Protegiendo archivos riesgosos

Autor: Diego Bruno

Edición y Corrección: Lic. Cristian Borghello, MVP - CISSP

Fecha Publicación: 05 de marzo de 2010

Publicado en Segu-Info

Introducción

Microsoft Windows XP Pro y Windows 2003, copian alrededor de 8000 archivos al disco local cuando inicialmente son instalados. Hay docenas de archivos que son propensos a ser usados en forma malintencionada por atacantes que por el usuario final en si mismo, o inclusive los administradores, y normalmente por default, los usuarios finales o regulares suelen tener los permisos NTFS de Read and Execute en la mayoría de los archivos y carpetas.

Por ejemplo, Debug.exe es un ejecutable de programa de Assembly, el cual era usado en la época del PC-DOS por los programadores para crear, ver y desamblar ejecutables de 8 y 16 bits (Archivos de programa con la extensión .com y .exe). La realidad es que los programadores de hoy no utilizan estos ejecutables debido a que son muy viejos, sin embargo un atacante malicioso si puede utilizarlos para crear programas de malware y sobrescribir archivos de programa legítimos.

En esta parte vamos a ver algunos de estos archivos de alto riesgo, como el Debug.exe que mencionábamos y cómo mitigar los riesgos sobre ellos.

¿Qué es un archivo de alto Riesgo?

La realidad es que últimamente, cualquier archivo puede ser utilizado en forma maliciosa, no importa que tan inocente pueda ser el formato del archivo, podrá ser malformado para que el mismo sea malicioso. Inclusive los archivos de texto plano pueden ser utilizados en forma maliciosa, en los días del DOS, un atacante podía enviar a la "víctima" un archivo de texto en formato ASCII puro, el cual al ser leído, formatearía el disco duro. Funcionaría porque un archivo de drive llamado ansi.sys convertiría caracteres de control de teclados embebidos. Esta clase de ataques eran llamados ANSI-bombs.

Los archivos de texto y los editores de texto como el Notepad o el Wordpad pueden utilizarse en forma maliciosa para sobrescribir archivos de texto legítimos (Cómo Autoexec.bat, Win.ini, Host, etc).

ARCHIVOS DEFECTUOSOS

Los archivos de programa pueden ser fallidos desde el su concepción de diseño o por un mal uso o uso indebido lo que de todas maneras lleva a una consecuencia no deseada.

Defectos por diseño

Diseñados sin la seguridad en mente: Hay muchos ejemplos ya más que obvios de las aplicaciones que se conciben desde su inicio SIN la seguridad. En el

caso de Microsoft podemos citar por ejemplo la tecnología de Windows Scripting Host, cuando la misma salio a la luz, cualquier archivo de script que tuviera la extensión .Hta, .Ws o Cs sería automáticamente ejecutado por Wscript.exe o Cscript.exe cuando se le hiciera un doble clic al mismo.

Los archivos .Hta pueden cargarse automáticamente en el Internet Explorer y luego tener un acceso completo al sistema (Utilizando las credenciales del usuario). Cuando Windows Scripting Host salió a la luz por primera vez, no existían un mensaje de runtime que advirtiera al usuario, y los scripts podían modificar valores del sistema.

No hubo desde el inicio de la construcción de Scripting Host, nada relacionado a seguridad y de hecho no lo hubo por el lapso de un año aproximadamente. Los archivos Hta y otros archivos de scripting se volvieron el sueño de los hackers. Visual Basic Script (.Vbs) tienen un tratamiento similar. Los macro virus se volvieron durante mediados de los 90 muy populares por la misma razón de fallo de seguridad en el diseño. Ninguna evaluación de riesgo de seguridad fue realizada antes de liberar el producto.

BUFFER OVERFLOWS

Otro problema muy común es que los formatos de archivo contienen muchas veces, agujeros explotables, los cuales a través de ellos permiten un uso malicioso para el cual no fueron concebidos. Por ejemplo, es una práctica muy común en los hackers malformar los formatos de archivos gráficos como PNG, GIF, JPG, IO, etc para que asi entonces el programa de renderizado asociado tire un error y realice un buffer overflow.

A menudo también, se cambia de manera muy sencilla en el encabezado del archivo el tamaño del mismo. Entonces por ejemplo un hacker puede crear un archivo gráfico con un tamaño escrito de 1 o 0 en el encabezado del archivo. El programa que interpreta el archivo va a leer al archivo mal formado, y de alguna manera calcula el tamaño del archivo para que sea un valor negativo a un billón y cómo resultado se produce un buffer overflow.

RIESGOS EMBEBIDOS

Muchos formatos de archivo permiten tener embebidos links y archivos dentro del mismo archivo original. Por ejemplo, los archivos de Microsoft Office pueden contener links a otra documentación, el documento linkeado asi, puede entonces bajarse y ejecutarse también.

Muchos tipos de archivos eran originalmente seguros pero fueron ganando la capacidad de contener documentos linkeados adicionales, a medida que la popularidad de los mismos crecía (Cómo por ejemplo PDF, RTF, XLS, etc)

Entonces mientras que el tipo de documento original es todavía seguro, los documentos linkeados y embebidos que contiene pueden ser usados para lograr el exploit. Muchos archivos cómo el Program Information Files (.Pifs) y las scrap shell (.Shs) contienen links a otras documentaciones ya por diseño.

Es común también que muchos hackers exploten los skins de programas GUI. Los skins fueron creados para que los usuarios finales puedan crear y fácilmente transferir diferentes aspectos de comportamientos y visualización.

Desafortunadamente para dichos usuarios finales muchos skins permiten tener links embebidos y dichos links embebidos pueden bajar o ejecutar código malicioso.

USO INDEBIDO DE LOS DEFECTOS

Es muy normal que los hackers tomen archivos de programa y hagan cosas que son inesperadas. Por ejemplo, la mayoría de las plataformas de sistemas operativos ofrecen una variedad de opciones de compresión para que con el mismo utilizar el programa compresor que corresponde. En el mundo de Windows, el formato de programa más popular es el Zip. Seguramente que sus creadores nunca tuvieron la intención de que dicho formato se utilizara en forma maliciosa, pero la realidad es que hoy por hoy muchos atacantes usan los archivos de formato .Zip en forma maliciosa para baypasear muchas protecciones de seguridad cómo por ejemplo:

- Archivar programas de malware dentro de archivos .zip para que los programas que no abren este tipo de archivos ni escanean los archivos contenidos (Llamado escaneo recursivo-recursive scanning) no detectarán las mañas de dicho malware.
- Que en forma continua re archivo el mismo archivo una y otra vez (Esta técnica se llama Nesting) para que asi si el programa de escaneo si abre los archivos escaneados, tal vez no desarchivo el archivo lo suficiente para escanear el contenido original.
- Sobrescribir un archivo legítimo con una versión maliciosa.
- Utilizar el formato del archivo para automáticamente correr uno de los programas contenidos cuando el archivo esta abierto.
- Crear una estructura de subdirectorio dentro de el formato del archivo, para que, cuando sea abierto, se abran una docena de millones de directorios hijos, por lo cual de esta manera saltean a muchos escaners de seguridad, ya que los mismos por arquitectura no pueden escanear hacia mas abajo después de una cierta cantidad de directorios. Otros ataques que utilizan esta misma técnica, crean tantos subdirectorios que el sistema operativo termina por quedarse sin espacio usable.

CONFIGURACIÓN DE IMPORTACIÓN DE ARCHIVOS

Muchos programas permiten la configuración de los archivos al ser creados, y luego cuando el archivo configurado es clickeado, modifica los seteos relacionados a dicho sistema. Por ejemplo, los seteos a nivel de registry pueden ser importados a un archivo .reg. Un hacker malicioso puede enviar vía mail un archivo .reg ya sea embebido o no dentro de otra aplicación y la victima al abrirlo y clickearlo estaría cambiando seteos en forma automática en la regedit.

Los archivos con extensión .Ins pueden ser usados para iniciar conexiones a sitios de Internet no autorizadas.

La tabla que sigue a continuación, pese a ser bastante extensiva, seguramente Uds. Podrían actualizarla aún más todavía. La misma lista muchos de los tipos de archivo que pueden manipular a Windows o un determinado seteo con sólo hacer doble clic sobre el mismo.

Extensión archivo	Tipo de Archivo	Detalle de uso Malicioso
.ade, .adp, .and	Microsoft Access project files	Pueden contener macros autoejecutables.
.ani	Windows Animated Cursor	Dos exploits fueron anunciados por Flashsky Fangxing (flashsky@xfocus.org) en Diciembre. 23, 2004. Primero, un exploit de DoS en el Windows Kernel: Windows XP SP2 no era vulnerable, pero los demás versiones de Windows (NT a 2003) si lo eran. Segundo, un buffer overflow del cual la mayoria de las versiones de Windows es vulnerable (NT to 2003), causada por la API LoadImage en USER32.Lib.
.arc	File Archivo File format	Antiguo formato de archivo, pre-Windows (Anterior al .Zip). Todavía usado ocasionalmente por malware para bypasear la seguridad de las computadoras.
.arj	File Archivo	Pueden ser usados por malware para bypasear la seguridad de las computadoras.. Los Arj files pueden ser creados y desarchivados por cualquier programa popular, incluyendo el WinZip. Mas detalles de programas .arj en el siguiente link: http://filext.com/detaillist.php?extdetail=ARJ.
.asf, .lsf, .lsx	Streaming audio or video file	Pueden ser exploiteados por buffer overflows, malformaciones del header, o contenidos de script peligrosos.
.atf	Symantec pcAnywhere autotransfer file	Puede inicializar una sesión de file transfer de pcAnywhere.
.bas	Visual Basic (VB) class module	Puede contener instrucciones de código maliciosas.
.bat	DOS batch file	Puede contener instrucciones interpretadas maliciosas de comandos DOS, cómo también código ejecutable (.Exe) el cual correría inclusive con la extensión incorrecta.
.bmp	Windows Bitmap graphics file	Buffer overflow de los enteros, anunciado en Diciembre 23, 2004. La mayoría de las versiones de Windows (NT a 2003) son vulnerables hasta que sean pacheados; es causado por la API LoadImage en USER32.Lib.
.cab	Microsoft cabinet archivo file	Se abren en Windows Explorer e IE, y pueden ayudar a instalar archivos maliciosos. Comúnmente usados por Microsoft para instalar archivos legítimos, pero pueden ser usados por malware para baypasear las defensas de seguridad de un sistema. Los archivos .cab inesperados

		que nos pudieran llegar a través de correo o sitios no confiables no deben ser abiertos.
.cbo, .cbl, .cbm	Microsoft Interactive Training file	User= campo que permite un buffer overflow explotable (SEH pointer). Microsoft Interactive Training (Orun32.exe) debe estar presente, aunque a menudo se encuentra ya por default en las versiones OEM de Windows XP. El primer exploit para este tipo de archivo fue anunciado en Junio 14, 2005 por iDEFENSE labs y pacheado por el hotfix MS05-31. En la clave HK_CR\MITrain.Document\shell\open\command esta relacionado el programa Orun32.exe.
.cer, .crt, .der	Security certificate	Puede instalar un certificado malicioso en el IE para permitir el downloading automático de código malicioso.
.chm	Windows Compiled Help File	Windows Help Files (.hlp) pueden ser compilados para una mejor performancecan y otros seteos. Los archivos de help malformados y luego compilados han estado envueltos durante años en muchos anuncios de exploits, incluyendo los boletines de seguridad de Microsoft MS05-031. Pueden ser abiertos en el IE en forma automática sin la intervención del usuario.
.cmd	Command file	Contienen archivos de Batch como el intérprete de comandos de DOS. Pueden contener instrucciones maliciosas.
.com	Program executable	Legado antiguo del DOS y de los ejecutables de windows de 16 bits. Todavía funciona en todas las versions de Windows, excepto en las versions de 64 bits.
.cpl	Control Panel Applet	Programa ejecutable escrito para correr en el contexto del panel de control. Puede ser infectado por virus o usado por programas de malware para autoinstalarse a ellos mismos cómo la variante del Win32.Beagle (http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle@mm!cpl.html). Si situado de forma tal como para ser parte del control panel, listándo los contenidos del panel de control, puede ejecutar código de malware, incluso antes de que cualquier ítem del panel de control pueda ser abierto. Este riesgo estuvo sin publicitar por muchísimo tiempo y no ha sido explotado todavía, sin embargo es conocido cómo una funcionalidad por diseño.
.css	Cascading Style Sheet	Usado por el IE y otros browsers. Usado por los desarrolladores web para entregar fácilmente un look-and-feel consistente a un web site sin tener que recodear el código en cada página web. Ha sido explotado en forma maliciosa muchísimas veces.
.ctl	Certificate Trust List	Puede ser utilizado por un atacante remoto para engañar a la víctima para que confíe en el atacante

		como un publicador seguro.
.cur	Windows cursor graphic file	Bufer Overflow integrado anunciado por flashsky fangxing (flashsky@xfocus.org) en Dec. 23, 2004; la mayoría de las versiones de Windows son vulnerable (NT to 2003).Esto es causado por la API LoadImage en USER32.Lib.
.dbg	Debug file	Pueden contener instrucciones de lenguaje de maquina malicioso, los cuales pueden ser compilados por debug.exe dentro de Malware.
.dll	Dynamic Linking Library	La mayoría de las Dlls son archivos de programas legítimos que contienen retinas de libreriaspre compiladas que otros programas pueden llamar o pueden contener programas completes. Han estado envueltas en muchos virus y gusanos. Debido al Windows file protection muchas de las Dlls del sistema de Windows no pueden ser sobrescritas o modificadas por malware, pero Dlls da Debido al Windows file protection muchas de las Dlls del sistema de windows no pueden ser sobreescritas o modificadas por malware, pero Dlls dañinas pueden ser instaladas.
.doc	Microsoft Office Word Document	Pueden contener macros maliciosos, scripts, objetos, links, y ejecutables. Muy difícil de bloquear debido al uso legitimo que suelen tener en la mayoría de las veces.
.dot	Microsoft Office Document Template	Pueden ser manipulador por malware para contener objetos maliciosos, los cuales serán agregados a cada document que se cree a través de dicha plantilla.
.dsm, .far, .it, .stm, .ult, .wma	Nullsoft WinAmp media file	Estas extensiones han estado envueltas en muchos exploits maliciosos.
.dun	DUN export file	Pueden contener información de conexiones de dial up maliciosas que realicen llamadas.
.edt	Adobe Reader PDF ebook file	Envuelta en al menos un exploit anunciado (www.idefense.com/application/poi/display?id=163) enel 2004. Si la funcionalidad de ebook no es necesaria se la recomienda deshabilitar sin temor a dejar menos funcional el acrobat reader.
.eml, .email	Outlook Express e-mail message	Usados por Ninda y muchos otros gusanos. Los archivos Eml son abiertos en el Outlook Express aun cuando se usa otra aplicación de mail como la default. Los Attachments pueden se ocultados en el archivo y será clickeable y entonces asi explotar cualquier exploit de Outlook Express.

.exe	Application file	Pueden ser utilizados para cargar ejecutables maliciosos.
.fav	IE Favorites list	Pueden ser utilizados para listar web sites maliciosos que el usuario después visitaría.
.gif	Graphic file format	GIF stands for Graphics Interchange Format. También normalmente una foto o archivo de dato de imagen, ha sido malformado para causar manejos inapropiados de la aplicación como asi también buffer overflows. Ha afectado a muchísimas aplicaciones incluyendo a Windows Messenger, el cual fue pacheado para arreglar un exploit de Gif (ver Microsoft Security Bulletin MS05-022).
.gzip, .gz, .taz, .tgz	Gzip file format	Puede ser utilizado por malware para baypasear diferentes defensas de computación. Muy común en entornos linux y unix, pero tambien utilizados en windows, igual que los .tar.
.hlp	Microsoft Help File	Puede ser utilizados en multiples exploits.
.ht	Hyperterminal file	Pueden iniciar conexiones de dial up hacia host no confiables.
.hta	HTML application	Frecuentemente usados por worms y trojanos.

Esta lista podría ser muchísimo más extensa (De hecho lo es) pero se la puede encontrar en diferentes fuentes de información publicas y libros. En mi caso me base en la página http://filext.com la cual realmente tiene una cantidad enorme de información sobres los tipos de extensión de archivos, como asi también en el libro de hardening de Windows de Roger Grimes.

Lo que es y no es es un archivo de alto riesgo, es totalmente diferente para una organización o empresa como para otra. Y es la misma de acuerdo a un análisis con los administradores y los desarrolladores quienes decidirán cuales se pueden bloquear o anular sin causar un problema en el desarrollo de la operatoria diaria.

High-Risk Windows Files

Windows instala por default cientos de archivos ejecutables y programas en los directorios de **Windows** y en **System32**. Por default todos los usuarios tienen el permiso de Read and Execute. De Nuevo, lo que los archivos de sistema de Windows son considerados como de alto riesgo o no depende del ambiente de cada administrador en particular

La table que vamos a ver a continuación lista los archivos que yo considero de alto riesgo. Todos los archivos **se encuentran dentro del directorio %Windir%\System32** a menos que se indique lo contrario. Obviamente pese a ser todos de alto riesgo no es el riesgo igual en todos los casos. El factor de riesgo esta dado en que tan seguido el archivo es usado en forma maliciosa y que puede o no hacer el archivo.

File Name	Description and Risk	Risk
Command.com	16-bit command-line shell. Puede ser usado como el Cmd.exe. Deshabilitarlo si no es necesario. No puede ser deshabilitado por Software restriction policys.	Alto
Ftp.exe	File Transfer Protocol (FTP) cliente. Usado por programas de malware y atacantes. Deshabilitarlo si no es usado por los usuarios finales.	High
Ntdvm.exe	Controla el ambiente de 16-bit DOS Virtual Machine. Deshabilitarlo para prevenir ejecución de programas de 16-bits.	High
Reg.exe	Permite la manipulación de la registry.	High
Regedit.exe	El editor legal de la registry. Los usuarios No administradores no deberían poder manualmente ver o manipular la registry. Esta dentro de %Windir%.	High
Regedt32.exe	Editor de 32-bits de la Registry. Los usuarios No-administradores no deben de tener el acceso.	High
Tftp.exe	Trivial file transfer protocol (TFTP) cliente. Usado para iniciar sesiones de FTP no autenticadas. Usado frecuentemente por programas de malware y atacantes.	High
Tlntsvr.exe	Telnet server. Deshabilitarlo si no se necesita I usa, puede ser utilizado para ganar acceso por los atacantes.	High
Wscript.exe	Windows Scripting Host para correr scripts de VBScript y de JavaScript por fuera del IE. Deshabilitarlo si no se usa.	High
Clipsrv.exe	Clip book service. Permite el acceso remoto a los datos almacenados en el clipboard de la computadora local. Deshabilitado por default.	High-Medium
Cmd.exe	32-bit command-line shell. Los usuarios finales no deben de tener acceso al DOS command line a menos que necesiten correr archivos de scripts .Bat o .Cmd	High-Medium
Cscript.exe	Version de Command-line de Windows Scripting Host. No es necesario que se pueda accede a el a menos que se necesite corer scripts de .Vbs o de java script.	High-Medium
Mshta.exe	Permite aplicaciones HTML (HTAs) a correr por afuera del IE. Los HTAs han sido victimas en numerosas ocasiones de explotaciones. Deshabilitarlo si no es necesario.	High-Medium
Debug.exe	Programa de assembler. Puede fácilmente ser explotado. Muy raramente usado por los usuarios, administradores o incluso programadores. Deshabilitarlo.	Medium
Format.com	Usado para formatear a los discos duros y floppy disks desde la línea de comando. Es muy raro que se lo necesite, deshabilitarlo.	Medium
Ntbackup.exe	Utilidad de backup de Windows. Puede ser usado para copiar información no autorizada si el usuario logueado tiene el privilegio de backup.	Medium

Ntdsutil.exe	Es como swiss-army knife para Active Directory. No es necesaria para los usuarios no administradores.	Medium
Regsvr32.exe	Permite a los usuarios a registrar y desregistrar objetos de Com y Dlls. No es necesario para los usuarios no administradores.	Medium
Savedump.exe	Salva el volcado de memoria en un archivo. No es necesario para los usuarios finales.	Medium
Sc.exe	Usado para ver y modificar informacion de servicios. No es necesario para usuarios finales.	Medium
Schtasks.exe	Usado par aver, modificar y schedulear tareas en Task Scheduler.	Medium
Secedit.exe	Usado para ver, aplicar y comparar security templates a un determinado equipo.	Medium
Shutdown.exe	Usado para apagar un equipo local o remoto. No es normalmente necesario que los usuarios finales tengan acceso.	Medium
Taskkill.exe	Permite a los usuarios matar tareas que esten corriendo. No necesario por lo usuarios finales y el mismo es utilizado por software de malware.	Medium
Tscon.exe	Atachea a un usuario a una nueva session de Terminal Server (RDP) . Ya ha habido algunos problemas mencionados, incluyendo: http://support.microsoft.com/default.aspx?scid=kb;en-us;302801).	
Medium		
Arp.exe	Address Resolution Protocol interface utility. Puede ser usado para crear entradas falsas de ARP y estar envuelto en ataques redireccionados.	Medium/Low
At.exe	Interface de Task Scheduler. Los usuarios regulares y finales no deberian de poder schedulear nuevas tareas.	Medium/Low
Attrib.exe	Despliega atributos standard de archivos. Puede ser utilizado en forma maliciosa para ocultar archivos.	Medium/Low
Bootcfg.exe	Permitiria a un usuario cambiar parámetros de booteo.	Medium/Low
Edit.com	Editor de línea de comando de 16-bits. Deshabilitarlo. No puede ser deshabilitado por SRP (Software restriction policys).	Medium/Low
Rasdial.exe	Realiza conexiones de RAS. Deshabilitarlo si no es necesario.	Medium/Low
Tsshutdn	Permite a los usuarios apagar en forma remota o local a un Terminal Server (RDP). Ha habido vulnerabilidades de DOS ya anunciadas.	Medium/Low
Alg.exe	Servicio controlador de Microsoft Internet Connection Sharing and Internet Connection Firewall/Windows Firewall. Los usuarios No-administradores no deberían poder ejecutarlo, normalmente se ejecuta en el contexto de la cuenta LocalService.	Low
Append.exe	Legacy executable. Allows a user to extend the path statement variable to access files as if they were in the current directory when they are in fact in the appended	Low

	path. This doesn't use the Path variable.	
Auditusr.exe	Nueva API de interfaz de programa incluida en XP Service Pack 2 and Server 2003 Service Pack 1.	Low
Cacls.exe	Permite a los usuarios ver y manipular permisos NTFS.	Low
Ddeshare.exe	Usado para crear sharesDDE. Normalmente no es necesario para los usuarios finales.	Low
Dsadd.exe, Dsget.exe, Dsmove.exe, Dsrem, Dsquery	Active Directory command-line tools. No es necesario que los usuarios finales tengan acceso. Hasta la fecha no hay exploits relacionados a esta utilidad de commandos.	Low
Edlin.exe	Editor de texto de command-line. No es necesario para nadie. Deshabilitarlo.	Low
Eventcreate.exe	Usado para crear eventos customizados (http://support.microsoft.com/default.aspx?scid=kb;en-us;324145). Deshabilitarlo.	
Low		
Eventtriggers.exe	Usado para definer eventos customizados que generan determinados eventos. No es necesario para los usuarios finales.	Low
Exe2bin.exe	Puede converter archivos pequeños .exe en archivos .com. No es necesario. Deshabilitarlo.	Low
Finger.exe	Aplicacion usada para recolectar informacion de la identificacion de servicios. No es necesario para los usuarios finales.	Low
Hh.exe	Windows Help. Puede contener archivos linkeables maliciosos. Deshabilitarlo si no se necesita. Se encuentra dentro del directorio %Windir%.	Low
Mmc.exe	Microsoft Management Console. Deshabilitarlo si no se necesita.	Low
Msconfig.exe	Utilidad de configuracion del sistema utilizado para visualizar y modificar algunas configuraciones del sistema y del startup de Windows. Localizado en %Windir%\PCHealth\HelpCtr\Binaries.	Low
Netdde.exe	Usado para crear canales DDE. Algunas veces necesario para aplicaciones que usan canales DDE. Deshabilitarlos si no son necesarios.	Low
Rcp.exe	TCP/IP Remote Copy Program. No es necesario para los usuarios regulares y finales.	Low
Recover.exe	Recupera fragmentos de archivos perdidos. Puede causar problemas con el recovery de datos. Deshabilitarlo.	Low
Regtrace.exe	Utilidad de troubleshooting programmable.	Low
Replace.exe	Permite a los archivos desde el origin a reemplazar archivos en su destino. No es necesario tenerlo habilitado.	Low
Reset.exe	Resets Terminal Server (RDP) sessions. No es necesario para los usuarios finales y regulares.	Low
Rexec.exe	Cliente de commando TCP/IP que corre commandos en host remotos que tengan corriendo el servicio REXECD.	Low

	No es necesario tenerlo habilitado.	
Route.exe	Permite a los usuarios ver y modoficar tablas de ruteo de TCP/IP . Puede ser utilizado para setear rutas maliciosas.	Low
Rsh.exe	Utilidad de cliente TCP/IP que corre commandos en host remotos que esten corriendo el servicio RSH. No es necesario tenerlo habilitado.	Low
Rsm.exe	Interface de línea de commando de Removable Storage Manager , utilizado para la manipulacion de storage.	Low
Subst.exe	Comando que permite a los usuarios mapearse una ruta de network drive a una ruta de disco. No es necesario.	Low
Sysedit.exe	Editor de configuracion del sistema. De ser posible deshabilitarlo.	Low
Telnet.exe	Telnet client. Deshabilitarlo si no es necesario. Al menos para los usuarios finales y regulares.	Low
Tskill.exe	Permite a los usuarios matar sesiones de terminal servers.. No es necesario para los usuarios finales y regulares.	
Xcopy.exe	Permite el copiado de archivos incluyéndo sus atributos. Deshabilitarlos.	Low