

Un enfoque sobre los programas espía. Segunda parte

✔ Le será de suma utilidad la revisión de la [primera parte](#) de este informe antes de comenzar la lectura de este documento.

En la sección anterior hemos mencionado las formas que adquieren los programas espía y cómo estos pueden infectar el ordenador.

Ahora trataremos el tema de cómo prevenir que los programas espía entren en nuestros sistemas y en los casos donde los mismos ya se han inmiscuido en nuestro ordenador, detallaremos qué debemos hacer para quitarlos.

Entre todo el material, también discutiremos cuáles configuraciones pueden ser modificadas para aumentar la protección general del ordenador contra los programas espía, más un breve comentario sobre el uso de las aplicaciones destinadas a neutralizar este tipo de código malicioso.

Síntomas de una infección

Existen varios síntomas de la posible actividad de programas espía en un ordenador:

- El tiempo de inicio del mismo puede haber aumentado de manera considerable.
- Puede parecer que todo se ejecuta mucho más lento.
- Es posible verificar tráfico en la red aún con todos los programas cerrados (esta es la indicación más clara, aunque las actualizaciones de los programas, especialmente Windows Update, pueden ser los responsables).
- La modificación de la página de inicio predeterminada del navegador de Internet.
- El secuestro de la página de búsqueda.
- Numerosas ventanas emergentes con contenido desconocido.
- Nuevas barras de herramientas nunca solicitadas.
- Entradas nuevas y desconocidas en la pestaña Favoritos del navegador.
- Nuevos iconos en el escritorio

La aparición de uno o más de estos síntomas puede estar sugiriendo que algún programa espía o alguna publicidad maliciosa sea el culpable más probable.

Cómo quitar los programas espía

Algunas utilidades sin cargo pueden ayudarle a descubrir programas sospechosos en el ordenador y le darán al usuario alguna pista si un programa espía está realmente presente en el ordenador:

- Process Explorer
<http://www.sysinternals.com/Utilities/ProcessExplorer.html>
- Port Explorer
<http://www.diamondcs.com.au/portexplorer/>

Desafortunadamente, los creadores de programas espía llegan muy lejos para evitar que sus creaciones sean eliminadas (pudiendo llegar hasta el bloqueo del acceso a páginas Web implementados con la mejor seguridad) y con ciertos tipos en particular (CoolWebSearch y ISTBar están dentro de esta clase) será necesario realizar otros pasos para limpiar completamente el ordenador.

En estos casos, se recomienda descargar (pero no ejecutar aún) una copia del programa **HijackThis!**, disponible en varios sitios de descarga como:

- <http://tomcoyote.com/hjt/>
- <http://aumha.org/freeware/freeware.php>
- Un breve manual se puede descargar desde <http://aumha.org/a/hjttutor.php>

También se recomienda visitar uno de los foros que se encuentran en la página de *Alliance of Security Analysis Professionals* (Alianza de profesionales del análisis sobre la seguridad):

- <http://asap.maddoktor2.com/>

Es necesario verificar las instrucciones sobre el uso de HijackThis! en el foro (no todos aceptan informes HJT) y cómo enviar los resultados para recibir los consejos adecuados sobre qué conviene hacer. Hay que tener en cuenta que el análisis HJT requiere de tiempo y habilidades, por eso es recomendable enviar a un foro el informe y seguir todas las instrucciones indicadas en el mismo.

En el peor de los casos (cuando se ha utilizado un *rootkit* para modificar Windows con el fin de ocultar el programa espía) será necesario dar formato al disco duro y reinstalar el sistema operativo, y esto debería ser el último recurso ya que derivará en la pérdida de toda información en el sistema, pero si esta fuera la única opción, entonces será necesario, antes de proceder:

- Hacer una copia, en medios externos, de la información importante (documentos, fotos, contraseñas, detalles de los registros de los programas).
- También hacer una copia en medios externos, de las aplicaciones de seguridad. Si su licencia de Outpost aún se encuentra vigente, descargue la última versión disponible.
- Imprimir toda la documentación para realizar la nueva instalación, ya que no tendrá acceso a Internet desde ese ordenador hasta que haya finalizado el proceso de instalación. Para Windows XP, las instrucciones de instalación se encuentran en: <http://support.microsoft.com/kb/315341/es>
- Instalar y configurar el programa de seguridad después de haber concluido la instalación del sistema operativo.
- Conectar el ordenador a Internet y actualizar Windows mediante la herramienta Windows Update.

Finalmente, si alguno de los programas antes mencionados informó la presencia de un *keylogger* (programa que captura las pulsaciones del teclado para descubrir las contraseñas) entonces será necesario contactarse con todos los sitios con acceso con contraseña (especialmente aquellos encargados de operaciones bancarias en línea o los sitios relacionados al mercado de acciones) para informar que esa cuenta corre peligro. Esto es sumamente necesario hacerlo para evitar cualquier pérdida financiera (los bancos no se hacen cargo de los fraudes si un programa espía estaba en el ordenador del usuario).

Cómo intensificar la seguridad

- Un navegador de Internet inseguro es la ruta más probable para la infección con programas espía. Visitar, con un explorador inseguro, un sitio Web que distribuye programas espía, puede accionar automáticamente la instalación de código malicioso.
✉ Consulte <http://www.benedelman.org/> para más información.
- Los usuarios de Windows XP deberán instalar el paquete de mantenimiento SP2 (*Service Pack 2*) desde: <http://www.microsoft.com/downloads/details.aspx?displaylang=es&FamilyID=049c9dbe-3b8e-4f30-8245-9e368d3cdb5a>
- Posteriormente deberán descargar e instalar todos los parches disponibles para corregir las sucesivas vulnerabilidades y modificaciones del sistema operativo, para lo cual se recomienda el uso de la herramienta Windows Update, incluida con el sistema operativo.

Los usuarios de Internet Explorer deberán modificar algunos parámetros de la configuración del navegador, estableciendo, como mínimo, las siguientes correcciones:

- El nivel de seguridad del navegador deberá elevarse al nivel Medio.
- Cambiar la opción "Ejecutar controles y complementos de ActiveX en Internet Explorer al valor "pedir datos", evitando que la ejecución automática del contenido de una página Web intente instalar un programa espía. Esta modificación puede originar que muchas ventanas de Windows se abran para pedir confirmaciones de todas las páginas Web que utilicen ActiveX.
Para aliviar esta situación, los usuarios de Internet Explorer pueden utilizar un filtro (como el de Contenido Activo de Outpost Firewall Pro) para bloquear ActiveX por defecto.

Cuando un sitio confiable necesita que se ejecuten controles ActiveX, se puede crear una regla de exclusión para habilitar el uso de esta función para ese sitio en particular.

Muchas personas adoptan otros navegadores de Internet como una forma para reforzar la seguridad de todo el sistema y para protegerse de los programas espía.

Estos exploradores a veces no trabajan con los servicios de Microsoft, como Windows Update, el cual requiere el uso de Internet Explorer (I.E.) y ActiveX así como las páginas específicas de I.E.

Pero por otra parte, el uso de otros navegadores, ofrecen practicidad y mejoras en el rendimiento comparados con I.E. (comúnmente la localización en pestañas, acceso rápido a motores de búsquedas, más control sobre lo que muestran las páginas Web, y mayor compatibilidad con las normas estándares.

Lo mejor que tienen estos navegadores es que están mejor equipados para resistir los programas espía y se actualizan más seguido que Internet Explorer.

En el sitio de Secunia podrá acceder a comparativas sobre seguridad, entre:

- Internet Explorer 6
<http://secunia.com/product/11/>
- Firefox
<http://secunia.com/product/4227/>
- Opera
<http://secunia.com/product/4932/>

Los navegadores como Firefox (<http://www.mozilla.org/products/firefox>) y Opera (<http://www.opera.com>) están ganando popularidad y además ambos son gratuitos (Opera solía ser respaldado por publicidades pero ha eliminado esto en la versión 8.50).

También es muy importante tomar ciertas precauciones básicas cuando se navega por la red: nunca se deben obtener y mucho menos ejecutar archivos descargados de fuentes dudosas, especialmente de redes que comparten archivos, el uso Internet Relay Chat (IRC), Usenet o sitios Web "warez" (sitios utilizados para la descarga de programas).

Cuando se visiten sitios Web desconocidos o sospechosos, es necesario modificar el nivel de seguridad del navegador al valor máximo ("Sitios restringidos" en Internet Explorer).

La publicidad no deseada (*Spam*) es un método popular para incitar a los usuarios a visitar los sitios Web con programas maliciosos (una de las tácticas utilizadas ha sido incluir un mensaje sobre transacciones de tarjeta de crédito de alto valor que serían cobradas al usuario si no presionaba en un vínculo determinado).

Hay que ser extremadamente cuidadoso con este tipo de correos electrónicos, y nunca usar Internet Explorer para investigar cualquier vínculo (ya que suelen utilizar las vulnerabilidades de I.E. recién descubiertas y por lo tanto sin correcciones todavía).

La defensa ante los programas maliciosos utilizando aplicaciones especializadas

Es mejor prevenir que curar en lo referido a programas espía.

Si un programa espía se instala en el sistema, es muy difícil quitarlo manualmente, por eso es mejor asegurarse que siempre tengamos en el ordenador un programa que detecte y elimine los programas espía (los programas antivirus pueden en muchos casos detectar programas maliciosos en general cuando entran al sistema, pero tienden a tener un menor rendimiento cuando se trata de limpiar un sistema ya infectado).

Un cortafuegos y un explorador antiespía pueden proporcionar una protección suficiente contra la infección (especialmente si el cortafuegos ofrece filtrado de páginas Web, como el complemento Contenido activo de Outpost Firewall Pro).

Un cortafuegos configurado de la forma apropiada detectará (y le permitirá al usuario bloquear) cualquier intento de comunicación por Internet por parte de un programa espía (aunque este debe ser eliminado, porque el peor daño que puede realizar un programa espía, es lograr exitosamente la comunicación para enviar información privada al distribuidor).

Un buen programa antiespía detectará los programas espía alojados en la memoria o en el disco y los eliminará.

La versión 3.0 de Outpost Firewall Pro combina la funcionalidad de estos dos productos de seguridad y con un solo producto brinda una protección exhaustiva contra los programas espía.

Conclusión

Los programas espía son un problema peligroso, en continuo aumento y cada vez más complejo que debe atacarse por múltiples frentes.

Uno de ellos incluye la configuración correcta de los complementos del sistema de seguridad y otro depende de la elección correcta de un programa de seguridad.

En Agnitum nos esforzamos por asegurarnos que el usuario esté equipado con los mejores recursos de protección contra los programas maliciosos para siempre.