Eduardo Quiroga Gómez -k idatzia
Asteartea, 2008(e)ko azaroa(r)en 18-(e)an 10:07etan

There are no translations available.
Descubre en este artículo, como deshacerte de este molesto virus..

Eliminar Virus W32. Fleck.A (También conocido como W32/Bagle)

Introducción

Con este mini manual, podremos deshacernos de este molesto virus, cuyos síntomas son los siguientes:

- Ralentización del sistema
- Bloqueo de la posibilidad de iniciar sesión en modo a prueba de fallos
- No permite mostrar los archivos ocultos del sistema, y elimina el menú desde el que se puede habilitar esta opción.
- Crea varios procesos que no se pueden detener, uno de ellos es visible, el flec006.exe, y otro oculto que consume casi el 50% del procesador del equipo que se llama hldrrr.exe.
- Finaliza procesos pertenecientes a antivirus y otros programas de seguridad.

No permite ejecutar o instalar una serie de programas como por ejemplo antivirus, programas antispyware, programas de limpieza de registro, etc, ya que cuando se ejecuta, crea varios archivos y luego intenta conectarse a una lista de sitios en internet desde donde puede seguir descargando archivos infectados y un listado de programas que luego impide ejecutar o instalar.

Vamos a englobar en 3 apartados los pasos necesarios para eliminar el Bagle virus, ya que este virus afecta a tres aspectos diferentes de nuestro sistema:

1. En este primer apartado vamos a recuperar la opción de ver los archivos ocultos y que nos vuelva a aparecer el menú **Archivos y carpetas ocultas** que nos ha desaparecido del menú Herramientas/Opciones de Carpeta/Ver
.

Para ello, copiamos el siguiente texto marcado en azul en un nuevo documento de texto y lo guardamos con extensión .reg , después ejecutamos el archivo que hemos creado y pulsamos aceptar cuando nos pregunte si queremos modificar el registro de windows:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerAdvancedFolderHidden]

"Text"=";@shell32.dll,-30499"

"Type"="group"

"Bitmap"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,00,74,

00,25,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,53,00,

48,00,45,00,4c,00,4c,00,33,00,32,00,2e,00,64,00,6c,00,6c,00,2c,00,34,00,00,

00

"HelpID"="shell.hlp#51131"

[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerAdvancedFolderHiddenNOHIDDEN]

"RegPath"="SoftwareMicrosoftWindowsCurrentVersionExplorerAdvanced"

"Text"=";@shell32.dll,-30501"

"Type"="radio"

"CheckedValue"=dword:00000002

"ValueName"="Hidden"

"DefaultValue"=dword:00000002

"HKeyRoot"=dword:80000001

"HelpID"="shell.hlp#51104"

[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerAdvancedFolderHiddenSHOWALL]

"RegPath"="SoftwareMicrosoftWindowsCurrentVersionExplorerAdvanced"

"Text"=";@shell32.dll,-30500"

"Type"="radio"

"CheckedValue"=dword:00000001

"ValueName"="Hidden"

"DefaultValue"=dword:00000002

"HKeyRoot"=dword:80000001

"HelpID"="shell.hlp#51105"

2. Lo segundo que vamos a hacer, es recuperar el modo a prueba de fallos de Windows, que el virus inutiliza para que no podamos atacarlo desde ahí.

Para conseguir esto, nos bajamos un programa que se llama RegUnlocker desde la siguiente dirección: http://ripfire.nireblog.com/post/2008/02/14/regunlocker-v195-en-espanol .

Una vez descargado, lo descomprimimos y no es necesario instalarlo, ya que simplemente se trata de un ejecutable en el que tenemos que seleccionar la opción **Reparar el Modo a prueba de fallos** que está en el apartado **Reparadores** :

Dejamos marcada la opción de **Realizar copia de seguridad de los cambios realizados**, para que, en caso de que necesitemos revertir este cambio, simplemente ejecutando un archivo con extensión .reg que nos crea, podamos deshacer los cambios que aplica este programa.

Una vez restaurado el modo a prueba de fallos, podemos iniciar sesión en este modo e intentar pasar el antivirus o eliminar manualmente los archivos infectados, aunque pocas veces podemos acabar con el Bagle desde el propio Windows, por lo que lo mejor es hacerlo como se explica en el paso 3.

3. El último paso y el más importante, es en el que vamos a eliminar los archivos causantes de todos los problemas comentados anteriormente.

Para hacer esto, vamos a utilizar una versión Live de cualquier distribución de Linux, en nuestro caso vamos a utilizar la versión 8.04 de Ubuntu, ya que nos ha dado buenos resultados.

Reiniciamos el equipo y ponemos el disco de Ubuntu en el lector, iniciamos la versión Live seleccionando la primera opción, (**Probar Ubuntu sin alterar su equipo**), y esperamos a que se inicie.

Una vez que haya cargado, en la barra superior desplegamos el menú **Lugares** y elegimos **Equipo** , que es el equivalente a Mi PC de Windows.

En la ventana que se nos abre, desplegamos el menú **Ver** y elegimos **Mostrar archivos Ocultos** , a continuación tenemos que encontrar las siguientes rutas:

a. **C:/Documents and Settings/ nombre de usuario /Datos de programa/m**

En la carpeta **m**, se guarda el ejecutable **flec006.exe**, junto a otros archivos. Tenemos que eliminar la carpeta **m** entera con todos los archivos que contenga.

b. **C:WINDOWSsystem32driversshldrrr.exe**

Eliminar **únicamente** el archivo **hldrrr.exe**

c. **C:WINDOWSsystem32driverssrosa.exe**

Eliminar **únicamente** el archivo **srosa.exe**

Una vez eliminados estos tres archivos, cerramos la sesión de Ubuntu y reiniciamos el equipo.

Conclusiones

Aunque hayamos hecho los pasos anteriores, es muy probable que el equipo siga teniendo archivos infectados, por lo que ahora que ya podemos, ejecutamos el antivirus que tengamos instalado y hacemos un escaneo en profundidad de todas las unidades.

También hay que revisar las tarjetas de memoria y dispositivos pendrive, ya que seguramente estén infectados, y son la forma más fácil de propagar este virus a otros equipos. En caso de estar infectadas, estas unidades extraíbles contendrán estos archivos que se llaman **nideiect.com** y un **autorun.inf**, que podemos eliminar manualmente. Si no nos deja eliminarlo, lo mejor es formatear la unidad, salvando previamente los datos que necesitemos.

Es muy recomendable pasar también algún antivirus o-nline, por ejemplo alguno de los siguientes:

http://www.pandasecurity.com/activescan/index/?track=1&Lang=es-ES&IdPais=62

http://www.eset-la.com/online-scanner/