Presentation about keyloggers

By

J.Jowin Helen Annie

III CSE

Reg.No.: 950921104015

Introduction to keyloggers

## Keyloggers

**A keylogger or keystroke logger**/keyboard capturing is a form of [malware](https://www.fortinet.com/resources/cyberglossary/malware) or hardware that keeps track of and records your keystrokes as you type. It takes the information and sends it to a hacker using a [command-and-control (C&C) server](https://www.fortinet.com/resources/cyberglossary/command-and-control-attacks). The hacker then analyzes the keystrokes to locate usernames and passwords and uses them to hack into otherwise secure systems.

## Types of Keyloggers

A software keylogger is a form of malware that infects your device and, if programmed to do so, can spread to other devices the computer comes in contact with. While a hardware keylogger cannot spread from one device to another, like a software keylogger, it transmits information to the hacker or hacking organization, which they will then use to compromise your computer, network, or anything else that requires authentication to access.

### Software Keyloggers

Software keyloggers consist of applications that have to be installed on a computer to steal keystroke data. They are the most common method hackers use to access a user’s keystrokes.

A software keylogger is put on a computer when the user downloads an infected application. Once installed, the keylogger monitors the keystrokes on the operating system you are using, checking the paths each keystroke goes through. In this way, a software keylogger can keep track of your keystrokes and record each one.

After the keystrokes have been recorded, they are then automatically transferred to the hacker that set up the keylogger. This is done using a remote server that both the keylogger software and the hacker are connected to. The hacker retrieves the data gathered by the keylogger and then uses it to figure out the unsuspecting user’s passwords.

The passwords stolen using the key logger may include email accounts, bank or investment accounts, or those that the target uses to access websites where their personal information can be seen. Therefore, the hacker's end goal may not be to get into the account for which the password is used. Rather, gaining access to one or more accounts may pave the way for the theft of other data.

### Hardware Keyloggers

A hardware keylogger works much like its software counterpart. The biggest difference is hardware keyloggers have to be physically connected to the target computer to record the user's keystrokes. For this reason, it is important for an organization to carefully monitor who has access to the network and the devices connected to it.

If an unauthorized individual is allowed to use a device on the network, they could install a hardware keylogger that may run undetected until it has already collected sensitive information. After hardware keystroke loggers have finished keylogging, they store the data, which the hacker has to download from the device.

The downloading has to be performed only after the keylogger has finished logging keystrokes. This is because it is not possible for the hacker to get the data while the key logger is working. In some cases, the hacker may make the keylogging device accessible via Wi-Fi. This way, they do not have to physically walk up to the hacked computer to get the device and retrieve the data.

## How to Detect a Keylogger?

The simplest way to detect a keylogger is to check your task manager. Here, you can see which processes are running. It can be tough to know which ones are legitimate and which could be caused by keyloggers, but you can differentiate the safe processes from the threats by looking at each process up on the internet. In some cases, you may find a warning written by another user regarding a process, or several processes, that indicate keylogger activity.

To access the task manager in Windows, right-click on the taskbar, and then choose "Task Manager" from the menu.

In this window, each program under the Apps section are the ones in use by your computer, which will appear in windows on your screen. You will not see a keylogger in this section. However, you may be able to find one by looking through the Background processes section.

Another good place to look for keyloggers is under the Startup tab. Keyloggers get set up to run all the time on a computer, and to do that, they need to be started up with the operating system. As you peruse the Startup list, look for anything you cannot remember installing yourself. If something seems out of place, click on its line and then click on the Disable button on the lower-right side of the window.

You can also check for keyloggers by examining your computer’s internet usage report. To access this in Windows, press the Windows button and “I” at the same time. This will bring you to the settings screen. Here, you should choose "Network & Internet," then "Data usage." A list of the programs that your computer is using to access the internet will appear. If anything seems suspicious or you simply do not recognize it, do a search to investigate what it is. It may be a keylogger.

## How Keyloggers Attack Your Device?

To gain access to your device, a keylogger has to be installed inside it or, in the case of a hardware keylogger, physically connected to your computer. There are a few different ways keyloggers attack your device.

### Spear Phishing

[Spear phishing](https://www.fortinet.com/resources/cyberglossary/spear-phishing) is one of the most prominent methods of initiating a malware infection. In most cases, a phishing email or link is used to target a consumer. The link looks legitimate—it may even appear to come from a relative or a friend. However, after you open the email or click on a link, a keylogger is installed on your device. Spear-fishing attacks may also be used to launch a sextortion attack.

### Drive-by Download

Drive-by downloading refers to when a keylogger is installed on your computer without you knowing. This is often accomplished using a malicious website. When you visit the site, malware gets installed on your computer. It then works in the background, undetected, logging your keystrokes, then sending them to the attacker.

## How to Protect My Devices from Keylogging?

The best way to protect your devices from keylogging is to use a high-quality antivirus or [firewall](https://www.fortinet.com/resources/cyberglossary/firewall). You can also take other precautions to make an infection less likely.

You may use a password manager to generate highly complex passwords—in addition to enabling you to see and manage your passwords. In many cases, these programs are able to auto-fill your passwords, which allows you to bypass using the keyboard altogether.

If you are not typing, a keylogger cannot record any strokes, and since password characters are usually replaced by asterisks, even a video surveillance system would not be able to figure out what was entered. In addition, use [multi-factor authentication (MFA)](https://www.fortinet.com/resources/cyberglossary/multi-factor-authentication) when you have the option. A keylogger may deduce your password, but  the second phase of the authentication process may deter them.

A virtual keyboard can also help prevent keyloggers from accessing your keystrokes. Even a hypervisor-based keylogger, which uses a separate operating system running underneath your main one, cannot access keystrokes performed on a virtual keyboard. On a Windows computer, you can press the Windows key and “R” at the same time to access its virtual keyboard.

It is also a good idea to periodically check the hardware connections on your computer. While hardware keyloggers are not as common, the back of a PC’s tower may be an inviting [attack surface](https://www.fortinet.com/resources/cyberglossary/attack-surface) for a keylogging hacker. This is also true when working on a public computer. The attacker may have installed a hardware keylogger days or weeks before you log in to your bank, brokerage, or email accounts.

**Prevention from key-loggers :** These are following below-

1. **Anti-Key-logger –** As the name suggest these are the software which are anti / against key loggers and main task is to detect key-logger from a computer system.
2. **Anti-Virus –** Many anti-virus software also detect key loggers and delete them from the computer system. These are software anti-software so these can not get rid from the hardware key-loggers.
3. **Automatic form filler –** This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed .
4. **One-Time-Passwords –** Using OTP’s as password may be safe as every time we login we have to use a new password.
5. **Patterns or mouse-recognition –** On android devices used pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.
6. **Voice to Text Converter** – This software helps to prevent Keylogging which targets a specific part of our keyboard.