

Forum:[Hack Forums](#)

Thread: [\[Mega-Thread\] Keyloggers | Compilation + FAQs + General Information](#)

Professor 0110 - June 7, 2011, 6:50 pm

Hello people of HackForums.net. This is another comprehensive mega thread/tutorial on keylogging, key strokes and keyloggers in general. I'm going to explain today how hackers obtain personal data from targeted people using a technique called Key Stroke Logging. I'm writing this tutorial to help all of the newbies that just registered here or the members who just wanna learn. Enough of the chit chat, this mega thread/tutorial will be divided in sections so head over to the table of contents.

Keystroke Logging

Software Based Keystroke Logging

Hardware Based Keystroke Logging

Compilation

A keystroke logger, sometimes called a keylogger, is a hardware device or a small program that monitors each keystroke a user types on his keyboard. As a hardware device, a keystroke logger is a [ps/2 connector](#) without a cable that serves as a connector between the user's keyboard and the computer. Because the device resembles as an ordinary connector it is easy for someone who wants to monitor user's actions. As the user types, the device gets each keystroke and saves it as a text file in it's own small sized HDD. So later the person who installed the keylogger must return to the computer and physically remove the device in order to get a hold of the keystrokes it has gathered.

A keystroke logging program doesn't require physical access to the computer, and it can be easily downloaded from the internet and executed as a part of a rootkit or remote administration file known as RAT. It usually consists of two files, a .DLL and a .EXE file, which does the recording of the keystrokes. Nowadays most keystroke logging programs only come with an executable file (.EXE) and without the .DLL file.

The keylogger records every keystroke the user makes and uploads it on an online FTP server or an online database which holds the keystrokes. That database belongs to whoever installed the keylogger, for later use. Keylogger programs are promoted for allowing parents to monitor their kids'

behavior on the internet, but their use is far from it. Keyloggers are mostly set-up for stealing a password from a targeted victim, in other words they are used for illegal purposes.

A log file from a keystroke logging program

A Keystroke logging program is a piece of software designated to work on the user's computer and log the keystrokes the user names. There are 5 categories, from a technical perspective:

Hypervisor-Based: The keystroke logging software can theoretically reside in a malware running underneath the operating system, which remains untouched. It effectively becomes a virtual machine, and the [Blue Pill](#) is a good example.

Kernel-Based: This method is very difficult both to write and to combat. Keystroke logging software resides at a kernel level and are difficult to detect, especially for user-mode applications. These are implemented as rootkits that subvert the operating system kernel and gain un-authorized access to the hardware making the keystroke logging software's power level beyond any limits and boundaries. A keystroke software that is kernel-based can act as a keyboard device and replicate the information typed on the real keyboard as it goes to the operating system.

API-Based: Keystroke logging software that's API-Based uses keyboard APIs. The operating system notifies the keylogger each time the user writes a key and the keylogger records it. Two of the most known windows APIs that do that are the `GetAsyncKeyState()` and `GetForegroundWindow()`. These types of keyloggers are the easiest to write, but they cause a noticeable increase amount of CPU usage and also can miss-record some keys. Keyloggers like that can be coded even by beginners at VB.NET and C#.

Form grabbing-Based: Form grabbing-based keyloggers are keyloggers that log web form submissions by recording the web browsing submit event functions. Keyloggers of this type records the data that is to be passed over the internet before it's actually sent and can bypass HTTPS encryption methods.

Remote access software keyloggers: These are local software keyloggers with a feature that allows the keylogger to access the locally stored data from a remote connection. Remote connections can be achieved by uploading the data to a website, database or a FTP server, e-mailing the data to a predefined e-mail address or the data is wirelessly transferred with the help of an attached hardware system.

Software keyloggers come with features that capture user's information without relying on keyboard key strokes as the input. There are a bunch of features, like:

Clipboard Logging: Anything that the user copies to the clipboard can be captured by the keylogger.

Screen Logging: Screenshots of the desktop are taken and are saved at a specified location or directly uploaded to a website, database or a FTP server. Applications with screen logging functions

may take screenshots of the whole screen or just some applications or even just a small place around the mouse cursor.

Antis: Some keyloggers have an option where you can choose an option to automatically kill the process of an antivirus or a software that prevents malware from being installed in your computer.

Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords. They can be implemented via BIOS-level firmware, or alternatively, via a device plugged inline between a computer keyboard and a computer. They log all keyboard activity to their internal memory. Hardware keyloggers have an advantage over software keyloggers as they can begin logging from the moment a computer is turned on.

There are various types of hardware keyloggers, like:

Regular Hardware Keylogger: A regular hardware keylogger is used for logging a keystroke by the means of a hardware circuit that's attached somewhere in between the computer keyboard and the computer. A hardware keylogger has an advantage over a software solution; because it is not dependent on the computer's operating system it will not interfere with any program running on the target machine and hence cannot be detected by any software.

Wireless Keylogger Sniffers: A WKS (Wireless Keylogger Sniffers) collect packets of data being transferred from a wireless keyboard and its receiver and then attempt to crack the encryption key being used to secure wireless communications between the two devices.

Firmware Keyloggers: A computer's BIOS, which is typically responsible for handling keyboard events, can be reprogrammed so that it records keystrokes as it processes them.

A screenshot of a hardware based keylogger

[img]<http://upload.wikimedia.org/wikipedia/commons/1/11/Keylogger-hardware-PS2.jpg>[img]

Keyloggers: (Note: I'm not responsible if the downloads are infected, you are responsible!) [Rapzo Logger v 1.5 \(Public Edition \) \[Firefox , No-Ip, FileZilla \] 0/32 FUD 100%](#)

[Jays Keylogger v1 \[TONS of Features!\]\[Icon Changer\]\[File Binder\]\[ANTIS\]\[Stealers\]](#)

[\[UD 4/33\] Grieve Logger V4 \[Binder At Last\]\[Many Features\]\[Awesome GUI\]\[Stable\]](#)

[\[Preview\]Promind Keylogger Private 3.0\[FUD\]\[More Functions\]\[Screen shots\]\[GUI\]](#)

[\(Noob-Friendly\) V0.3D \[In-Dev\]\[Polymorphic/Unique Output\] Polymorphic Keylogger V0.3d \[100% FUD\]\[Stable\]\[56KB Bin\]](#)

[\[UD\]Predator Pain 4.x.x\[Free V.\]\[Binder\]\[Stealers many\]\[Keylogger\]\[Encryption\]New D/L](#)

[\[UD\]\[Cyber-Shark ? Zero Edition\]\[Multi-Stealers\]\[Stable\]\[FREE & Noob-Friendly\]](#)

[\[reFUD\] \[UD\] \[PUBLIC\]Decay Logger Public Version\[ICON CHANGER\] \[VB.Net\] \[100% Unique\]](#)

Tutorials:[\[TuT\]How To Make A Advanced Keylogger & Stealer Using Drops Detection 2/20 \[Source\]](#)

[\[TuT\] How to make ALL Trojan/Virus/Keylogger UNDETECTABLE](#)

[How To Make Your Keylogger FUD 100% Without Crypter/Encryption!!!](#)

[\[TuT\] Make Own FUD Keylogger in Visual Basic \(Pictures Included\)](#)

[\[TUT\]\[VB8-10\] How to Make a Simple eMail Sending Keylogger! \[N00B FRIENDLY\]\[VIDEO+SOURCE\]](#)

That's it for this tutorial.
If u need any help
with keyloggers
please PM me
I'll gladly
help!

John* - June 8, 2011, 8:18 am

That is one of the greatest tutorials i have seen in awhile. This deserves sticky and it should be sticky without any doubt.

Mr Kewl - June 8, 2011, 8:35 am

Good thread,
Thanks for it.

Professor 0110 - June 8, 2011, 9:06 am

No problem to both of you guys, glad you had a good read. Also, if you have any queries regarding keyloggers please contact me via PM or post in this thread. I'll gladly help you in any way, shape or form. :)