DOCUMENTOS TÉCNICOS
- Imprescindibles
- Recomendados
- Todos
  - Por título
  - Por entorno
  - Por tema
  - Por aplicación
- Últimos documentos

ARCHIVO
- Documentos archivados

Virus en dispositivos USB

Este documento reseña la existencia de virus informáticos para sistemas Windows que utilizan unidades de almacenamiento USB para propagarse y propone medidas para mitigar sus efectos.

Entorno	Windows	Tema	Seguridad
Aplicación		Dificultad	Usuario Medio

La gran popularidad que en los últimos tiempos han alcanzado los dispositivos de almacenamiento USB ha provocado que los creadores de virus informáticos hayan puesto su atención sobre ellos con el fin de utilizarlos para propagar malware.

Para ello aprovechan una funcionalidad de los sitemas Windows que permite la reproducción automática de contenidos alojados en unidades de almacenamiento extraíble, pendrives, cámaras digitales, reproductores MP3 y MP4...

A día de hoy no existe una solución universal y sencilla para combatir este problema, aunque se dispone de algunas medidas parciales que pueden ayudar a mitigarlo.

Propagación desde PC infectado a unidad USB

Los dispositivos USB que disponen de protección por hardware (equivalente a la pestaña de los disquetes de 3.5") son muy escasos, por lo que la mayoría se hallan absolutamente inermes si se introducen en sistemas Windows infectados.

En diversos foros se ha apuntado la posibilidad de crear un archivo de nombre (preferentemente una carpeta) Autorun.inf en el directorio principal del dispositivo USB. Con ello el virus activo en el PC "entendería" que la unidad ya se encuentra infectada y no actuaría sobre ella. Esta técnica podría proporcionar un cierto grado de protección frente a alguno de estos virus, sin embargo no hay garantía de que no existan (o puedan aparecer en el futuro) nuevos virus capaces de eludir esta medida.

En aquellos PCs de los que nunca sea necesario extraer información a dispositivos USB puede optarse por bloquear la escritura sobre los mismos.

Para ello se utiliza el editor del registro de Windows para crear la siguiente entrada:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies

y en ella establecer un nuevo valor de nombre WriteProtect y tipo DWORD a 1.

La manipulación del registro de Windows es una tarea delicada que deben realizar unicamente usuarios avezados, ya que cualquier error puede inutilizar el sistema.

Antes de manipular el registro de Windows se recomienda realizar una exportación del mismo que permita restaurarlo en caso de problemas.

Propagación desde unidad USB infectada a PC

Los sistemas Windows permiten desactivar la función de Reproducción automática que viene activada por defecto. Con ello se evita la propagación automática de este tipo de virus, aunque la opción de utilizarla sigue estando disponible en el menú contextual.

En todos los casos se utiliza el editor de políticas del sistema.

Contenido de éste documento en PDF:

DOCUMENTOS RELACIONADOS

Edición del Registro de Windows

Virus y Antivirus: Análisis de muestras

Acceso a servidores Windows

Windows 2000:

Menú Inicio -> Ejecutar -> gpedit.msc -> Directiva Equipo local -> Configuración del equipo ->Plantillas Administrativas -> Sistema -> Desactivar reproducción automática -> Habilitada

y aplicarla a Todas las unidades (por defecto se aplica sólo a unidades de CD-ROM).

Windows XP:

Menú Inicio -> Ejecutar -> gpedit.msc -> Directiva Equipo local -> Configuración del equipo ->Plantillas Administrativas -> Sistema -> Desactivar reproducción automática -> Habilitada

y aplicarla a Todas las unidades (por defecto se aplica sólo a unidades de CD-ROM).

Esta configuración no afecta a la reproducción automática de CD de audio analógico.

La configuración de opciones de la pestaña Reproducción automática accesibles desde Propiedades del dispositivo (menú contextual desde el icono correspondiente en Mi PC) no afectan más que a los contenidos multimedia, por lo que no son de aplicación en esta situación).

Windows Vista:

En su configuración por defecto este sistema no ejecuta los comandos contenidos en archivos Autorun.inf de unidades extraíbles, por lo que el riesgo de infección es considerablemente menor, ya que se requeriría la intervención del usuario.

Asimismo, Windows Vista permite controlar los modos de reproducción automática desde dos difrentes tipos de herramientas:

Panel de control:

El Panel de control Reproducción automática permite activar o desactivar esta característica en todas los medios y dispositivos, así como predeterminar el comportamiento según el tipo de medio y el contenido.

Editor de políticas:

En Menú Inicio -> Ejecutar -> gpedit.msc -> Directiva Equipo local -> Configuración del equipo ->Plantillas Administrativas -> Componentes de Windows -> Directivas de reproducción automática

se dispone de las opciones Desactivar Reproducción automática y Comportamiento predeterminado para la ejecución automática. Esta última permite bien deshabilitar completamente los comandos de ejecución automática, bien volver al comportamiento por defecto de las versiones anteriores de Windows.

En Menú Inicio -> Ejecutar -> gpedit.msc -> Directiva Equipo local -> Configuración del equipo ->Plantillas Administrativas -> Sistema -> Acceso de almacenamiento extraíble se dispone de herramientas para permitir o de negar el acceso de lectura y/ o escritura a los diferentes tipos de dispositivos.

Envío de muestras

Los usuarios que sospechen que alguno de los ficheros presentes en sus sistemas o sus dispositivos USB son en realidad virus pueden depositarlos en

\\Psfunizar3\Usuarios\Buzon

Se trata de una carpeta de "sólo escritura" por lo que no puede abrirse, tan sólo arrastrar ficheros a ella. Se ruega a los usuarios que depositen muestras que lo comuniquen por correo electrónico a la dirección:

distribucion.software@unizar.es

a fin de que puedan ser analizados y, eventualmente, remitidos al fabricante del antivirus corporativo para que puedan incorporarse a sus detectores.

Apoyo adicional

Si ha tenido problemas al aplicar estos procedimientos o requiere de apoyo adicional, recuerde que puede solicitarlo cumplimentando el formulario ubicado en la dirección:

http://moncayo.unizar.es

a través del enlace Solicitar intervenciones al SICUZ.

Noviembre de 2007
Informática Distribuida
Servicio de Informática y Comunicaciones
Universidad de Zaragoza

SERVICIO DE INFORMÁTICA Y COMUNICACIONES - UNIVERSIDAD DE ZARAGOZA

dt0112.pdf