

Cuando el ordenador te espía

Muchos programas instalan subrepticamente pequeñas aplicaciones que registran la actividad de los usuarios

El ordenador conectado a Internet, sin la precaución y protección necesaria, es muy vulnerable a la invasión de 'parásitos' capaces de tomar el control del equipo. Hay programas que se instalan furtivamente en el disco duro y que convierten el ordenador en un escaparate publicitario, espían la actividad del usuario, usurpan la conexión a Internet para enviar información sobre sus hábitos o sus datos personales, e incluso lanzan ventanas, cambian la página de inicio, añaden nuevos favoritos o instalan barras de navegación casi imposibles de eliminar.

Son intrusos, que a diferencia de los virus, no destruyen pero sí recopilan información no autorizada por el usuario, con la violación de la privacidad que ello supone. Además, ralentizan el funcionamiento del ordenador y la conexión a Internet.

'Malware'

Se pueden definir tres tipos de programas maliciosos (*malware*): aquellos que, con la excusa de rentabilizar el software que se regala, incluyen aplicaciones para lanzar anuncios; otros que, además, registran la actividad del usuario e informan de sus movimientos, y unos terceros que modifican el PC a su antojo. Aunque muchos claman por la legalidad de estos programas espía, lo cierto es que la mayoría ocultan sus intenciones tras una cantidad ingente de letra pequeña.

Si el usuario comienza a percibir comportamientos extraños en su ordenador —iconos desconocidos en el escritorio, constantes ventanas con anuncios, una página de inicio desconocida y habitualmente pornográfica...—, es probable que se le haya instalado uno de éstos parásitos. Lo peor es que son complicados de detectar y destruir, pues a veces incluso eliminan las opciones para deshacerse de ellos "por las buenas".

De la publicidad al espionaje

Se conoce como *adware* a los programas que muestran publicidad mientras están en uso. Estos programas, de por sí molestos, están bajo sospecha por su habitual tendencia a registrar hábitos o información personal del usuario para vendérselo a terceras partes, convirtiéndose en *spyware*. No todo el *adware* actúa como programa espía, y para muchas empresas esta forma de publicidad es la única posibilidad de ofrecer productos de forma gratuita.



>>> **Navegar a la carta**

Herramientas anti-intrusos
 ↗ www.spychecker.com

En Spychecker.com se pueden encontrar todo tipo de herramientas para descargar y proteger la intimidad en la Red.

Buscador de espías
 ↗ www.spywareguide.com

Una completa base datos con empresas y programas sospechosos de espíar a los usuarios.

Lo que deberían hacer durante la instalación es advertir claramente de sus intenciones. Quien no quiera que el programa despliegue anuncios, simplemente deberá optar por comprarlo, igual que hace al abonarse a una televisión de pago para no ver anuncios en las cadenas generalistas.

Sin la autorización del usuario, y muy a menudo sin su conocimiento, el *spyware* graba sus movimientos recopilando datos de toda índole. Los más inocuos registran el número de conexiones a Internet y su duración, el sistema operativo y navegador utilizado, etc. Pero en su versión más ladina son capaces de añadir al informe las páginas visitadas, los *banners* que se pinchan, los archivos descargados... hasta llegar a fichar información tan personal como el software instalado, el número de IP (que identifica al ordenador al conectarse a Internet) o la dirección de correo electrónico.

Sospechosos habituales

Lo más habitual es que estos compañeros de viaje no deseados se cuelen en la computadora a través de un virus o al instalar un programa nuevo, pero a veces basta con utilizar un navegador poco seguro (como, según muchos expertos, es el Internet Explorer) para resultar infectado. Determinado código incrustado en páginas web o mensajes de correo electrónico es suficiente para rastrear la actividad del usuario.

El riesgo de albergar programas maliciosos está directamente relacionado con la actividad del internauta,

aunque nadie debe sentirse a salvo. Los programas para intercambio de archivos (P2P) son habituales en las listas negras. Morpheus, Imesh, Limewire o Grokster son malvados habituales, y KaZaa se lleva la palma al incluir software espía como eZula, Gator o Cydoor.

Muchos implicados

El entramado de la 'red de espionaje' es abarca desde agencias de publicidad *online* (como DoubleClick, Web3000 o SaveNow) hasta aplicaciones que se instalan para servir anuncios o coleccionar información (Cydoor, WebHancer o Delfin) y los programas que los albergan (tipo KaZaa). Hay quien incluye a los que recopilan datos sin relación con la publicidad (Alexa, Hotbar, CuteFTP o GetRight) y a los reproductores (Media Player y Real Player) que registran las canciones escuchadas por el usuario, una información valiosa para las discográficas y los gestores de derechos de autor. La primera medida de protección pasa por prestar atención al instala-

lar un programa gratuito y andar con ojos de camaleón al navegar.

Es recomendable utilizar un navegador seguro, como Mozilla, o si se usa Explorer extremar la vigilancia. No obstante, se pueden levantar barreras para parapetarse frente a los programas malignos. La primera, un cortafuegos (*firewall*) para detectar y bloquear los intentos de conexión indeseados. También hay programas, como *StartPage Guard* o *Spyware Blaster*, dedicados a prevenir el 'secuestro' del navegador.

Una vez que los intrusos se han instalado en el ordenador, se puede echar mano de programas para detectarlos y eliminarlos. Dos de los más populares, y gratuitos, son *Ad-aware* de Lavasoft (www.lavasoftusa.com) y *Spybot Search & Destroy* (www.safer-networking.org), aunque si se trata de *spyware* sofisticado habrá que pagar por programas como *SpyCop* y *Evidence Terminator* (www.spywareinfo.com).e han detectado programas, como *SpyBan*, que eliminan programas espía a la vez que introducen otros. ◀

ESTAS APLICACIONES SE APROVECHAN DE QUE POCOS USUARIOS LEEN LA LETRA PEQUEÑA ANTES DE HACER CLIC

Espías de andar por casa

Hay una buena cantidad de software comercial cuya finalidad es controlar computadoras ajenas de forma remota. Estos programas son capaces de monitorizar cualquier movimiento en los PCs, desde las páginas web visitadas hasta el correo electrónico o los textos de la mensajería instantánea y *chats*. Especialmente diseñados para que las empresas vigilen el rendimiento de sus empleados o los padres controlen la actividad *online* de sus hijos, es muy fácil cometer abusos con ellos si se instalan sin el conocimiento del usuario.

En EEUU, más del 50% de las empresas reconocen controlar la conexión de sus trabajadores, por lo que la privacidad en el ordenador del trabajo no existe en absoluto. Depende del afán de control que aplique el responsable de la empresa. El nivel de espionaje se puede limitar a, por ejemplo, aquellos empleados que colapsan la red descargando música o películas, o convertirse en un auténtico Gran Hermano que intercepta los correos con determinadas palabras clave.

Navegar más seguro

➤ www.mozilla.org

Sitio web oficial de dos alternativas a Internet Explorer (Mozilla y Firefox) y una de Outlook Express (Thunderbird), menos expuestas a los programas maliciosos.