

El **keylogger** es un diagnóstico utilizado en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero o enviarlas a través de internet.

El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software. Los sistemas comerciales disponibles incluyen dispositivos que pueden conectarse al cable del teclado (lo que los hace inmediatamente disponibles pero visibles si un usuario lo revisa) y al teclado mismo (que no se ven pero que se necesita algún conocimiento de como soldarlos). Escribir aplicaciones para realizar keylogging es trivial y, como cualquier programa computacional, puede ser distribuido a través de un troyano o como parte de un virus informático o gusano informático. Se dice que se puede utilizar un teclado virtual para evitar esto, ya que sólo requiere clicks del mouse. Sin embargo, la aplicaciones más nuevas también registran pantallazos que anulan la seguridad de esta medida. Además, esto sería falso ya que los eventos de mensajes del teclado deben ser enviados al programa externo para que se escriba el texto, por lo que cualquier keylogger podría registrar el texto escrito mediante un teclado virtual.

Para prevenir este tipo de ataque con la instalación de un buen antivirus es una medida suficiente, aunque en seguridad no hay un 100% de total seguridad

Ejemplo tipo

1. El keylogger instalado en el equipo está programado para comprobar continuamente la dirección accedida por el navegador.
2. El usuario accede a la página de inicio de su banco o caja (<http://www.caja-bancoX.com>) para realizar una consulta de sus movimientos.

El troyano reconoce esa dirección y a partir de ese momento, registrará todas las pulsaciones que se efectúen sobre el teclado, que serán primero el 'nombre de usuario' y después la 'contraseña de acceso'.

3. La información capturada se envía por cualquier método al atacante (correo electrónico, IRC, etc) de modo que este sabe: el banco, el usuario y la contraseña.

Con esa información puede acceder en cualquier momento a la cuenta del usuario afectado.