www.juventudrebelde.cu

Códigos malignos en los USB

Con la extensión del uso de dispositivos como memorias flash, reproductores de música y discos externos, se han disparado los programas nocivos para ellos

Publicado: Jueves 01 noviembre 2007 | 01:29:57 am.

Publicado por: Amaury E. del Valle

El desarrollo tecnológico cambia la moda, y si el disquete en su momento constituyó el soporte de almacenamiento portátil más empleado para el intercambio de información, actualmente las memorias flash y discos externos USB son los más populares.

Es por eso que los creadores de códigos malignos se han fijado en estas para la propagación de sus creaciones, en una estrategia que ha cogido de sorpresa a muchos usuarios de los Sistemas Operativos Windows, quienes sufren las consecuencias de estas acciones dañinas con solo insertar los dispositivos externos en los correspondientes conectores de las computadoras personales.

El nivel de propagación por esta vía es tal, incluso en Cuba, que ya es cotidiano escuchar «tengo la flash infectada». E incluso hay quienes, irresponsablemente, ni siquiera se preocupan por esta situación, contribuyendo a propagar cada vez más los programas dañinos.

SEGAV sí descontamina
Una de las variantes más empleadas para garantizar la ejecución de los programas malignos por esta vía, consiste en crear un fichero nombrado autorun.inf en el directorio raíz, el cual incluye comandos que «ordenan» al sistema operativo la ejecución de un fichero ejecutable o programa almacenado dentro del dispositivo USB, con solo insertarlo en el conector.

Por tal motivo, al ver el contenido del fichero «.inf», con un editor como el notepad.exe, es frecuente observarlos a continuación de la etiqueta [autorun]. Mientras que el programa al cual se hace referencia, no es otro que el mismo código maligno.

Un ejemplo simplificado de los ficheros de este tipo creados por W32.Dilalupass.c es:

[AutoRun]

open=MSOCachedoWTP_RESTORE.exe

shellexecute=MSOCachedoWTP_RESTORE.exe

En este caso, el W32.Dilalupass.c utiliza este mecanismo para ejecutar el fichero WTP_RESTORE.exe que se encuentra en la carpeta MSOCache.

Otro caso es el del programa maligno W32.Delf.aws que utiliza los siguientes comandos para ejecutar el fichero autorun.pif contenido en la carpeta:

[AutoRun]

open=RUNAUT~1autorun.pif

shellexecute=RUNAUT~1autorun.pif

En el caso específico de este programa maligno, en dependencia de los métodos de descontaminación empleados por diferentes productos antivirus, es posible encontrar dispositivos externos en los que se encuentra todavía la carpeta anterior (runauto...), la cual no se borra empleando el Explorador.

Sin embargo, el producto antivirus nacional, SEGAV, desarrollado en la Empresa de Consultoría y Seguridad Informática Segurmática, sí la elimina.

No obstante, es posible hacer su borrado «manual» ejecutando el comando cmd o command, en dependencia de la versión del sistema operativo.

Para esto hay que ir al menú de Inicio, seleccionar la opción Ejecutar, teclear el comando anterior, pulsar la tecla Intro (Enter) y una vez en modo texto, en la nueva ventana que se abre:

- Escribir la letra asignada a la unidad correspondiente al disco externo seguida del caracter “:”, por ejemplo «G:»

- Pulsar la tecla Intro (Enter)

- Escribir rd runaut~1 /s

- Pulsar la tecla Intro (Enter)

- Confirmar que se desea borrar la carpeta.

Otro de los métodos utilizados por estos intrusos dañinos es hacer una copia de sí mismos en el directorio raíz del dispositivo externo, autoasignándose nombres de carpetas que allí se encuentren, a la vez que las ocultan, es decir, las suplantan desde el punto de vista del usuario.

Generalmente el engaño surte efecto, pues el código maligno se encuentra en un fichero, cuyo icono es el

correspondiente a una carpeta, por lo que el usuario desconoce que al intentar acceder a su contenido, lo que realmente hace es ejecutar el código maligno, máxime cuando la extensión ejecutable del fichero también es ocultada, como por ejemplo: .exe, .pif, etc.

Lo anterior ocurre de manera transparente, es decir, se accede finalmente al interior de la carpeta seleccionada. Este ardid lo emplean, entre otros, las variantes del W32.Efecto.

Sin embargo, en este caso un usuario alertado puede comprobar que el Explorador —con la opción de «Detalles» activa— muestra en la ventana que se abre a la derecha que el tipo del fichero con el icono de carpeta es una aplicación (Application) y no una carpeta de archivos (File Folder).

Deshabilitar el autorun
Conociendo las maneras de propagación, podemos aplicar un grupo de acciones sencillas para limitar esta situación, aún cuando no se cuente con un antivirus actualizado que sea capaz de identificar y descontaminar el código maligno.

Lo primero es deshabilitar la propiedad de que se ejecute el autorun.inf con solo insertar el dispositivo USB. Para ello en Windows NT4, 2000 y XP es necesario realizar modificaciones en los registros, específicamente en el valor: NoDriveTypeAutoRun, siempre y cuando se tengan los permisos de administrador del sistema.

La herramienta que debe emplearse es la aplicación regedit.exe que acompaña al sistema operativo, la cual se puede ejecutar desde el menú «Inicio» y la opción «Ejecutar». Para esto se debe:

- Ejecutar regedit.exe

- Con el auxilio de la opción «Buscar», dentro de «Edición», localizar el valor «NoDriveTypeAutoRun» y abrirlo con el botón izquierdo del ratón.

- Seleccionar la opción «Modificar» con el botón derecho del ratón, y cambiar el valor que se encuentra por defecto, generalmente 91, sustituyéndolo por 95, teniendo activa la opción «Hexadecimal».

- Aceptar la modificación.

Esta operación se debe repetir tantas veces como se localice en el registro NoDriveTypeAutoRun. Para ello es posible emplear la opción «Buscar siguiente» dentro de «Edición», hasta que finalmente se muestre en pantalla un mensaje informando que se «Finalizó la búsqueda en el Registro».

Por otra parte, mediante políticas de grupo, un administrador de manera centralizada también puede «Desactivar reproducción automática». Para ello en Windows 95, 98 y Me, los valores son iguales, no así el formato de entrada del dato, lo cual hay que tener en cuenta.

Es muy importante saber que las modificaciones en los registros, si no se realizan cuidadosamente, pueden ocasionar un mal funcionamiento del sistema, por lo que se recomienda la máxima concentración al realizar esta tarea.

Mostrar ficheros y carpetas ocultos
Las operaciones descritas anteriormente limitan la ejecución de un código maligno al conectar los dispositivos externos, sin embargo, no imposibilitan su ejecución cuando accedemos a ellos.

Por eso, hay que tener en cuenta que con el Explorador (explorer.exe), se debe acceder «indirectamente» al contenido del dispositivo externo. En ese caso, se puede escoger la opción «Carpetas», dentro de ella «Mi PC» y finalmente elegir la unidad asociada al disco extraíble.

Una vez allí, se puede analizar el contenido del directorio raíz, e incluso comprobar la presencia del autorun.inf o su alteración, si existiera uno conocido con antelación.

No puede olvidarse que los creadores de programas malignos ocultan al fichero autorun.inf de modo que no se pueda acceder simplemente a este con el auxilio del Explorador. Por lo tanto, una medida para evadir esta situación es tener activa la opción de poder observar ficheros y carpetas ocultos.

Para ello dentro del Explorador se debe seleccionar la opción «Herramientas», dentro de ella escoger «Opciones de carpeta» y seguidamente, en «Ver» activar «Mostrar todos los archivos y carpetas ocultos».

Incluso, para evitar más engaños, es recomendable desactivar las opciones: «Ocultar archivos protegidos del sistema operativo» y «Ocultar las extensiones de archivos para tipos de archivo conocido».

Debe educarse a quien opera la computadora
Habiendo tomado las medidas correspondientes, estaremos mejor preparados para trabajar la próxima vez con un dispositivo externo en la computadora personal y prevenir la propagación de programas malignos.

Sin embargo, lo visto hasta aquí es efectivo solo si la computadora no se encuentra infectada. De lo contrario, cada vez que se borren del dispositivo externo los ficheros del código maligno, estos reaparecerán debido a que el programa maligno que se encuentra ejecutándose en la memoria, los creará otra vez.

Otro aspecto que no se debe olvidar, es que una vez detectado un dispositivo infectado, es probable que en el mismo lugar de trabajo otras computadoras y dispositivos empleados se encuentren también contaminados y puedan ocurrir reinfecciones.

Los productos antivirus desarrollados en Segurmática son capaces de identificar y eliminar, entre otros, a estos códigos malignos para dispositivos USB. En el sitio web www.segurmatica.cu se puede consultar información sobre códigos malignos, así como los servicios y productos que la empresa brinda.

De cualquier forma, las infecciones a través de dispositivos USB como las memorias portátiles, reproductores de música o discos externos son cada vez más comunes en el mundo y también en Cuba.

Para evitarlas, no basta con elevar el nivel de seguridad tecnológica en una empresa o cualquier otra entidad, pues la acción de quien opera la computadora es determinante. A ella o él es a quienes se debe educar ante todo.

*** Especialista principal del Laboratorio Antivirus de la Empresa de Consultoría y Seguridad Informática, Segurmática.**

http://www.juventudrebelde.cu/suplementos/informatica/2007-11-01/codigos-malignos-en-los-usb