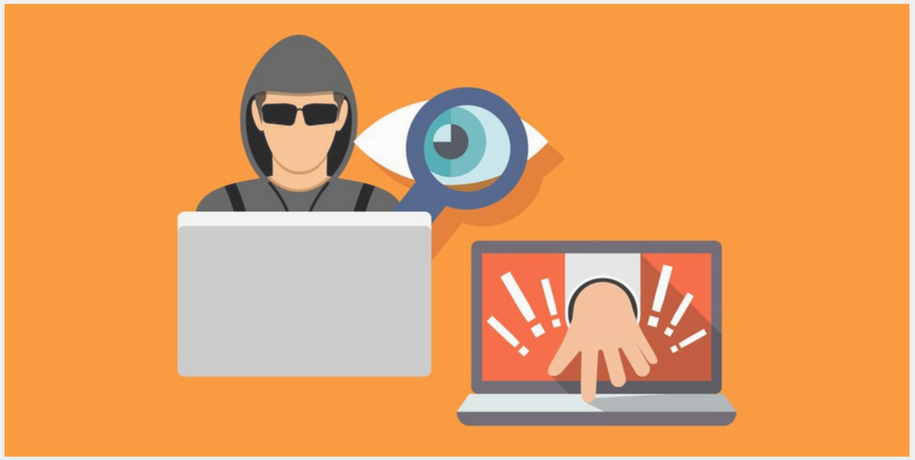

Keyloggers and security

Presented by:
S.Naveen Kumar
priyadarshini engineering college
cse(dp)

Outline

1.Introduction
2.Definition of Keyloggers
3.Types of Keyloggers
4.Detect a Keylogger
5.Protecting devices form keyloger
6.Conclusion

Introduction

A keylogger or keystroke logger/keyboard capturing is a form of 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.

Definition of Keyloggers

A keylogger is a type of spyware that records and tracks your keystrokes, and then sends the information to a hacker using a command-and-control (C&C) server. The hacker can then use the keystrokes to find passwords and usernames to gain access to secure systems. Keyloggers can be hardware-based or software-based, and can capture information such as:

Passwords
Credit card numbers
Web pages
Screenshots
Clipboard contents
Microphone or webcam inputs

Type of keylogers

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.

There are two type

- Hardware keyloger
- Software keyloger

Software keyloger

- software keyloggers consist of applications that have to be installed on a computer to stealkeystroke 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.

Hardware keyloger

- 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.

Detection of 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.

Protecting devices form keylogers

1.

Keep your operating system and security software up-to-date
2.Use firewall protection
3.Use a secure browser and a virtual private network (VPN), especially when connecting to public Wi-Fi
4.Use automatic form filler
5.Use one-time-passwords (OTPs) as password
6.Use patterns or mouse-recognition
7.Use voice to text converter software

conclusion

Keyloggers are a serious threat to users and their data, as they can track keystrokes to intercept sensitive information typed through the keyboard. This includes passwords, credit card numbers, email IDs, and other confidential information. If this data falls into the wrong hands, it can lead to identity theft, financial loss, and other serious consequences

End

Thank you

Do you have any questions?