2021

Keylogger

ISMS
AREEB HUSSAIN

JAN 18,2021 |

Table of Contents

1. What is a Keylogger?

Short for Keystroke logging, Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party.

Criminals use keyloggers to steal valuable information like

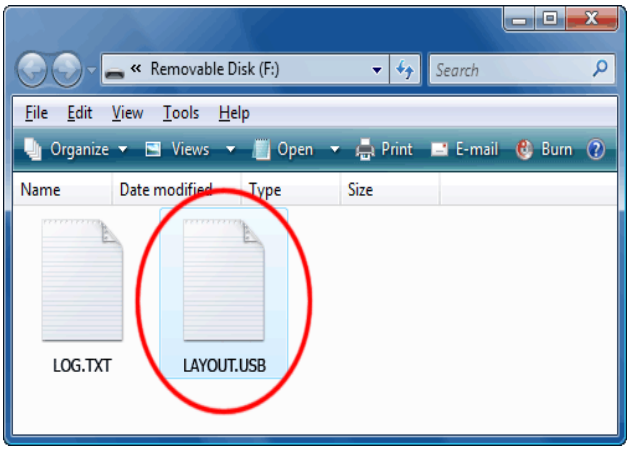
- Usernames and passwords
- Credit card number and verification code
- Chat history
- Applications you have used
- Documents you have opened

However, they also have legitimate uses within businesses to troubleshoot, improve user experience, or monitor employees. Law enforcement and intelligence agencies also uses keylogging for surveillance purposes.
Unlike other types of malicious programs, keyloggers present no threat to the system itself. Nevertheless, they can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard. As a result, cybercriminals can get PIN codes and account numbers for e-payment systems, passwords to online gaming accounts, email addresses, usernames, email passwords, etc.

2. How does keylogger works?

A keylogger can be installed on your computer any number of ways. Anyone with access to your computer could install it; keyloggers could come as a component part of a virus or from any application installation. keyloggers have root-kit functionality. That means they're hiding in your system. It records every keystroke that the user inputs and discreetly stores in a log.txt file. If it is a software keylogger then you can remotely access the data logs or if it is a hardware keylogger you have to connect the keylogger in-line between the keyboard and computer. It will record keystrokes and store the data logs on your system. After the targeted user have left the vicinity, the attacker can access the data logs on the same computer or disconnect the Keylogger and retrieve the data later.

https://www.researchgate.net/figure/USB-Keylogger-Keelogger_fig5_228797653



https://www.keelog.com/usb-keylogger/

3. Types of Keyloggers

Keyloggers can be divided into two categories: keylogging devices and keylogging software. Keyloggers which fall into the first category are usually small devices that can be fixed to the keyboard or placed within a cable or the computer itself. The keylogging software category is made up of dedicated programs designed to track and log keystrokes.

3.1 Keylogger Software:

The most common methods used to install keylogging software are as follows.

Trojan virus/Phishing email

Hackers sometimes use Trojan viruses to deliver and install keyloggers via phishing and fake emails and attachments. While phishing emails are fake emails that appear to be from a known source, hackers also can get to know something about you and send fake emails with things such as coupons you might be interested in — and might click on. New keylogger Trojans are frequently being written to steal payment data entered online by device users.

Webpage script

Keyloggers can get into your devices when you visit a fake or malicious website. The web page script is then able to exploit a vulnerability in your browser.

Infected system

Keyloggers can exploit an already-infected device or system and install other malicious software into that system.

Remote- access software keyloggers can allow access to locally recorded data from a remote location. This communication can happen by using one of the following methods:

- Uploading the data to a website, database, or FTP server.
- Periodically emailing data to a predefined email address.
- Software enabling remote login to your local machine.

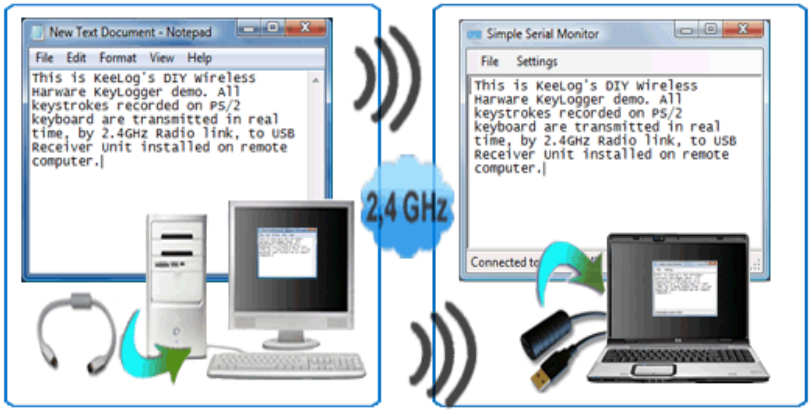
Some examples of Keyloggers are keylogger elite PRO, Windows Keylogger, Kidloggeretc.

3.2 Keylogger Hardware:

Hardware-based keyloggers can monitor your activities without any software being installed at all. Examples of these include:

- **Keyboard hardware:** These loggers take the form of a piece of hardware inserted somewhere between the computer keyboard and the computer, typically along the keyboard's cable connection. There are of course more advanced implementation methods that would prevent any device from being visible externally. This type of hardware keylogger is advantageous because it is not dependent on any software nor can it be detected by any software.

- **Wire-less keylogger/Airdrive:** It is possible for the signals sent from a wireless keyboard to its receiver to be intercepted by a wireless sniffer.
- **Keyboard overlays:** Overlays are popular in ATM theft cases where thieves capture a user's PIN number. This device is designed to blend in with the machine so that people are unaware of its presence.



https://www.keelog.com/

4. Advantages of Keylogger

- 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 of “virtual cheating”.
- Company security: tracking the use of computers for non-work-related purposes, or the use of workstations after hours.
- Company security: using keyloggers to track the input of keywords and phrases associated with commercial information which could damage the company (materially or otherwise) if disclosed.
- Other security (e.g., law enforcement): using keylogger records to analyse and track incidents linked to the use of personal computers.

5. How to detect keyloggers

It’s important to recognize the warning signs that a keylogger may have infected your system. Hardware may be easier to spot, like a new USB drive that is attached to your computer.
Keylogger software may be more difficult to detect. Common signs your device has been infiltrated can include slower computer performance when browsing or starting programs, abnormal delays in activity, pop-ups, new icons on your desktop or system tray, or excessive hard drive or network activity.

There are a variety of ways to detect a keylogger, though none are a catchall, so if you have reason to suspect your computer has a keylogger, we recommend trying a variety of these tactics:

- Begin by running your antivirus, which can often detect a keylogger on your system.
- Run a program like Spybot Search and Destroy or MalwareBytes to check for certain types.
- Check your task list by pressing ctrl+alt+del in Windows. Examine the tasks running, and if you are unfamiliar with any of them, look them up on a search engine.

- Scan your hard disk for the most recent files stored. Look at the contents of any files that update often, as they might be logs.

- Use your system configuration utility to view which programs are loaded at computer start-up. You can access this list by typing “msconfig” into the run box.

6. How to protect yourself from keyloggers

Let’s take a closer look at the methods that can be used to protect against unknown keyloggers or a keylogger designed to target a specific system.

6.1 Anti-Keyloggers

An **anti-keylogger** (or **anti–keystroke logger**) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on a computer. Anti-keyloggers detect keyloggers on your computer by comparing your files against those in a keylogger database. Examples are iSpy, Zemana Anti-logger, SpyShelter premium, Data guard anti keylogger etc.

6.2 Anti-spyware/Anti-virus

These applications can’t catch hardware-based keyloggers, but they can detect, quarantine, disable, and eradicate many software-based keyloggers. It uses heuristic and behaviour analysis to detect this type of malware. So, if it finds a program recording and sending your keystrokes, it will raise a red flag and act accordingly.

6.3 Network monitors

Network monitors (also known as reverse-firewalls) can be used to alert the user whenever an application attempts to make a network connection. This gives the user the chance to prevent the keylogger from "phoning home" with their typed information.

6.4 Automatic form fillers

Automatic form-filling programs may prevent keylogging by removing the requirement for a user to type personal details and passwords using the keyboard. Form fillers are primarily designed for Web browsers to fill in checkout pages and log users into their accounts. Once the user's account and credit card information has been entered into the program, it will be automatically entered into forms without ever using the keyboard or clipboard, thereby reducing the possibility that private data is being recorded.

6.5 One-time passwords

Using a one-time password can help minimize losses if the password you enter is intercepted, as the password generated can be used one time only, and the period during which the password can be used is limited. Even if a one-time password is intercepted, a cyber criminal will not be able to use it to obtain access to confidential information.

In order to generate one-time passwords, you can also use mobile phone text messaging systems that are registered with the banking system and receive a PIN-code as a reply. The PIN is then used together with the personal code for authentication.

6.6 On-screen Keyboards/Virtual Keyboards

Some keyboards don't use the QWERTY layout. That means the keystrokes tracked won't translate, because most keyloggers rely on the traditional layout. Virtual keyboard software enables you to input characters without typing on actual keys. However, on-screen keyboards aren't a very popular method of outsmarting keyloggers. They were not designed to protect against cyber threats, but as an accessibility tool for disabled users. Information entered using an on-screen keyboard can easily be intercepted by a malicious program.

https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/

7. Security controls to prevent Keylogging according to ISO 27k2

7.1 Hardware Keylogger prevention

A 11.1.2 – Physical entry controls

a) There should be monitoring and recording of visitor's entry and exit times. Only authorized access should be given to visitors upon thorough checking.

b) Company should implement two factor authentication mechanism for areas with systems containing confidential information.

c) The organization should maintain a physical logbook or electronic trail of all access.

d) To better identify people roaming around in restricted areas or in general public access places of the premises. All employees and crew/staff must wear a visible identification. Visitors or unauthorized personnel should be identified immediately with this method

A.11.1.3 – Securing offices, rooms, and facilities

b) Identification of the access-restricted rooms/areas should be kept to a minimum. If, in case an intruder makes his way in, he would not be given obvious signs of presence of areas containing information processing activities.

d) Locations of confidential information processing facilities through directories or internal books should not be readily accessible to anyone unauthorized.

A.11.2.8 – Unattended user equipment

b) When leaving their desk, employees should log off from their system and network services.

c) Computer systems should be secured by a key lock when not in use.

7.2 Software Keylogger Prevention

A.12.2.1 – Controls against malware

a) Strict policy should be drafted which forbids the installation of unauthorized software's.

b) The organization will make use of application whitelisting to keep in check, which types of software's are being installed by the employee. The company has all the right to delete or disable any application and will only permit installing application deemed required by the administrators. A basic way is to create a software shop of preselected authorized software.

c) The organization should also make use of blacklisting to block unauthorized websites which could contain malware and could potentially be a way for a software keylogger attack

g) There should be regular update for malware protection (Firewalls etc.) and detection applications. The files received over the network, webpages, email attachments should be routinely scanned for any hiding malware.

Moreover, malware protection should deny starting any suspicious software.

h)/A.7.2.2) Employees should be given adequate training to make sure that their systems are protected by malware which includes taking personal responsibilities and familiarizing with recovery methods from malware attacks.

A.12.5.1 – Installation of Software on operating systems

a) Only trained administrators are in charge of downloading and updating software application on the employee's system

c) Before being implemented, the software should be tested which covers usability, security, and user friendliness.

12.6.2 – Restriction on Software installation

The organization should draft and implement a policy on which types of software's are permitted and forbidden to install. Usually, the administrators are responsible for installing and updating software's but if the employees are given this privilege, there should be clear guidelines for them follow

8. References

1. https://www.keelog.com/
2. https://en.wikipedia.org/wiki/Keystroke_logging
3. https://us.norton.com/internetsecurity-malware-what-is-a-keylogger
4. https://morioh.com/p/d3f49699389a
5. https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/tech_keystrokelogging.html
6. https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/
7. https://www.makeuseof.com/tag/track-what-others-do-on-your-computer-ispy/
8. https://www.veracode.com/security/keylogger
9. https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/
10. http://www.securityfocus.com/infocus/1829
11. http://www.pcworld.com/article/id,94603-page,1-c,privacysecurity/article.html
12. http://msdn2.microsoft.com/en-us/library/ms644990(VS.85).aspx
13. http://www.usatoday.com/tech/news/2001/12/27/fbi-snooping.htm
14. http://epic.org/crypto/scarfo/opinion.html
15. http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=25471
16. http://www.wired.com/politics/law/news/2007/07/fbi_spyware
17. http://www.pcworld.com/article/id,78070-page,1/article.html