Malware Un Problema En Windows

Cómo El Malware AutoRun Se Convirtió En Un Problema En Windows

Gracias a malas decisiones de diseño de software, AutoRun se volvio un gran **problema de seguridad enorme en Windows**. AutoRun permitió que una gran cantidad de software malicioso se ejecutara tan pronto se haya insertado discos y unidades extraibles en un PC con Windows.

Este fallo no sólo fue aprovechada por los creadores de malware. Fue utilizado por Sony BMG para ocultar un **rootkit en los CD de música**. El problema en Windows, resultaba cuando se insertaba un CD de Sony que contenía este código malicioso, instalaba automáticamente el rootkit en el computador del usuario sin que este se diera cuenta.

El origen del AutoRun como

problema en Windows

El AutoRun era una **característica introducida en Windows 95**. Cuando ha insertado un disco de software en su computadora, Windows podría leer automáticamente el disco, si encontraba un **archivo autorun.inf** en el directorio raíz del disco, este ejecutaba automáticamente el programa especificado en el archivo autorun.inf.

Es por esto que, cuando se insertaba un CD de software o disco de juego de PC en el ordenador, se ponía en marcha automáticamente una pantalla de instalación o de opciones. La característica fue diseñada para hacer este tipo de discos fácil de usar, reduciendo la confusión del usuario. Si la **ejecución automática** no existiera, los usuarios tendrían que abrir la ventana del explorador de archivos, ir al disco, y ejecutar el archivo setup.exe desde allí.

Esto funcionó bastante bien durante un tiempo, y no hubo grandes problemas. Después de todo, los usuarios domésticos no contaban con una manera fácil de grabar sus propios CD antes de los quemadores de CD se usaran cotidianamente. Normalmente usaban sus computadores para escuchar música o ejecutar programas de fuentes «confiables».

Reproducción automática en Windows XP

Windows XP refinó esta función con una función de «reproducción automática». Cuando el usuario ha insertado un disco, una unidad flash USB o cualquier otro tipo de dispositivo de medios extraíbles, Windows examinará su contenido y sugería acciones adecuadas para cada tipo de archivo. Por ejemplo, si el usuario ingresaba una tarjeta SD que contenía fotos de su cámara digital, se le recomendaba hacer uso del visor de imagen o algún otro programa para archivos de imágenes. Si una unidad tiene un archivo autorun.inf, podrás ver una opción que le pregunta si desea ejecutar automáticamente un programa de la unidad también.

Sin embargo, Microsoft todavía quería CDs a trabajar el mismo. Así, en Windows XP, los CDs y DVDs seguirían ejecutando automáticamente programas en ellos si tenían un archivo autorun.inf, o empezarían a reproducir automáticamente su música si fueran discos CD de audio. Y, debido a la arquitectura de seguridad de Windows XP, estos programas probablemente lanzará con acceso de administrador. En otras palabras, tendrían pleno acceso a su sistema.

Con las unidades USB que contiene los archivos autorun.inf, el programa no se ejecuta automáticamente, sino que le presentará la opción en una ventana de reproducción automática. Aún se podía desactivar este comportamiento. Había opciones ocultas en el propio sistema operativo, en el registro, y el editor de directivas de grupo. También se podía mantener pulsada la **tecla Mayús** mientras introducido un disco y Windows no realizaría el comportamiento de ejecución automática.

Algunas unidades USB emulaban ser un CD

Esta protección comenzó a ser «vulnerada» inmediatamente. SanDisk y M-Systems vieron el comportamiento de AutoRun en un CD y querían usar este comportamiento en sus propias unidades flash USB, así que crearon las unidades flash U3. Estas unidades flash emulan ser una unidad de CD cuando se conecta a un ordenador, por lo que un sistema Windows XP iniciará automáticamente programas en ellos cuando están conectados.

Por supuesto, incluso los CDs no son seguros. Los atacantes podrían grabar fácilmente una unidad de CD o DVD, o utilizar una unidad regrabable. Es un grave error pensar que los CDs son de alguna manera más seguros que las unidades USB.

Desastre 1: El Fiasco Del Rootkit De Sony BMG

En 2005, Sony BMG comenzó a enviar **rootkits de Windows en millones de sus CDs de audio**. Una vez insertado el CD de audio en el ordenador, Windows podría leer el archivo autorun.inf y

ejecutar automáticamente el instalador rootkit, que a escondidas infectaba el equipo. El propósito de esto era evitar que la copia del disco de música fuera vulnerabada. Debido a que estos son funciones que normalmente soportan, el rootkit tuvo que subvertir el sistema operativo completo para reprimirlos.

Esto fue posible gracias al AutoRun. Algunas personas recomendaban mantener oprimida la tecla Shift siempre que se ha insertado un CD de audio en el ordenador. Digamos que el rootkit era inestable, el malware aprovechó el rootkit para infectar más fácilmente los sistemas Windows, y Sony tiene un el estigma que se ha ganado gracias a esta pequeña movida para proteger los derechos sobre sus productos.

Desastre 2: El Gusano Conficker Y Otros Tipo De Malware

Conficker fue un gusano particularmente desagradable detectado por primera vez en 2008. Entre otras cosas, infecta los dispositivos USB conectados y crea archivos autorun.inf en ellos que se ejecutan automáticamente el malware cuando sean conectados en otro equipo. Segun la compañía de antivirus ESET:

«Las unidades USB y otros medios extraíbles, los que se accede por las funcionalidades de ejecución automática / Reproducción automática cada vez (por defecto) al conectarlos al ordenador, son los portadores de virus más frecuentemente utilizados en estos días.»

Conficker fue conocida la mayoría, pero no fue el único software malicioso que abusaba de la funcionalidad del peligroso AutoRun. Simplemente esta característica era prácticamente un regalo para los autores de malware.

Windows Vista AutoRun desactivado por defecto, pero …

Microsoft finalmente recomienda a los usuarios de Windows **deshabilitar la funcionalidad AutoRun**. Windows Vista hizo algunos cambios que Windows 7, 8 y 8,1 han heredado. En lugar de ejecutar automáticamente los programas de los CD, DVD y unidades USB disfrazados de discos, Windows simplemente muestra el cuadro de diálogo de reproducción automática para estas unidades también. Si un disco o una unidad conectada tiene un programa, podrás **verlo como una opción en la lista**. Windows Vista y versiones posteriores de Windows, no ejecutaran automáticamente programas sin tu consentimiento, es por esto que hasta estas versiones, el **AutoRun deja de ser un peligro**, por así decirlo ;)

Pero aún sería posible que el malware se propague a través de Reproducción automática. Si conecta una unidad USB con código malicioso en su ordenador, sigues estando a un sólo clic de distancia de ejecutar el malware a través del diálogo Reproducción automática, al menos con la configuración predeterminada. Otras características de seguridad como UAC y su programa antivirus pueden ayudarle a proteger, pero aún debe estar alerta.