



KEYLOGGERS

A.SARANYA

CSE-3RD YEAR

UNIVERSAL COLLEGE OF
ENGINEERING AND TECHNOLOGY

OUTLINE:

- What is KEYLOGGERS
- Types of KEYLOGGERs
 - Hardware
 - Software
- Uses of KEYLOGGERs
- Advantages of KEYLOGGERs
- Disadvantages of KEYLOGGERs
- Problem statement
- Conclusion

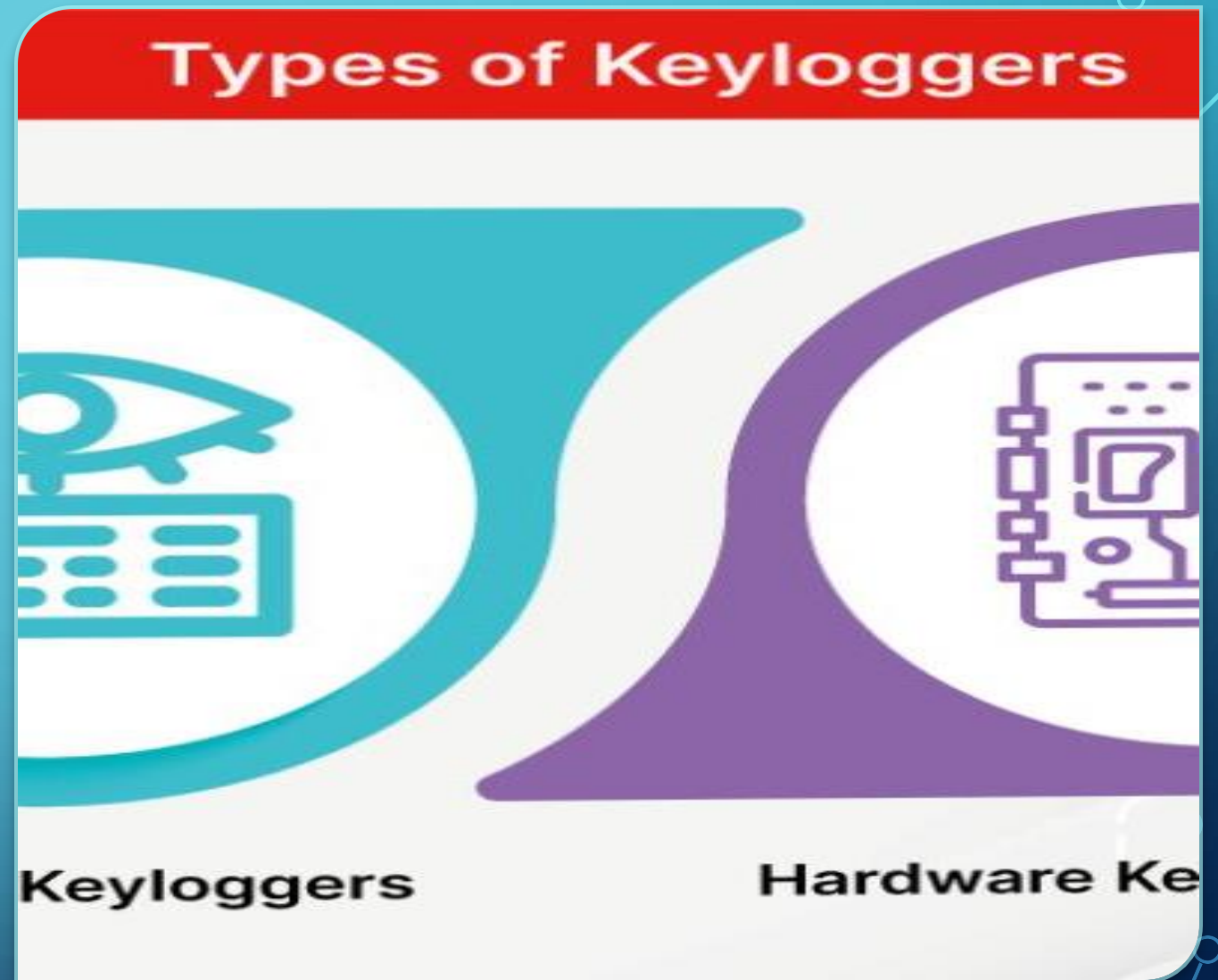
WHAT IS KEYLOGGERS:

Keyloggers are tools that can record every keystroke that you type into a computer or mobile keyboard. Because you interact with a device primarily through the keyboard, keyloggers can record a lot of information about your activity. For example, keyloggers can track credit card information that you enter, websites you visit and passwords you use.



TYPES OF KEYLOGGERS:

- Hardware KEYLOGGERS
- Software KEYLOGGERS



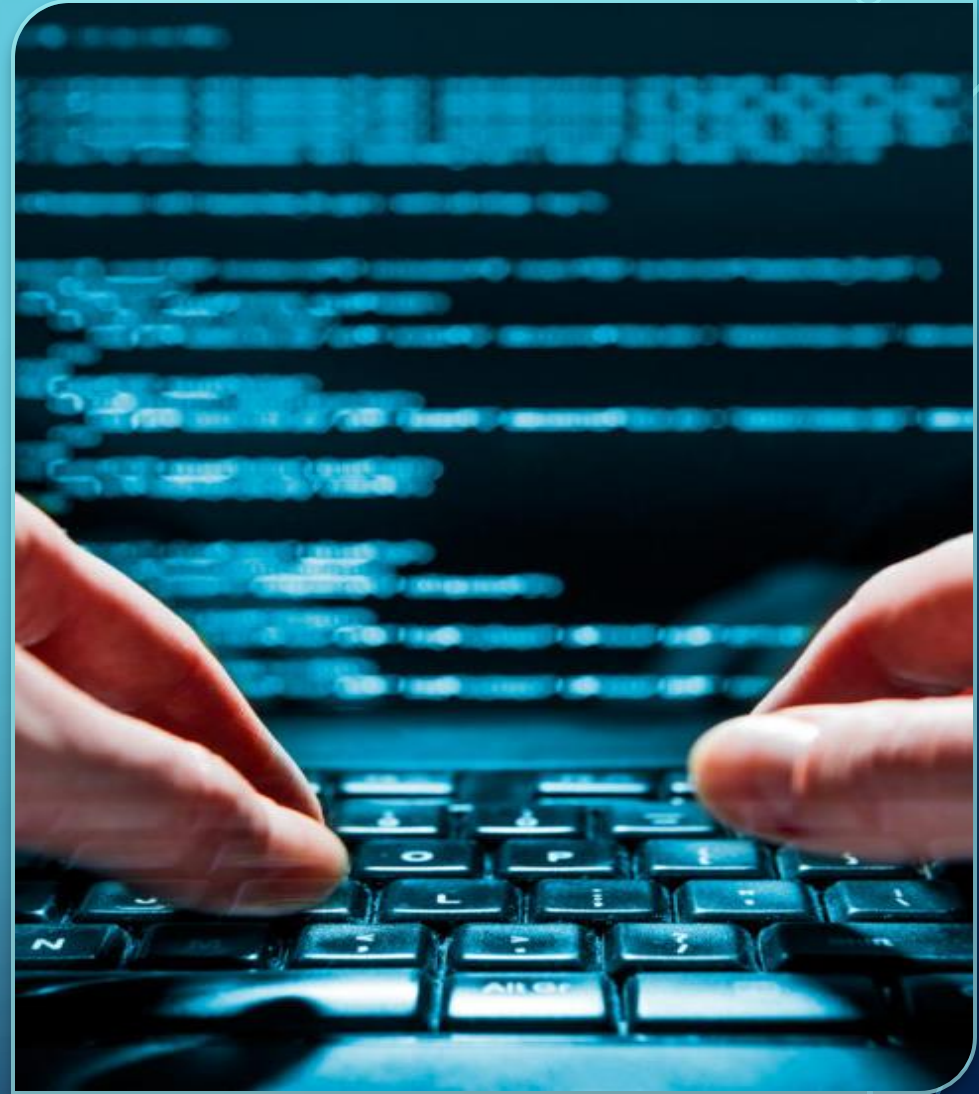
HARDWARE KEYLOGGERS :

- Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords.
- They can be implemented via BIOS-level firmware, or alternatively, via a device plugged inline between a computer keyboard and a computer.



SOFTWARE KEYLOGGERS:

- Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored.
- Data can then be retrieved by the person operating the logging program.



USES OF KEYLOGGERS:

- Keyloggers are tools that can record every keystroke that you type into a computer or mobile keyboard.
- Because you interact with a device primarily through the keyboard, keyloggers can record a lot of information about your activity.

ADVANTAGES OF KEYLOGGERS:

- Full Transparency. ...
- More Productivity. ...
- Clearer Understanding of Performance. ...
- Less Risk of Data Theft. ...
- Better Password Access. ...
- Tougher Deterrent Against Phishing and Viruses. ...
- Clearer Protection Against Liability.

DISADVANTAGES OF KEYLOGGERS:

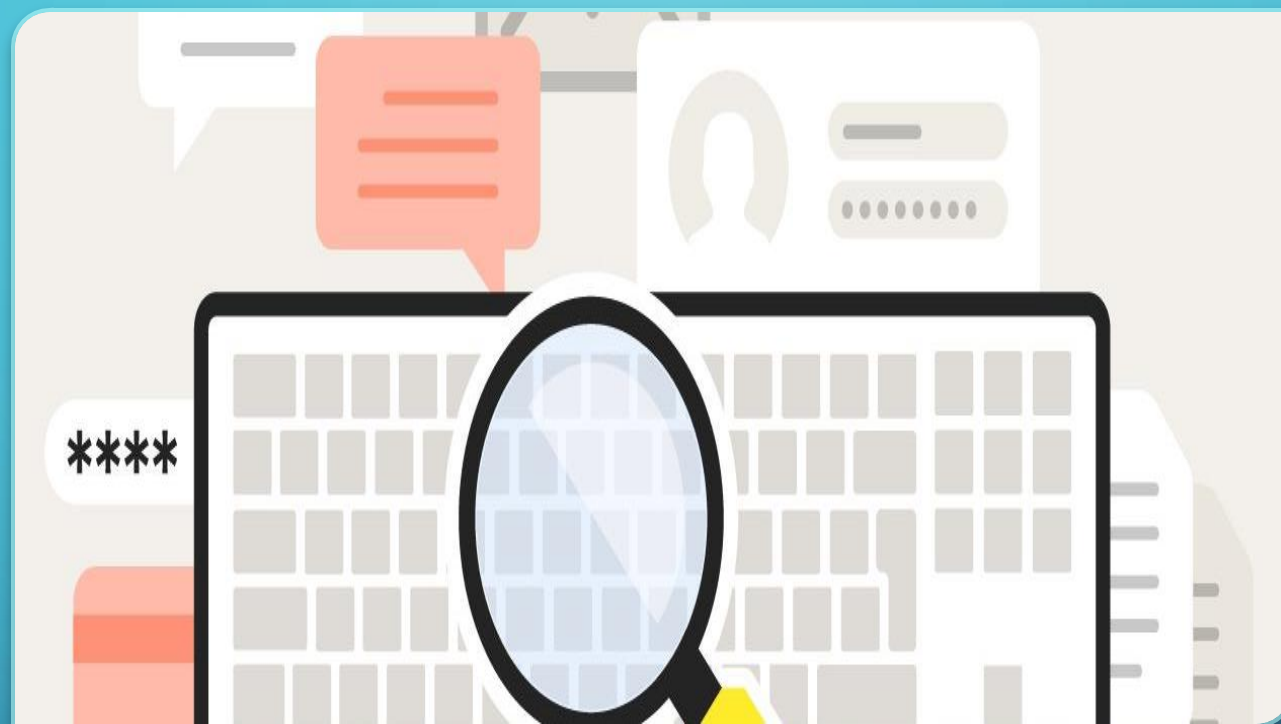
- It can be Spotted by a Suspicious user.
- Although there are some legitimate uses of keyloggers, such as in the workplace, or to track the internet activities of children, you are also at risk of these programs turning your computer into a spy for hackers.
- . If this data falls into the wrong hands due to a malicious keylogger, it can lead to identity theft, financial loss, and other serious consequences.

PROBLEM STATEMENT:

- The problem statement is that the keyloggers can be detected using antiviruses. Installation of hardware keyloggers is difficult without the knowledge of the owner of the system.
- The solution to the above existing problem is that we can build a software keyloggers instead of hardware keyloggers.

CONCLUSION:

- Keyloggers are a potent threat to both individuals and enterprises, with the potential to cause significant harm if left undetected.
- 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.



THANK YOU!