Video Soft BBS

VSAntivirus

Esta página es un servicio gratuito de Video Soft BBS - SUBSCRIBASE en nuestras listas de correo.
Es usted nuestro visitante número 568777 desde el 12 de agosto de 1996

Video Soft BBS

Menú Principal
Anti Trojans
Antivirus
Hoaxes
Subscripciones
Otro software
Artículos
Links
Sugerencias
Sobre el BBS
Direcciones
Las Noticias
Galería
Chat

Controlado desde el 19/10/97 por NedStat

Virus: W32/Fiend.Worm. Se propaga por IRC y falla en el Outlook

VSantivirus No. 320 - Año 5 - Jueves 24 de mayo de 2001

Nombre: W32/Fiend.Worm
Tipo: Gusano de Internet
Fecha: 17/may/01
Tamaños: 6656, 662, 141 bytes

Es un gusano que se propaga vía IRC, e intenta hacerlo a través del Outlook y Outlook Express.

Cuando el gusano se ejecuta, el mismo libera el archivo **NETFRIENDS.EXE** en la carpeta de Windows (**C:\WINDOWS** por defecto), y luego se copia a si mismo como:

C:\Mirc\Script.ini
C:\Mirc32\Script.ini

Esto ocurre si se tiene instalado el programa de IRC (1) mIRC. De ese modo, cuando el usuario infectado se conecta a un canal de chat con ese programa, enviará sin saberlo el archivo **ISETUP.EXE** a quienes estén conectados al mismo canal.

Luego, crea el siguiente archivo y lo ejecuta:

C:\Friends\Maya.vbs

Este script en Visual Basic, se supone debería enviar el archivo **C:\Windows\Netfriends.exe** a todos los contactos de la libreta de direcciones del Outlook. Sin embargo, debido a errores en su código, esto no funciona, limitando la capacidad de propagación del virus a los canales de chat.

Después de este intento fallido, el virus se copia a si mismo en **C:\Windows\iesetup.exe**

Dependiendo de la versión de Windows instalada, el gusano modifica el registro o el archivo **WIN.INI** para ejecutarse más tarde, con cada reinicio de Windows.

Windows 95/98/Me - Modifica la siguiente línea del archivo **C:\WINDOWS\WIN.INI**:

[windows]
run=c:\windows\iesetup.exe

Windows NT/2000 - Modifica el registro:

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\run
run = C:\WINDOWS\Iesetup.exe

Luego muestra una ventana con este mensaje:

WinZip Self-Extractor
WinZip Self-Extractor header corrupt.
Possible cause: bad disk or file transfer error.
[Aceptar]

El gusano altera los nombres registrados en Windows, de usuario y de compañía pero debido a un error, no guarda ningún nuevo texto en lugar de los anteriores.

Si la fecha actual es 5 de cualquier mes, este mensaje es mostrado:

```
I-Worm.Friends
Coded by PetiK (c)2001
To my friends Maya and Laurent.
[  Aceptar  ]
```

Para remover manualmente el virus de un sistema infectado, primero ejecute dos o más antivirus al día, y luego deberá actuar de acuerdo al sistema operativo utilizado:

Windows 95/98/Me

1. Desde Inicio, Ejecutar, escriba WIN.INI y pulse Enter

2. Ubique la siguiente línea:

```
[windows]
run=c:\windows\iesetup.exe
```

3. Borre lo que sigue después de RUN= de modo que la línea quede así:

```
[windows]
run=
```

4. Grabe el archivo (Archivo, Guardar) y salga del bloc de notas.

Windows NT/2000

1. Pinche en Inicio, Ejecutar, y teclee REGEDIT (más ENTER).

2. En el panel izquierdo del editor de registro de Windows, pinche en el signo "+" hasta abrir la siguiente rama:

```
HKEY_CURRENT_USER
Software
Microsoft
Windows NT
CurrentVersion
Windows
```

3. Pinche sobre la carpeta "**Windows**". En el panel de la derecha debería ver algo como:

```
run        C:\WINDOWS\Iesetup.exe
```

4. Borre la entrada donde figure "**C:\WINDOWS\Iesetup.exe**" en el panel de la derecha. Para ello, pinche sobre esta línea y pulse la tecla SUPR o DEL. Conteste afirmativamente la pregunta de si desea borrar la clave.

5. Use "Registro", "Salir" para salir del editor y confirmar los cambios.

6. Reinicie su computadora (Inicio, Apagar el sistema, Reiniciar).

Recomendaciones

Se recomienda precaución al recibir archivos a través de los canales de IRC. Sólo acepte archivos de personas que realmente conoce, pero aún así, jamás los abra o ejecute sin revisarlos antes con dos o tres antivirus actualizados.

Jamás acepte archivos SCRIPT a través del IRC. Pueden generar respuestas automáticas con intenciones maliciosas.

En el caso del mIRC, mantenga deshabilitadas en su configuración, funciones como "**send**" o "**get**" y comandos como "**/run**" y "**/dll**". Si su software soporta cambiar la configuración de "DCC" para transferencia de archivos, selecciónelo para que se le pregunte siempre o para que directamente se ignoren los pedidos de envío o recepción de éstos.

Glosario

(1) IRC (Internet Relay Chat) - Un sistema de conversación multiusuario, donde la gente se reúne en ambientes virtuales llamados "canales", normalmente identificados con temas definidos de conversación, para poder charlar en grupo o en privado. IRC trabaja en arquitectura Cliente/Servidor. El usuario ejecuta un programa cliente (los más conocidos son mIRC y Pirch), el cual se conecta a través de la red (Internet por ejemplo) con otro programa servidor. La misión del servidor es pasar los mensajes de usuario a usuario.

(c) Video Soft - http://www.videosoft.net.uy