protegemos su mundo digital

Script de servicio en ESET SysInspector

c/ Martínez Valls 56, bajos-46870 Ontinyent (Valencia)
ayuda@eset.es - Teléfono 902.33.48.33
Fax 96.191.03.21 http://www.eset.es

Título del documento:	Script de servicio en ESET SysInspector
Nombre del archivo del documento:	Script_sysinspector.pdf
Versiones del producto compatibles:	SysInspector 1.x
Fecha de creación:	08/07/2010
Fecha de modificación:	08/07/2010
Estado del documento:	Por Revisar
Versión del documento:	2.1

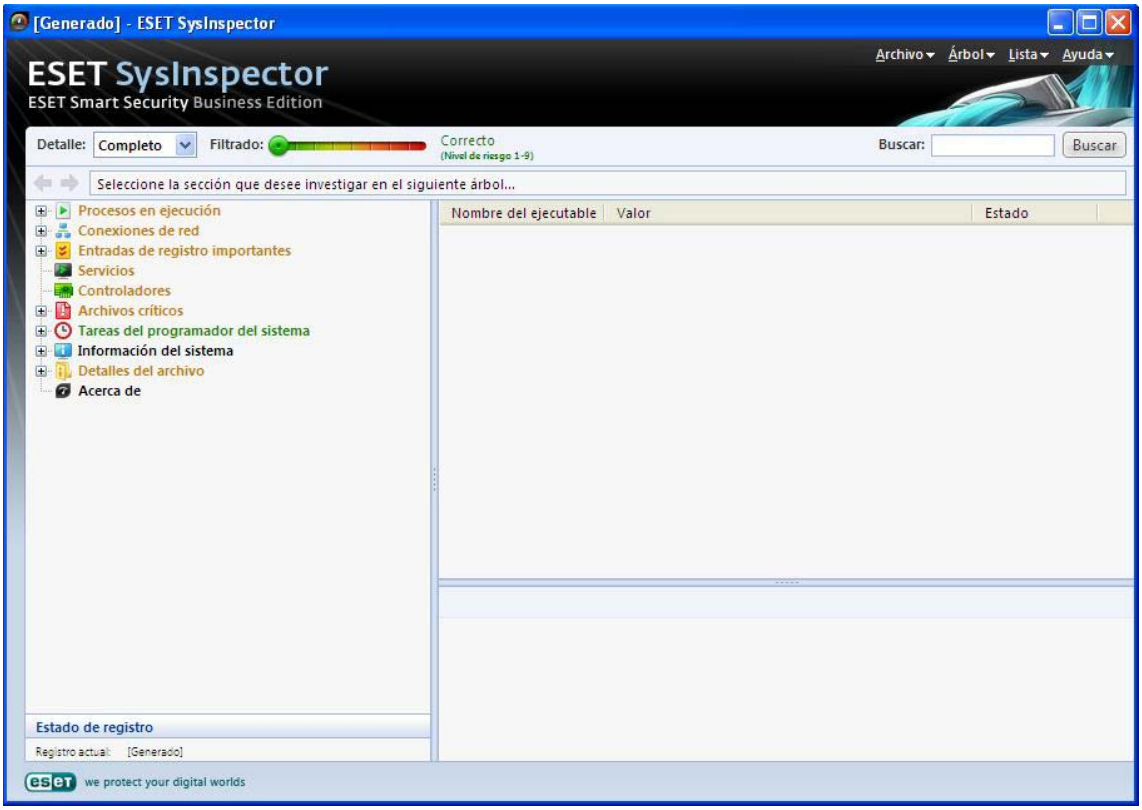
Tabla de contenido

Introducción

El script de servicio es una herramienta avanzada que ofrece asistencia a los clientes que utilizan ESET SysInspector. Sirve para eliminar objetos no deseados del sistema.

El script de servicio permite al usuario exportar el registro completo de ESET SysInspector o únicamente las partes seleccionadas. Tras la exportación, puede marcar los objetos que desee eliminar. A continuación, puede ejecutar el registro modificado para eliminar los objetos marcados.

El script de servicio es útil para usuarios avanzados con experiencia previa en el diagnóstico de problemas del sistema. Las modificaciones realizadas por usuarios sin experiencia pueden impedir el funcionamiento del sistema operativo.



Ejemplo

Si tiene la sospecha de que el ordenador está infectado por un virus que el antivirus no detecta, siga las siguientes instrucciones:

- Ejecute **ESET SysInspector** para generar una nueva instantánea del sistema.

- Seleccione el primer elemento de la sección que se encuentra a la izquierda (en la estructura de árbol), pulse **Ctrl** y seleccione el último elemento para marcarlos todos.

- Suelte la tecla **Ctrl**.

- Haga clic con el botón secundario en los objetos seleccionados y elija la opción **Exportar las secciones seleccionadas al script de servicio en el menú contextual**.

- Los objetos seleccionados se exportarán a un nuevo registro.

- Este paso es el más importante de todo el procedimiento: abra el registro nuevo y cambie el atributo **-** a **+** para todos los objetos que desee eliminar. Asegúrese de no marcar ninguno de los objetos necesarios para el correcto funcionamiento del sistema.

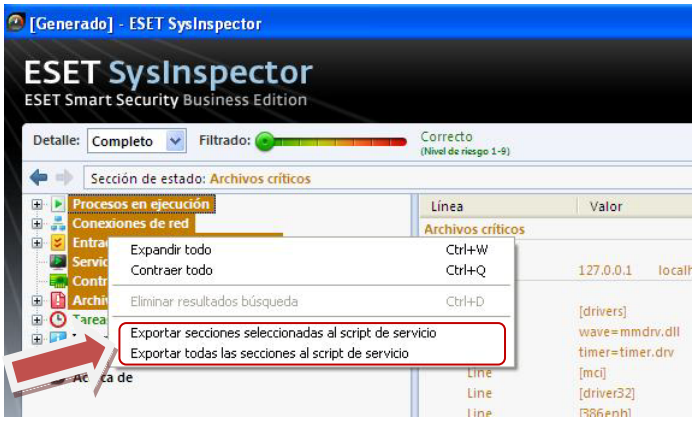
- Abra ESET SysInspector, haga clic en **Archivo - Ejecutar script de servicio** e introduzca la ruta del script.

- Haga clic en **Aceptar** para ejecutar el script

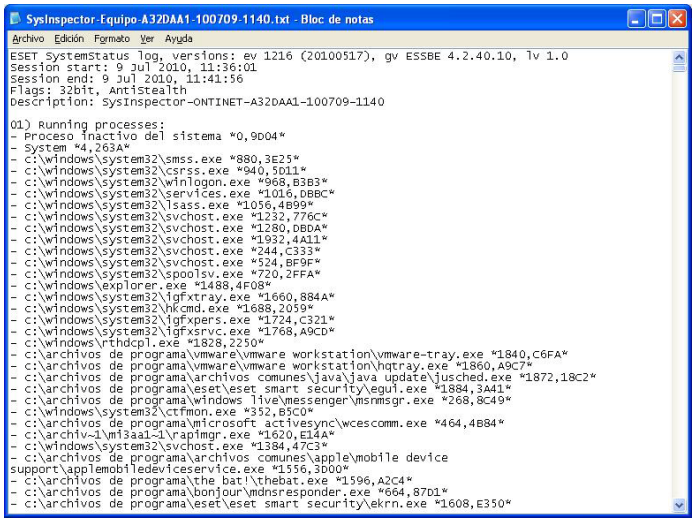
Paso a paso

Generación de scripts de servicio

Para generar un script de servicio, haga clic con el botón secundario en cualquier elemento del árbol de menús (en el panel izquierdo) de la ventana principal de ESET SysInspector. En el menú contextual, seleccione la opción **Exportar todas las secciones al script de servicio** o la opción **Exportar las secciones seleccionadas al script de servicio**.



NOTA: Cuando se comparan dos registros, el script de servicio no se puede exportar.



Cambie el atributo **-** a **+** para todos los objetos que desee eliminar. Asegúrese de no marcar ninguno de los objetos necesarios para el correcto funcionamiento del sistema.

01) Running processes (Procesos en ejecución)

En esta sección se incluye una lista de todos los procesos que se están ejecutando en el sistema. Cada proceso se identifica mediante su ruta UNC y, posteriormente, su código hash CRC16 representado mediante asteriscos (*).

Ejemplo:

01) Running processes:
*- \SystemRoot\System32\smss.exe *4725**
*- C:\Windows\system32\svchost.exe *FD08**
*+ C:\Windows\system32\module32.exe *CF8A**
[...]
En este ejemplo se ha seleccionado (marcado con el carácter "+") el proceso module32.exe, que finalizará al ejecutar el script.

02) Loaded modules (Módulos cargados)
En esta sección se listan los módulos del sistema que se utilizan actualmente.

Ejemplo:

02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
En este ejemplo, se marcó el módulo khbekhb.dll con el signo "+". Cuando se ejecute, el script reconocerá los procesos mediante el módulo específico y los finalizará.

03) TCP connections (Conexiones TCP)

En esta sección se incluye información sobre las conexiones TCP existentes.

Ejemplo:

03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
*- Listening on *, port 135 (epmap), owner: svchost.exe*
*+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:*
System
[...]
Cuando se ejecute, el script localizará al propietario del socket en las conexiones TCP marcadas y detendrá el socket, liberando así recursos del sistema.

04) UDP endpoints (Puntos finales UDP)

En esta sección se incluye información sobre los puntos finales UDP.

Ejemplo:

04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)

[...]

Cuando se ejecute, el script aislará al propietario del socket en los puntos finales UDP marcados y detendrá el socket.

05) DNS server entries (Entradas del servidor DNS)

En esta sección se proporciona información sobre la configuración actual del servidor DNS.

Ejemplo:

05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]

Las entradas marcadas del servidor DNS se eliminarán al ejecutar el script.

06) Important registry entries (Entradas de registro importantes)

En esta sección se proporciona información sobre las entradas de registro importantes.

Ejemplo:

06) Important registry entries:
** Category: Standard Autostart (3 items)*
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe /c
** Category: Internet Explorer (7 items)*
HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]

Cuando se ejecute el script, las entradas marcadas se eliminarán, reducirán a valores de 0 bytes o restablecerán en sus valores predeterminados. La acción realizada en cada entrada depende de su categoría y del valor de la clave en el registro específico.

07) Services (Servicios)

En esta sección se listan los servicios registrados en el sistema.

Ejemplo:

07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup: Automatic

- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup: Manual
[...]

Cuando se ejecute el script, los servicios marcados y los servicios dependientes se detendrán y desinstalarán.

08) Drivers (Controladores)

En esta sección se listan los controladores instalados.

Ejemplo:

08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]

Cuando se ejecuta el script, se anula el registro del sistema de los controladores seleccionados, que después se eliminan.

09) Critical files (Archivos críticos)

En esta sección se proporciona información sobre los archivos críticos para el correcto funcionamiento del sistema operativo.

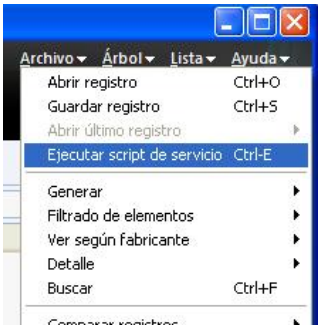
Ejemplo:

09) Critical files:
** File: win.ini*
- [fonts]
- [extensions]
- [files]
- MAPI=1
[…]
** File: system.ini*
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[…]
** File: hosts*
- 127.0.0.1 localhost
- ::1 localhost
[…]

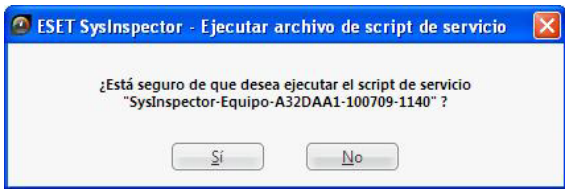
Los elementos seleccionados se eliminarán o restablecerán en sus valores originales.

Ejecución de scripts de servicio

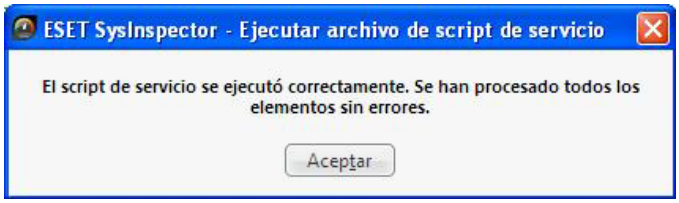
Seleccione todos los elementos que desee y, a continuación, guarde y cierre el script. Ejecute el script modificado directamente desde la ventana principal de ESET SysInspector, con la opción Ejecutar el script de servicio del menú Archivo.



Cuando abra un script, el programa mostrará el mensaje siguiente: **¿Está seguro de que desea ejecutar el script de servicio "%Scriptname%"?** Una vez que haya confirmado la selección, es posible que se muestre otra advertencia para informarle de que el script de servicio que intenta ejecutar no está firmado. Haga clic en **Ejecutar** para iniciar el script.

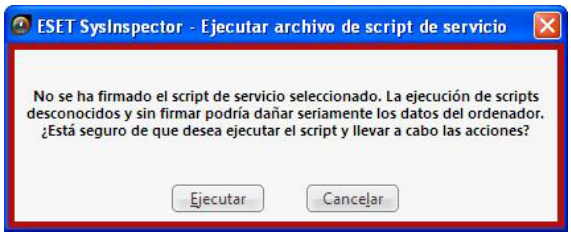


Se mostrará una ventana de diálogo para confirmar la correcta ejecución del script.



Si el script no se puede procesar por completo, se mostrará una ventana de diálogo con el mensaje siguiente: **El script de servicio se ejecutó parcialmente. ¿Desea ver el informe de errores?** Seleccione Sí para ver un informe de errores completo con todas las operaciones que no se ejecutaron.

Si no se reconoce el script, aparece una ventana de diálogo con el mensaje siguiente: **No se ha firmado el script de servicio seleccionado. La ejecución de scripts desconocidos y sin firmar podría dañar seriamente los datos del ordenador. ¿Está seguro de que desea ejecutar el script y llevar a cabo las acciones?** Esto podría deberse a que el script presenta inconsistencias (encabezado dañado, título de sección dañado, falta línea vacía entre secciones, etc.).Vuelva a abrir el archivo del script y corrija los errores o cree un script de servicio nuevo.



Para cualquier tipo de consulta técnica rogamos se ponga en contacto con nuestro departamento técnico en la siguiente dirección de correo electrónico:

ayuda@eset.es

Soporte técnico de Ontinet.com

Síguenos en Twitter

Ontinet.com distribuidor exclusivo de los productos ESET en España.