Virus y otras amenazas en Internet

Le mostramos una lista de los principales programas que pueden resultar nefastos para la salud de su equipo:

Adware: un Adware rastrea sus costumbres en Internet y puede, por ejemplo, mostrar ventanas publicitarias en función del perfil establecido. Multitud de sitios Web pueden instalar este tipo de programa, a sus espaldas.

Drive-by download: se trata de un programa que se descarga sin su consentimiento. Esto puede ocurrir cuando intenta cerrar un cuadro de diálogo.

Redirección de páginas: es un programa que redirigirá una parte o todas las páginas predefinidas (página de inicio, de búsqueda, etc.) hacia un sitio malintencionado.

Spam: e-mail comercial que no se solicita.

Spyware o Programa espía: programa que espía y después transfiere a una tercera persona su información confidencial.

BHOs o *Browser Helper Objects*: son programas que permiten personalizar y controlar algunas configuraciones de un navegador como Internet Explorer. Puede ser creado con fines "pacíficos" (la barra de herramientas que propone Google) o malintencionados.

Dialer: es un programa que creará, además de su conexión predeterminada, una conexión de acceso telefónico con una tarifa extra en la factura.

Troyano o Caballo de Troya: programa que tiene funciones escondidas que se pueden ejecutar en un segundo plano a espaldas del usuario. Permiten acceder al equipo en el que se están ejecutando, ya que abren una puerta secreta (Backdoor).

Virus: es un programa capaz de infectar archivos y propagarse utilizando soportes extraíbles o redes.

Debemos señalar que la frontera entre los diferentes tipos de amenaza no es demasiado precisa y muchos programas maliciosos pueden utilizar diferentes técnicas para extenderse.

1. Eliminación de un virus

Primero debemos recordar algunas reglas esenciales:

- Su antivirus debe mantenerse actualizado constantemente.
- No debe instalar varios antivirus a la vez, ya que podría provocar conflictos en el sistema.
- Que un antivirus sea gratuito no quiere decir que sea menos eficaz que otros productos más costosos.
- A pesar de las afirmaciones de los especialistas y los test que aparecen en las revistas especializadas, todos los antivirus son válidos.
- Existen comportamientos de riesgo y otros que no lo son.

Es una manera de decir que a menudo se trata de una cuestión de sentido común y que con frecuencia aquellos que se quejan de una falta de eficacia de los antivirus, a menudo son los mayores consumidores de sitios para "adultos" y redes peer-to-peer.

Le mostramos un ejemplo clásico para la erradicación de un virus.

- Actualice las definiciones de virus de su antivirus.

Si no puede acceder a Internet, descargue desde otro equipo la lista de definiciones para poder realizar la actualización de manera manual. De hecho, la mayoría de los antivirus poseen un archivo de definiciones que es posible descargar si su antivirus no puede actualizar de manera automática la base de definiciones de virus.

- Desactive el proceso de restauración del sistema de todas las unidades.

En los sistemas NT, este directorio forma parte de las carpetas protegidas. Un antivirus no tiene acceso a ellas, pero un virus es capaz de alojarse en los archivos guardados en este directorio. Dicho de otro modo, no podrá eliminar un virus mientras tenga esta función activada.

- Desconecte la conexión de Internet físicamente, quitando el cable USB o Ethernet.

Ésta es una manera de asegurarse de que el virus no pueda comunicarse con el exterior y utilizar otra información para esconderse de los ojos del antivirus.

- Reinicie en modo seguro.
- Realice una comprobación completa de todas las unidades.

No siempre es posible iniciar un antivirus en el modo seguro, ya que puede que sean necesarios algunos servicios que no se inician en este modo.

- Inicie en modo normal.
- En un motor de búsqueda como Google, lance una búsqueda introduciendo el nombre del virus.

Si busca bien, encontrará páginas y sitios de los fabricantes de antivirus que explican la manera manual de eliminar un virus o Troyano. La mayoría de las veces, consiste en eliminar las entradas que aparecen en el Registro y archivos del Explorador de Windows.

- Una vez esté seguro de que el equipo está "sano" puede reactivar la función de restauración del sistema.

La experiencia nos dice que muchos antivirus no detectan correctamente todas las amenazas y sobre todo las que crean los spywares y algunos Troyanos. No dude en utilizar varios programas de desinfección. Sí, a veces se trata de un verdadero combate.

2. Los antivirus en línea

Las siguientes direcciones permiten hacer un análisis del equipo en línea. Esto nunca debe reemplazar la instalación de un antivirus actualizado correctamente, pero puede ayudarle a detectar un posible problema.

- http://security.symantec.com/sscv6/default.asp?langid=es&venid=sym
- http://housecall.trendmicro.com/es/
- http://home.mcafee.com/Downloads/FreeScan.aspx
- http://www.kaspersky.com/sp/virusscanner
- http://www.bitdefender.es/scan_es/scan8/ie.html

3. Las herramientas especializadas

Se trata de simples archivos ejecutables que le permitirán eliminar un virus específico. La ventaja es que esto le

permite reparar una situación comprometida si su antivirus no está actualizado.

- http://www.symantec.com/es/es/business/security_response/removaltools.jsp
- http://www.avg.com/es.52
- http://www.pandasecurity.com/spain/homeusers/downloads/repair-utilities/
- http://esp.sophos.com/support/disinfection/
- http://www.bitdefender.es/site/Downloads/browseFreeRemovalTool/

4. Desinstalación completa de un antivirus

Si no puede eliminar su antivirus a través de la funcionalidad de eliminación de programas de Windows en el panel de control, tendrá que suprimirlo manualmente.

En la mayoría de casos, necesitará hacerse con un programa especial que puede descargar del sitio del fabricante. Tomemos el ejemplo de los productos Sysmantec: Norton Removal Tool es una herramienta que le permitirá desinstalar todos los productos Norton presentes en el sistema. Antes de continuar, compruebe que dispone de los CD de instalación o de los archivos de instalación descargados de los productos Norton que desea reinstalar. Es compatible con todas las versiones NT de Windows. Puede descargarlo directamente del sitio de la compañía Symantec desde esta dirección: https://www-secure.symantec.com/norton-support/jsp/help-solutions.jsp?docid=kb20080710133834EN_EndUserProfile_en_us&product=home&pvid=f-home&version=1&lg=en&ct=us

5. Herramienta de desinfección de software malintencionado

La herramienta de eliminación de software malintencionado se instala y mejora con regularidad cada vez que realiza una actualización con Windows Update. Puede ejecutarla en línea haciendo clic en el enlace que aparece en la página Web. También es posible comprobar el disco mediante las herramientas de WinRE. Esto puede ser útil si no puede acceder al equipo en modo normal y si el antivirus no puede ejecutarse en modo seguro. Veamos cómo podemos hacerlo:

Una vez que ha arrancado desde el DVD-ROM de instalación de Windows Vista, haga clic en el enlace **Reparar el equipo** y acceda a la opción de Símbolo del sistema.

Le aparecerá el prompt **x:\sources>**. Mediante el comando cd, vaya a este directorio: C:\Windows\System32. A continuación, introduzca el siguiente comando: **`mrt.exe`**. Finalmente marque el botón de acción correspondiente al tipo de análisis que desea realizar y déjese guiar por el asistente.

Los modificadores autorizados son los siguientes:

- **/Q** o **/quiet**: modo silencioso, no se muestra ninguna interfaz.
- **/?** o **/help**: muestra la sintaxis y la versión del motor de detección.
- **/N**: modo de detección solo.
- **/F**: realiza un análisis completo.
- **/F:Y**: realiza un análisis completo y limpia los archivos infectados.