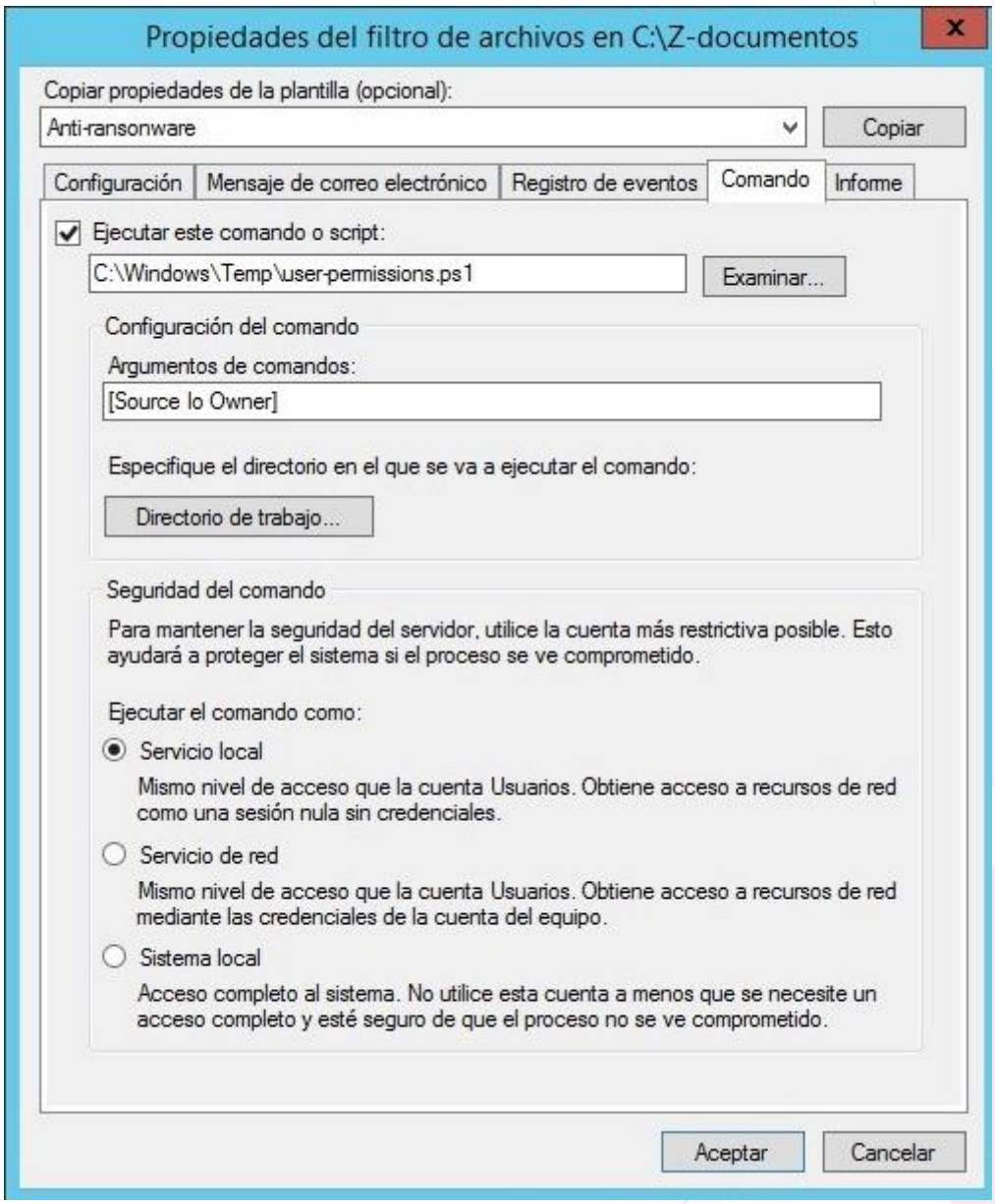


Una de las opciones básicas es configurar un mensaje y cuenta de correo para notificar el incidente:



A continuación sería una buena idea escribir un evento en el registro de Windows para reenviar posteriormente a un sistema de correlación SIEM o simplemente para efectos de control.

Claro que no solo queremos detectar una posible infección por ***ransomware***, sino que queremos prevenir o mitigar las temidas consecuencias. Para ello, habilitamos una sesión de comandos al encontrar un cambio en los archivos:

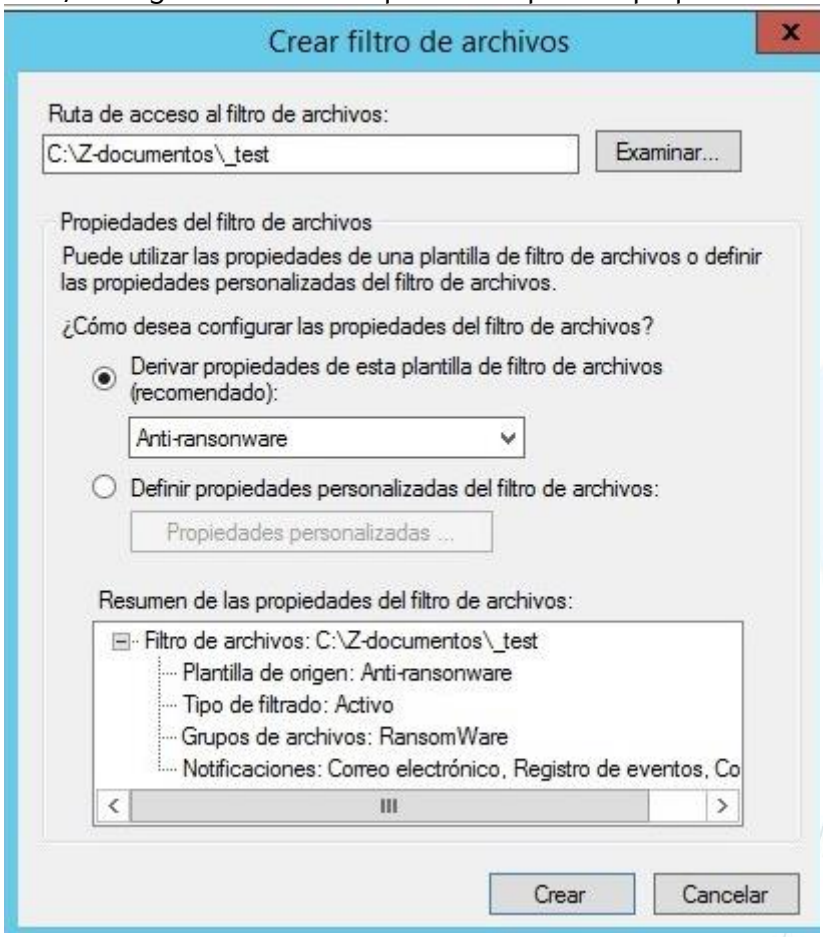


El comando o los comandos que podemos ejecutar mediante este "disparador" o monitor son infinitos.

Podemos optar por apagar el servidor de archivos, bloquear el acceso al usuario de red que ha intentado modificar los archivos (el malware), o bloquear la dirección IP de entrada al servidor desde el equipo que origina la infección.

Particularmente prefiero apagar el servidor. Esto dejará a los usuarios sin servicio, pero es una manera radical de evitar la infección.

Por último, configuramos dónde queremos que se aplique el filtro:



Tenemos que ser conscientes de que este servicio de monitorización consume recursos en el sistema, y que en grandes entornos con miles y millones de archivos podría producir penalizaciones en el rendimiento del servicio.

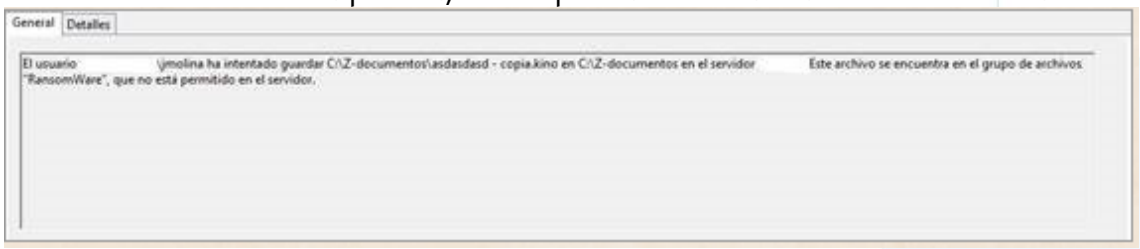
Para ello empleamos un pequeño truco. En los sistemas Windows el guion bajo (_) es el primer carácter que aparece en una ordenación, por lo que creamos una carpeta con este nombre y será la que sea monitorizada.

A efectos prácticos en caso de producirse una infección, el proceso de cifrado comienza por la carpeta "señuelo".

En un entorno real, se produce un lapsus de tiempo entre que el malware comienza a cifrar la carpeta señuelo, ejecuta el comando deseado (apagar) y se apaga el equipo o se ejecuta cualquiera otra opción, por lo que tenemos que contar con 5/10 archivos cifrados.

Este es un pequeño defecto en el concepto, aunque en un entorno de millones de archivos es un mal menor, que seguro estamos dispuestos a pagar por evitar el temido cifrado del servidor de archivos.

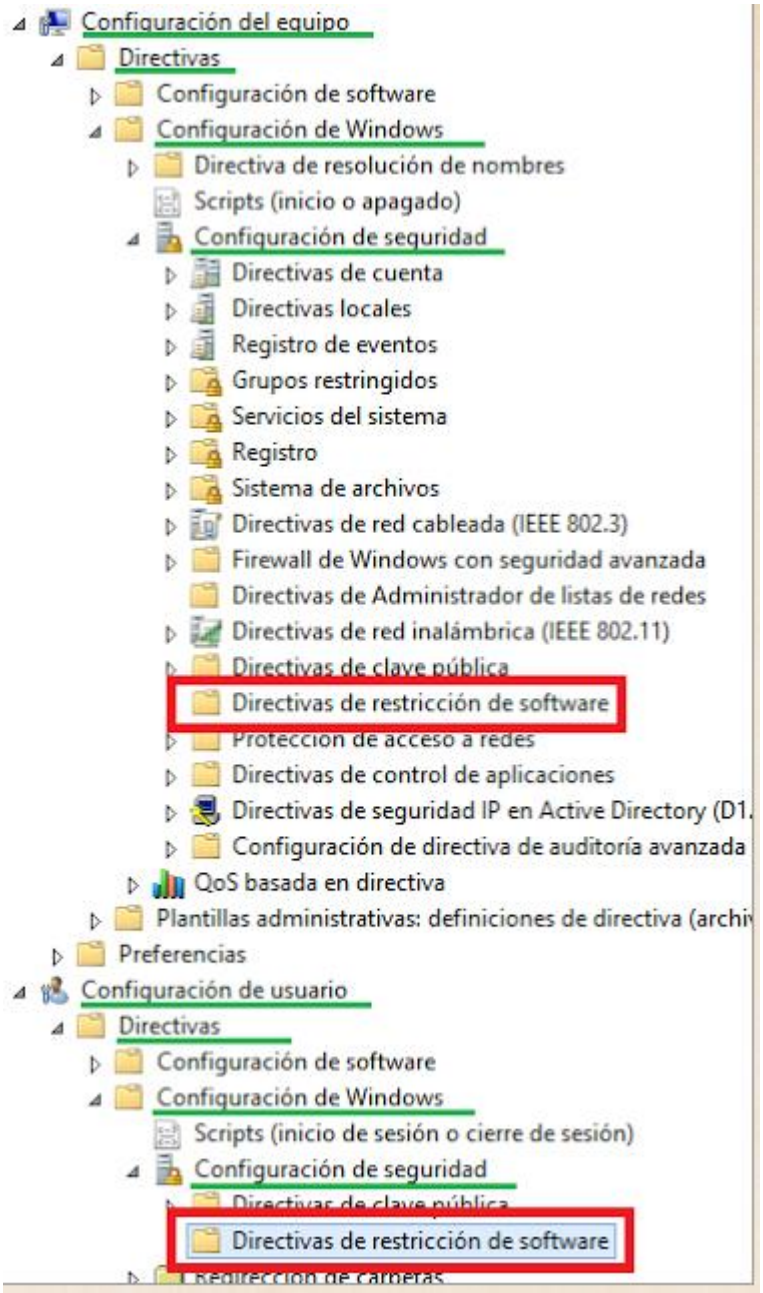
Para terminar, podemos ver cómo se ha producido el correspondiente registro en el visor de eventos. En esta prueba, un simple cambio manual de nombre de archivo:



Windows: GPO para prevenir Cryptolocker

Podemos utilizar GPOs para fortificar la configuración e intentar evitar la ejecución de Cryptolockers.

Para ello, utilizaremos las *Software Restriction Policies (SRP)*. Encontraremos la posibilidad de configurar directivas SRP como GPOs de equipo o usuario:



Podemos configurar GPOs SRP que bloqueen extensiones en rutas. Una GPO SRP de bloqueo de rutas, el bloqueo se efectuará independientemente de los permisos NTFS asignados en la ruta.

Deberemos personalizar la GPO con las exclusiones necesarias según nuestro entorno: aplicaciones instaladas, sistema operativo, descompresor utilizado, etc.

Vista completa de la GPO SRP texto: User Configuration (Enabled) > Policies > Windows Settings > Security > Settings > Software Restriction Policies

El presente documento técnico es una recopilación de diversas fuentes públicas.
Fuentes:
https://josecarlosnietoramos.wordpress.com/2015/01/30/como-evitar-que-el-ordenador-se-infecte-con-cryptolocker/
http://www.welivesecurity.com/la-es/2016/04/12/evitar-ransomware-cifre-servidor-de-ficheros-w2012/
http://www.hackplayers.com/2016/04/de-como-protegerse-contra-cryptolocker-2.html
http://www.sysadmit.com/2015/04/windows-gpo-para-prevenir-cryptolocker.html
http://blog.elhacker.net/2016/04/como-evitar-prevenir-que-un-ransomware-cifre-secuestre-los-ficheros-archivos-en-servidor-windows.html

**********FIN DEL DOCUMENTO**********