¿Qué es un keylogger?

Un keylogger, también llamado capturador de teclas, es un software o hardware instalado en un ordenador que tiene la capacidad de registrar y memorizar todo lo que se teclee en el teclado que va unido a dicho ordenador. Todo lo tecleado se envía a un fichero que puede ser recuperado de forma manual o de forma clandestina a la personas que instalo el keylogger sin el consentimiento del dueño del ordenador.

Cuando el objetivo del keylogger es un ordenador remoto sin un acceso directo, el keylogger puede ser enviado para su instalación sin que sepamos nada integrándolo en un programa cualquiera, un anexo a un email, o cualquier ejecutable disfrazado que se nos pueda ocurrir. El software básico de un keylogger realmente solo se compone de unas cuantas líneas de código y normalmente opera de tal forma que es indetectable en muchos casos. Esto lo hace muy peligroso si usamos nuestro sistema para temas laborales o uso personal.

Para hacernos una idea, según el usuario va tecleando cada una de las teclas, el software hace una captura de cada una de las teclas en su propio espacio de memoria o en el disco duro. Esto es particularmente un riesgo si solemos introducir contraseñas, acceder a información privilegiada o acceso a nuestras cuentas bancarias. Podemos tener el ordenador infectado con uno de estos programas y no saberlo, lo cual puede desembocar en un problema grave. Un programa de este tipo, normalmente consiste (exceptuando keyloggers más sofisticados) en dos ficheros que quedan instalados en el mismo directorio: una librería dinámica o DLL, el cual hace las capturas, un ejecutable que instala el DLL y lo activa. Hay que decir que no siempre un keylogger puede ser “maligno” y perjudicial para nuestro ordenador. De hecho, hay muchas compañías que ofrecen este tipo de programas para que los padres tengan algún control sobre la actividad de sus hijos en Internet. Se han dado casos de empresas que han instalado este tipo de software para hacer un seguimiento del trabajo de sus empleados, aunque esto no es legal.

Una vez que el keylogger ha capturado los datos de una sesión de nuestro ordenador, tiene varias formas de actuar. Si es un ordenador compartido con otras personas, la persona que lo instaló puede ir más tarde a recuperar la información que ha conseguido.

Si el ordenador es de acceso remoto, el propio keylogger puede enviar la información capturada por email sin que nosotros sepamos nada de lo que está ocurriendo. Aunque en el siguiente apartado daremos algunos consejos para combatir esta forma de robar datos privados, diremos que para evitar que el programa mande emails sin nuestro consentimiento, lo mejor es tener instalado un buen firewall, como por ejemplo el zone-alarm, el cual nos avisará si algún programa quiere acceder a Internet.

¿Qué podemos hacer contra los keylogger?

Lo primero que debemos tener es un buen antivirus y un buen anti spyware que pueda detectar estos programas. Hay que tenerlo actualizado para las nuevas versiones de los keylogger existentes que evolucionan rápidamente, pudiendo pasar desapercibidos para nuestros sistemas de protección. Como ya se ha dicho, un firewall puede detectar si algo quiere ser enviado a Internet sin nuestro permiso, y que podría ser un keylogger mandando datos capturados.

Muchos bancos en la actualidad utilizan lo que se llama un teclado virtual para evitar la captura de lo tecleado cuando accedemos al banco por Internet. Es un teclado que aparece en nuestra pantalla del monitor y donde seleccionamos nuestro código con el ratón. De esta manera el keylogger simplemente no captura nada al no utilizar el teclado.

En algunos bancos todavía no ofrecen este tipo de teclados virtuales, aunque existe una alternativa si estamos utilizando el sistema operativo Windows XP. Si nuestro banco no tiene teclado virtual para introducir la contraseña, en XP tenemos uno si seleccionamos inicio > Todos los programas > Accesorios > Accesibilidad > Teclado en pantalla. De esta manera no usaremos el teclado evitando el keylogger si sospechamos que podemos tener uno instalado. De hecho, deberíamos acostumbrarnos de meter las contraseñas de este modo.
Otro modo de burlar un keylogger y sin utilizar un teclado virtual, es cambiar de ventana varias veces mientras introducimos la contraseña. Un keylogger hace las capturas de lo que tecleamos de forma lineal y “tontamente”. Por ello, si la contraseña es “transatlántica” por ejemplo, podemos cambiar de ventana cada cierto número de letras y teclear lo que sea de forma aleatoria. No tiene que ser en un archivo no nada parecido, simplemente teclear. De esta forma el keylogger capturará todas las teclas seguidas y hará que la contraseña pierda significado. La contraseña “transatlántica” quedaría en la captura del keylogger como “trakjkjhkjhdnsatlkljvantica”. Lo importante es que cojamos la idea de esto.