

## Infecciones con código malicioso: Qué buscar y cómo superar la crisis

La mayoría de los usuarios de ordenadores han experimentado alguna forma de infección con código malicioso en algún momento. Si bien existen muchas herramientas que ayudan a automatizar el proceso de detección, contención y eliminación de amenazas, existen también algunos pasos simples y prácticos que los usuarios pueden realizar, y que no involucran programas sofisticados.

Con un poco de conocimiento, algunas herramientas gratuitas y un pequeño esfuerzo, los usuarios de ordenadores pueden aislar, de manera relativamente sencilla, las amenazas y asegurarse que su ordenador, por lo menos, no pueda infectar otros equipos. En este artículo, hablaremos acerca de los métodos de primeros auxilios para detectar y eliminar, de forma manual, programas maliciosos de un ordenador, y preparar el sistema para una inspección más completa con el antivirus y/o aplicación contra programas espía.

### Introducción

Como estoy estrechamente vinculado con los ordenadores y los programas de seguridad, a menudo mis amigos me piden que los visite y vea si sus equipos están protegidos contra código malicioso. Muchos de ellos no se toman en serio el tema de la seguridad y piden ayuda cuando hay un problema serio, como por ejemplo cuando el ordenador está muy lento o no se puede utilizar en absoluto. Aunque realmente no estoy de acuerdo con este tipo de enfoque a la seguridad, siempre termino ayudándolos. Mi experiencia directa con muchos de los problemas en los ordenadores que he visto, me ha llevado a escribir este artículo.

La siguiente información explica cómo utilizar las herramientas y programas utilitarios gratuitos disponibles para contener o desactivar las amenazas, incluso aquellos integrados con Windows o descargables de forma gratuita desde Internet.

Estas herramientas pueden almacenarse fácilmente en una unidad portable USB y ser llevadas al ordenador infectado.

### Desactivación temporaria de código malicioso

Existen diversas situaciones que podrían indicar la presencia de código malicioso en un ordenador:

- Rendimiento lento,
- Fallas al iniciar o cerrarse,
- Programas extraños que se cargan cuando Windows se inicia,
- Comportamiento inesperado o errático de los programas instalados.

Cualquiera de estas situaciones, u otro comportamiento inusual del equipo, puede indicarle que el código malicioso es el culpable. Básicamente, desactivar una amenaza tiene dos pasos:

1. Cerrar el código malicioso en la sesión actual de Windows.
2. Evitar que el código malicioso vuelva a cargarse en sucesivos sesiones.

### Primer paso

Para cerrar el código malicioso activo, debe conocer la lista de todos los programas que están funcionando actualmente en su ordenador. De esta forma, puede elegir cuál quiere desactivar y así puede "matar" al programa perjudicial. Para ver la lista de todos los programas que están funcionando actualmente en su sistema:

1. Presione al unísono las teclas **Ctrl + Alt + Supr** (*Ctrl+Alt+Del*) (Control + ALT izquierda + Suprimir) y se abrirá el **Administrador de tareas de Windows**.
2. Pulse en la pestaña **Procesos**.

Puede ordenar las entradas, en las columnas del *Administrador de tareas*, para visualizar las mismas en orden alfabético ascendente o descendente.

Es posible cerrar programas que se están ejecutando si pulsa con el botón derecho del ratón en la tarea objetivo, y posteriormente selecciona el comando **Finalizar tarea**.

Tenga cuidado al cerrar programas de esta forma, ya que si se finaliza, por error, una aplicación equivocada, como por ejemplo, *svchost.exe*, que es esencial en Windows, el sistema se cerrará de emergencia, lo que resultaría en una posible pérdida de los datos sin guardar.

Recomiendo que realice una investigación preliminar del programa que está intentando detener, en el **Administrador de tareas**, antes de proceder a su cierre forzado.

Por ejemplo puede realizar una búsqueda en [Google](#) con el nombre del archivo ejecutable o yendo al portal de [Librerías de procesos](#) para obtener más información acerca de las tareas que realiza dicho proceso.

Si efectúa este procedimiento para el archivo *svchost.exe* recibiría los siguientes [resultados](#), los que muestran que el programa es legítimo y no debería cerrarse.

Por otro lado, si ve un programa con un nombre como *msblast.exe*, un [virus conocido](#) que está en ejecución en su ordenador, es una indicación segura de un problema serio y el programa debería cerrarse inmediatamente.

Si bien el **Administrador de tareas** es útil para verificar, de manera sencilla, los programas activos, no puede decirle dónde encontrar el archivo ejecutable en su ordenador o qué aplicación hizo que se iniciará la tarea.

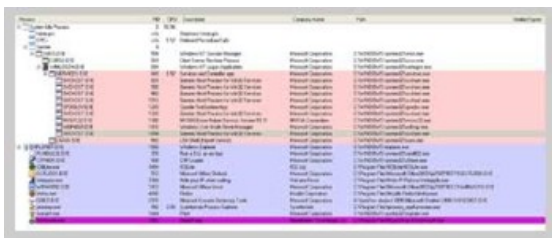
Para una mirada más detallada de las tareas activas, recomiendo utilizar el **Explorador de procesos**, un programa utilitario gratuito disponible desde el sitio de Internet [Sysinternals](#).

En el **Explorador de procesos** cuenta con una vista mucho más detallada de la actividad del sistema.

Si elige las columnas adecuadas en el menú **Ver**, podrá visualizar la ruta de todos los archivos ejecutables que están funcionando, el nombre de su publicador y descripciones importantes del programa.

En conjunto, esto debería brindar información suficiente acerca de la autenticidad de cualquier aplicación que se está ejecutando para determinar su legitimidad.

Puede organizar los datos ordenando a través de cualquiera de las columnas.



Al pulsar con el botón derecho del ratón en la tarea seleccionada y elegir **Google**, será llevado a la página de resultados de la consulta del motor de búsqueda para el ejecutable especificado.

Si elige **Mostrar árbol de procesos** (cuarto icono desde la izquierda), verá una jerarquía de eventos y las aplicaciones iniciales. Si observa detenidamente, verá que la mayoría de las tareas que se están ejecutando son productos de Microsoft y ese es un gran paso para resolver el problema.

Observe los programas que no sean de Microsoft, particularmente si son de origen sospechoso o si no sabe por qué se están ejecutando. Controle especialmente las aplicaciones que no tienen información en el campo publicador.

La mayoría de los desarrolladores de código malicioso no se preocupan en completar este campo, por lo tanto, esa es una pista importante de que el programa en cuestión puede ser ilegal.

El **Explorador de procesos** una vez me ayudó a ubicar el virus *Mrak5* que se llamaba a sí mismo *svchost.exe*. Sin embargo, a diferencia del proceso legítimo con este nombre (con múltiples instancias ejecutándose al mismo tiempo), se inició desde otro lugar diferente al del ejecutable original y no mostraba la identidad del nombre de la compañía.

El **Administrador de tareas** no hubiera podido ayudarme en esta situación, aunque sí noté que el nombre aparecía en mayúsculas, que no es lo habitual.

Al igual que con el **Administrador de tareas**, puede finalizar un proceso, en el **Explorador de procesos**, utilizando los comandos del menú contextual.

Este programa también le permite realizar otras acciones realmente útiles como listar todas las librerías (DLL) que se están ejecutando y que pertenecen a un proceso, o realizar un seguimiento de una asignación de recursos para una aplicación en particular. Pero eso es bastante más avanzado y no necesitamos ir al detalle, si solamente queremos saber qué se está ejecutando y si es legítimo.

## Eliminar la capacidad de que el código malicioso se inicie automáticamente

Ahora que sabemos cómo derrotar al código malicioso de manera local, en una sesión actual de Windows, el próximo paso es evitar que vuelva a cargarse automáticamente la próxima vez que se inicie el sistema.

### Segundo paso

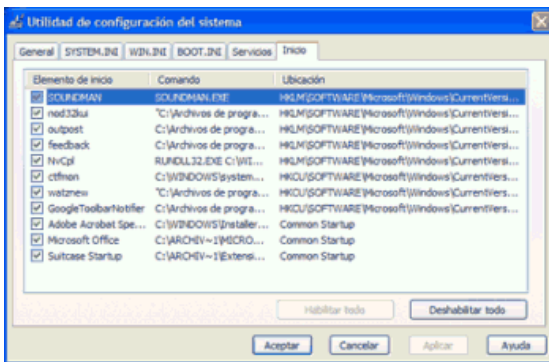
Una herramienta integrada de Windows, llamada **Utilidad de configuración del sistema**, está diseñada para brindar a los usuarios una manera flexible de configurar la forma en que el sistema comienza y cuáles programas se cargan en el inicio.

1. Pulse en el menú **Inicio**.
2. Seleccione el comando **Ejecutar**.
3. Escriba **msconfig** y presione el botón **Aceptar**.
4. Se abre una nueva aplicación denominada **Utilidad de configuración del sistema**.
5. Recorra sus pestañas para descubrir sus posibilidades.

Simplemente desactivando la línea correspondiente, el objeto seleccionado se elimina de la ejecución automática. Cuando revisé el ordenador de mi amigo el otro día y encontré que había sido infectado por un programa espía llamado *WhenU*, utilicé esta herramienta para desactivar dos objetos. De esta forma el programa espía no podría reiniciarse y borré, de forma manual, todos los objetos relacionados del disco duro.

Una vez más, puede realizar una búsqueda en Internet de información adicional acerca del programa que está pensando en desactivar. Si resulta que realizó alguna acción equivocada, puede deshacerla simplemente volviendo a marcar la casilla del objeto que desactivó anteriormente.

Al igual que con cualquier tarea que involucra el cambio de configuraciones, es aconsejable realizar una copia de seguridad primero, para que pueda restaurarse fácilmente si algo sale mal.



Para realizar esto, puede utilizar el programa **Restauración del sistema**:

1. Pulse en el menú **Inicio**.
2. Seleccione el comando **Ejecutar**.
3. Escriba “**%SystemRoot%\system32\restore\rstrui.exe**” y presione el botón **Aceptar**.

Incluya las comillas de apertura y cierre de la instrucción.

Este programa permite crear un punto de restauración, antes que decida realizar algún cambio significativo al sistema y podrá volver a la configuración anterior al momento de la copia de seguridad, de ser necesario.

Puede encontrar [detalles adicionales](#) en el sitio de Microsoft.



En la solapa **Servicios** de *msconfig.exe* también puede seleccionar cuáles servicios quiere iniciar al mismo tiempo que Windows. Marque la entrada **Ocultar todos los servicios de Microsoft** para ver una lista de otros servicios que no sean de Microsoft, que quizás considere desactivar.

Una vez más, sea precavido y utilice un motor de búsqueda para averiguar los servicios que se están ejecutando que no fueron desarrollados por Microsoft.

Hacer esto en otras oportunidades, me ha permitido desactivar un virus conocido que se estaba ejecutando automáticamente, utilizando el nombre habitualmente de confianza **Servicio de corrección de errores del protocolo TCP**. Un programa muy potente, pero al mismo tiempo fácil de usar, para configurar las propiedades de inicio es la aplicación **Ejecuciones automáticas** de Sysinternals.

Las solapas útiles para la mayoría de los usuarios serían **Inicio** y **Servicios**. El programa presenta diversas opciones de personalización, lo que le permitirá modificar todo, hasta los mínimos detalles.

## Resumen

Los antivirus y las aplicaciones contra programas espía son esenciales para la seguridad en línea, así como también el uso de un cortafuegos bi-direccional potente como Outpost Firewall Pro.

Pero además, el conocimiento acerca de cómo utilizar las herramientas sencillas del sistema, es una información de respaldo valiosa de tener cuando, por algún motivo, no puede acceder o utilizar sus herramientas de seguridad habituales.