

Secciones

Editoriales más leídos

Notas más leídas

Inicio

Nacional

Internacional

Negocios

Espectáculos

Deportes

Cultura

Tendencias

Trascendió

Las firmas de hoy

El Ángel Exterminador

QRR

Humor

Especiales

Periódicos

- Milenio Diario
- Milenio Monterrey
- Público Milenio
- Diario de Tampico
- La Opinión Milenio
- Milenio Veracruz
- Milenio Tabasco

Servicios

Milenio en tu palm

Cartelera

Publicidad

Contacto



Suspenden operaciones de combate en torno a mezquita en Nayaf



Nayaf: Sadr sigue en control

Búsqueda

Buscar

Clima

MILENIO VERACRUZ / XALAPA Lunes 23-agosto. Actualización 03:40 Hrs.

Software espía, los ojos de extraños en nuestra computadora

23-agosto-04

El llamado spyware o software espía son programas que se esconden en otros o en aplicaciones que se descargan libremente en la web y se instalan en las computadoras personales sin que el usuario lo note.



El uso de la supercarretera de la información o Internet es cosa común en nuestros días. Amas de casa, estudiantes, empleados, en cualquier ámbito del quehacer diario se utiliza una computadora a través de la cual se tiene acceso a un universo infinito de información.

Internet se ha convertido en una poderosa herramienta que facilita el acceso a datos, noticias, compras en línea y entretenimiento en cuestión de

segundos y suministra diversos servicios para la comunicación entre la gente como el correo electrónico y los famosos chats.

Ante las ventajas que ofrece la web para el intercambio de archivos, día con día se amplía la gama de servicios que se ofrecen a través del ciberespacio, muchos de los cuales manejan información de carácter privado de los usuarios.

Este detalle no es algo intrascendente, en un mundo globalizado la información se ha convertido en una posesión sumamente valiosa. Como parte de sus estrategias mercadotécnicas, un gran número de empresas han encontrado un campo fértil en la red para obtener datos de potenciales clientes.

Pero el ser víctima de publicidad no deseada no es el mayor riesgo: el verdadero peligro está en el intercambio de información valiosa a través de Internet, como números de cuentas, de tarjetas de crédito, claves de acceso, una serie de referencias que pueden utilizarse para la comisión de fraudes y estafas.

¿Cómo es que el navegar por la red puede entrañar un riesgo de esta naturaleza? Todo es debido a la creciente amenaza que representa el llamado spyware o software espía, programas que se esconden en otros programas o aplicaciones que se descargan libremente en la web y que se instalan en las computadoras personales sin que el usuario lo note.

El impacto de este tipo de software está generando problemas cada vez más graves. En Estados Unidos, el 91 por ciento de las computadoras contiene al

menos un programa espía, según un estudio de la Alianza para la ciberseguridad nacional. A raíz de ello, autoridades federales de comercio discuten las medidas para enfrentar el spyware.

En nuestro país existe un gran vacío legal al respecto, pero no sólo eso sino que entre los mismos

Buscar

usuarios hay un enorme desconocimiento de lo que es el software espía y las consecuencias de no reforzar la seguridad informática.

Robo de información

El spyware se está convirtiendo en una de las principales preocupaciones de las empresas de seguridad a nivel mundial, además de los conocidos virus y el correo basura o spam, porque se trata de programas que recopilan información confidencial de los usuarios sin que se den cuenta.

Esta forma de invasión a la privacidad tiene dos vertientes: por un lado, detrás del spyware pueden estar empresas que utilizan sus programas para obtener datos estadísticos, los hábitos del usuario en la red, qué páginas visita, para después bombardearlo con publicidad a través del correo electrónico o de las ventanas que se abren repentinamente conocidas como pop ups, explica el maestro Mario Farias Elinos.

El académico de la Universidad La Salle, coordinador del grupo de seguridad de la red Corporación Universitaria para el Desarrollo de Internet (CUDI), agrega que la otra vertiente del spyware es la que se apropia de información sensible del usuario, como puede ser la referente a números de tarjetas de crédito, cuentas bancarias, claves de acceso, etcétera.

El rango de ataque del software espía es muy amplio, menciona por su parte el maestro Carlos Vicente Altamirano, de la Dirección General de Servicios de Cómputo Académico de la UNAM y también integrante del CUDI. Va desde el simple aspecto de la mercadotecnia

hasta objetivos más dañinos como los mencionados referentes a información confidencial o la intromisión en la computadora de programas llamados dialers (marcadores) que se conectan automáticamente vía telefónica con páginas de contenido pornográfico, cargándole el costo de la llamada – que es de larga distancia internacional- al usuario.

Hay aplicaciones que registran todo lo que el usuario escribe mandando la información a un agente externo, el cual puede obtener números de cuenta o claves de tarjetas de crédito. Los principales blancos de estos espías son empresas del área financiera, las cuales pueden estar expuestas a algún tipo de fraude cibernético.

Cómo funciona

El software espía tiene diversas formas de introducirse a la computadora personal. Una de las más comunes es a través de las descargas gratuitas de programas y aplicaciones que generalmente se utilizan para el intercambio de archivos, ya sean de música o imágenes. También se ofrecen como herramientas para facilitar la navegación en Internet o mejorar alguna función de la computadora. Con el atractivo de que resultan gratuitos, estos programas son muy populares y al bajarlos de la red se instalan en el disco duro obteniendo información del usuario.

Los pop ups pueden ser un síntoma de la presencia de spyware o, en sentido contrario, pueden ser el medio para la intromisión de este tipo de software, precisa el maestro Altamirano.

Por lo tanto, apunta Farias Elinos, no es recomendable confiar ciegamente en las descargas gratuitas sobre todo cuando el proveedor es desconocido, aunque en muchos casos ni siquiera

informan que al ingresar a determinada página web automáticamente se abren las ventanas publicitarias o se instalan unos archivos parecidos a los conocidos como cookies, para registrar datos del comportamiento del usuario en la Internet.

El desconocimiento de los riesgos de este tipo de situaciones hace más vulnerables a los usuarios, que en muchas ocasiones ignoran que pueden configurar su máquina para evitar la instalación de software espía, destaca el académico. “ Utilizar este tipo de herramientas no muy acreditadas

implica el conocimiento ahora no sólo de virus, también de spyware” .

Los proveedores de software gratuito se aprovechan también de la poca atención que ponen los usuarios a los términos del servicio, ese molesto contrato al que muy pocos hacen caso y que se acepta sin leer las letras pequeñas. En muchas ocasiones, las cláusulas establecen que además de la aplicación se instalarán algunos archivos adicionales para obtener información de hábitos, lo cual se traducirá en el envío o aparición de ventanas de publicidad.

Síntomas de espionaje

En ocasiones resulta difícil detectar la intromisión de un programa que rastrea información en nuestro ordenador, pero hay algunos síntomas muy indicativos de que algo anda mal. Si al iniciar la navegación en Internet la página de inicio cambia apareciendo material pornográfico o publicidad, si se abren constantemente ventanas promocionales ofreciendo regalos, viajes, si se recibe más correo basura de lo habitual o si aparecen íconos desconocidos en el escritorio, es probable que la máquina haya sido invadida por un programa espía.

El maestro Altamirano recomienda utilizar software de las mismas empresas reconocidas que ofrecen productos contra virus, para detectar y eliminar los programas espía y advierte que en la red se pueden encontrar programas antispyware pero se debe tener cuidado que el proveedor sea confiable porque el mismo remedio puede contener la enfermedad. Una alternativa segura y que se puede descargar gratuitamente la ofrece el sitio www.lavasoftusa.com o también en la base de datos Spychecker brinda una fuente de consulta de suma utilidad.

Los especialistas mencionan que para prevenir un ataque se debe empezar por cambiar la configuración de seguridad del navegador o utilizar navegadores distintos a Internet Explorer de Microsoft, el más popular pero a la vez de los menos seguros. Entre las opciones más confiables está Mozilla Firefox, es gratuito y se puede descargar del sitio www.softonic.com.

Aceptar plug ins o programas añadidos de los cuales se tiene un origen incierto no es recomendable; del mismo modo conviene desconfiar de la mayor parte del software gratuito si no se tienen referencias certeras sobre el proveedor.

De las innovaciones más recientes puestas en marcha por empresas que recaban información sin consentimiento de los usuarios, están en las barras de navegación, herramientas gratuitas que auxilian en las búsquedas en Internet. Las barras registran las visitas, los formularios que se llenan, las páginas consultadas y envían los datos a la empresa proveedora del software.

Nula regulación

Los problemas que implica el spyware no deben soslayarse. Proveedores de acceso a Internet en Estados Unidos estiman que uno de cada diez equipos contiene troyanos, el tipo más dañino de programas espía -los cuales permiten el acceso de terceros al disco duro de una computadora- por lo que las autoridades de ese país trabajan ya para combatirlo.

Mientras tanto, existe en el vecino país una ley de protección a la información privada – aclara el maestro Mario Farias- que de alguna manera permite frenar el uso del spyware, ya que se puede demandar a una persona no tanto por el programa espía sino por el robo de información personal no autorizada.

Desgraciadamente, apunta el académico, en México existe un vacío legal en la materia. No hay ninguna normatividad en cuanto a protección de información confidencial a través de Internet y tampoco está regulada la cuestión del software espía.

A nivel federal, la Secretaría de Seguridad Pública creó una Policía Cibernética que atiende algunos delitos que se dan a través de Internet, pero está enfocada básicamente a la detección de bandas

dedicadas a la elaboración y difusión de pornografía infantil, subraya el académico de la Universidad La Salle.

Cúidese de...

El grupo de seguridad de la red CUDI alerta que debe haber por lo menos unas 500 aplicaciones en Internet que contienen spyware. Según el investigador español Gonzalo Álvarez Marañón, el de la compañía Aureate/Radiate fue uno de los primeros casos de software espía. Se trataba de un conjunto de programas que incluían publicidad para financiarse a través de las barras conocidas como banners. Además de descargar los banners, los programas enviaban a la empresa Aureate información del usuario sobre sus hábitos en la red.

Entre los programas que contienen spyware podemos mencionar los de Webhancer, Customer Companion, Conducent/Timesink, Cydoor, Comet Cursor o Web3000.

Entre las aplicaciones más conocidas que recaban información de los usuarios están Audiogalaxy, Babylon Tool, Copernic 2000, CrushPop, CuteMX, EZForms, Gator, KaZaa, LimeWire, Grokster, FlashGet, Gif Animator, iMesh, JPEG Optimizer, MP3 Downloader, Neoplanet Browser, Net Scan 2000, Net Tools 2001, NetMonitor, Odigo Messenger, Opera Freeware, Oligo Browser, Real Audioplayer, Spam Buster, TIFNY, TypeItIn, WebCopier, Zip Zilla y Go! zilla.

Otras aplicaciones que hay que evitar son E Blaster, Download Plus, Safe Kiss, Search Sex, Spy Aol, Adult Links, Adult Chat Dialer, Flycast, Adforce, Teknosurf, Flyswat, Comet Cursor, Matchlogic, AdSoftware, Doubleclick, Adsmart, Adserver, Qualcomm, Conducent, GoHip, Real Networks, Webferret y Worldonline.

Jesús Velázquez Álvarez • Xalapa



© Derechos Reservados © Grupo Multimedia 2004 Privacidad | Aviso Legal
Desarrollado por Multimedia En-Línea