

¿CÓMO DETECTAR A LOS ESPÍAS?

No tenga duda acerca de esto, el espiar a través de Internet se está haciendo cada vez más usual y más sofisticado. Es importante saber, que hay diferentes niveles de espías. Por ejemplo, Alexa, el popular programa desarrollado por Amazon.com, podría ser denominado un "Puerta Trasera Santa" porque no realiza realmente un registro de las teclas apretadas ni toma fotografías de nuestro sistema, pero si graba algunas de nuestras actividades al navegar por la red. Sin embargo, programas como Spector son expertos en recabar sigilosamente información como claves, registros de navegación, e incluso, usuarios de "chat" y correos electrónicos.

Entonces, ¿cómo podríamos saber si estamos siendo espiados?. A continuación podemos encontrar una lista de puntos sobre cómo podemos darnos cuenta, sin contar con un software especializado, si nuestros movimientos están siendo registrados por un programa espía, comprobando algunas marcas o huellas que suelen dejar estos programas.

1) Ambiente de Trabajo: dé por hecho que está siendo espiado. La mayoría de los lugares de trabajo tienen el derecho a hacerlo, entonces, por defecto acostúmbrese a que de hecho alguien lo está haciendo. Hay varias maneras en que los empleados pueden estar espiando a otros empleados. Algunos utilizarán los programas que registran su actividad para ver qué programas han sido utilizados y por cuánto tiempo. Naturalmente, muchos utilizan unos programas espías también conocidos como "snoop ware" (snoop: del inglés, curioso) o un registrador de teclas para tomar el estado del sistema en un momento determinado o grabar las teclas que han sido presionadas. Un empleador puede de hecho registrar el tráfico de Internet como si se moviera a través de una intranet.

2) Programas Anti-Spy: es la manera más popular de saber si estamos siendo espiados. Los programas Anti-Spy buscan marcas o huellas que van dejando ciertos programas espías. Algunos hacen simples recorridos de cadenas de textos para encontrarlos, y otros realmente extraen e intentan remover los programas espías. En términos generales, estos programas funcionan de una manera muy similar a la de un antivirus. Tienen una lista de spyware conocidos y revisan el disco rígido buscando los rastros que dejan este tipo de aplicaciones al instalarse en la computadora. Si encuentran programas espías los eliminan, liberando a la máquina.

Hay que tener cuidado con los que utilizan solamente el recorrido de texto para hallarlos. Esta forma de búsqueda de código espía puede darnos falsos positivos y en algunos casos pueden eliminar realmente programas anti-spy.

También se deben tener en cuenta con los programas anti-spy dos cosas: primero, que igual que los antivirus requieren ser actualizados con frecuencia para evitar que los spyware nuevos no sean detectados. Segundo, que el software espía puede ser al mismo tiempo una aplicación. Por lo tanto, el uso de un limpiador borrará también la parte útil del programa.

3) Recursos del Sistema: programas espías escritos deficientemente que casi siempre pondrán manos en los recursos del sistema. Viendo que existen escasos recursos, quedándose sin memoria, detectando mucha actividad del disco o viendo parpadear la pantalla. Esto es causado por programas espías que toman fotografías de la pantalla de la computadora lo que requiere el uso de recursos importantes del sistema.

4) Acceso a la Computadora: esté atento a personas que estén intentando ganar acceso a su máquina. Muchos programas diseñados para espiar necesitan tener acceso físico a la máquina objetivo. No importa si la función en sí para la que está destinado el programa no hace uso alguno de Internet, como sería el caso de un editor de imágenes o una herramienta de verificación del disco duro. A pesar de todo, puede notar que misteriosamente el modem se pone en funcionamiento sin que haya abierto el

navegador ni el correo electrónico, ni ninguna otra de sus aplicaciones de Internet. Puede tratarse en este caso del programa espía. Si su conexión es a través de un modem telefónico, el programa delatará su presencia cada vez que intenta conectarse por los ruidos que hace el modem o por el juego de luces que muestra en el caso de un modem externo. Sin embargo, si su conexión es del tipo ADSL o cable modem, es muy probable que nunca advierta nada especial.

5) Registro de Instalaciones: actualmente existen en el mercado programas que registran cada una de las actividades de instalación de programas que ocurren en una máquina. Es mejor dejar que estos programas funcionen en segundo plano en la computadora así como lo hacen por ejemplo los anti-virus. Es posible que ellos detecten la instalación de muchos programas espías de esta manera.

6) Anti-Virus: muchos programas anti-virus pueden detectar gran cantidad de programas espías, especialmente aquellos que han sido clasificados como "Caballos de Troya" un tipo especial de virus. Mantenga el anti-virus actualizado y corriendo en segundo plano. Este es muy posible que no lo proteja de todos los programas espías pero le avisará sobre el propósito de instalación de cualquier "Trojano". Tenga en mente que los "Trojanos" como NetBus o DeepBO están también clasificados como programas espías porque permiten la apertura del sistema a conexiones externas. Sin embargo, no se sienta tranquilo por el sólo hecho de tener un anti-virus instalado. Ellos son útiles pero no son 100% seguros ante este tipo de programas.

7) Cortafuegos Personal: en el inseguro Internet de hoy en día, es de mucha utilidad la instalación de un programa denominado cortafuegos (firewall) personal. Los cortafuegos alertan tanto sobre actividad de entradas a la máquina como de salida. De esta forma se puede tener un control de las cosas que pasan en ambos sentidos, permitiendo reconocer a aquellos programas sospechosos que intentan enviar información fuera del sistema. Sin embargo, si piensa que instalando un cortafuegos personal estará seguro, esto no es así. Estos programas espías suelen utilizar en sus comunicaciones la misma forma de comunicaciones que usted utiliza cuando descarga de Internet una página, lo que normalmente se conoce como protocolo HTTP y que es utilizado por los navegadores para recorrer la red. Dado que normalmente la operación de este protocolo está permitida por su cortafuegos, su actividad puede pasar totalmente desapercibida.

8) Descargas Peligrosas: simplemente utilice el sentido común cuando realice descargas de programas de Internet y evite así el código en el cual no pueda confiar. Si usted es uno de aquellos que frecuenta los sitios de descarga de programas de distribución ilegal o que han sido modificados para instalarlos sin licencias, es mucho más probable que se cruce con uno que pueda tener incluido un "Trojano" o cualquier otro tipo de virus.

9) Sentido Común: tenga cuidado con lo que instala en la computadora. No ejecute los archivos que vienen adjuntos con sus correos electrónicos y lea los contratos de licencia de uso de los programas. Mantenga actualizados los paquetes de programas anti-spy en su máquina.

10) Programas Espías: irónicamente podremos reconocer a los programas que espían instalando primero uno de estos programas en nuestra computadora. Desde que los programas espías pueden grabar las teclas que han sido presionadas también pueden controlar y grabar la instalación de otros programas espías. Nuevamente, esto lo convierte en una carrera de armas virtual, pero esto requiere que tenga siempre en mente que muchos programas espías son vulnerables a los ataques anti-spy.

AHORA NOS QUEDA ELIMINARLOS

En las siguientes secciones desarrollamos algunos de los diferentes métodos que existen para eliminar los programas espías. Sólo recomendamos la primera de las metodologías para aquellas personas que no tienen algún conocimiento técnico en informática y el manejo de los sistemas operativos debido principalmente en que de otra manera el remedio puede ser peor que la enfermedad. Sin embargo, existen en el mercado gran cantidad de programas anti-spy muy recomendables y absolutamente gratuitos. Pueden comunicarse a cualquiera de nuestros correos electrónicos y con mucho gusto podremos recomendarles alguno que en ese momento pueda ser de utilidad para nuestros suscriptores.

A)- CÓMO FUNCIONAN LOS PROGRAMAS ANTI -SPY

En general, todos de los programas anti-spy operan de la misma forma, por lo que a continuación veremos una serie de pasos que se deben seguir para eliminar los programas espías con alguna de estas aplicaciones.

Paso 1: conviene realizar, cada vez que vamos a buscar programas espías, una actualización de la lista de spyware que puede reconocer el programa anti-spy, esto generalmente lo realizan descargando un archivo actualizado de Internet.

Paso 2: seleccionar qué partes de la computadora van a ser recorridos para la búsqueda, pueden ser discos, el registro del sistema, la memoria, etc. Recomendamos seleccionar una opción para analizar todo el sistema y que en general es la opción por defecto.

Paso 3: al hacer un clic del ratón sobre el botón de comenzar, revisará todos los archivos según las opciones seleccionadas, buscando el código que está reconocido como perteneciente a una aplicación espía. Esto puede durar un largo rato por lo que se recomienda dejarlo funcionando en segundo plano o en algún momento en que no es utilizada la computadora.

Paso 4: cuando termina el recorrido, muestra qué programas espías fueron encontrados. Suele existir alguna opción para obtener mayor información sobre cada uno de los programas encontrados. Luego, permite elegir qué cosas se eliminarán y la opción de que sea almacenado un resguardo de lo que borró para poder restaurarlo en caso en que lo haya hecho por error.

Paso 5: procede a borrar los programas que han sido seleccionados y termina el proceso.

B)- BLOQUEAR EL DOMINIO DE QUIEN ESPÍA

No es necesario ningún programa especial para realizar esto. Todo lo que necesitamos conocer es el nombre de dominio de quien intenta conectarse. Con algunos de los programas espías (que no realizan la conexión con ningún propósito legítimo, sólo para descargar publicidad y recabar información privada) es sencillo conocerlo, ya que los servidores involucrados suelen estar listados en la descripción del programa.

Una forma de bloquear el dominio es buscando en el directorio Windows un archivo sin extensión denominado Hosts, solamente Hosts. En Windows NT/2000/XP, este archivo está ubicado dentro del directorio donde está instalado el sistema operativo, en \system32\drivers\etc\).

Si este archivo no existe, puede ser creado en este momento. Abra el archivo en un editor de texto, por ejemplo con el Bloc de Notas, y agregue líneas como las que siguen:

```
127.0.0.1 ad.server.com
127.0.0.1 junk.factory.com
127.0.0.1 adspam.com
```

utilizando los nombres de estos servidores que recogen la información y que usted no desea que realicen la conexión. Lo primero que debe aparecer en la línea es el número de IP de la misma máquina en la que está, por ejemplo

127.0.0.1 y luego debe guardar el archivo. Ahora, cuando el programa intente una conexión no lo podrá hacer debido a que está enviando información a su propia máquina en vez de a su servidor central.

Por supuesto, si ya contamos con un programa que realice un filtrado, siéntase seguro de usarlo para bloquear el acceso si el programa que espía tiene que pasar a través del filtro, en vez de utilizar el archivo Hosts.

Debe saber que existen algunos programas para los cuales el truco del archivo Hosts no funcionan ya que saltan este archivo y utilizan su propio servidor de nombres.

C) - ARCHIVOS SIMULADORES

Existen programas que se hacen pasar por el servidor central de los programas espías pero que residen en nuestra propia computadora y bloquean las llamadas al exterior de los spyware. También se puede intentar con una lista de componentes que simulan ser los archivos espías para las aplicaciones en las que vienen incluidos, pero no realizan ninguna conexión a Internet, simplemente retornan valores falsos en respuesta a requerimientos de estas aplicaciones que los patrocinan.

D) - LIMPIAR LAS ENTRADAS DE PROGRAMAS DE INICIO

Los programas espías muchas veces agregan una línea que permite que sean ejecutados cuando se inicia el sistema operativo. Liberar estas entradas puede poner no solamente al programa espía en aprietos sino que también hará que la máquina inicie más rápido. También hay que notar que en ciertos casos el hecho de correr el programa asociado puede realizar una re instalación de la llamada en el inicio, e incluso también una nueva instalación del programa espía.

Bajo algunas versiones del sistema operativo Windows hay un programa que se llama MSCONFIG que permite ver y activar o desactivar las aplicaciones que deben correr al inicio. Este puede resultar muy útil para desactivar aquellos programas espías que se cargan automáticamente. Para ejecutar MSCONFIG, en el caso de tenerlo, haga un click en el botón de "Inicio", luego seleccione la opción "Ejecutar", y escriba msconfig en el cuadro, por último apriete el botón "Aceptar".

E) - PREVI NI ENDO EL I NGRESO DE ACTI VEX SPYWARE

Muchos de los productos espías que andan circulando actualmente son escritos utilizando una tecnología desarrollada por Microsoft que se denomina ActiveX. Esta peste es comúnmente instalada mediante un método que se denomina algo así como "provocados por descarga" (en inglés "drive-by download").

Afortunadamente, hay una característica de seguridad que permite configurar un bit "asesino" para los controles ActiveX que conocemos como espías, para que el sistema desactive efectivamente su funcionamiento. SpywareBlaster es un programa que sistemáticamente fija ese bit asesino a los ActiveX espías que se encuentran dentro de una lista conocida.

Fuentes:

[Http://www.spywareguide.com](http://www.spywareguide.com)

<http://cexx.org>