**Keyloggers**

**What is a Keylogger?**

     A keylogger, sometimes called a keystroke logger, key logger, or system monitor and is a hardware device or a software program that records the real time activity of a computer user including the keyboard keys they press.

* **Software keylogger:** Unlike other types of malicious program, keyloggers present no threat to the system itself. If it is a software is a type of surveillance software considered to be spyware that has the capability to record everystroke user make to a log file, usually encrypted.
* **Hardware keylogger:**As a hardware device, is a small battery-sized plug that serves as a connector between the user's keyboard and computer. As the users types, the device collects each keystroke and saves it as a texts in its own miniature "hard drive". At a later point in time, the person who installed the keylogger must return and physically remove the device in order to access the information the device has gathered.

**A keylogger can usually used for:**

* **Parental control:** parents can track what their children do on the Internet, and can opt to be notified if there are any attempts to access websites containing adult or otherwise inappropriate content.
* **Jealous spouses or partners** can use a keylogger to track the actions of their better half on the Internet if they suspect them on "virtual cheating".
* **Company security:**using keyloggers to track the input of key words and phrases associated with commercial information which could damage the company (materially or otherwise) if disclosed.
* **Company security:** tracking the use of computers of non-work-related purposes, or the use of workstations after hours.
* **Other security (e.g law enforcement):** using keylogger records to analyze and track incidents linked to the use of personal computers.
* **Cyber criminals:**can get PIN codes and account numbers for e-payment systems, passwords to online gaming accounts, email addresses, user names, email passwords etc.

**What it can do?**

* Can capture any passwords entered by users on the device.
* Can capture a screen captures of the device at periodic intervals.
* Can capture a picture at periodic intervals if the user's device support camera.
* Can record the URLs that were visited via Web browsers and possibly also take screen captures of the Web pages viewed.
* Can record a list of the applications run by users on the device.
* Can record the time when the applications started to run by the user and also when the user started to type and where.
* Capture logs of all instant messaging sessions.
* Capture copies of sent emails.
* Automatically send the reports containing stored logs and emails to remote location (by email, FTP or HTTP).
* The whole program can hide itself and autostart.

**Is it legal to use keylogger?**

The answer is "yes" and "no" because it depends how it is being to used.

* **It is legal:**
  + If a family using it to monitor their child's activity for the purpose of maintaining their safety online.
  + When it comes to employee monitoring as long the company using it in a location where the laws permit this type of monitoring.
* **It is illegal:**
  + If using it for criminal purposes such as stealing personal data and financial information.

**How they spread?**

     Keyloggers spread in much the same way that other malicious programs spread. Excluding cases where keyloggers are purchased and installed by a user, by security services but mostly:

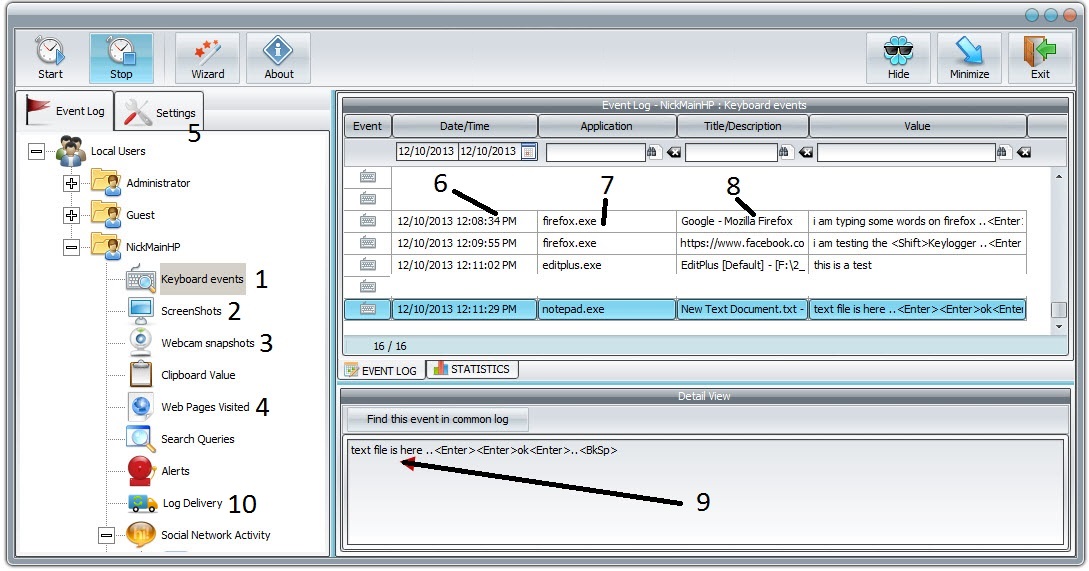
* can be installed when a user opens a file attached to an email.
* can be installed when a file is launched from an open-access directory on a P2P (peer-to-peer) network .
* can be installed via a web page script which exploits a browser vulnerability. The program will automatically be launched when a user visit an infected site.
* can be installed by another malicious program already present on the victim machine, if the program is capable of downloading and installing other malware to the system.

**How to protect from keylogger?**

     Most antivirus companies have already added known keyloggers to their databases but some more advanced keylogger programs cannon be detected from antivirus products. The most common protections:

* using one-time passwords or two-step authentication.
* using a system with proactive protection designed to detect keylogging software.
* using a virtual keyboard.
* avoid to make payments from public computers.

This is an example of how a simple keylogger software looks like:



**1. Keyboard events**(This tab shows the event, date/time, application, title/description, value, search box)

**2. ScreenShots**(Settings of screenshots eg HQ screen shot and the time interval of screenshots)

**3. Webcam snapshots**(Settings of Webcam snapshots eg time interval of snapshots)

**4. Web Pages Visited**(This tab shows the web pages that user visited)

**5. Settings**(eg. password to open the keylogger if someone find it, hide settings, run at startup etc.)

**6. Date/Time**(Date and timethat user types in the keyboard)

**7. Application**(The applicationthat user opened that time)

**8. Title/Desription**(eg. the user opened firefox.exe and was in facebook)

**9. Event Log**(This is the field that all the keystrokes are saved)

**10. Log Delivery**(The "attacker" can use a method to tell to the program how, when and where to sent all the log files and screenshots to have access to them)

This is how a hardware keylogger looks like:



Two huge disadvantages of hardware keyloggers are:

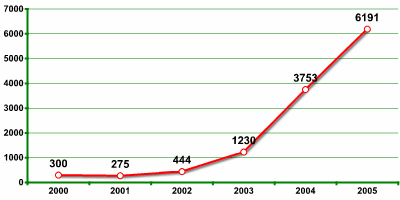
* Easy to detect.
* The "attacker" must come back physically and take the this small USB connector.

This is how a virtual keyboard looks like:



     A virtual keyboard is a software component that allows a user to enter characters. A virtual keyboard can usually be operated with multiple input devices, which may include a touchscreen, an actual computer keyboard and a computer mouse. Until today keylogger softwares **CAN'T**  detect where the mouse clicks. So users are safe to enter their online game password in the internet caffe or enter to their bank account.

Or they are not?



     Until 2005, around 6191 different keylogger softwares found and until today the number is keep growing with new modifications but also so friendly and easy in use with out any special computer knowledge. Also the number of "attackers" is growing every day who are trying to steal bank accounts, PINs and most of the times a facebook password.

    Overall keylogger softwares either are used for good or bad they still are invaders to other people privacy.

**Reference:**

* **https://en.wikipedia.org/wiki/Keystroke\_logging**
* **ZDNet: Haxdoor Trojan Claims Thousands of UK Victims**
* **https://www.refog.com/is-a-keylogger-legal.html**
* **New York Times: Cyberthieves Silently Copy Your Passwords as You Type**
* **United States Emergency Readiness Team: Home Network Security**
* **http://www.gohacking.com/how-to-use-keyloggers/**
* **https://en.wikipedia.org/wiki/Hardware\_keylogger**
* **https://www.keelog.com/**
* **http://www.keyghost.com/**
* **https://en.wikipedia.org/wiki/Hardware\_keylogger**
* **https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/**
* **http://keysoftwaresee.blogspot.co.uk/2011/04/advantages-of-keylogger-software.html**
* **http://techcloud.in/benefits-of-using-a-keylogger/**
* **https://www.keelog.com/keystroke\_recorder.html**
* **http://www.webopedia.com/TERM/K/keylogger.html**
* **http://searchmidmarketsecurity.techtarget.com/definition/keylogger**