

SysConfig.

Aplicación para revertir los cambios efectuados en el sistema después de haberse contaminado con el programa maligno W32.EFECTO.A. o W32.EFECTO.B. (Ver Anexo 1).

Este programa finaliza los procesos relacionados con W32.EFECTO.A. o W32.EFECTO.B si están en ejecución y restablece las restricciones que aplican los programas malignos en el sistema.

Forma de uso:

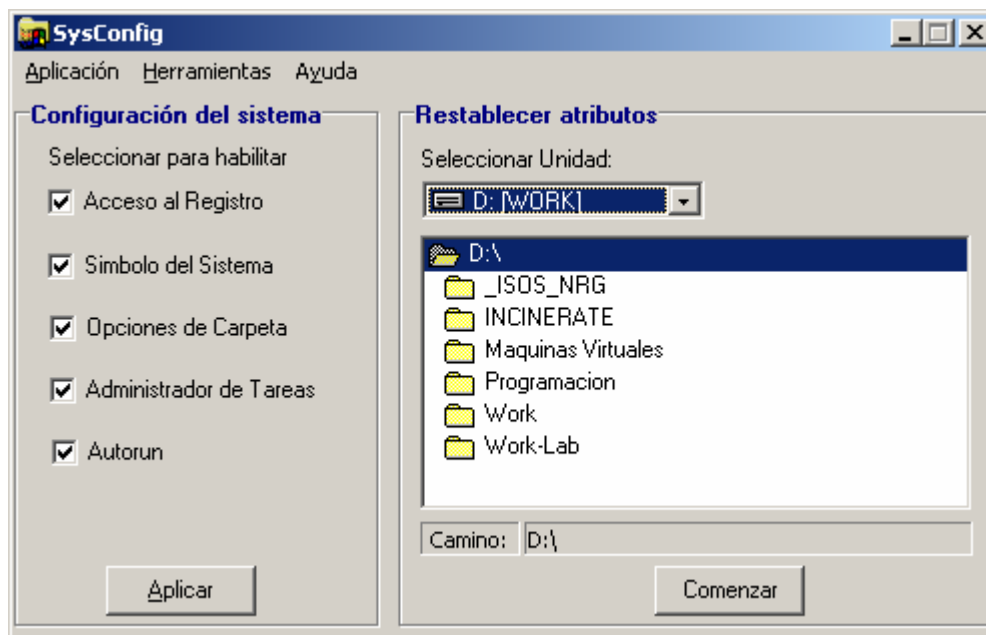


Figura 1: Ventana principal del programa

- El panel de la izquierda (Configuración del sistema, figura 1.) permite restablecer las modificaciones que el programa maligno realizó en el registro para impedir el acceso a algunas funciones o herramientas del sistema.

Si la casilla de verificación correspondiente a cualquiera de las opciones está seleccionada cuando se presiona el botón Aplicar, la opción relacionada quedará habilitada, de lo contrario se deshabilita. Esta acción también restablece la configuración del servicio de cola de impresión y elimina el valor del registro que garantiza la ejecución del programa maligno cada vez que se inicializa el sistema.

La casilla Autorun es una opción adicional que permite habilitar o deshabilitar esta característica del sistema. Por motivos de seguridad es recomendable no seleccionarla para eliminar una de las posibles vías de contaminación por programas de este tipo (la utilizada por W32.EFECTO.A. o W32.EFECTO.B), aunque si lo hace debe tener en cuenta que para acceder al contenido de los CDs de multimedia, CDs de instalación de software, etc, debe hacerse a través de Mi PC o del explorador de Windows ya que la aplicación que se encarga de esta función no se ejecutara al insertar el dispositivo.

- El panel de la derecha (Restablecer atributos) permite visualizar todos los ficheros y carpetas que el programa maligno ocultó modificando los atributos de los mismos. La unidad de disco en la que desee revertir los cambios debe ser seleccionada en la lista desplegable que aparece al presionar click sobre la flecha. Ver figura 2.

Para ejecutar esta acción en la unidad de disco seleccionada, debe presionar el botón Comenzar. Si durante el proceso de escaneo para restablecer atributos se encuentra un

fichero relacionado con el programa maligno será eliminado, garantizando que no queden rastro del mismo.

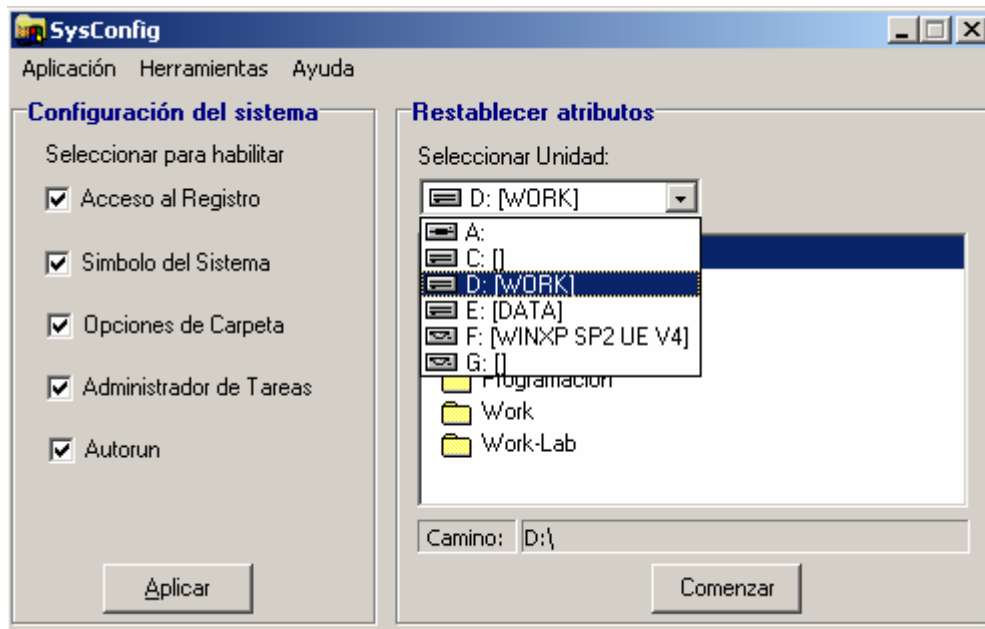


Figura 2. Seleccionando la unidad de disco.

- La consola de comandos (CMD) y el editor de registro (REGEDIT) pueden ser ejecutados desde la aplicación a través del menú Herramientas. Ver Figura 3.

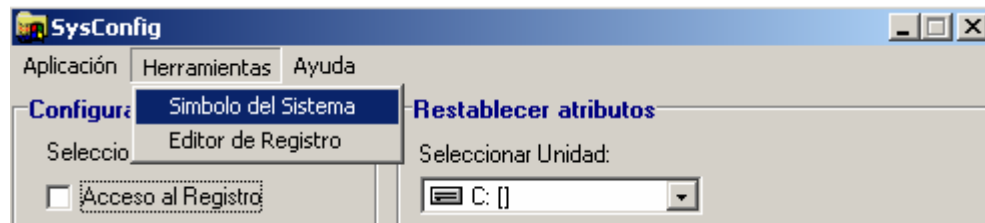


Figura 3. Ejecución de herramientas del sistema.

Notas importantes:

1. El programa fue probado siendo exitoso el resultado en Windows 2000, Windows XP y Windows 2003 Server. En Windows 9x o Me el panel de la izquierda (Configuración del sistema) quedará deshabilitado automáticamente por ejecutar acciones no compatibles con dichos sistemas.
2. Si usted deshabilitó la característica autorun, puede usar nuevamente el programa para volver a habilitarla presionando el botón Aplicar. Las opciones relacionadas deben quedarse seleccionadas (estado por omisión).
3. Después de trabajar con el panel Configuración del sistema debe reiniciar el equipo para que algunos cambios realizados tengan efecto.

Anexo 1. Sobre los programas malignos W32.EFECTO.A. o W32.EFECTO.B.

Crean las siguientes entradas en el registro para ejecutar Win2x.exe al inicio del sistema y Save.exe durante la ejecución de cualquier tarea de impresión:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
Win2x: %SystemRoot%\system32\Win2x.exe
```

```
HKLM\SYSTEM\ControlSet003\Services\Spooler  
ImagePath: %SystemRoot%\system32\save.exe
```

Modificando o creando otras llaves del registro inhabilitan el acceso al Editor de Registro (REGEDIT) de Windows y al Administrador de Tareas. Impide la ejecución de cajas de diálogo MSDOS, inhabilita el acceso al comando CMD y ocultan las opciones de carpeta (disponible en el menú Herramientas del Explorador de Windows).

Ocultan las carpetas de la raíz de los discos y cambian sus atributos a Readonly, Hidden y System.

Crean una gran cantidad de copias del troyano en la raíz de los discos con iconos de carpeta y nombres similares a los de las carpetas existentes para proporcionar la reinfección del sistema utilizando al propio usuario.

A cerca de...

Programa para revertir los cambios efectuados en el sistema por la contaminación con los programas malignos W32.EFECTO.A. o W32.EFECTO.B.

Copyright © 2007. Yusleivi Mompeller Aguiar
Especialista en seguridad informática.
Grupo soporte técnico. Segurmatica

Email: yusleivi@segurmatica.cu