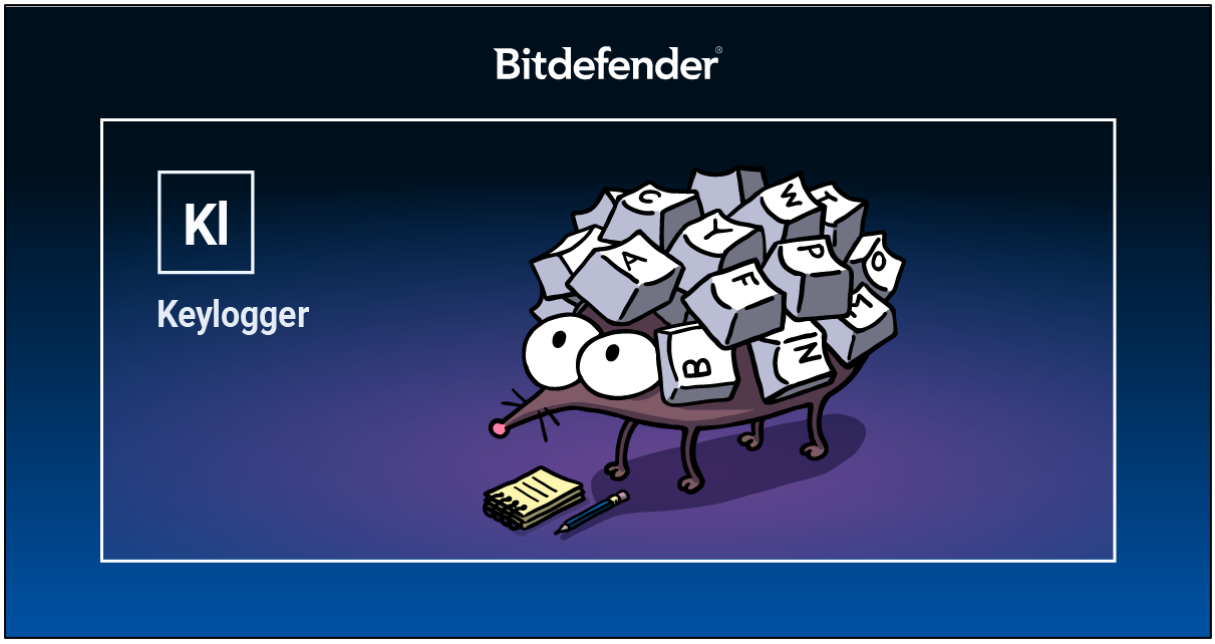
What is a Keylogger? Prevention & Removal

In this article, you will learn more about the Keylogger – an info-stealer that harvests sensitive information from infected systems and has keyboard logging and screenshot capabilities, as well as the ability to extract information from systems' clipboards.

What is a Keylogger?

Imagine you're in front of an ATM and the next person in line peers over your shoulder as you enter your credit card's PIN number on the keypad. That wouldn't feel right, would it? A keylogger practically does the same, except data theft does not take place over your shoulder but gets collected from underneath the keypad. This highly specialized surveillance software allows an attacker to log keystrokes, mouse movements, and virtual on-screen key presses inside browsers or applications. Keyloggers come in both software and hardware versions (physical devices that sit between the computer and the keyboard), albeit the former are the most widely spread.



While allowing normal operation of the infected computers, they monitor, log, and send each keystroke to a remote location, either using e-mail or FTP services. While some keyloggers are sold as legit, commercial software designed to monitor children's online activity, most of these apps are used for malicious purposes, such as stealing login credentials, spying on users' activity, or intercepting banking information.

Modern keyloggers are extremely sophisticated: they can only monitor activity within specific applications or web pages to keep the size of log files to a minimum. For instance, they can record only information passed to specific forms belonging to specific URLs (the primary targets are online stores, e-banking services, or e-mail service providers).

Who uses keyloggers and why?

There are plenty of reasons to use a keylogger, most of them bad. Keyloggers are mainly abusively used by jealous spouses or come bundled with Trojans to steal login credentials. Sometimes, keyloggers are used legally, by parents to monitor how their children use the family computer or even by companies attempting to discourage employees from using the company computers for personal purposes.

What happens when you get a keylogger?

A system monitored by a keylogger – be it software or hardware-based – intercepts everything you type and clusters the information by application. Occasionally, the keylogger takes screenshots, which are stored along with the text in a local database. This technique is used by keyloggers to re-compose passwords entered via on-screen keyboards – an anti-keylogging feature used mostly by e-banking platforms. From time to time, the database gets sent to the person that controls the keylogger.

How to know if you're getting key logged. Simple tips to stay safe

Keyloggers are extremely difficult to detect, especially on computers you don't own or manage, like those in coffee shops, public libraries, or hotel lobbies. This is why you should avoid as much as possible logging into your accounts on public computers. If possible, use a live Linux distribution to boot the respective computer from, run your errands, and then shut it down normally.

To help protect yourself against keylogger attacks, always verify the origin and validity of correspondence before interacting with links or attachments. Ensure that accounts are protected via two-factor (2FA) or multi-factor (MFA) authentication processes that will prevent hackers from logging into accounts should your system get compromised.

On your home devices, make sure to have a security solution installed and keep it up to date. An antimalware solution automatically scans your system and takes appropriate action when keyloggers are found.