Un Keylogger es un programa informático que registra las pulsaciones del teclado y guarda los datos en un archivo o envía los datos a través de Internet.

Por mucho tiempo se ha utilizado como malware del tipo daemon, debido a que usuarios mal intencionados lo utilizan para obtener datos confidenciales como contraseñas o números de tarjetas de crédito.

El registro de lo que se teclea puede hacer mediante software o hardware. Hablando del software, se instalan los programas en la computadora y al ponerlos a trabajar, comienzan a almacenar todas las pulsaciones, sin importar en qué se esté trabajando. Comúnmente estos programas pueden hacerse invisibles, para que el usuario no sepa que se está ejecutando mientras utiliza la computadora.

Puede ser utilizado por algún usuario que desea almacenar lo que escribe, o como ocurre generalmente, lo utilizan delincuentes cibernéticos para conseguir datos confidenciales, ya sea instalando el programa directamente en la computadora de la víctima, o de forma remota, mediante un troyano de conexión inversa.

Algunos programas de este tipo también incluyen la opción de crear capturas de pantalla cada determinado tiempo.

Por otro lado, cuando se utiliza un keylogger por medio de hardware, es más difícil para un delincuente instalarlo en la computadora, ya que necesariamente se debe tener acceso al teclado para poder realizar las modificaciones necesarias.

También existe hardware ya fabricado que se puede encontrar fácilmente en el mercado, existen tres tipos:

1.- Adaptadores en línea que se intercalan en la conexión del teclado, estos cuentan con la ventaja de poder instalarse de forma rápida.

Sin embargo, aunque pueden ser escondidos y muchos de los usuarios no lo notarán, puede detectarse fácilmente un con una revisión detallada.

2.- Dispositivos que se instalan dentro de los teclados estándares, estos deben soldarse y tener acceso al teclado. La ventaja de estos es que no son detectables a menos que se desarme el teclado.

3.- Teclados con el keylogger previamente instalado.

Programar un keylogger es relativamente fácil, se requiere un conocimiento básico de la API que proporciona el sistema operativo. Los keyloggers de software se dividen en tres, estos son:

1.- Basado en núcleo. Este es el método más fácil, tanto para el desarrollo como para la detección. Estos keyloggers se quedan en el núcleo, lo que permite que sean invisibles.

Por lo general siempre tienen acceso autorizado al hardware, por lo que podría ser utilizado como driver del teclado por ejemplo y acceder a la información que se pulsa.

2.- Enganchados. Estos registran las pulsaciones de las teclas mediante funciones proporcionadas por el sistema operativo. El SO activa el keylogger en el momento en que se presiona una tecla y luego realiza el registro.

4.- Métodos creativos. Para este método el programador utiliza funciones como GetAsyncKeyState, GetForcegroundWindow, entre otros. Estos son los más fáciles de desarrollar, pero como requieren de una revisión del estado de cada tecla varias veces por segundo, pueden causar un aumento en el uso del CPU, y dejar escapar algunas pulsaciones, es decir, no alcanzar a registrarlas.

Como protección, es recomendable utilizar un buen anti-spyware o anti-keylogging.