
Un promedio de 28 programas espías en cada ordenador que accede a Internet

Un estudio realizado por uno de los más importantes proveedores de acceso a Internet nos permite conocer, con detalle, el gran impacto de los programas espías instalados en los ordenadores de los usuarios que acceden a Internet.

Earthlink es uno de los principales proveedores de acceso a Internet en los Estados Unidos, con ya una decena de años a sus espaldas y un historial de implicación con la comunidad de usuarios. Una de las últimas muestras de participación es el estudio efectuado recientemente que permite cuantificar el impacto real del spyware en los ordenadores de los usuarios.

Por spyware entendemos todas aquellas tácticas utilizadas para, literalmente, espiar la actividad de los usuarios. Habitualmente estos mecanismos de espionaje son utilizados por empresas de
publicidad con el objeto de rastrear, identificar y perfilar las actividades de los usuarios. Este espionaje se realiza frecuentemente totalmente a espaldas del usuario, de forma poco ética.

Entre los mecanismos de espionaje utilizados encontramos desde la utilización de cookies en las páginas web, utilizadas para determinar las páginas visitadas por los usuarios y así ofrecerles una publicidad más "a medida" de su perfil, hasta la instalación de programas en el ordenador que se encargan de que cada intento de acceso a una determinada dirección (por ejemplo, un buscador) sea redirigida hacia otra dirección.

Mención aparte dentro del spyware merecen aquellos programas que no sólo son utilizados para perfilar al usuario sino que van más allá y registran indiscriminadamente toda la actividad del ordenador: todo lo que se escribe y se visualiza en pantalla).

EarthLink acaba de presentar un servicio denominado "SpyAudit" que consiste en ofrecer a los usuarios de este ISP la posibilidad de detectar la presencia de spyware en sus ordenadores. El objeto de este servicio es

mostrar el autentico alcance del problema y la importancia que está alcanzando. La idea es que, conociendo el alcance del problema, los usuarios podrán ser conscientes del mismo y aplicar las medidas de protección para evitarlo.

Los primeros resultados de este estudio comprenden el período de tiempo entre el 1 de enero y el 31 de marzo del presente año. Durante este tiempo se han realizado un total de 1.062.756 comprobaciones de presencia de spyware, lo que ha permitido detectar un total de 29.540.618 instancias de programa espías... o lo que es lo mismo: casi 27,8 programas espías por ordenador con spyware.

Entre los programas espías encontramos diversas familias. La más frecuente es la utilización de cookies en los navegadores web que pueden ser utilizadas para rastrear al usuario. Las cookies son un valioso mecanismo para la construcción de webs interactivas, pero utilizadas de forma poco ética por parte de las empresas de publicidad, permiten identificar las áreas de interés y los hábitos de utilización de páginas web por parte de los usuarios. En el periodo de tiempo analizado, EarthLink ha detectado un total de 23.826.785 cookies utilizadas con finalidad de espionaje.

El segundo sistema más habitual es el conocido como adware. Son los programas que incluyen sistemas de espionaje. El más habitual es la visualización de publicidad mientras se está utilizando el programa aunque existen otros que van más allá y, sin informar al usuario (o incluso, cuando el usuario expresamente no autoriza esta actividad) instalan componentes en el ordenador para registrar la información personal del usuario. De este tipo, EarthLink ha detectado 5.344.355 instancias.

El tercer grupo es lo que se conoce como monitores del sistema que capturan virtualmente todo aquello que el usuario realiza en su ordenador y la almacenan en un archivo cifrado en el propio ordenador o, incluso, puede ser enviada automáticamente. Se trata de una violación flagrante de la intimidad y privacidad de los usuarios del ordenador. Un total de 184.559 programas de monitorización han sido identificados entre los usuarios de EarthLink.

El cuarto y último tipo de programas espía son los caballos de Troya. De hecho, este tipo de aplicaciones más que spyware o programas espías pueden considerarse ya como autentico malware o programas que realizan acciones negativas de cara al usuario. Entre los caballos de Troya encontramos sistemas de acceso remoto, destrucción de archivos en el ordenador, instalación automática de programas... De este tipo de spyware/malware, EarthLink ha detectado 184.919.

Evitar el spyware

Desgraciadamente no es fácil evitar la entrada de spyware en nuestro sistema cuando utilizamos determinados servicios de Internet. Esto es especialmente cierto en el caso de las cookies, ya que generalmente los usuarios tienen sus navegadores configurados para permitir el acceso a las mismas y no siempre es fácil discernir entre las cookies utilizadas legítimamente y aquellas utilizadas por empresas de publicidad con finalidades poco éticas.

En lo referente al adware, los monitores del sistema y los caballos de Troya el usuario si que puede aplicar una medida de protección básica: aplicar el sentido común ("el menos común de los sentidos").

A las clásicas medidas de no abrir archivos asociados en mensajes que no esperamos recibir (vía habitual de entrada de los caballos de Troya y los monitores del sistema), el usuario debe ser consciente de los posibles riesgos asociados a la instalación de determinados programas y el acceso a determinado contenido.

Programas de eliminación de spyware

Existen diversos programas que permiten detectar la presencia de Spyware. No obstante es preciso indicar que muchos de estos programas en realidad utilizan esta presunta acción de detección y eliminación de spyware como sistema para la instalación de programas espías. Conviene evitar aquellos programas que carecen de reputación o se presentan ofreciendo 'milagros'.

Kaspersky antivirus utiliza lo último en tecnología para interceptar virus, spam en tiempo real. Busca por virus en todos los archivos en el momento en que son leídos, creados o modificados, asegurando el control completo de todos los archivos. Protección completa que comprende: virus (gusanos, troyanos, backdoors, java applets active x), phishing, pornware, riskware, spyware, adware, x-files.

Fuente: http://www.hispasec.com/unaaldia/2002