

EVITANDO QUE SPYWARES Y ADWARES SECUESTREN SU COMPUTADORA

Por Steven Presar

La Comisión Federal de Comercio (FTC) (de Estados Unidos) anunció que había utilizado leyes comerciales existentes para pedir que una corte federal cierre algunas de las distribuidoras principales de software malicioso "spyware" o "adware". Este tipo de programa puede ser agrupado junto a los virus, los gusanos, y el sp@m, y suelen ser denominados a todos como "malware".

¿QUÉ SON LOS PROGRAMAS SPYWARE Y ADWARE?

Los Spyware y adware son programas que se instalan en su computadora, generalmente sin su conocimiento, y 'observan' o controlan el uso de la misma. El programa puede abrir ventanas de publicidad, redireccionar su pedido hacia un sitio Web no solicitado cuando está navegando en Internet, controlar su actividad mientras navega o grabar las pulsaciones sobre el teclado mientras está en línea. Esta grabación de golpes de teclado puede conducir al hurto de la identidad o a un fraude con su tarjeta de crédito.

Los términos "spyware" y "adware" identifican esencialmente al mismo tipo de programas. Son programas de los que no se entera que están funcionando en su computadora.

Los vendedores en línea que distribuyen este tipo de software sostienen que usted ha descargado el software para ayudarlos a dar un mejor servicio para sus necesidades de comercialización en Internet. También pueden indicar que usted recibió el programa como parte de otro paquete gratuito de programas que descargó e instaló. O sino, que durante el proceso de descarga, usted presionó sobre un botón de aceptación, donde había una declaración de que usted aceptaba recibir publicidad de los productos que anunciaban.

Estos mismo programa que tiene convierten en víctimas a individuos con cambios misteriosos en sus páginas de inicio, con nuevos motores de búsqueda por defecto, con avalanchas de publicidad que se abren en nuevas ventanas mientras navega, o que degradan el funcionamiento o directamente bloquean la computadora – suelen ser conocidos como spyware.

Cualquier programa no solicitado funcionando en su computadora es conocido como spyware.

DISTRIBUCIÓN DE LOS SPYWARE

Sin importar cómo se llaman - su computadora está infectada de cualquier manera.

Simplemente haciendo clic en un aviso de publicidad (banner) puede estar instalando un programa spyware. Los gusanos, que son virus que se propagan a si mismos, pueden propagar también a los spyware. Ellos buscan máquinas que no tengan al día las actualizaciones de seguridad e instalan su programa malicioso. Los spyware también pueden distribuirse a través del correo electrónico.

Según lo indicado antes, el método más importante de distribución de spyware es asociarlos secretamente con software gratuito que puede descargar de Internet. Sitios que ofrecen música, videos, datos del tiempo, juegos, salva pantallas, barras de herramientas, o programas que sincronizan el reloj de su computadora, a menudo son pagados para distribuir el spyware como adware.

Programas que permiten compartir archivos como el Kazaa tienen adware incluido en el mismo paquete de descarga.

Antes de que estos programas estén instalados, usted tiene que hacer un clic en una caja que dice que debe aceptar el acuerdo contractual. Estos acuerdos pueden estar compuestos de miles de palabras y la gente raramente los lee. Haciendo un examen más exhaustivo, sin embargo, encuentran que están aceptando el programa que muestra publicidad como condición para conseguir el paquete.

Otro método común es un mensaje que le dice que necesita descargar un control ActiveX para ver un sitio o mensaje de correo electrónico. ¡No lo haga! Es apenas otro método para conseguir el sí para instalar un adware.

A veces, la presentación es una falsificación absoluta de un acuerdo de Microsoft o de de algún otro documento reconocible. Una regla segura a seguir: si no está seguro de qué es, no haga clic en 'Aceptar'. Salga del programa de cualquier manera que pueda, incluso si esto implica el reinicio de su computadora.

Al contrario de los desarrolladores de virus, que desean principalmente infectar tantas computadoras como puedan para después jactarse de ello, las firmas que distribuyen spyware tienen un incentivo financiero para mantener funcionando el programa en su computadora tanto tiempo como sea posible. Cuanta mayor cantidad de publicidad se muestre sobre su pantalla, más probablemente usted hará un clic sobre una de ellas.

¿ESTÁ SU COMPUTADORA INFECTADA?

Para eliminar el spyware, usted debería dar de baja cada archivo que esté en funcionamiento y borrarlo totalmente. Sin embargo, pueden ser muy resistentes puesto que el spyware se oculta dentro del sistema operativo de su computadora, haciéndolo difícil de encontrar.

Si usted sospecha que su computadora está infectada y desee buscar el Internet una solución "anti-spyware" - tenga cuidado.

Una búsqueda en Google devolverá más de 1.500.000 resultados para "anti spyware software". Conseguirá cerca de 749.000 páginas para la frase "software anti-spyware". Algunas compañías que ofrecen soluciones para este tipo de programas también los desarrollan. ¿Quién podría saber más sobre la forma de quitar el spyware que los mismos fabricantes del programa? El programa anti-spyware puede quitar de su computadora una versión del spyware, pero discretamente cargar una versión más actual del mismo que se disparará algunos días después, cuando ya pensaba que había limpiado el programa de su computadora.

Puede descargar tres programas anti-spyware gratuitos de:

- Ad-Aware (<http://www.lavasoftusa.com/>)
- Spybot (<http://www.security.kolla.de/>)
- Cwshredder (<http://www.intermute.com/spysubtract/>)

Antes de hacer funcionar cualquiera de estas soluciones, utilice su característica de actualización automática para conseguir la protección más actualizada. Algunos usuarios consiguen mejores resultados cuando realizan pasadas sucesivas con cada uno de estos tres programas.

Los programas limpiadores pueden quitar la mayoría de las infecciones, haciéndolas temporalmente inactivas. Pero, a veces, siguen quedando algunos componentes que descargan más archivos y re-infectan su computadora. Puede resultar de ayuda, desconectar momentáneamente la computadora de Internet y reiniciarla luego de hacer funcionar el programa limpiador. Si usted sabe cómo utilizar un programa cortafuegos como el Zone Alarm, puede utilizarlo para evitar que spyware persistente se

reconstituya.

Si su computadora está tan empantanada con el spyware, quizás tenga problemas para descargar el anti-spyware antes de que su computadora se reinicie. En tal caso, podría obtener el programa a través de otra computadora utilizando por ejemplo una quemadora de CD, y entonces instalar el software en su computadora utilizando ese CD.

Explore su disco duro por lo menos una vez por semana con dos o más programas anti-spyware porque probablemente cada uno encontrará archivos que el otro pasa por alto.

PROTECCIÓN ANTI -SPYWARE EN FUNCIONAMIENTO

Para prevenir una futura infección, no haga clic en cualquier ventana de avisos publicitarios o en el cuerpo de cualquier correo sp@m. Intente cerrar esas ventanas de publicidad no solicitada utilizando Alt-F4 en Windows. Alt-F4 es una combinación de teclas que disminuyen el riesgo de hacer clic sobre un botón que simula ser el botón que cierra la ventana y que realmente abre otra.

Mantenga su computadora al día con las últimas actualizaciones de seguridad. Microsoft ofrece descargas de actualizaciones gratuitas y CDs gratuitos para aquellos usuarios con conexiones a Internet lentas.

Windows recientemente ha anunciado que está disponible el Service Pack 2 de XP, que provee medidas de seguridad adicionales como un bloqueador de spyware limitado y un cortafuegos.

La protección es un proceso en constante cambio debido a que los fabricantes de spywares están creando constantemente nuevas amenazas. Puede descargar un buen administrador de recursos de la computadora y administrador de seguridad de OnlineSoftwareGuide.com.

Instale un cortafuegos personal. ZoneAlarm de Zone Labs tiene una versión gratuita básica para uso personal. Symantec y McAfee venden reconocidos programas cortafuegos, anti-virus y anti-spyware personales.

Luego, configure el sistema operativo de su computadora para que diariamente descargue actualizaciones en forma automática.

También configure su navegador de Internet para que le provea un nivel medio o alto de seguridad. Para Windows, ingrese al sitio de Microsoft para recibir instrucciones de cómo hacerlo. Los usuarios de Windows XP deben instalar el Service Pack 2, lo que hace casi imposible a los programas instalarse sin que primero usted sea alertado. Considere también el cambiarse hacia un navegador menos popular que el Internet Explorer, como el Mozilla Firefox o el Opera. Con ellos es menos probable ser atacados.

Si tiene problemas implementando alguno de los puntos anteriores, asegúrese de consultar a su asesor en temas informáticos.

Finalmente, practique una navegación segura. Esto significa descargar solamente programas confiables, la lectura de los acuerdos de licencia, evitar los banners de publicidad, y eliminar el correo basura sin abrirlo.

PUNTOS PARA PROTEGERSE USTED Y SU COMPUTADORA

:: No haga clic en "Aceptar" cuando un control ActiveX solicite su autorización sin antes averiguar exactamente que es lo que está descargando.

- :: No abra, y borre cualquier correo electrónico sospechoso.
- :: No complete ningún formulario donde pidan su número de Seguridad Social, licencia de conducir, claves de correo electrónico, información de cuentas bancarias, o el nombre de soltera de su madre.
- :: No descargue ni instale programas a menos que usted sepa y confíe 100% en la fuente.
- :: No dé su correo electrónico a cualquiera aunque no lo conozca.
- :: Limpie periódicamente las cookies y otros datos de seguimiento de su computadora.
- :: Utilice un correo desechable cuando rellena formularios en Internet.
- :: No participe de concursos o loterías en línea. Muchas de ellas capturan su información personal y la venden a terceras personas.
- :: Instale software para contraatacar el Spyware, Adware, correo Sp@m y publicidad no solicitada.

SI TIOS EN LOS QUE PUEDE CONFIAR

- Ad-Aware (<http://www.lavasoftusa.com/>)
- Spybot (<http://www.security.kolla.de/>)
- CWshredder (<http://www.intermute.com/spysubtract/>)
- WinTask, administra los recursos y mejora la seguridad. (<http://www.onlinesoftwareguide.com/wintask>)
- Descarga de programas anti-spyware. (<http://www.download.com/>)
- herramientas de información sobre spyware, consejos, y vendedores de programas de Trend Micro. (<http://housecall.trendmicro.com/>)
- McAfee programas anti-virus y anti-spyware. (<http://www.mcafee.com/>)
- Actualizaciones de seguridad e información sobre protección contra spyware de Windows. (<http://www.microsoft.com/athome/security/viruses>)
- Control de virus y spyware. (<http://www.pcpitstop.com/>)
- Lista de programas que pueden contener spyware. (http://www.spywarewarrior.com/rogue_anti-spyware.htm)
- Información sobre spyware de Norton. (<http://www.symantec.com/avcenter/>)
- Spy Sweeper programa anti-spyware. (<http://www.webroot.com/>)
- Cortafuegos Zonelabs. (<http://www.zonelabs.com/>)

Todos los derechos de Steven Presar

ACERCA DEL AUTOR

Steven Presar es un reconocido capacitador de tecnología para pequeñas empresas, editor de artículos para Internet, autor, orador, y entrenador. Proporciona soluciones de seguridad personales, para el hogar, y para computadoras en ProtectionConnect.com. También revisiones de software de negocio en OnlineSoftwareGuide.com. Además, publica artículos sobre cómo comenzar y poner a funcionar una pequeña empresa en Agora-Business-Center.com. Puede registrarse para recibir su boletín sobre negocios en este sitio.