La infección

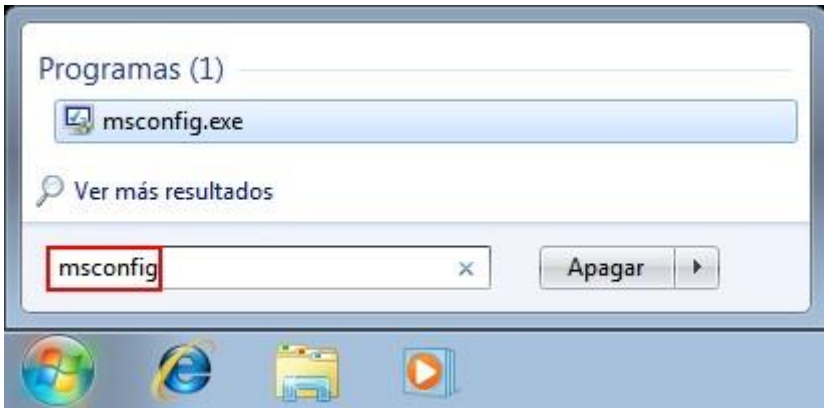
Esta tarea suele ser la más complicada de determinar de forma efectiva ya que la mayoría de las actuales amenazas suelen no llamar la atención para así evitar ser eliminadas. **Existen muchos factores o "pistas" que nos pueden llevar a la conclusión de que nuestro equipo se encuentra comprometido**, entre ellas las siguientes:

- Lentitud repentina en el procesamiento del equipo.
- Apertura de ventanas o programas sin que esto sea indicado por el usuario.
- Funcionalidades o programas deshabilitados (Administrador de tareas, Registro de Windows, etc).
- Notable lentitud al navegar por Internet o realizar descargas.
- Alertas de seguridad por parte del sistema operativo o de falsas soluciones antivirus.
- Imposibilidad de iniciar el sistema operativo tanto en "modo normal" como en "modo seguro".
- Redirecciones a sitios web de aspecto dudoso.
- Cambio del fondo de escritorio del sistema operativo u otro aspecto estético.
- Correos enviados desde nuestra propia casilla de correo sin nuestra autorización.

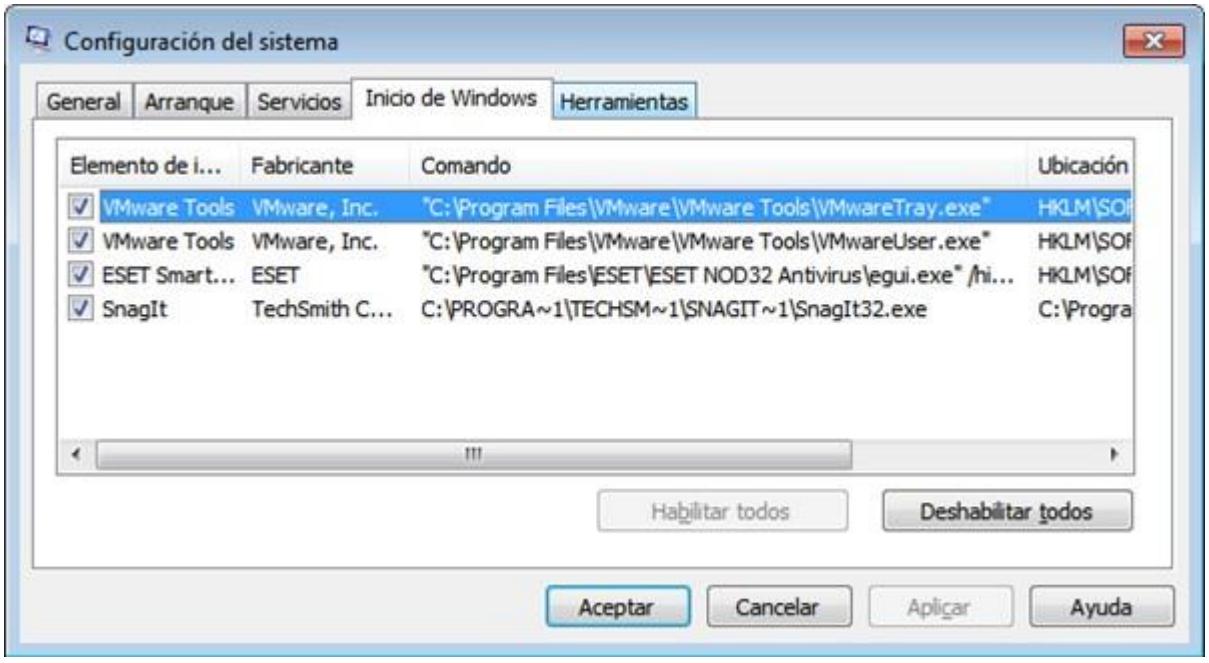
Cabe aclarar que **estos posibles "síntomas" pueden también ser producto de problemas de hardware o del sistema operativo** y no necesariamente estar vinculados a una infección. Es por esto por lo que se recomienda descartar dichas posibilidades antes de proceder.

Identificar la infección

Una vez que se determinó que efectivamente el equipo se encuentra infectado deberemos determinar dónde se encuentra la infección y qué acciones maliciosas realiza la misma. Existen varias formas de determinar esto, entre ellas **revisar los procesos que se cargan al iniciar el sistema operativo**. Para realizar lo antes mencionado, primero se deberá abrir la "*Utilidad de Configuración de sistema de Windows* ", por lo que se debe hacer clic en el botón de "*Inicio*" de Windows para luego escribir "*msconfig*" en la barra de búsqueda como se muestra en la imagen a continuación:



Al presionar la tecla "*Enter*" se iniciará dicha aplicación, donde deberemos seleccionar la solapa "Inicio de Windows". Allí podremos observar todos aquellos procesos que son ejecutados al iniciar nuestro sistema operativo:



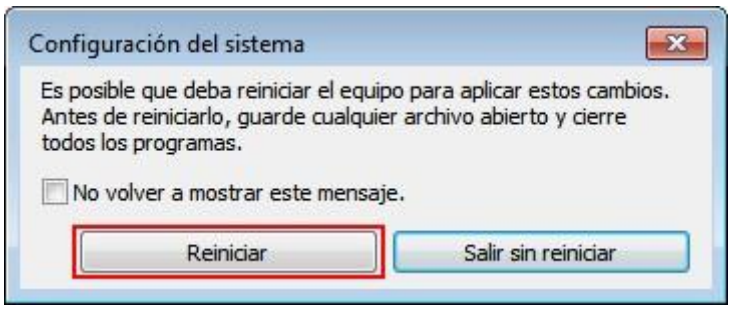
Es muy importante poder reconocer todos los elementos aquí detallados ya que de esta forma podremos determinar rápidamente si existe alguna amenaza entre ellos. En este caso se observan los siguientes programas:

- 2 procesos llamados VMware Tools (VMwareTray.exe y VMwareUser.exe) – Herramientas de la máquina virtual donde realice la captura.
- ESET Smart Security (egui.exe) – Interfaz gráfica de la solución antivirus.
- Snagit (SnagIt32.exe) – Programa que utilice para realizar las capturas.

Como pueden ver, todos los procesos son fácilmente identificables. En el caso de que aquí existiera un archivo no reconocido por el usuario, existe una posibilidad de que esa es la amenaza. Una fácil forma de verificar esto es mediante la utilización del servicio en línea que brinda VirusTotal, donde **permite subir el archivo en cuestión a sus servidores para que éste luego lo analice con 43 motores antivirus**.

De ser detectado por alguno/s de dichos motores se deberá destildar dicho proceso para así evitar que el mismo se inicie automáticamente en el próximo reinicio. Luego se deberá hacer clic en "*Aplicar*" y luego "*Aceptar* ".

Inmediatamente se presentará la siguiente pantalla:



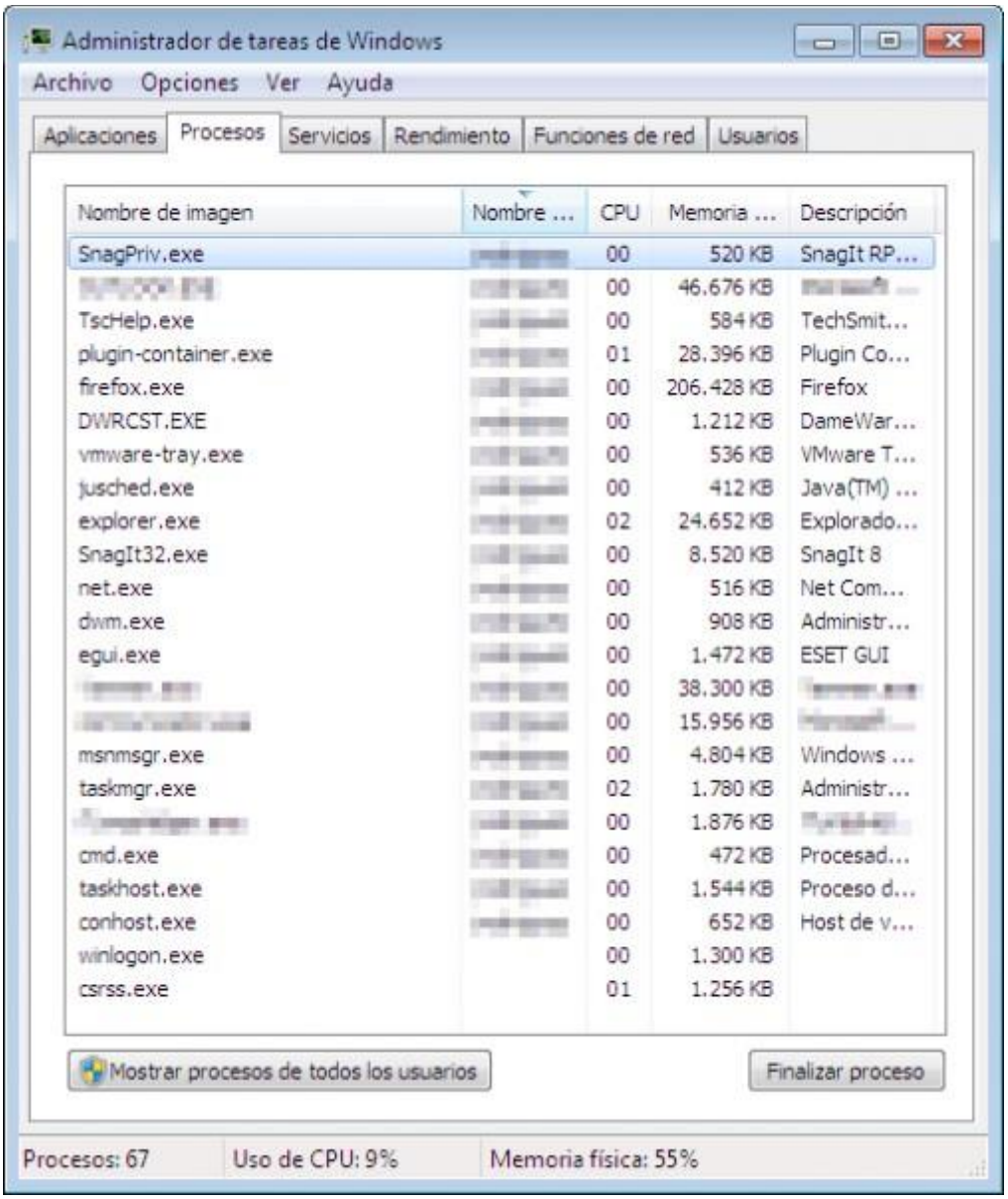
Se deberá reiniciar el equipo para que se apliquen los cambios y así evitar que la amenaza se vuelva a cargar.

Adicionalmente se recomienda eliminar de forma manual dicho archivo y vaciar la papelera de reciclaje.

Existe la posibilidad de que la amenaza que nos haya afectado no permita la apertura de *Msconfig*, por lo que deberemos recurrir al editor de registro (*RegEdit*), al administrador de procesos (*TaskManager*) o, dependiendo de la cantidad de servicios afectados, incluso de un Live CD/DVD/USB. De igual manera **estos casos serán tratados en la segunda entrega de este post**.

Eliminar la infección

Como indicamos anteriormente, se deberá eliminar la amenaza manualmente una vez identificada la misma y siempre y cuando ésta no se encuentre en ejecución. Caso contrario se deberá abrir el "Administrador de tareas" (*Ctrl+Alt+Supr*), buscar el nombre que la identifica y luego hacer clic en "*Finalizar proceso* ". A continuación, una captura representativa:



En caso de que aun así no se pueda eliminar la misma se deberá ingresar al sistema en "Modo seguro" para intentarlo desde allí. Una vez realizado esto **se deberá analizar el equipo con una solución antivirus**, de no poseer una instalada, se puede optar por utilizar por ejemplo ESET Online Scanner y/o Kaspersky Virus Removal Tool.

Prevenir la reinfección

Se recomienda instalar una solución antivirus con detección proactiva al igual que mantener el sistema operativo y las aplicaciones instaladas con las actualizaciones al día. Adicionalmente **es altamente recomendable mantenerse informado en materia de seguridad y malware** para así conocer las últimas tendencias y posibles vectores de ataque.
En conclusión, existen muchos métodos o comprobaciones que se pueden realizar para determinar fehacientemente si nuestro equipo fue comprometido o no, por lo cual los invitamos a realizarlos. La seguridad de nuestro equipo es un tema serio que debe ser considerado para evitar que nuestros datos y privacidad sean expuestos.

Servicios bloqueados

Es muy normal que una amenaza realice modificaciones al registro de Windows, no solo para garantizar su posterior ejecución, sino también para evitar ser removido de manera sencilla del sistema. Entre estos servicios, los que suelen ser afectados son:

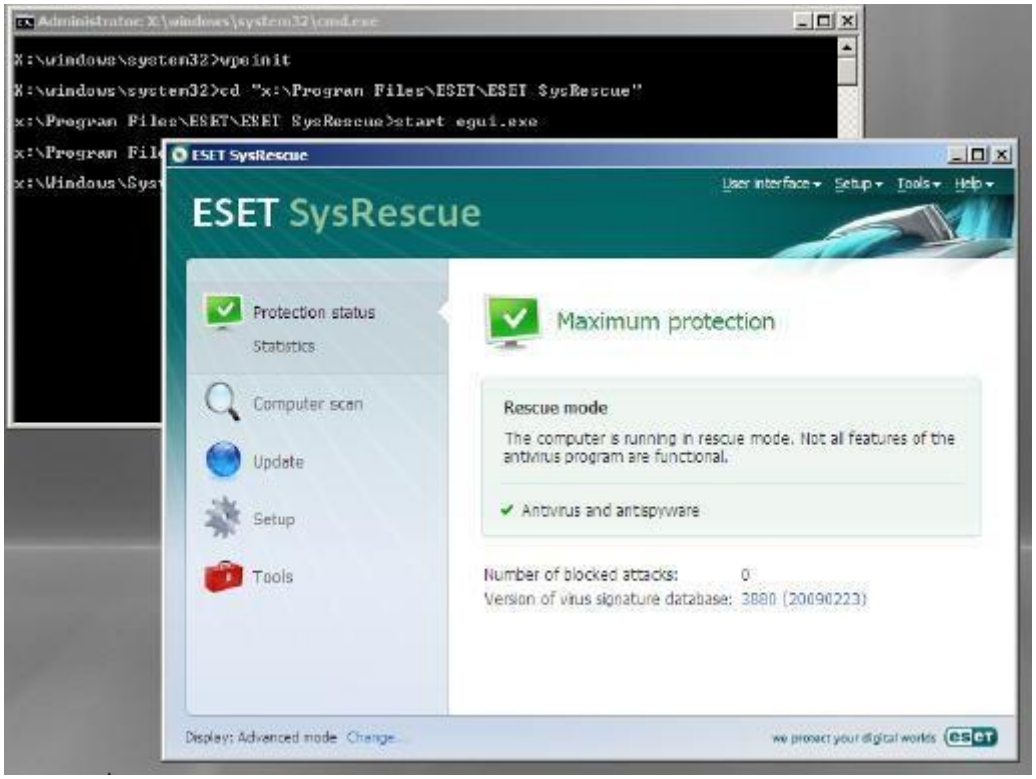
- Administrador de Tareas (Task Manager)
- Registro de Windows (Windows Registry)
- Utilidad de Configuración de sistema de Windows (MsConfig)
- Navegadores de Internet (Firefox, Internet Explorer)

De esta forma, la amenaza, limita de forma considerable las posibilidades de que el usuario pueda eliminarla del sistema. Más allá de esto, **existen herramientas de análisis automatizado que buscan cualquier incongruencia dentro del registro de Windows y posteriormente las solucionan**. Una de ellas, gratuita y de alto rendimiento, es CCleaner, la cual luego de realizar el análisis permite tomar acción sobre cada uno de los problemas encontrados.
También existe la posibilidad de que la amenaza bloquee la ejecución de ciertas aplicaciones, como es CCleaners y otras herramientas de seguridad, por lo que se deberá recurrir, como mencionamos en el post anterior, a un Live CD/DVD/USB.

Alternativas de limpieza

Un Live CD es básicamente un sistema operativo booteable, es decir que se inicia directamente desde una unidad óptica o USB. De esta forma **es posible poder analizar el disco duro como a un medio extraíble** y así solucionar cualquier problema que afecte al mismo sin preocuparnos por procesos corriendo en memoria o aplicaciones bloqueadas.

ESET y Kaspersky ofrecen una solución de este tipo denominada ESET SysRescue / Kaspersky Rescue Disk, la cual es creada desde cualquier solución para Windows y puede ser utilizada en cualquier equipo.



Para utilizar la misma se debe ingresar el CD/DVD o USB en el equipo y luego se deberá presiona la tecla F8 (o la que corresponda según el BIOS del equipo) para así seleccionar dicha unidad. Esta selección también puede ser realizada desde el *Setup* del BIOS, cambiando el orden de booteo de las unidades, pero se debe tener en cuenta que luego se deberá restablecer el orden original.

Una vez realizado esto, se iniciará una versión de ESET NOD32 Antivirus la cual nos permitirá **analizar el disco como una unidad física externa eliminando cualquier amenaza que allí resida**.

Luego se deberá reiniciar el equipo e iniciarla en modo normal, para poder verificar que la amenaza fue eliminada y no quedan rastros de esta.

Son varias las metodologías que pueden ser utilizadas para solventar un problema de infección, sin la necesidad de formatear el equipo, pero es mejor aún prevenir este tipo de dificultades mediante la utilización de una solución antivirus