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 keylogger attacks your device and what it gets

Financial and identity theft: Keyloggers capture sensitive financial data such as bank account details, credit card numbers, and online payment information, enabling fraudsters to make unauthorized purchases or empty your accounts. They also steal login credentials for online shopping and other services, which can then be sold on the dark web or used to open new accounts in your name.

1.**Compromise of personal and professional information:** The malicious software records everything you type, including private messages on social media or email, work-related documents, and other personal data. This gives attackers a transcript of your communications, which can be used for blackmail or corporate espionage. In a business setting, it can lead to the compromise of confidential client data or intellectual property.

2.**Widespread security breaches:** The theft of login credentials for one account can lead to more widespread security compromises. Since many people reuse passwords across different platforms, criminals can use a keylogger to gain access to multiple accounts, from email and social media to other sensitive corporate systems. This can result in further security breaches and the installation of other, more dangerous malware.