boletín técnico®

imef ejecutivos de finanzas

NUM. 16 / 2005

COMITÉ TÉCNICO NACIONAL
DE TECNOLOGÍA DE INFORMACIÓN

Seguridad contra Spyware y Adware

Introducción

En la actualidad encontramos una serie de comentarios acerca de diferentes amenazas a la información de nuestras computadoras personales; términos hasta cierto punto confusos, que nos crean sensaciones de inseguridad y desconcierto.

Pensábamos que los "famosos" virus informáticos eran lo único que podría amenazar y destruir la valiosa información almacenada en nuestras computadoras, pero ... desafortunadamente, estamos equivocados. Ahora existe una nueva amenaza a nuestra información y privacidad: Los programas conocidos como "spyware".

Ante este panorama la pregunta que nos hacemos es:

¿Qué es el Spyware?

En términos simples, "spyware" se le conoce al programa informático que se instala en una o varias computadoras, sin o con el consentimiento y/o permiso del usuario. Monitorea el uso

de la computadora y envía la información correspondiente hacia la empresa, hacker o terceros que controlan a este programa. Registra contraseñas (passwords) y graba pulsos de teclas (keylogger). Y provoca problemas de inestabilidad de las computadoras: congelamiento, reinicios inesperados, errores en Windows (pantallas azules de error) y pérdida de rendimiento (lentitud) de más del 50%.

El spyware llega en diferentes tamaños y presentaciones; por ejemplo hay spyware que incrementa el correo SPAM que el usuario recibe o bien; aparecen infinidad de ventanas emergentes en su escritorio en Windows: conocidos como "pop-ups". Otro tipo de spyware representa una verdadera amenaza a la seguridad de la empresas, ya que puede robar información confidencial y hacerlas más vulnerables a ataques de otros tipos de programas maliciosos.

La información empresarial más expuesta al spyware es la siguiente:

- Bases de datos de clientes, números de seguridad social de los empleados.
- Información de números de tarjetas de crédito e historial crediticio. Así como cuentas bancarias e información sobre inversiones.
- Información de registros sobre compras y adquisiones.
- Secretos industriales de manufactura de productos y otro tipo de información propietaria.
- Registros médicos y de salud en general del usuario.
- Información relativa a contratos, documentos de orden legal y correos electrónicos.
- Planes y estrategias comerciales, industriales, etc.

Evolución del Spyware

El 16 de Octubre de 1995 se acuñó por primera vez el término spyware en un Usenet (sistema de información distribuída en Internet). El tema se refería a lo divertido que sería jugar con el modelo de negocio de Microsoft. Posteriormente, el término fue empleado para referirse a equipo de espionaje como las microcámaras.

En 1999 Zone Labs empleó el término spyware en una nota de prensa referente a su producto: "Zone Alarm Personal Firewall". A partir de entonces los usuarios le dieron el sentido que actualmente se maneja para esta palabra.

También en 1999 aparece el primer programa "freeware" (software gratis) con un spyware dentro de él, llamado "Elf Bowling". Este programa era un juego en Internet donde el usuario actúa como Santa Claus en un juego de boliche, donde los pinos son sustituídos por sus duendes. El programa enviaba información del usuario hacia el creador del juego Nsoft.

En el año del 2000 Steve Ginbson de Gibson Research liberó el primer programa antispyware: OptOut, desde entonces ha ido apareciendo nuevos programas antispyware hasta la fecha.

Sin bien el spyware tiene como finalidad robar información y causar inestabilidad en los sistemas, ¿será lo mismo que un virus?

Diferencias entre el spyware y los virus

Entre los virus y el spyware hay cierta semejanza, pero diferencias muy marcadas como son:

Un virus informático tiene la capacidad de replicarse así mismo y enviar sus copias tan rápido como sea posible y tomando rutas que le permitan pasar inadvertido y por ende, no ser detectado y detenido. El spyware por su parte, confía en persuadir a usuarios fáciles de convencer o bien, sin conocimientos en seguridad.

Esto lleva a que el usuario instale el programa y reciba un beneficio especial al instalarlo. Ejemplo de ello, el spyware conocido como Bonzi Buddy. Una vez instalado tiene una rutina que le permite ejecutarse cada vez que el equipo es encendido, monitorea el uso de Internet y envía la información recolectada a terceros.

Un virus siempre tiene una rutina de daño, la cual está programada para ejecutarse bajo ciertas circunstancias y dañar deliberadamente información del usuario, como pueden ser archivos de datos, documentos, etc. El spyware en cambio, el daño que pueda causar a un equipo, se puede catalogar de incidental como consecuencia del consumo de los recursos del mismo. Por ejemplo, ancho de banda de Internet, recursos del procesador, recursos de memoria RAM, entre otros.

¿Cómo saber si mi PC tiene spyware?

Los síntomas más notables acerca de la prescencia de spyware en la computadora son:

- La computadora es muy lenta al encenderla y cuando se está trabajando con algún programa, como Word, Excel u otra aplicación.
- La computadora tiene repentinos y frecuentes problemas de programas "congelados".
- La PC hace conexiones a Internet sin haber hecho el usuario la conexión por sí mismo.
- Dificultades al hacer conexión a Internet, tales como pérdida repentina de la conexión, aparición de ventanas emergentes de error desconocidas. La página de inicio del navegador de Internet (Internet Explorer por ejemplo) aparece cambiada, y cuando se intente restablecerla; vuelve a ser cambiada de forma misteriosa.
- Al navegar en Internet aparecen ventanas emergentes (pop-ups) no solicitadas, generalmente de tipo pornográfico y comercial.

¿Cómo eliminar el spyware de mi computadora?

El Spyware es un problema difícil de erradicar en las computadoras; esto se debe a su naturaleza regional (el spyware en Norteamérica es diferente del spyware europeo o latinoamericano) y la forma en que se "ancla" en las computadoras.

Además de los sistemas de autoprotección con que cuenta normalmente.

- Los programas antispyware son una solución inmediata, pero no total al problema del spywware, por las razones arriba mencionadas. Lo que se tiene que implantar son normas preventivas que eviten el riesgo de ser afectado por el spyware. Entre las cuales podemos mencionar:

- Evitar navegar en páginas en Internet sospechosas de contener virus y por ende, spyware.

- Mantener los sistemas operativos (Microsoft Windows) actualizados en sus "parches de "seguridad" con el fin de minimizar riesgos.

- Contar con un firewall personal instalado en la PC reduce la posibilidad de que un spyware se instale en el sistema.

- Evitar descargar software "gratis" de Internet, aunque sea éste para niños. Normalmente, estos programas contienen spyware del cual no se le notifica al usuario. Y provoca muchos problemas.

- Evitar instalar barras de "herramientas" adicionales a los navegadores de Internet (Internet Explorer por ejemplo). Estas "herramientas" son prescencia más que notable de spyware en un PC.

Sin embargo, ¿Cual sería la protección ideal si ahora?...

La solución consiste en una estrategia de seguridad integral para la red de una empresa, como de las computadoras en un hogar. Programas Antispyware son una de las soluciones que pueden controlar este problema. Sin embargo, una solución que protega contra spyware y virus sería ideal; ya que existen virus (como los "troyanos") que llevan consigo spyware.

Por lo que una solución contra virus y spyware minimiza al mínimo los riesgos y los efectos de virus y el spyware. Y si además esta solución cuenta con un firewall (cortafuegos) integrado, el riesgo se reduce a casi 0%.

Algunos de los programas antispyware integrales que se pueden encontrar en el mercado son:

Trend Micro Office Scan. Solución para estaciones de trabajo corporativas, diseñada para destectar virus, spyware y ataques. Ver http://www.trendtyc.com/

Trend Micro PC-Cillin. Solución destinada para el usuario casero que requiere un producto modular que cuente con antivirus, antispyware, firewall, entre otras funciones. Ver. http://www.trendtyc.com/.

Webroot (www.webroot.com), es otra empresa reconocida por sus soluciones antispyware tanto para usuario casero como para corporaciones. Abajo encontrarán los links para sus productos:

Corporativo:

http://www.webroot.com/products/enterprise/?WRSID=dea58f0287f0d46590124aa2b1094a17

Casero:

http://www.webroot.com/products/spysweeper/?WRSID=dea58f0287f0d46590124aa2b1094a17

Otra solución excelente para la detección y eliminación de spyware es Spyware Doctor de PC Tools (www.pctools.com). El link es el siguiente para más nformación:

https://www.pctools.com/es/spyware-doctor/

Los páginas web de las empresas antes mencionadas, cuentan con opciones de escaneo y detección de spyware en línea. Con el fin de valorar las bondades que cada producto ofrece al usuario.

ES POR ESTO, QUE SE DEBE BUSCAR UNA SOLUCIÓN QUE NOS DE LO SIGUIENTE:

1. Dormir tranquilo y asegurarme de que mi información personal residente en mi PC está segura y sin riesgo de ser asechada por el spyware.

2. Que la solución prevenga y proteja antes de que el spyware, virus y otro tipo de programa malicioso se introduzca en la PC.

3. Los sistemas operativos de Microsoft sufren de vulnerabilidades, y son un medio de ataque de los virus y el spyware, entonces se hace necesario que algo me ayude a realmente cubrir o aislar tales vulnerabilidades y evitar además el ingreso del spyware en la PC, como en la red de la empresa.

4. Una solución antispyware que opere en tiempo real monitoreando la navegación hacia Internet, como los archivos que van hacia y desde la PC. Que funcione de forma automática en su operación como en su actualización constante en búsqueda de nuevas amenazas.

5. Estar seguro que el 100% de los equipos con que cuento en la empresa tienen una solución antispyware y antivirus actualizada.

6. Disminuir cualquier riesgo de carácter legal que pueda derivarse de la existencia de spyware en las PC´s.

Y el Adware?...

El adware es un primo hermano del spyware que se dedica a monitorear los hábitos de uso de la computadora por parte del usuario, para enviarle vía correo electrónico mensajes Spam relativos a sus hábitos o bien, pantallas emergentes relativas a las páginas que normalmente visita. Ejemplo de ello, es la persona que navega mucho en páginas pornográficas o de viajes.

El adware instalado en su PC enviará la información recolectada a terceros, lo que llevará posteriormente a que reciba e-mails con pornografía, productos "eróticos". Y si se trata de Vacaciones; recibirá ofertas de hoteles y agencias de viajes, normalmente desconocidas, ofreciendo tales servicios, sea por el correo electrónico o por ventanas emergentes en Microsoft Windows. A diferencia del spyware el Adware normalmente notifica al usuario de su intención antes de instalarse. Pero normalmente esta información va escondida entre cientos de líneas de texto, ocultando con ello; sus verdaderas intenciones.

Eliminar el Adware requiere de la solución integral que mencioné en párrafos anteriores: que contenga, antispyware, antiadware, firewall (cortafuegos) y antivirus.

ESTIMADO SOCIO

Cualquier comentario, observación o sugerencia a este Boletín, favor de hacerlo llegar directamente al autor. Por: Lic. Arturo Fernández Maldonado
Pre-Sales Antivirus Manager
mailto:arturo.fernandez@trendtyc.com
Tel. 5536-7900, Nextel: 10899302