DESINFECCIÓN POR ROOTKIT + ROGUE

Tipo de infección: Falso antivirus + Rootkit

Nombre de los ejecutables instalados:

Nombre del virus	Nombre del proceso	Tipo
Malware Defense	Mdefense.exe	Rogue
Setdebugx	Settdebugx.exe	Malware
H8SRT…	H8SRTovfuohojmb.dll	Rootkit
krl32mainweq	krl32mainweq.dll	TrojanDNS Changer
MEMSWEEP2	4.temp	Trojan/Backdoor

Acciones del virus:

- **Desactivar toda protección instalada en el ordenador.**
- **Instalación de falso antivirus.**
- **Instalación de Rootkit.**
- **Instalación de Troyano camuflado por la acción del Rootkit**

Lo ideal ante este tipo de casos sería:

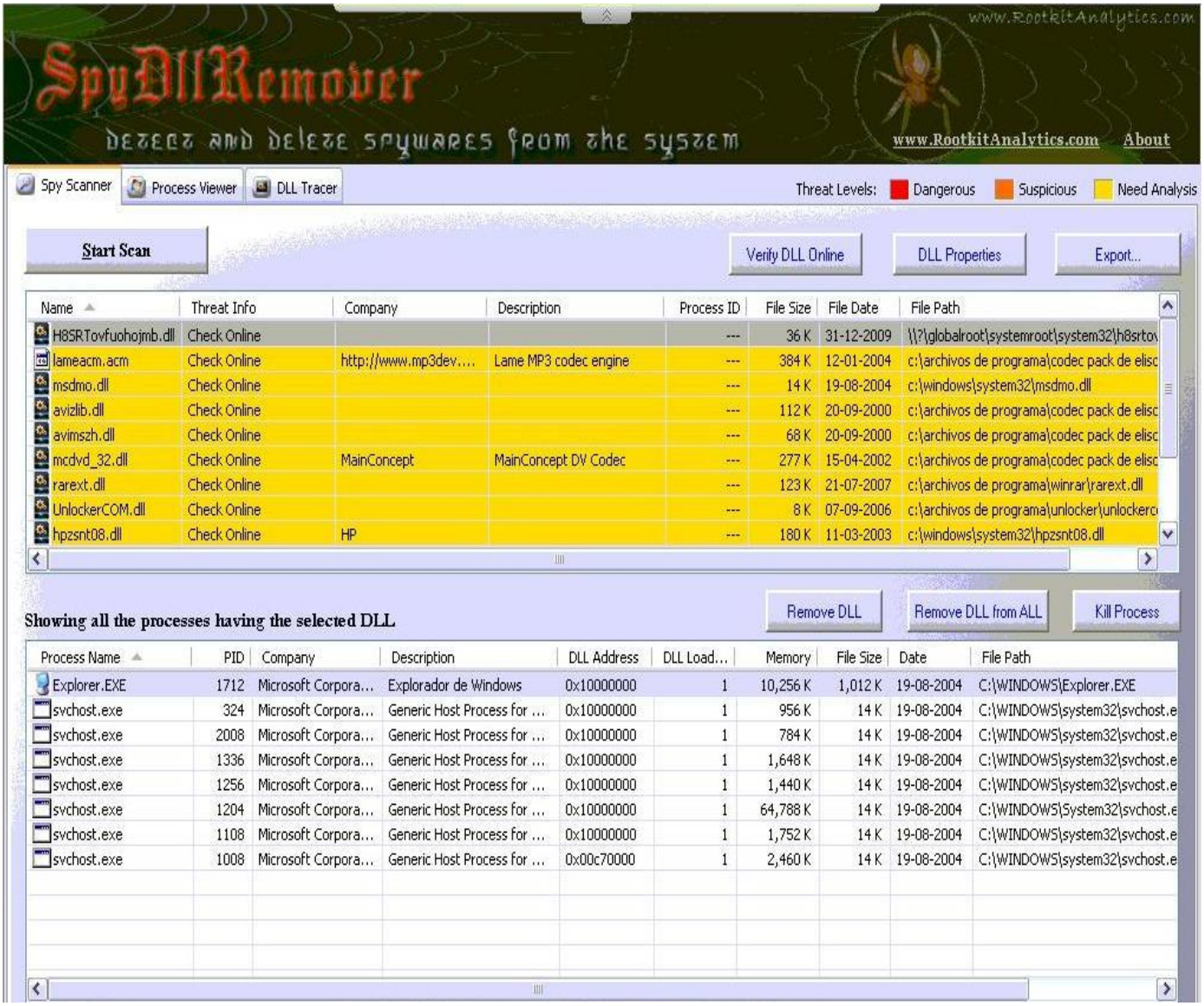
- **Cortar la conexión a internet lo antes posible para interrumpir que se descarguen ficheros a tu ordenador o al menos evitar que el atacante pueda seguir manipulando tu ordenador.**
- **No reiniciar el ordenador.**
- **Intentar NO conectar el ordenador comprometido a Internet para descargar las herramientas que te hagan falta, ten en cuenta que esta infección está activa incluso en modo seguro.**
- **Desactivar Restaurar Sistema.**
- **Eliminar los procesos creados por el virus en el Administrador de tareas.**
- **Comenzar a eliminar manualmente y con diferentes herramientas todo lo relacionado con el virus.**

Herramientas para la eliminación de los diferentes virus instalados:

Nombre de la utilidad:	Enlace de descarga:
Ccleaner	http://www.ccleaner.com/download
RegSeeker	http://www.hoverdesk.net/freeware.htm
Gmer	http://www.gmer.net/
SpyDLLRemover	http://www.rootkitanalytics.com/tools/spy-dll-remover.php
Svchost Process Analizer	http://www.neuber.com/free/svchost-analyzer/
Malwarebytes Antimalware	http://www.malwarebytes.org/mbam.php
Spybot Search&Destroy	http://www.safer-networking.org/es/spybotsd/index.html
Dr.Web Anti-Virus	http://download.drweb.com/demoreq/
Hijackthis	http://free.antivirus.com/hijackthis/

Las herramientas “SpyDLLRemover” y “Svchost Process Analizer” se utlizarán solo para comprobar que estamos hablando de la misma infección, alguna variante del mismo o similar:

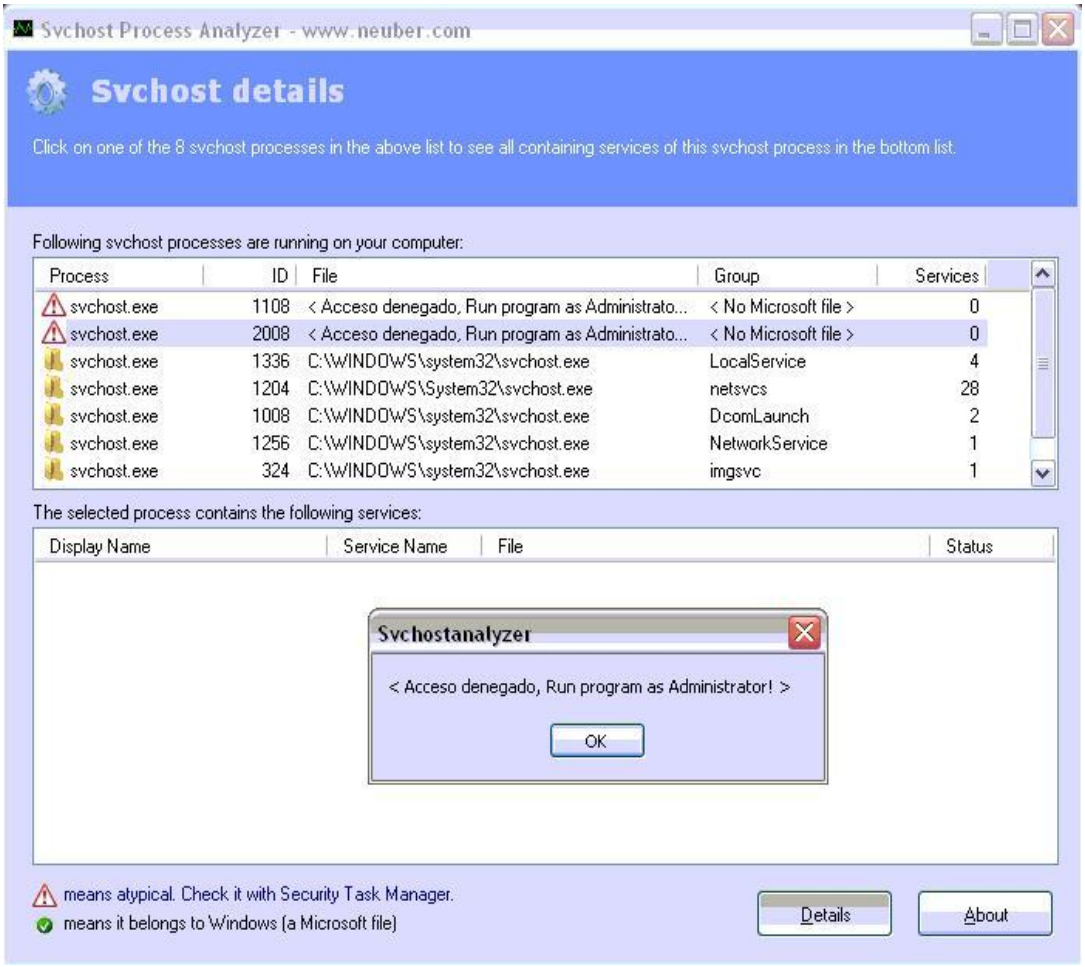
Análisis con SpyDLLRemover:



Con esta herramienta podrás comprobar el archivo sospechoso, la fecha de creación y la ruta donde se aloja. Nos da la opción de eliminar el archivo infectado resaltado en la imagen en gris, pero corremos el riesgo que al eliminar “H8SRTovfuohojmb.dll” dañemos algunos de los procesos “Svchost” legitimos del sistema en los cuales se ha inyectado.

***** Si lo haces es bajo tu responsabilidad. Si no ha variado mucho el código del virus, siguiendo el tutorial queda desactivado, así que bajo mi punto de vista no tendría que ser eliminado con esta herramienta. *****

Analisis con Svchost Process Analizer:

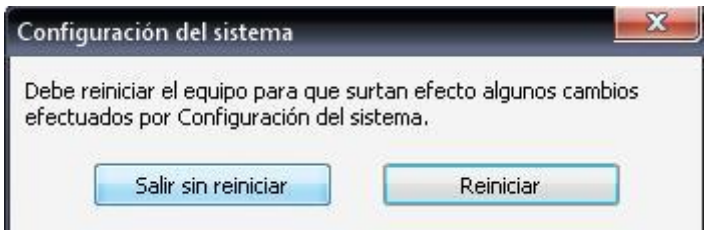


Comenzemos:
Una vez el ordenador infectado, no podremos hacer uso de ninguna opción en el escritorio. Solo mostrará acceso al falso antivirus y el resto del escritorio permanecerá inaccesible.
Presionaremos la secuencia de teclas (Ctrl+Alt+Supr) y para acceder al "Administrador de tareas", buscamos los siguientes procesos y los eliminamos:

- **mdefense.exe**
- **settdebugx.exe**

Son los dos únicos procesos "visibles" de la infección y forman parte del falso antivirus (Rogue), el resto permanece oculto por la acción del Rootkit.
Una vez terminados los procesos podremos observar que el falso antivirus desaparece y nos deja actuar sobre cualquier parte del escritorio y ejecutar algún que otro programa, aunque los procesos de las principales herramientas de desinfección están bloqueados.
Borrar la carpeta creada por "Malware Defense" en:
C:\Archivos de programa\Malware Defense
Eliminaremos las entradas creadas en el "MSConfig", así iremos borrando todos los restos:
Inicio → Ejecutar → Escribir en la ventana: msconfig

En la nueva ventana, navegaremos hasta la pestaña "Inicio" y desmarcan las dos entradas relacionadas con "mdefense.exe" y "settdebugx.exe". Ahora clickamos sobre Aplicar, Aceptar y en la nueva ventana que aparezca clickamos sobre: Salir sin reiniciar.



A parte de desmarcar los casilleros pertencientes al virus, borrámos las entradas creadas en el Msconfig. Podemos utilizar Ccleaner o borrarlas manualmente desde el registro. Entrar al "Editor del registro": Inicio → Ejecutar → escribir regedit en la ventana y aceptar.

Busca y elimina las entradas relacionadas con "MDefense.exe" y "Settdebugx.exe" en las siguientes rutas:

- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**

Una vez delante del editor del registro pulsa las teclas (Ctrl+b) y aparecerá una pantalla de búsqueda, introduce los nombres de los procesos y borra todo lo relacionado con ellos.
Rutas a borrar (eliminar la carpeta con todo el contenido) :

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\Malware Defense**

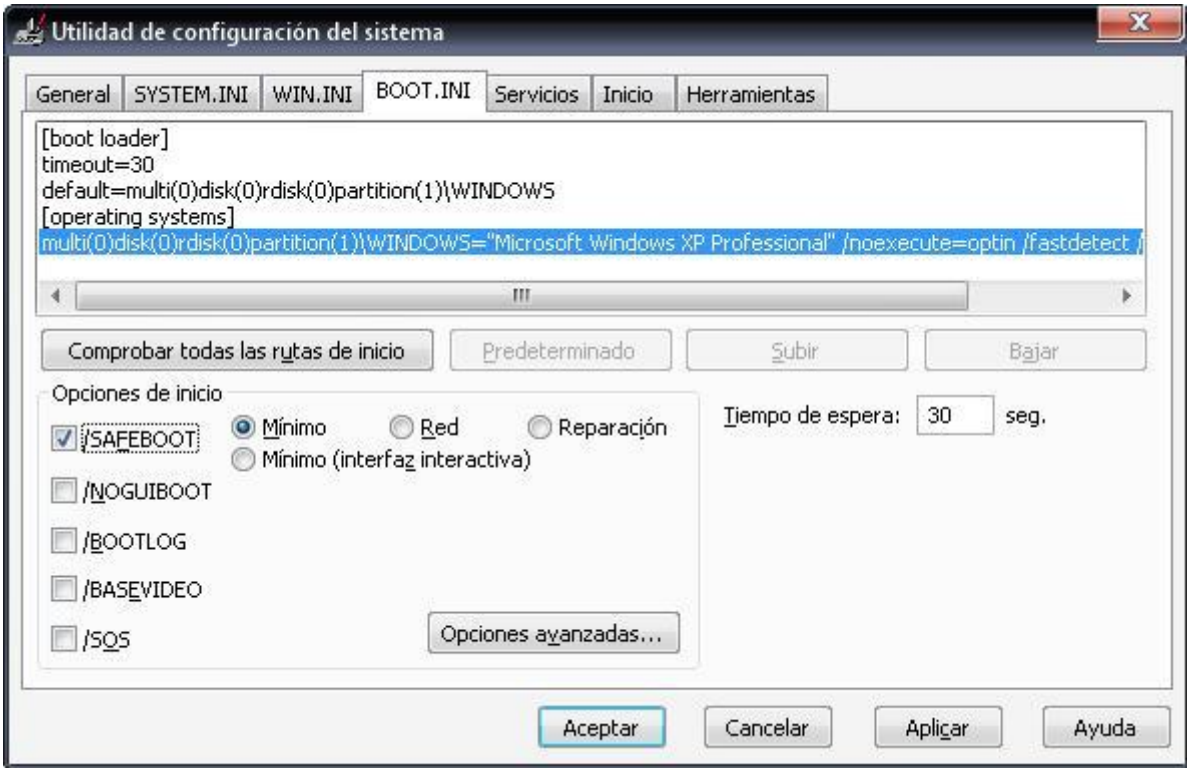
Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
command	REG_SZ	"C:\Archivos de programa\Malware Defense\mdefense.exe" -noscan
hkey	REG_SZ	HKCU
inimapping	REG_SZ	0
item	REG_SZ	mdefense
key	REG_SZ	SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\settdebugx.exe**

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
command	REG_SZ	C:\DOCUME~1\Oscar\CONFIG~1\Temp\settdebugx.exe
hkey	REG_SZ	HKCU
inimapping	REG_SZ	0
item	REG_SZ	settdebugx
key	REG_SZ	SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Una vez terminado de borrar todo lo relacionado a los procesos visibles, pasaremos Ccleaner al sistema de archivos y al registro, borrando todo lo que encuentre.
(Si lo tienes instalado se ejecutará con normalidad, no es bloqueado…)

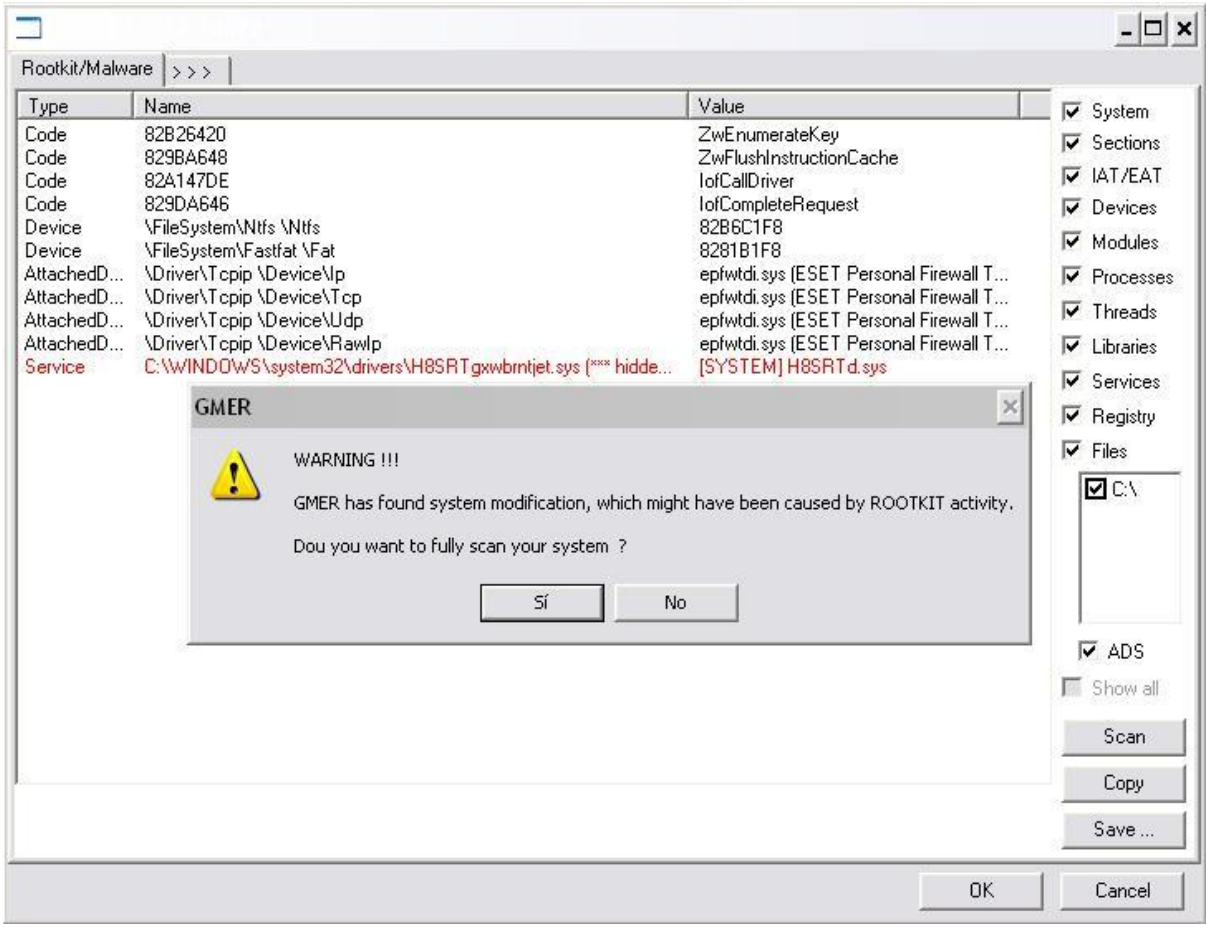
Ahora necesitamos reiniciar el pc pero en “Modo a prueba de fallos”, esto se hace para que el pc cargue solo los controladores y servicios básicos. Entraremos al “Msconfig”, vamos hasta la pestaña “BOOT.INI” y marcamos el casillero “/SAFEBOOT”, por defecto se activará la casilla “Mínimo”. Click sobre Aplicar, Aceptar;



Nos aparecerá una ventana donde nos dará la opción de reiniciar o no, ahora le decimos que SI queremos reiniciar y esperamos a que lo haga. Verás que carga Windows y nos muestra una ventana informativa donde nos dice que estamos ejecutando Windows en modo a prueba de fallos, aceptamos y esperamos que cargue el escritorio.

Ahora toca echar mano de algunas herramientas para poder eliminar el rootkit instalado en el sistema. El problema es que no podrás hacer uso de ninguna herramienta de desinfección a no ser que renombres el nombre del ejecutable SIN modificar su extensión (.exe). Una de las herramientas que mas utilizaremos es “Gmer antirootkit”, pero si intentamos ejecutarla se nos dirá que no se puede por que se han modificado los permisos sobre la cuenta del administrador. El nombre del ejecutable del Gmer es “Gmer.exe”, lo que haremos es renombrarlo como “er.exe” y ahora si se ejecutará;

Una vez ejecutado, hará un leve escaneo y nos mostrará la siguiente pantalla:



El mensaje de advertencia nos dice que Gmer ha encontrado una modificación en el sistema y podría ser causado por la acción de un Rootkit. Nos da la opción de realizar un escaneo completo del disco. De momento le decimos que NO, y eliminamos el servicio creado por el Rootkit, marcado en rojo :

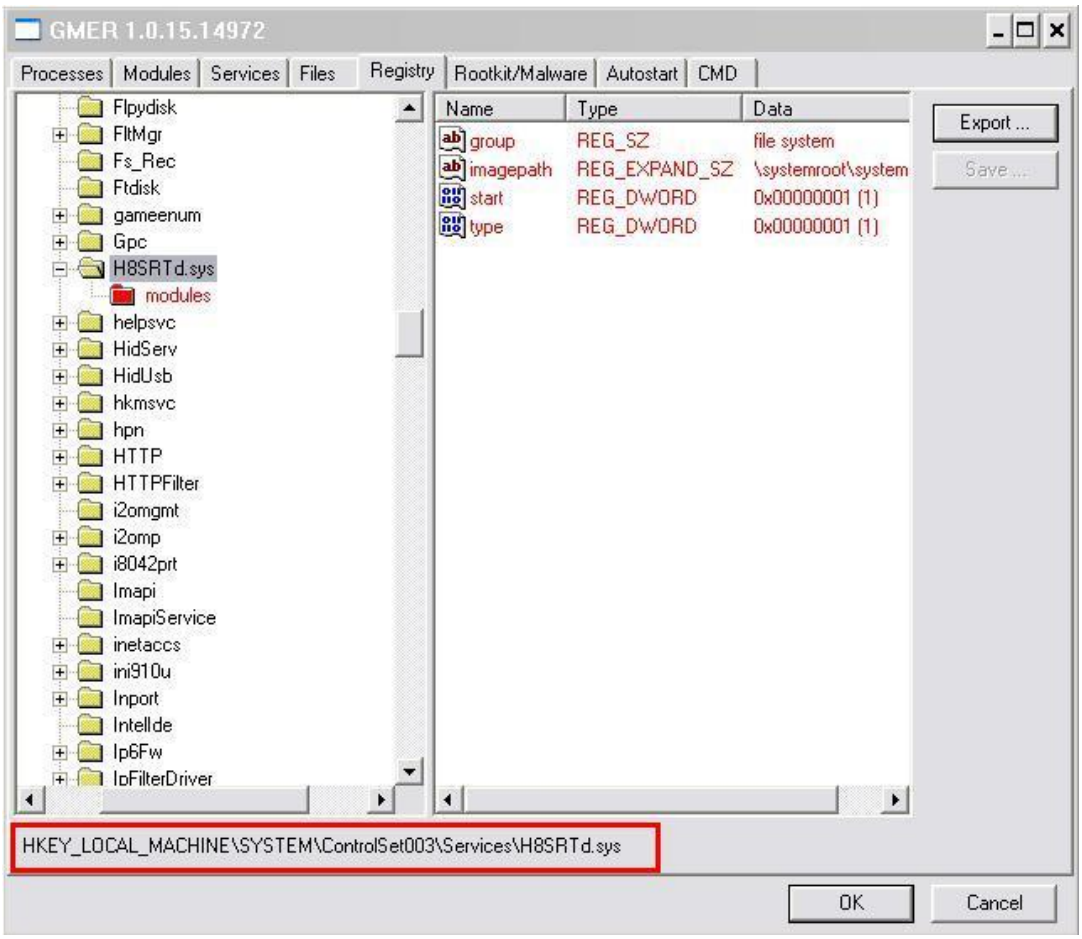
Service → C:\WINDOWS\system32\drivers\H8SRTgxwbrntjet.sys → [*hidden***] → [SYSTEM] H8SRTd.sys**

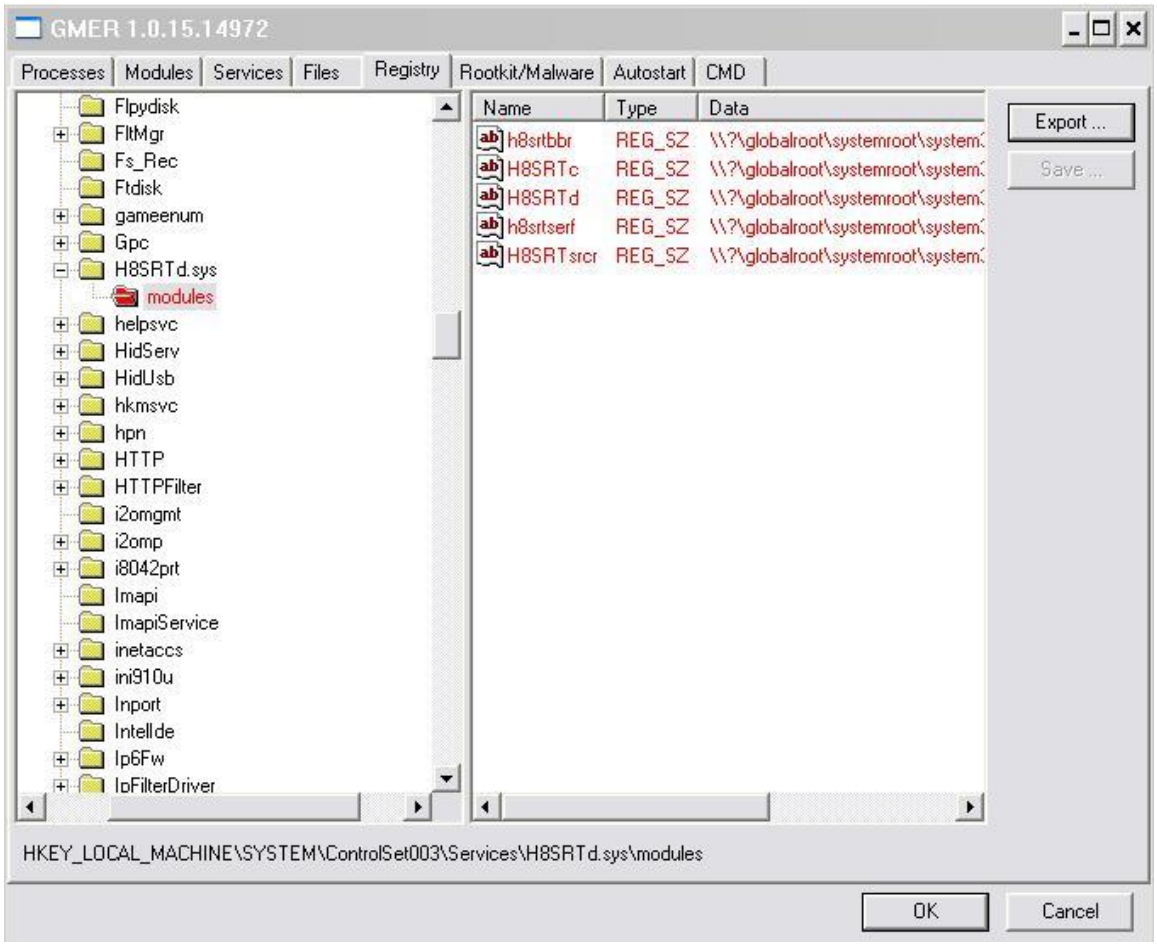
Clickamos con el derecho del ratón en el texto y aparecerá un desplegable, clickar sobre “Delete Service”.
Ahora SI haremos un escaneo completo, clickar sobre el botón “Scan” y dejarlo haciendo (dependiendo del procesador, memoria y cantidad de archivos tardará más o menos tiempo).
Una vez terminado nos mostrará en pantalla todo lo que haya encontrado y nos dará la opción de guardarlo en un log (esto puede ser útil, pues al presentarse en un foro con un problema les servirá de ayuda a solucionarlo).
Ya guardado el log del análisis, nos centramos en el Gmer y podrás comprobar que de todas las rutas donde se encuentran los rastros del rootkit, al clickar con el botón derecho del ratón para poder eliminarlo no deja elegir “ninguna” opción.

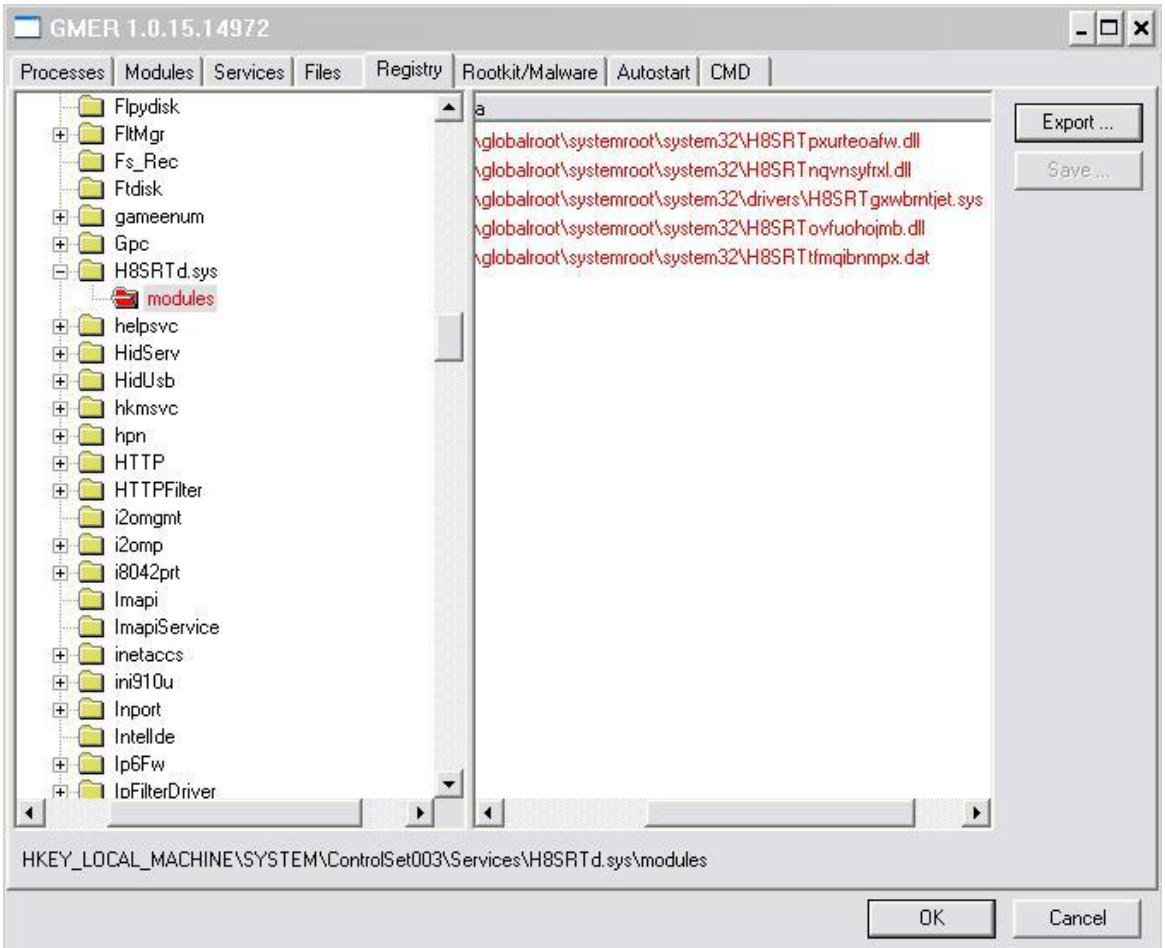
En la primera pantalla nada más iniciar Gmer, podrás ver que solo tenemos dos pestañas en el menú superior/izquierda. La primera pestaña "Rootkit/Malware" es donde haremos los escaneos en el sistema y la segunda "> > >" desplegará varias pestañas nuevas donde podremos ver/escanear también en el registro, sistema de archivos, módulos cargados, procesos en ejecución (con opción de terminar "x" proceso) y alguna cosa más que por ahora no tocaremos. Fijense que la pestaña para los análisis "Rootkit/Malware" ha quedado en sexto lugar después de clickar sobre "> > >".
Primero veremos unas capturas de las rutas y subcarpetas donde se alojan los diferentes archivos del Rootkit y luego miraremos la forma de eliminarlas:

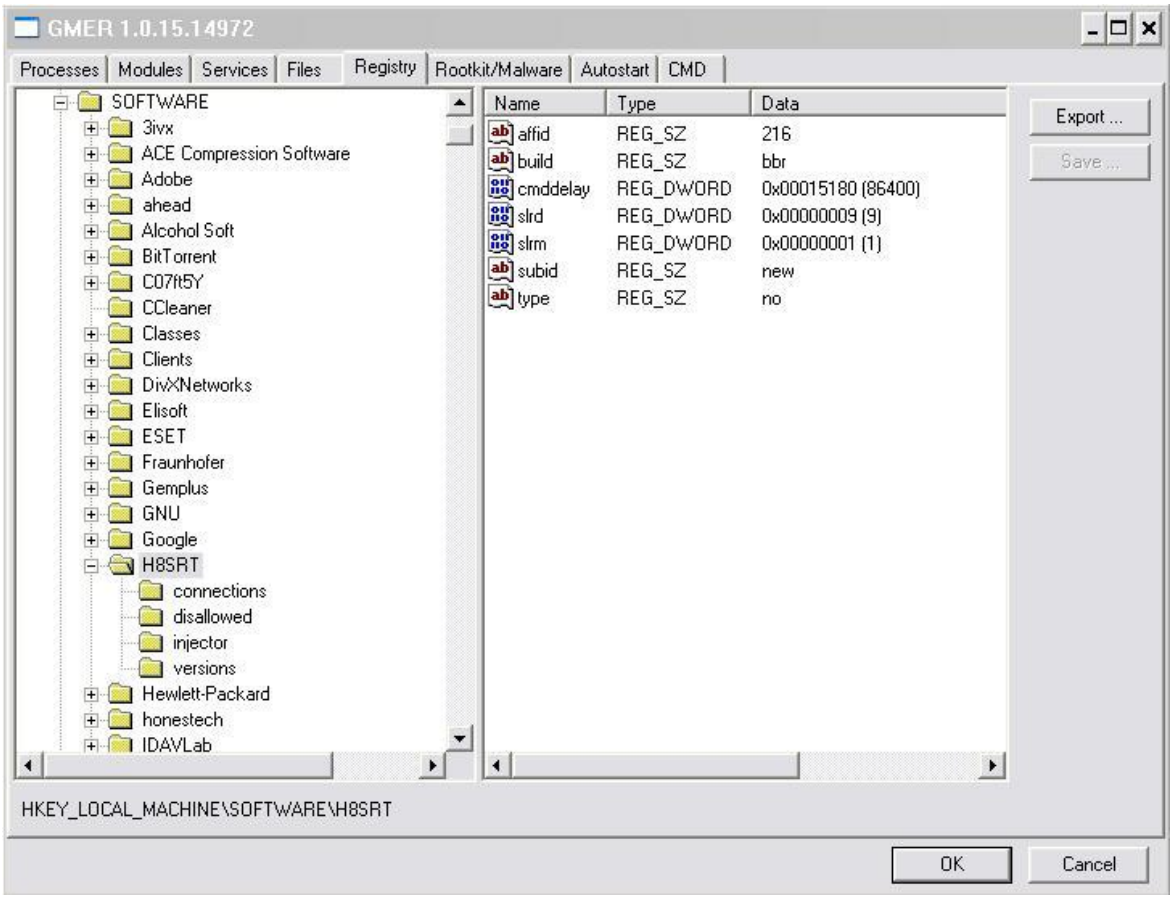
**** Justo debajo de las dos ventanas de datos, podrás ver las rutas completas donde está alojado :**

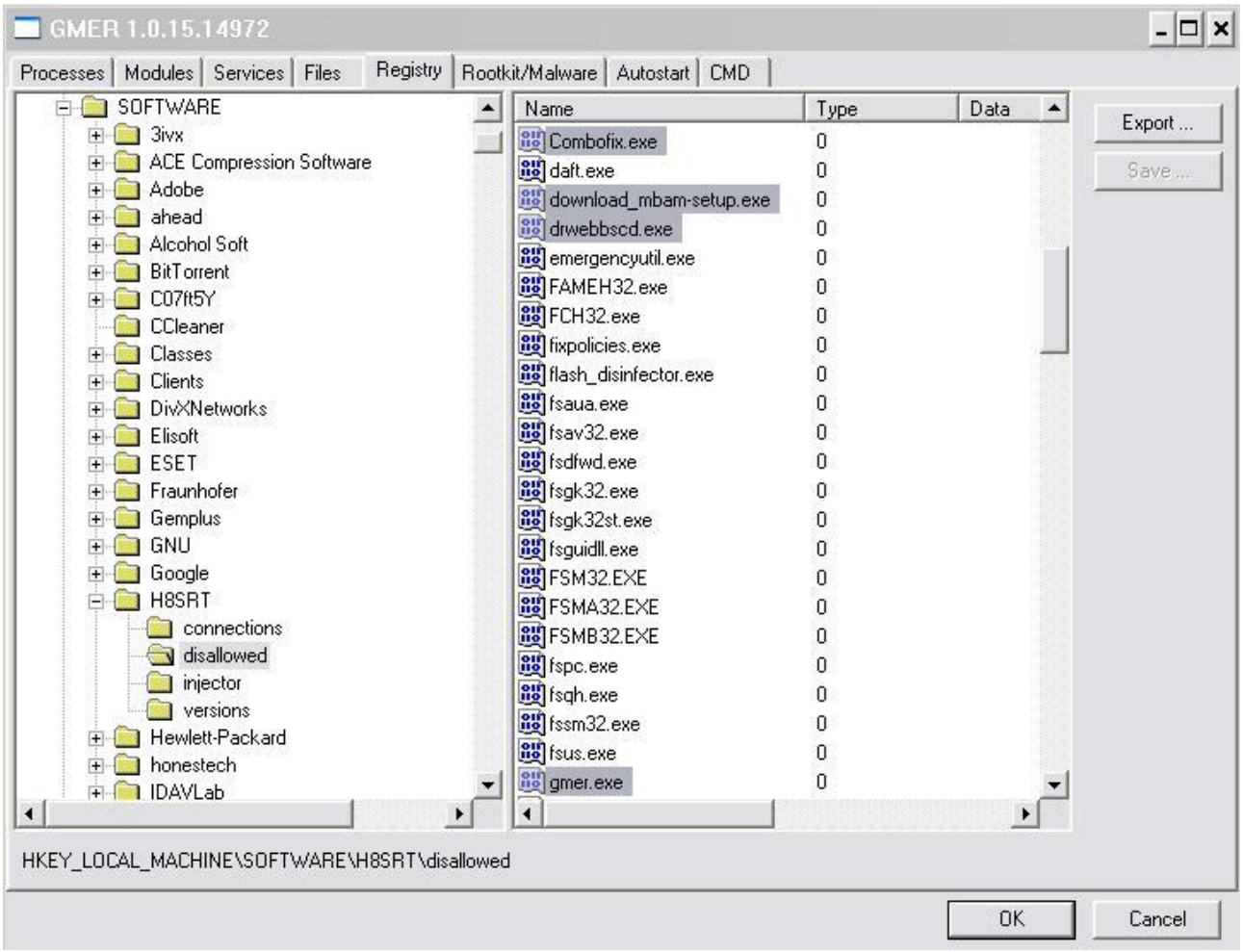
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\H8SRTd.sys




GMER 1.0.15.14972
Processes
Modules
Services
Files
Registry
Rootkit/Malware
Autostart
CMD
Flpydisk
FltMgr
Fs_Rec
Ftdisk
gameenum
Gpc
H8SRTd.sys
modules
helpsvc
HidServ
HidUsb
hkmsvc
hpn
HTTP
HTTPFilter
i2omgmt
i2omp
i8042prt
Imapi
ImapiService
inetaccs
ini910u
Inport
Intelide
Ip6Fw
IpFilterDriver
Name
Type
Data
h8srtbbr
REG_SZ
\\?\globalroot\systemroot\system
H8SRTc
REG_SZ
\\?\globalroot\systemroot\system
H8SRTd
REG_SZ
\\?\globalroot\systemroot\system
h8srtserf
REG_SZ
\\?\globalroot\systemroot\system
H8SRTsrcr
REG_SZ
\\?\globalroot\systemroot\system
Export ...
Save ...
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\H8SRTd.sys\modules
OK
Cancel

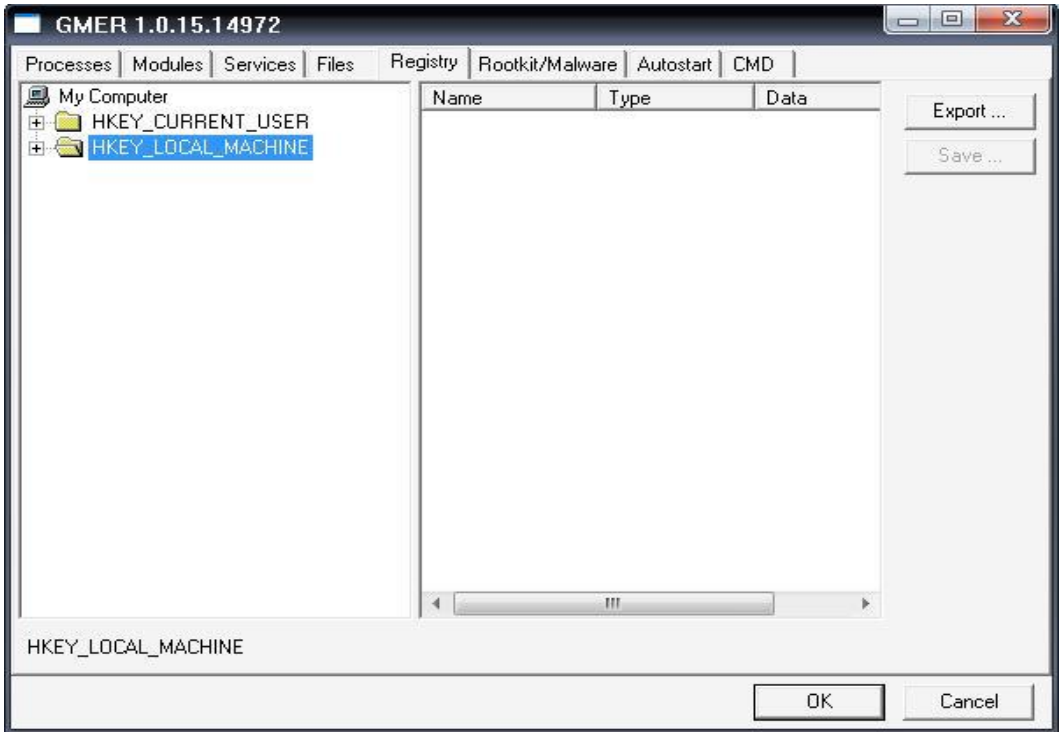

GMER 1.0.15.14972
Processes
Modules
Services
Files
Registry
Rootkit/Malware
Autostart
CMD
Flpydisk
FltMgr
Fs_Rec
Ftdisk
gameenum
Gpc
H8SRTd.sys
modules
helpsvc
HidServ
HidUsb
hkmsvc
hpn
HTTP
HTTPFilter
i2omgmt
i2omp
i8042prt
Imapi
ImapiService
inetaccs
ini910u
Inport
Intelide
Ip6Fw
IpFilterDriver
a
\globalroot\systemroot\system32\H8SRTpxurteoafw.dll
\globalroot\systemroot\system32\H8SRTnqvnsyfrxl.dll
\globalroot\systemroot\system32\drivers\H8SRTgxwbrntjet.sys
\globalroot\systemroot\system32\H8SRTovfuohojmb.dll
\globalroot\systemroot\system32\H8SRTtfmqibnmpx.dat
Export ...
Save ...
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\H8SRTd.sys\modules
OK
Cancel





En la ruta de la captura superior, podrás ver todos los ejecutables de las herramientas de desinfección que bloquea para hacer mejor su estancia en tu ordenador…

Ahora vamos hasta la pestaña “Registry”:



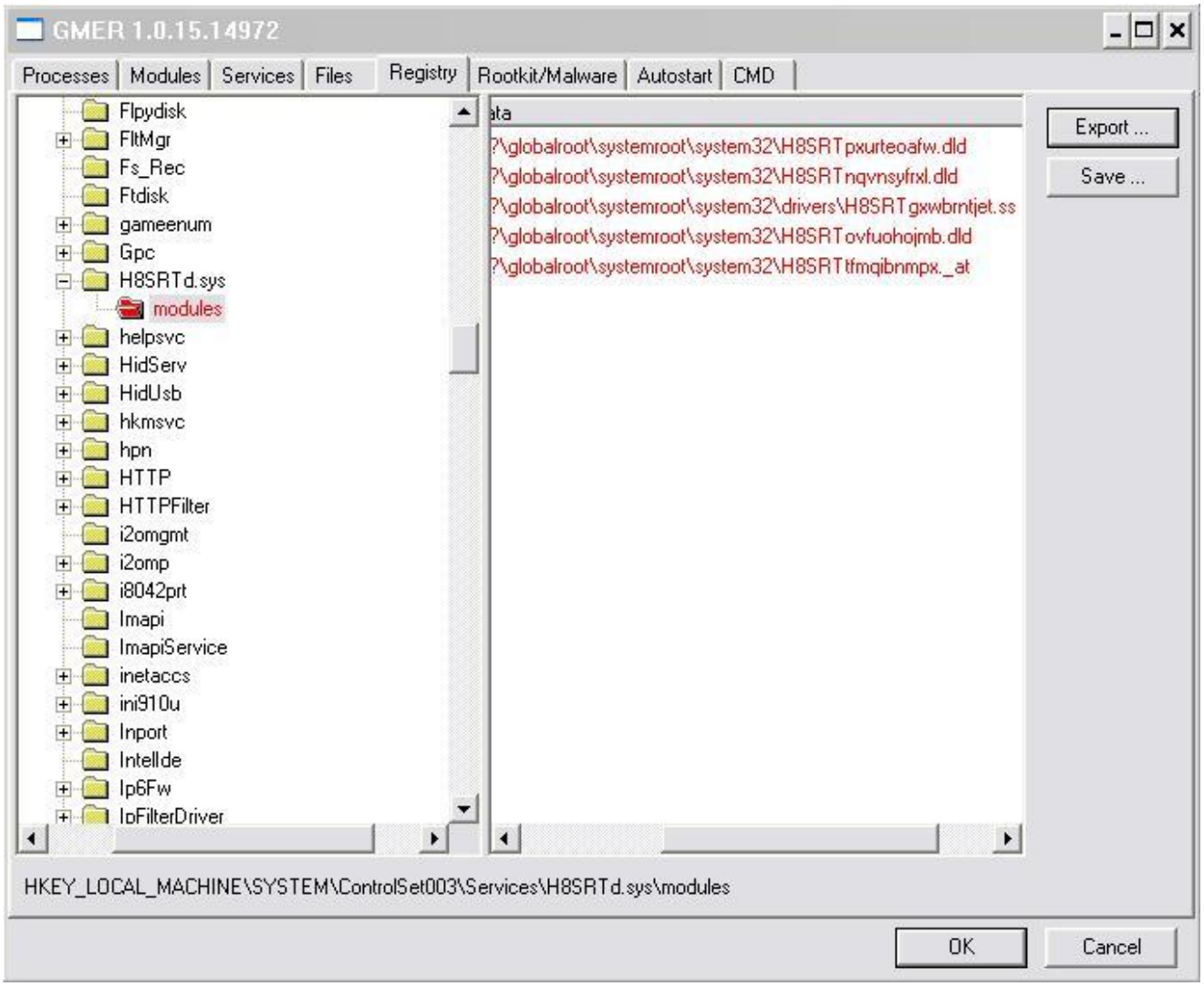
Para navegar y poder modificar las diferentes claves del resgistro (ya que no nos deja eliminarlas), veremos que la pantalla se divide en dos secciones, en la ventana izquierda veremos las diferentes ramas del registro y al llegar a la ruta del archivo que deseamos eliminar y clickarle con el ratón, nos mostrará en la ventana derecha los valores del archivo. Esto es lo que tendremos que modificar, bien cambiándole la extensión al archivo o renombrándolo como valor “0”.
En mi caso renombré las extensiones de los archivos.
Empezaremos modificando los valores del registro para inutilizar/hacer inservibles los ficheros creados por el Rootkit.

Navegar hasta:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\H8SRTd.sys

Al clickar sobre la carpeta “modules” verás que en la ventana de la derecha muestra la ruta de unos cuantos archivos, haz click con el botón derecho del ratón sobre el primero y verás que se abre una pequeña ventanita que dice “Modify”, clickale y se abrirá una nueva ventana donde tendrás que modificar el valor del archivo como hemos mencionado un poco más arriba.
De los tres casilleros de la ventana con datos, verás que solo deja modificar en el último, eso es lo que hay que modificar.

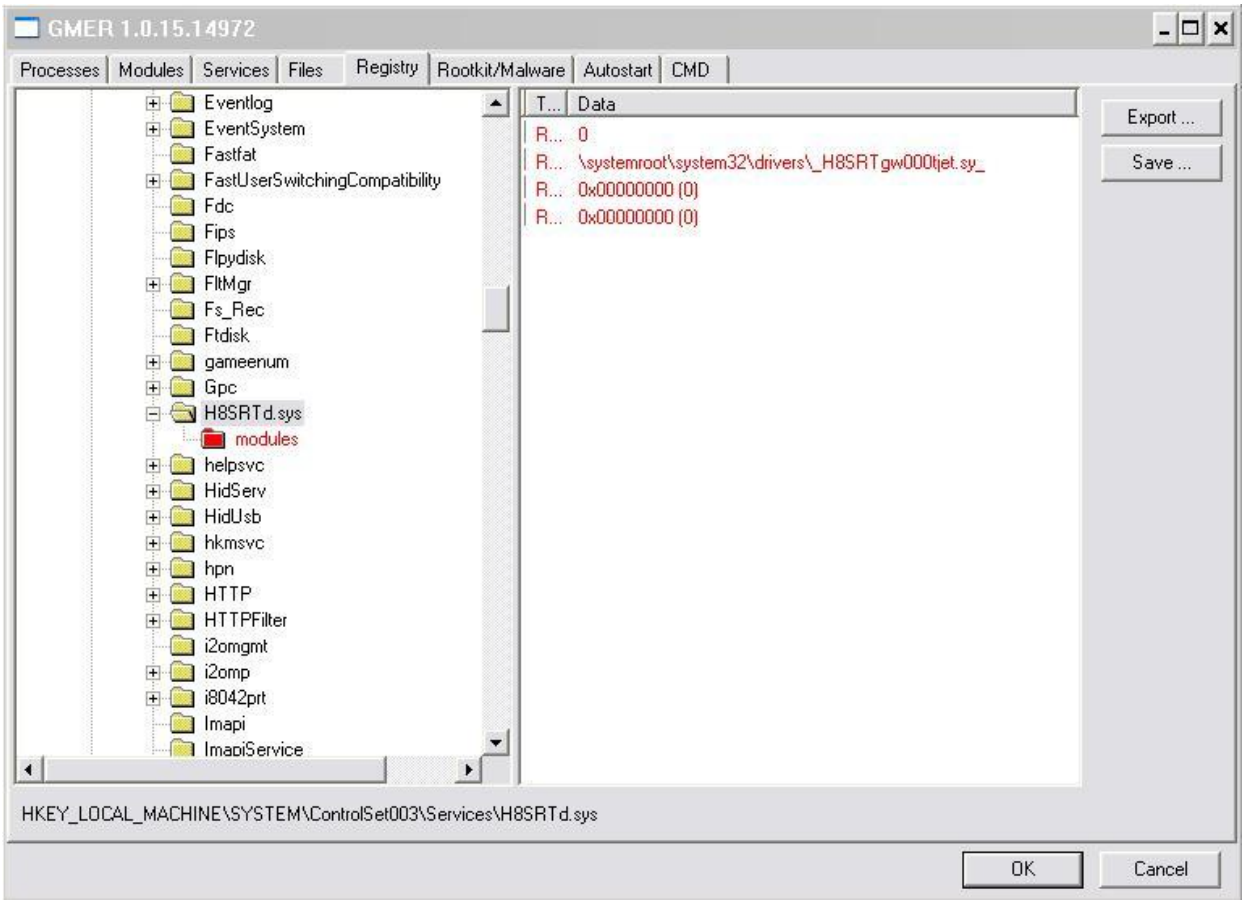
**** En esta imagen ya están modificados los archivos, fíjate en la extensión de cada uno de ellos…**

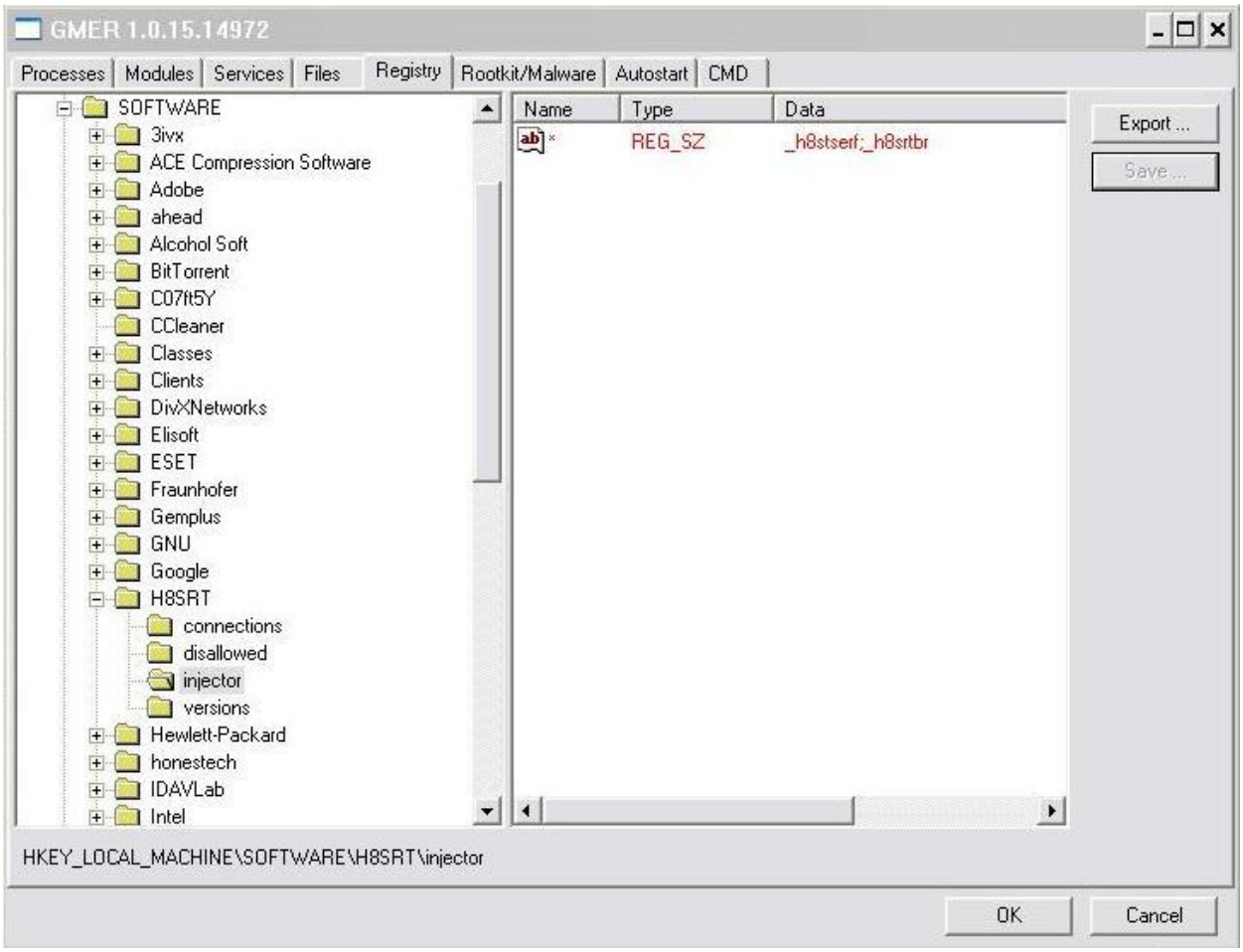


Cuando termines de modificar las rutas, al volver hacia la ventana de la izquierda para buscar otra ruta a modificar, nos mostrará un pequeño aviso conforme hemos modificado ciertos valores de los ficheros, aceptamos y a por las siguientes rutas.
Tendrás que repetir los pasos de arriba en todas y cada una de las rutas expuestas a continuación, y si ves alguna ruta nueva que no esté en la imagen también tendrá que ser renombrada:

*** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**
*** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services**
*** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services**

Aquí unas cuantas capturas más de las rutas a modificar:

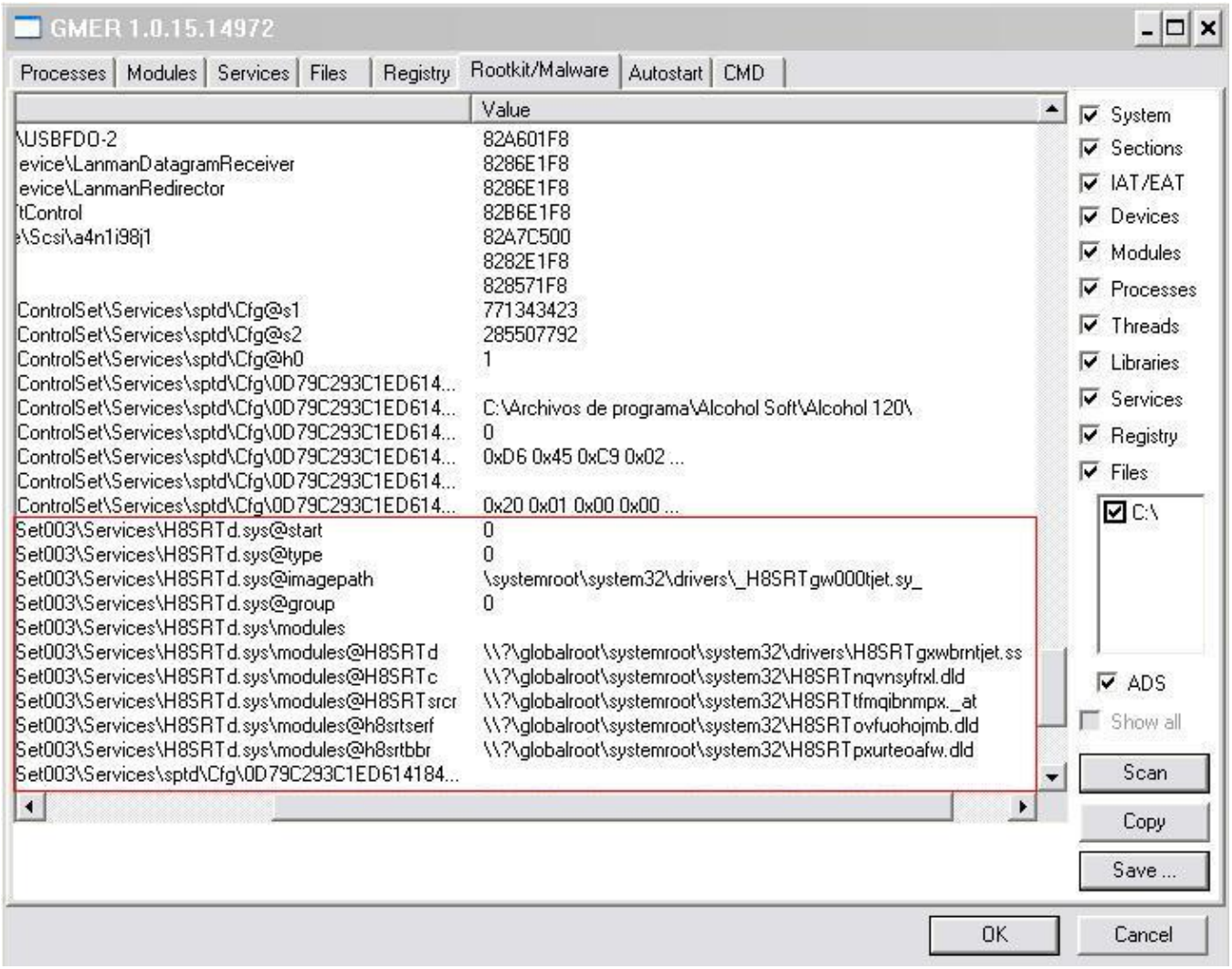




Una vez modificadas todas las rutas, aceptaremos los cambios realizados y haremos un nuevo escaneo en la pestaña <Rootkit/Malware>. Recuerda que primero realiza un breve escaneo y ya no tendría que mostrar el servicio que creaba y mostrado en rojo en el primer escaneo del Gmer.

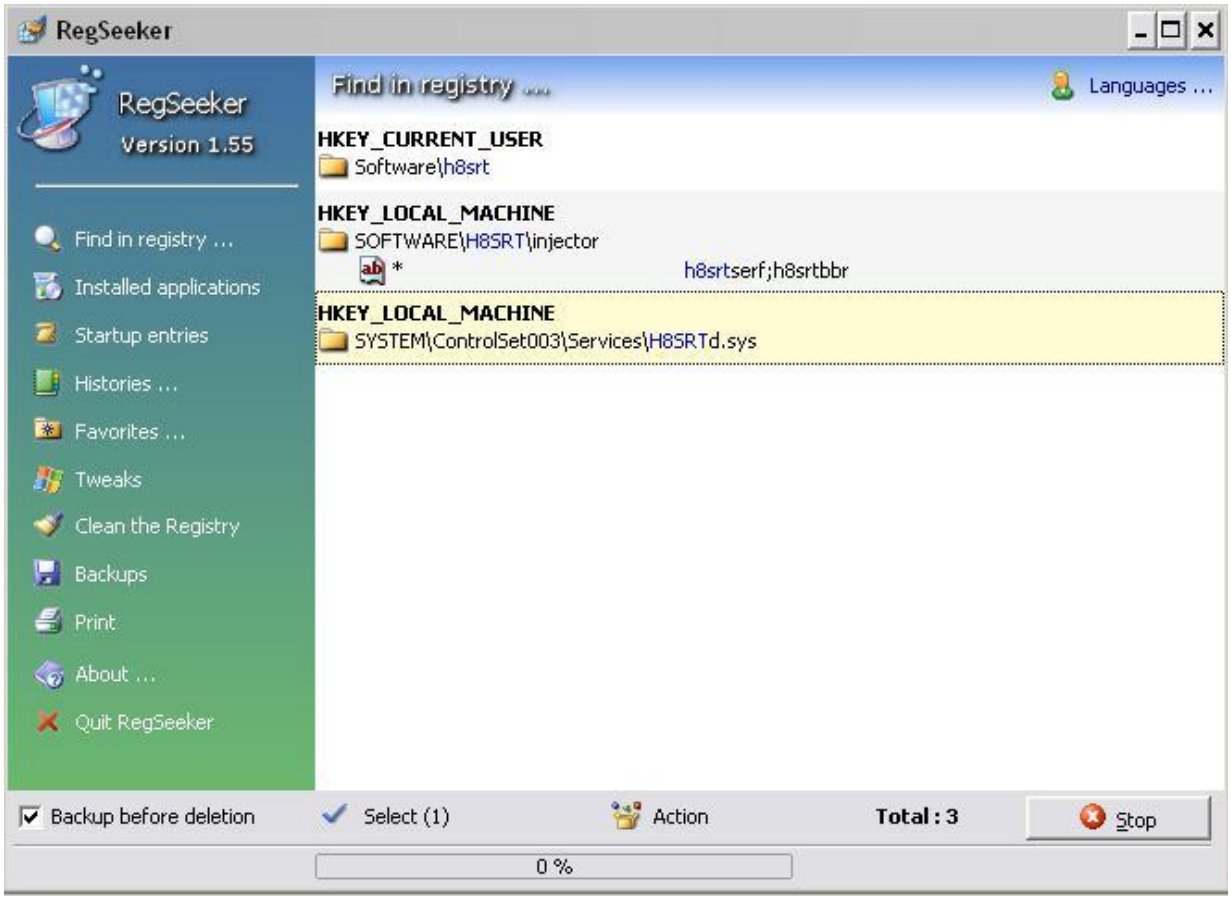
Service → C:\WINDOWS\system32\drivers\H8SRTgxwbrntjet.sys → [*hidden***] → [SYSTEM] H8SRTd.sys**

Hacemos un escaneo completo y cuando termine mostrara en pantalla lo que haya encontrado. Si modificaste las extensiones a las entradas creadas, mostrará la modificación en el log:



Si las modificaste con valor "0", nos mostrará ese valor en vez de la ruta con la extensión modificada.

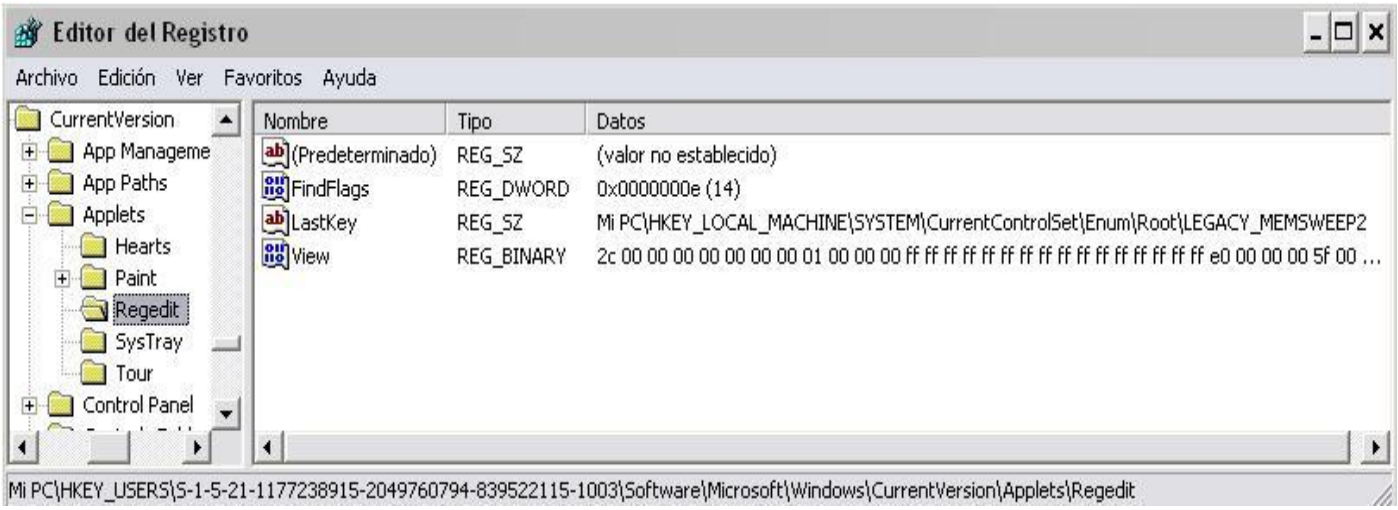
Ya terminadas las modificaciones, pasamos de nuevo Ccleaner borrando lo que encuentre en el sistema de archivos y en el registro.
Reiniciamos el pc sin modificar el cambio en el Msconfig, para que vuelva a iniciar en modo a prueba de fallos. Una vez cargue el escritorio ejecutamos Regseeker, y clickamos sobre <Clean the registry>, borramos todo lo relacionado con "H8SRT…".
Nos mostrara algunas rutas donde se alojan varios archivos, eliminamos las entradas, cerramos y volvemos a pasar Ccleaner borrando lo que encuentre.



Entramos al Msconfig y en la pestaña <BOOT.INI> dejamos marcada la entrada "/SAFEBOOT" pero clickamos sobre la opción "Red" (se desmarcará Mínimo), esto lo hacemos para que podamos tener acceso a internet y poder actualizar las bases de datos de las herramientas que a continuación utilizaremos. Una vez cambiado aceptamos y que reinicie…
Ahora instalamos "Malwarebytes Antimalware". Sin renombrar la extensión del programa, tendría que dejar instalarlo sin problemas. Antes de nada actualizar el programa…
Lo dejamos que haga un escaneo completo y nos arrojara la siguiente infección:

Eliminamos el archivo infectado y si podemos en modo seguro hacemos un escaneo con el antivirus que tengamos (dependiendo del antivirus puede ser que encuentre algún archivo infectado o no).
Acabado el escaneo con antivirus si pudimos hacerlo, instalamos Spybot Search&Destroy y actualizamos también. Hacemos un escaneo completo y reparamos todas las entradas encontradas (no tengo captura de esto, pero eran tres o cuatro entradas, no más).

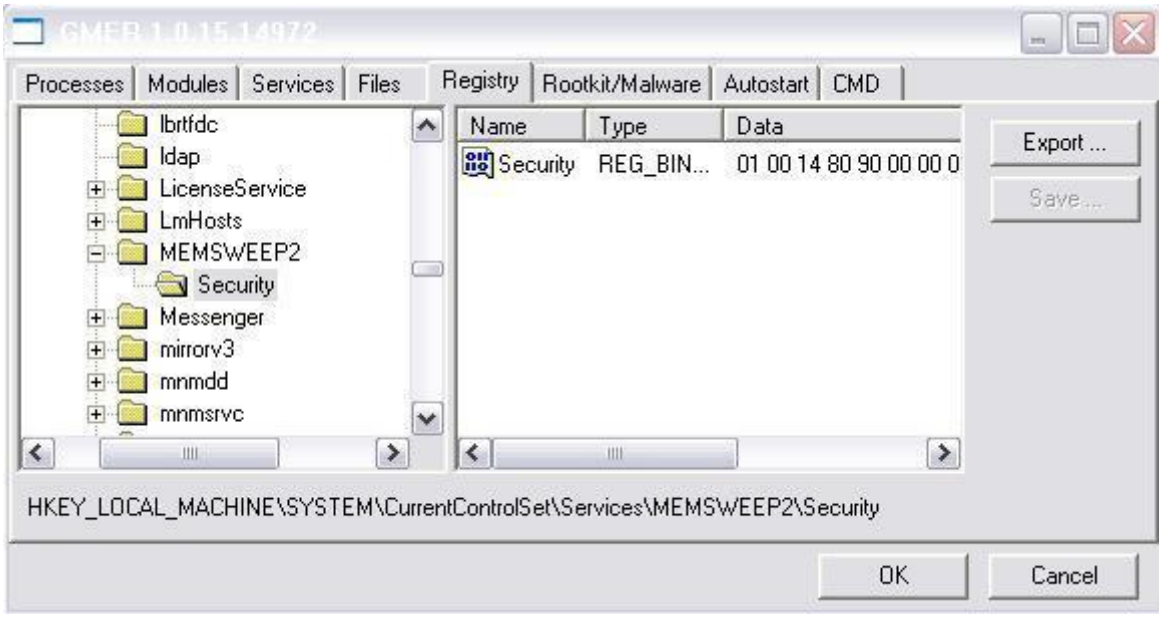
Entramos al editor del registro y eliminamos la carpeta siguiente (en el pie de foto pueden ver la ruta):

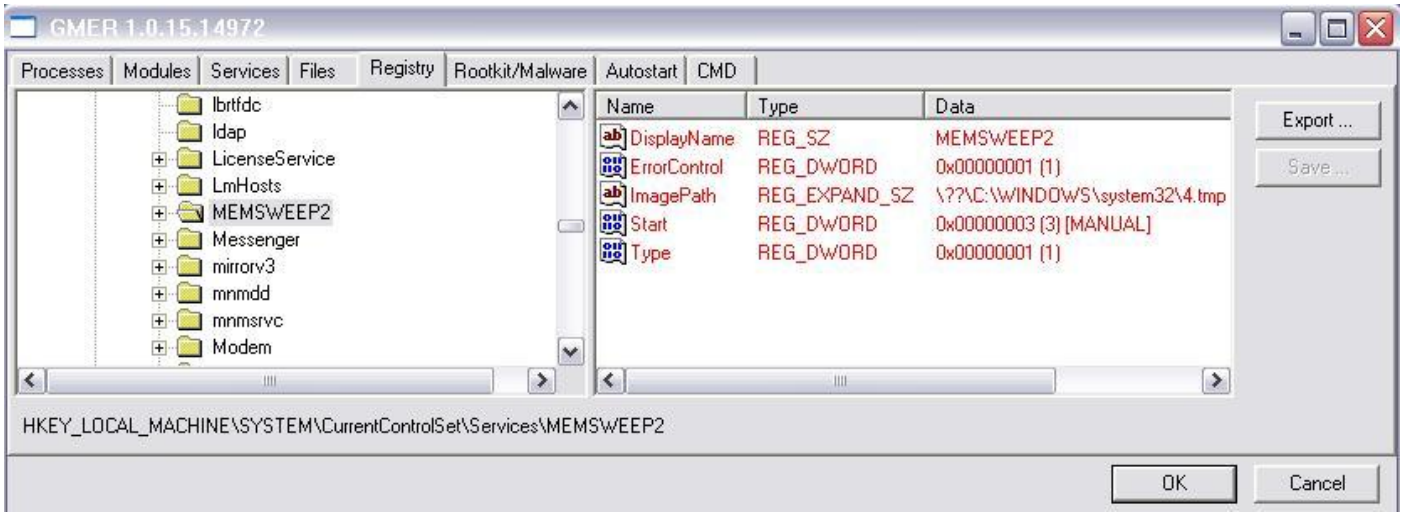


Cerramos el Regedit y volvemos a ejecutar la herramienta "Gmer" para eliminar del registro todo lo relacionado con las entradas creadas en la ruta "MEMSWEEP2".
Abierto el Gmer vamos a la pestaña Registry y modificamos el contenido de todas las entradas creadas, con valor "0" de la siguientes rutas:

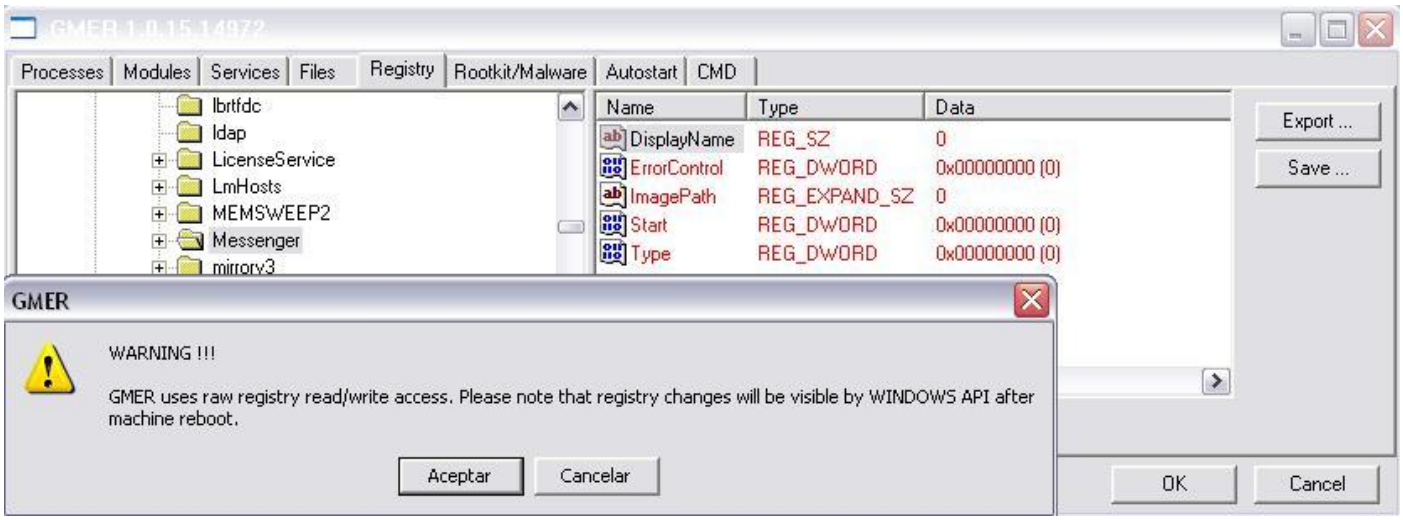
* HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
* HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
* HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services

Aquí unas capturas de las entradas aun sin modificar;





En esta captura puedes ver los valores ya modificados de la imagen superior:



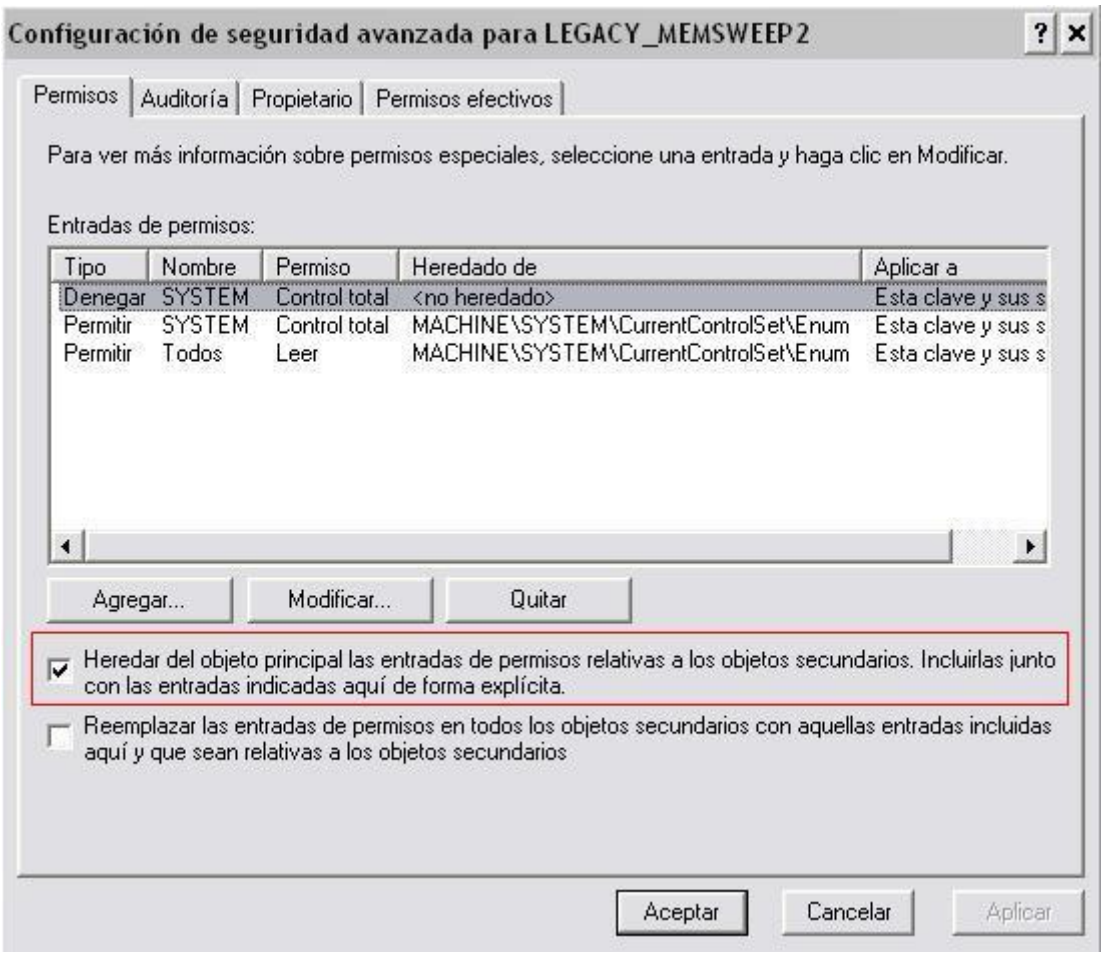
Aceptar los cambios realizados al registro.
Una vez que vuelvas a realizar un escaneo con Gmer la entrada “MEMSWEEP” no volverá a parecer.
Cerramos el Gmer y realizamos una limpieza con Cleaner borrando los restos que encuentre.

Ya con los valores modificados haremos la última modificación para denegar los permisos creados sobre las cuentas de administrador del sistema en la rama del registro “LEGACY_MEMSWEEP2” pues no se puede eliminar, pero la dejaremos vacia por completo y sin permisos.

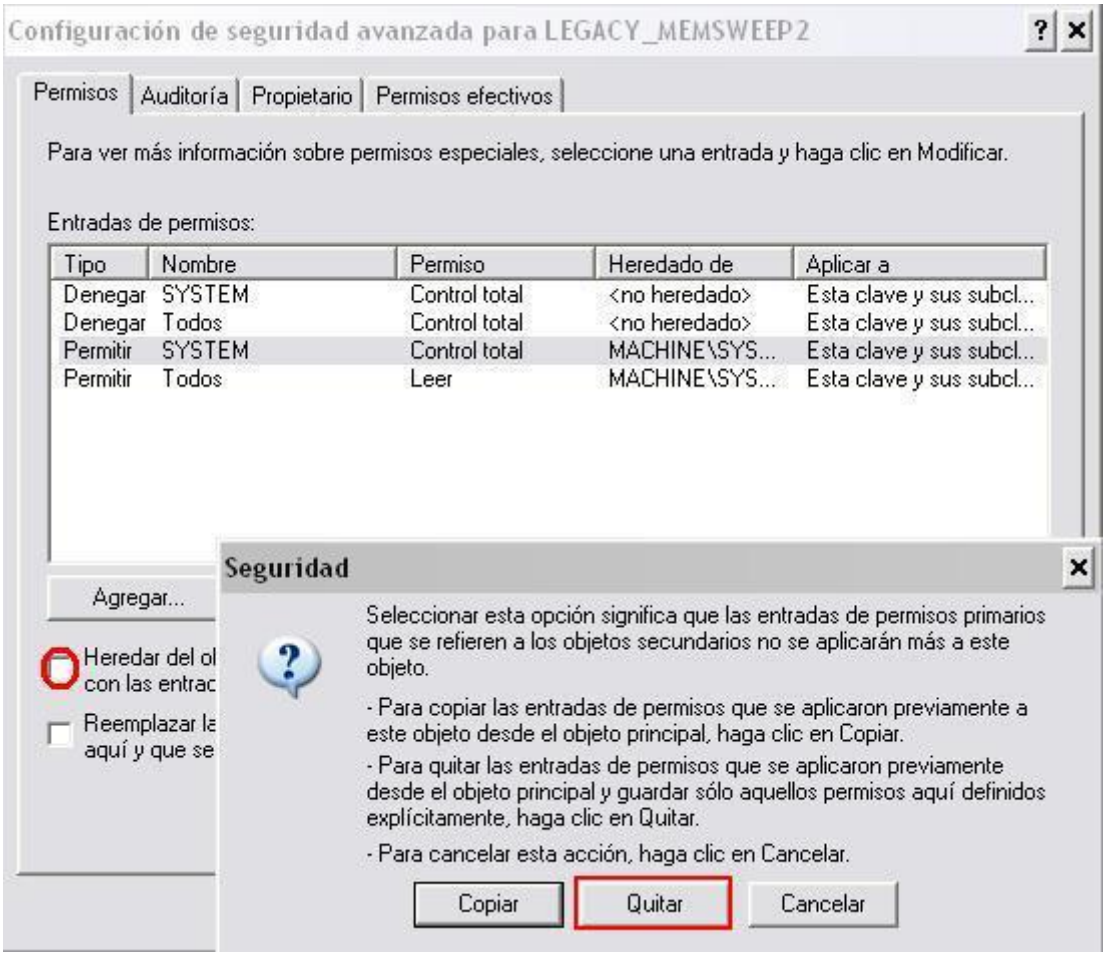
Abrimos el editor del registro (regedit). Una vez dentro pulsamos (ctrl+b) y buscamos la entrada creada “LEGACY_MEMSWEEP2”.

Le hacemos un click con el botón derecho del raton y elegimos “Permisos”, nos mostrará esta ventana:

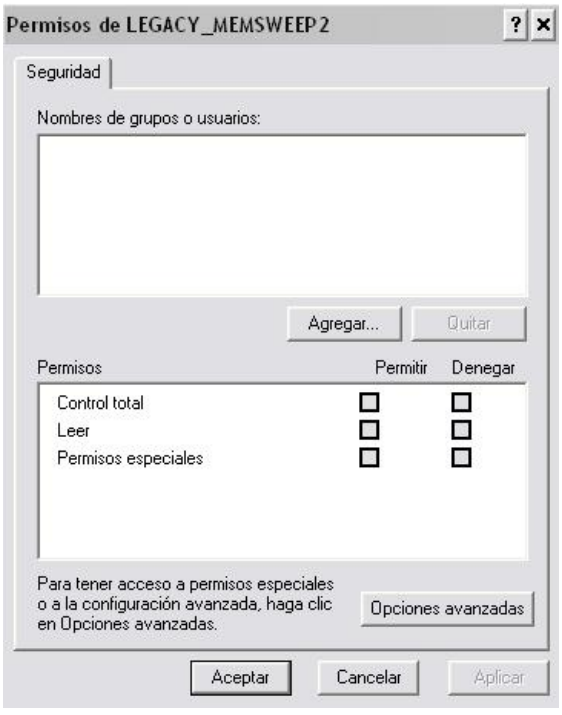
Una vez en esta ventana, clickamos sobre el botón “Opciones avanzadas” y nos aparecerá la siguiente ventana de configuración de permisos:



Para modificar los permisos desmarcaremos la entrada enmarcada en color rojo en la foto superior, de forma que nos aparecerá una ventana informativa:



Clickamos sobre el botón “Quitar” y eliminamos las dos cuentas creadas que contienen las rutas con los archivos del MEMSWEEP2.
Aplicar y aceptar los cambios creados. aHora nos mostrará la siguiente ventana con el contenido completamente vacío:

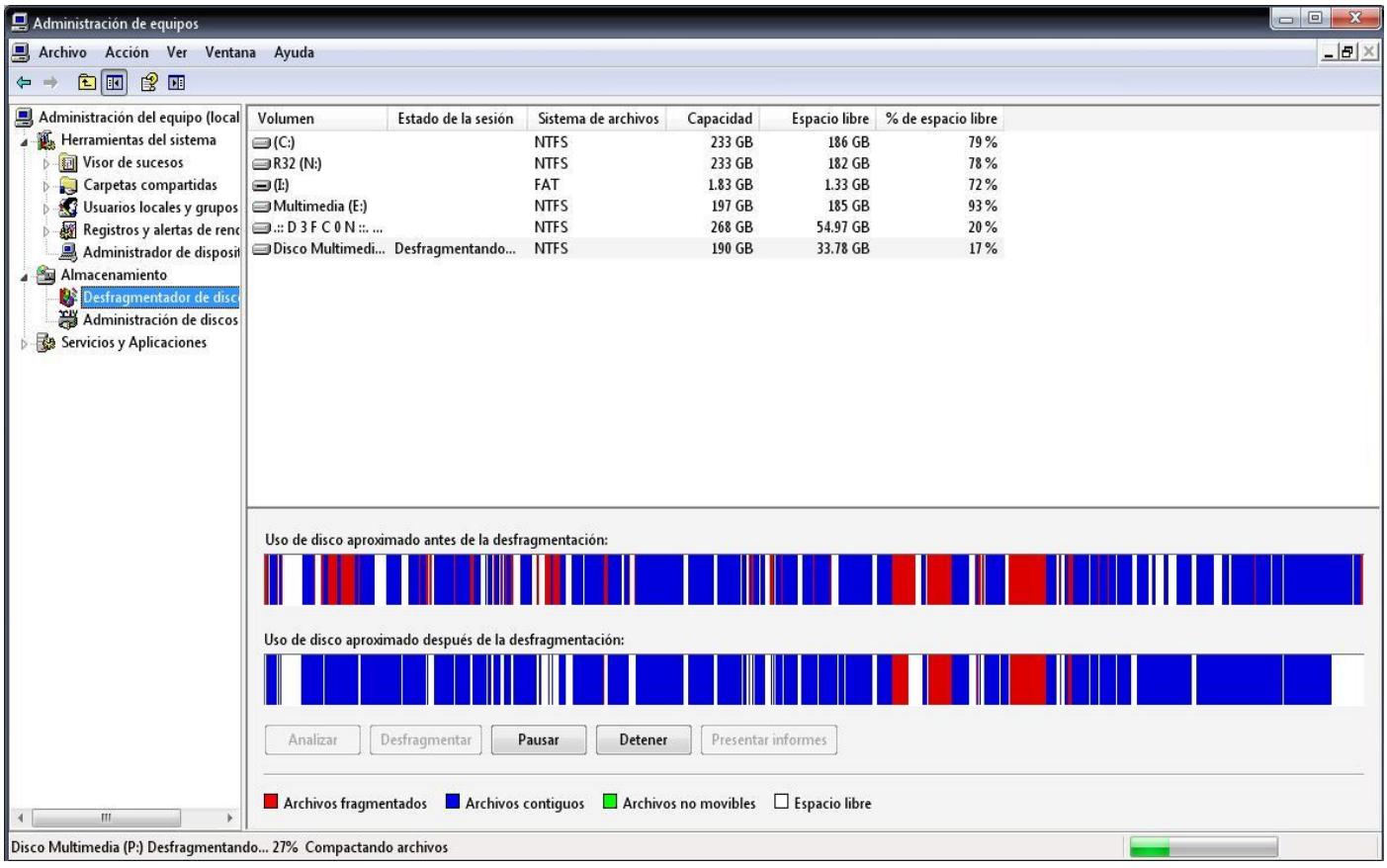


Una vez hecho todo lo expuesto podemos entrar al Msconfig y desmarcar la opción "/SAFEBOOT" para poder reiniciar en modo normal. Una vez en el escritorio de Windows nos aseguraremos de que no queden rastros realizando escaneos con tu antivirus preferido, Spybot, y Malwarebytes, por supuesto "actualizando las bases de firmas" antes de realizar los escaneos.

En caso que el pc tenga tiempo ya instalado el sistema operativo, sería conveniente hacer "Desfragmentación" al disco duro (ya que estamos liados). No se eliminaran datos, digamos serán ordenados y agrupados de forma que no queden espacios entre ellos . Es una tarea simple y eficaz para mantener tu disco ordenado:

Inicio → Panel de control → Herramientas administrativas → Administración de equipos

Nos mostrará la siguiente ventana, en la etiqueta "Almacenamiento" clicka sobre el texto "Desfragmentador de discos" y listará los discos instalados. Haremos un click sobre la unidad (C:) y se activarán los botones para analizar el disco y comprobar si necesita ser desfragmentado o desfragmentar directamente. Esto dependerá como hemos dicho antes del tiempo que lleves con Windows instalado, la cantidad de archivos alojados o si has realizado alguna vez una desfragmentación. Puedes recibir el mensaje de que no se necesita desfragmentar el disco.



Espero les pueda ayudar en algo este tutorial pues aun siendo una infección diferente, los pasos a seguir para la desinfección pueden ser similares a los aquí expuestos.

Un saludo ☺

R32 – Usuario del foro de seguridad: http://www.infomalware.net/

[++]