

Spyware, el software espía

Por Cristos Velasco San Martín y Jesús Ramón Jiménez Rojas

Originalmente publicado en Entérate en Línea, Dirección General de Servicios de Cómputo Académico (DGSCA) de la UNAM (Marzo del 2005) <http://www.enterate.unam.mx/>

1. Cuestiones prácticas y jurídicas

El término spyware o malware se refiere a los programas de software espía que tienen la capacidad de auto-instalarse en las computadoras personales de los usuarios, con objeto de conocer su identidad y monitorear su comportamiento al usar sistemas de cómputo o navegar en Internet. El software espía —al igual que las famosas cookies— es capaz de crear bases de datos y proporcionar información y updates sobre las preferencias y hábitos personales de los usuarios.

La denominación spyware fue idea del creador de software norteamericano Steve Gibson, quien al realizar una investigación descubrió algunos mecanismos espías en una gran cantidad de programas de software, comúnmente utilizados por empresas e individuos. Al respecto, Steve Gibson señala: “si una persona regularmente utiliza una computadora personal, es muy probable que ésta contenga algunos programas de spyware escondidos en la misma”...“en los Estados Unidos existen más de veinte millones de tipos de spyware actualmente instalados en computadoras sin el consentimiento de los usuarios”.

El spyware acarrea grandes problemas jurídicos, como es el de la invasión a la privacidad de los individuos —garantía individual consagrada en la mayoría de las constituciones del mundo—, puesto que dichos programas son instalados sin el consentimiento expreso —y sin ni siquiera dar la opción al usuario de no hacerlo (opt-out)—, y permiten rastrear con cierta facilidad sus hábitos sin saber que están siendo vigilados.

Asimismo, el spyware puede ser utilizado por hackers y alguno que otro tech savvy para llevar a cabo actividades ilícitas como el robo de identidad, o conocer información personal que incluye, por ejemplo, detalles de acceso a portales, números de cuenta bancarios y otras claves personales con los cuales los delincuentes usan la identidad de determinada persona para retirar dinero de cuentas bancarias, realizar compras o cometer otra serie de ilícitos.

El software espía, tal y como algunas enfermedades del ser humano, se manifiesta en distintas formas dependiendo de los sistemas y computadoras utilizados por los usuarios. Actualmente, no se conoce una causa específica relacionada con el spyware que permita controlar su crecimiento, sin embargo, los principales síntomas pueden ser: (i) lentitud del sistema operativo, tanto al abrir programas como al guardar documentos en el disco duro; (ii) funcionamiento inadecuado del teclado y otras funciones primordiales de la computadora y en general, cambios sorpresivos en las barras de herramientas de la computadora que puedan llevarla hasta el famoso “crash”; (iii) desplegar una dirección en Internet o URL distinta a la que originalmente se tecleó, o incluir direcciones Web en la lista de sitios favoritos del navegador; (iv) el navegador baja e instala programas de manera automática o cambia constantemente la página principal e inclusive; (v) registro de números telefónicos en el extranjero a través del uso del módem, lo que representa cargos importantes de llamadas de larga distancia para el usuario.

Mucho se ha dicho —sin que se haya comprobado de manera fehaciente— que la mayoría de los programas de software gratuitos existentes en la red, sobre todo aquellos utilizados para compartir música en Internet entre distintos usuarios ([P2P File Sharing](#)), como [Kaaza](#) y [Gnutella](#), contienen spyware y otros virus que son la causa de que muchos usuarios hayan tenido que reinstalar sus discos duros y recargar nuevamente sus programas y software.

Actualmente, la [Cámara de Diputados de Estados Unidos](#) analiza la conveniencia de promulgar una ley federal para regular la problemática del spyware. El año pasado se dieron los primeros pasos y dicha Cámara votó la aprobación del [Internet Spyware Prevention Act](#), mejor conocida como “Spy Act” por un margen de 399-1 votos. Sin embargo, existe cierta renuencia y diversas críticas sobre esta iniciativa, puesto que algunos grupos y expertos en el tema señalan que, al igual que el [CAN-SPAM](#), puede tener efectos adversos, es decir, en vez de aminorar o reducir el problema, podría incrementarlo aún más.

En México, no existe una legislación específica para regular el software espía y dudamos mucho que se defina una a corto plazo puesto que por un lado, todavía existe un gran desconocimiento del “usuario promedio” acerca de los sistemas de cómputo y programas de software, y por el otro, el tema no es prioritario en la agenda de nuestros legisladores.

La cultura de la seguridad informática en nuestro país se encuentra aún en una etapa intermedia de desarrollo y, actualmente, su papel es de carácter preventivo, debido a que se limita a proporcionar herramientas educativas y crear conciencia en los empleados de empresas y usuarios del Internet con el objeto de que puedan incrementar la seguridad en sus sistemas de cómputo y redes, para poder evitar daños, perjuicios y pérdidas económicas. Sin embargo, es conveniente que los usuarios mexicanos profundicemos en este problema, para salvaguardar la seguridad de los equipos de cómputo y software en los que hemos invertido.

Los casos más conocidos de spyware, se han dado, por supuesto, en Estados Unidos de Norteamérica. Por ejemplo, en fechas recientes un periodista americano descubrió después de haber instalado un juego de la empresa de juguetes [Mattel®](#) en la computadora de su hija, una pieza de software conocida como “Broadcast” que sin saberlo conectaba directamente la computadora de su hija hacia el servidor Web de Mattel, hecho que la compañía señala que se hacía únicamente con el propósito de proporcionar software updates a sus usuarios.

Como consecuencia de este suceso, algunos grupos de [lobbying](#), en defensa de las garantías individuales y los derechos de la privacidad alrededor del mundo, señalaron que el software de Mattel contenía capacidades técnicas adicionales que permitían invadir de manera flagrante los derechos de privacidad de los usuarios, al acceder a archivos personales del disco duro y monitorear de forma detallada la frecuencia con la que los usuarios empleaban los juegos de Mattel en sus sistemas de cómputo. Finalmente, después de una serie de negociaciones, Mattel acordó remover completamente el “Broadcast” de sus productos.

El primer caso anti-spyware investigado por la agencia de protección a los consumidores en Estados Unidos, la [Comisión Federal de Comercio](#) (FTC, por sus siglas en inglés) fue en octubre de 2004 en contra de [Seismic Entertainment Productions, Inc.](#), [Smartbot.Net](#), y un famoso spammer Sanford Wallace, quienes operaban portales que permitían la distribución y descarga de spyware, mediante mensajes pop-ups que ofrecían una solución inmediata a los consumidores para remediar dicha eventualidad mediante la venta de otros productos. La FTC realizó una investigación exhaustiva y acusó a los demandados de incurrir en prácticas desleales y engañosas lo que instó, posteriormente, a la propia FTC a llevar directamente el caso a un Juzgado de Distrito en el estado de New Hampshire, donde se

solicitaba al juez girar una “orden de abstención” para evitar que los demandados continuaran diseminando el spyware en la red y obteniendo ganancias ilícitas.

Otro caso reciente y curioso que tiene que ver con spyware y la interceptación de comunicaciones electrónicas es: O’Brien v. O’Brien; 2005 Fla. App. LEXIS 1408, Court of Appeal of Florida, Fifth District, February 11, 2005. En éste, la esposa de un señor con domicilio en el estado de Florida, instaló un programa spyware de nombre “Spector” en la computadora de su esposo —a sabiendas de que este último le era infiel—, con el objeto de poder intervenir y conocer las comunicaciones que su esposo realizaba con la susodicha y, de esa forma, tener pruebas suficientes para solicitar la disolución del vínculo matrimonial.

En este caso, la cuestión principal a decidir por el Tribunal de primera instancia fue si las comunicaciones electrónicas que interceptó la esposa contravinieron las disposiciones de la Ley de Intercepciones (Wiretap Act) y la Ley de Seguridad de Comunicaciones (Security of Communications Act) del estado de Florida. El tribunal de primera instancia resolvió que las comunicaciones electrónicas fueron ilegalmente interceptadas por la esposa, y ordenó que no se admitieran como pruebas en el juicio de divorcio, puesto que carecían de validez jurídica por haber sido obtenidas de manera ilegal y en contravención a dichas leyes. Posteriormente, el caso fue apelado en segunda instancia por la esposa y el tribunal de apelación confirmó la decisión y la orden de la corte de primera instancia.

2. Recomendaciones preventivas

Existen algunos síntomas que indican el tipo de software spyware instalado en el equipo:

- Redireccionamiento a sitios Web diferentes a los que se escriben en el navegador de Web.
- Aparición de gran cantidad de ventanas de mensajes emergentes.
- Aparición de barras de herramientas en el navegador de Web que el usuario nunca instaló.
- Nuevos íconos en la barra de tareas (parte inferior izquierda de la pantalla).
- Fallo al accionar ciertas teclas en el navegador (por ejemplo, que la tecla Tab no funcione cuando se trate de mover al siguiente cambio en una forma).
- Aparición de mensajes de error de Windows aleatorios.

¿Cómo puedo prevenir el spyware?

Para evitar que software de este tipo se instale en el equipo, es necesario seguir algunas buenas prácticas de seguridad:

- No hacer clic en vínculos que aparezcan en ventanas de mensajes emergentes. Debido a que las ventanas de mensajes emergentes son frecuentemente producto del spyware, al hacer clic sobre alguna de ellas, podría instalarse software spyware en el equipo. Para cerrar las ventanas de mensajes emergentes, se debe hacer clic en el ícono “X” en la barra de título o presionar las teclas ALT + F4 en lugar de hacer clic en un vínculo “Cerrar” dentro de la ventana.
- Escoger la opción “No” cuando aparezcan preguntas no deseadas. Se debe ser cuidadoso cuando algunos cuadros de diálogo tienen la leyenda de si se desea ejecutar un programa o realizar otro tipo de tarea. Siempre se debe seleccionar la opción “No” o “Cerrar”, o también hacer clic en el ícono “X” en la barra de título o presionar las teclas ALT + F4.
- Ser cuidadoso al descargar software gratuito. Existen muchos sitios que ofrecen barras de herramientas personalizadas u otras características que son atractivas para los usuarios. No se deben descargar programas de sitios Web que no son confiables debido a que el equipo

puede estar expuesto a la instalación de spyware al descargar algunos de estos programas.

- No hacer clic en vínculos contenidos en correos electrónicos que ofrezcan software anti-spyware. Al igual que los virus de correo electrónico, los vínculos podrían tener una función totalmente opuesta e instalar spyware en lugar de proporcionar información sobre herramientas de cómo eliminarlo.

- Ejecutar un navegador de Web que permita el bloque de ventanas de mensajes emergentes y cookies. Las ventanas de mensajes emergentes son generadas a menudo por algún tipo de scripts o contenido activo. Ajustando las configuraciones en el navegador de Web para reducir o prevenir el scripting o el contenido activo se podrían reducir considerablemente las mismas. La mayoría de los navegadores de Web ofrecen una opción para bloquear o limitar las ventanas de mensajes emergentes. Ciertos tipos de cookies a menudo son consideradas como spyware debido a que revelan las páginas Web que el usuario visita.

- Utilizar un navegador alternativo a Internet Explorer. La mayoría del spyware toma ventajas de las vulnerabilidades de seguridad en el navegador de Web Internet Explorer, por lo que debería omitirse su empleo en el sistema y utilizar otro navegador de Web. Existe una variedad amplia de navegadores que pueden instalarse, entre los principales de encuentran: - Mozilla Firefox (<http://www.mozilla.org/products/firefox/>) - Netscape (<http://www.netscape.com/>) - Opera (<http://www.opera.com/>).

¿Cómo elimino el spyware?

Existen un par de herramientas que pueden instalarse en un equipo para protegerse contra el spyware:

- **Software antivirus.** Es necesario instalar, actualizar y ejecutar periódicamente algún tipo de software antivirus. Algunos de los software antivirus encontrarán y removerán spyware, pero no podrían ser capaces de encontrar spyware al estar monitoreando el equipo en tiempo real. Se debe establecer el software antivirus de tal forma, que se ejecute un escaneo completo del equipo de forma periódica.

Entre los distribuidores antivirus más importantes se encuentran:

- Symantec Corporation (<http://www.symantec.com>)
- Trend Micro (<http://www.trendmicro.com>)
- Panda Software (<http://www.pandasoftware.com>)
- McAfee (<http://www.mcafee.com/mx/>)
- Sophos (<http://esp.sophos.com>)
- F-secure (<http://www.f-secure.com>)
- Computer Associates (<http://www.ca.com/offices/mexico/>)

- **Herramientas anti-spyware.** Muchos distribuidores ofrecen productos que escanearán el equipo en busca de spyware y lo removerán. Este tipo de software puede ser configurado de forma similar a un antivirus y, a menudo, es fácil de administrar.

Entre los principales productos utilizados para remover spyware se encuentran:

- Microsoft AntiSpyware (<http://www.microsoft.com>)
- Ad-Aware (<http://www.lavasoftusa.com>)
- SpySweeper (<http://www.spysweeper.com>)
- PestPatrol (<http://www.pestpatrol.com>)

- Spybot Search and Destroy (<http://www.safer-networking.org>)

• **Información adicional sobre problemas de spyware.** Es importante mantenerse actualizado con información reciente sobre problemas de spyware y de seguridad en cómputo en general, relacionados con el sistema operativo que presenta este tipo de problemas: el sistema operativo Windows.

Algunos sitios Web que pueden proporcionar información sobre seguridad en el sistema operativo Windows de Microsoft son:

- Portal del Departamento de Seguridad en Cómputo. (<http://www.seguridad.unam.mx>)
- UNAM-CERT. (<http://www.cert.org>)
- Lista de discusión SegWin. (<http://www.seguridad.unam.mx/listas/segwin/>)
- US-CERT. (<http://www.us-cert.gov/>)
- Microsoft Trustworthy Computing Security (<http://www.microsoft.com/security/default.mspx>)

Apéndice: terminología y definiciones

Adware. Cualquier aplicación de software que muestra banners publicitarios. El adware mantiene un registro de los hábitos de navegación del usuario y muestra publicidad basada en las actividades de navegación en un sitio Web. Los sitios Web frecuentemente depositan adware en el equipo cuando el usuario navega. Un programa adware debería ser considerado spyware, cuando ha sido instalado sin la aprobación del usuario y envía información a organizaciones no autorizadas.

Firewall. Previene de los equipos en la red que se comunican directamente con sistemas de cómputo externos. Un firewall típicamente consiste de hardware o software que actúa como una barrera entre las redes internas o equipos y los sistemas externos. El firewall analiza la información que se transmite entre las dos partes y la rechaza si no cumple con la reglas preconfiguradas; asimismo, proporciona una protección efectiva contra gusanos, pero no contra un spyware o troyanos, los cuales se ocultan bajo aplicaciones legítimas.

Software antispymware. Los productos antispymware protegen al equipo de la infección de spyware. Este tipo de software puede encontrar y remover software spyware sin la interrupción del sistema.

Spam. Correo electrónico comercial no solicitado, el cual es enviado frecuentemente en cantidades masivas a millones de usuarios a través de relays abiertos.

Spyware. Software que trasmite información a terceros sin el consentimiento del usuario; se instala y se ejecuta sin pedir ninguna autorización al usuario.

Pop-ups o ventanas de mensajes emergentes. Pequeñas ventanas que aparecen de forma inesperada en la pantalla del equipo de un usuario, comúnmente a consecuencia de algún tipo de software malicioso como spyware o adware.

Para mayor información:

<http://www.ftc.gov/bcp/online/pubs/alerts/spywarealrt.htm>

<http://spotlight.getnetwise.org/spyware/>

<http://enterprisecurity.symantec.com/content.cfm?ArticleID=5392>

[http://news.com.com/2038-12_3-0-topic.html?id=7107&name=Spyware/adware&tag=st.topic.](http://news.com.com/2038-12_3-0-topic.html?id=7107&name=Spyware/adware&tag=st.topic)