KEYLOGGERS PROJECT

PRESENTED BY:

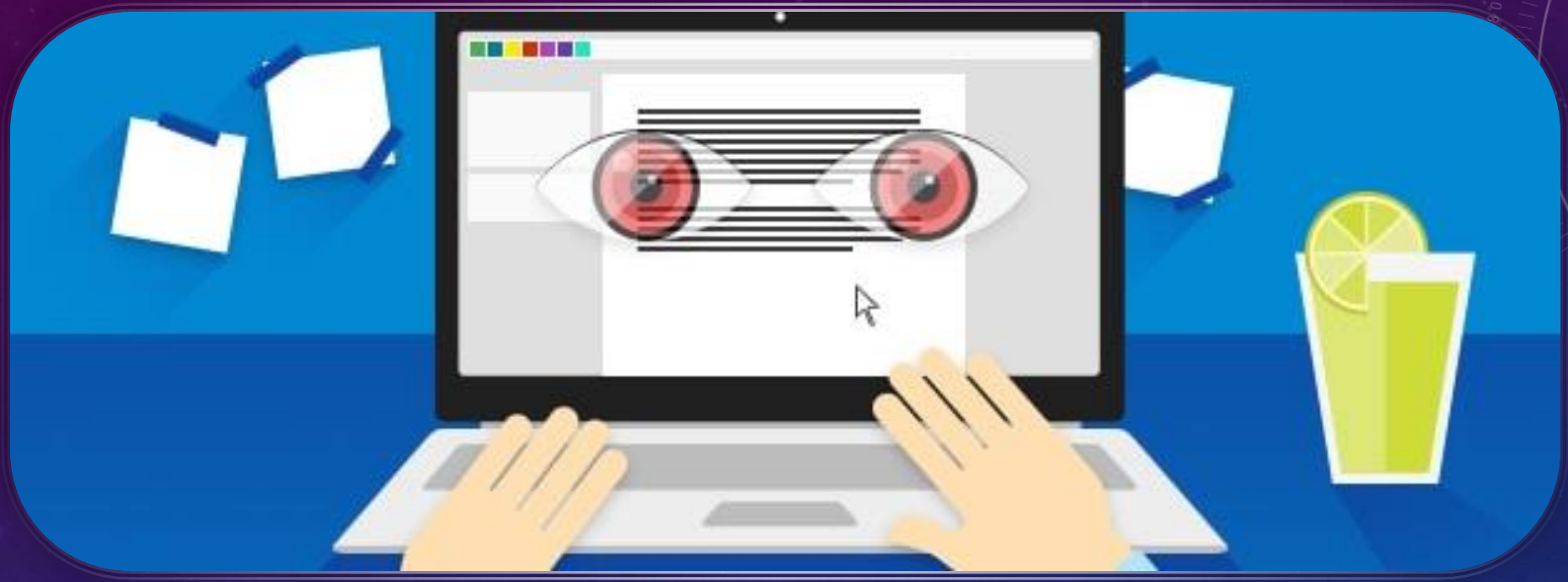
B.MUTHU ABHINAYA

CSE-3RD YEAR,

UNIVERSAL COLLEGE OF ENGINEERING AND TECHNOLOGY

OUTLINE:

- What is KEYLOGGERS
- Types of KEYLOGGERs
  - Hardware
  - Software
- Keyloggers uses
- Problem statement
- Disadvantages of KEYLOGGERs
- Example for KEYLOGGERs
- Reference
- Conclusion

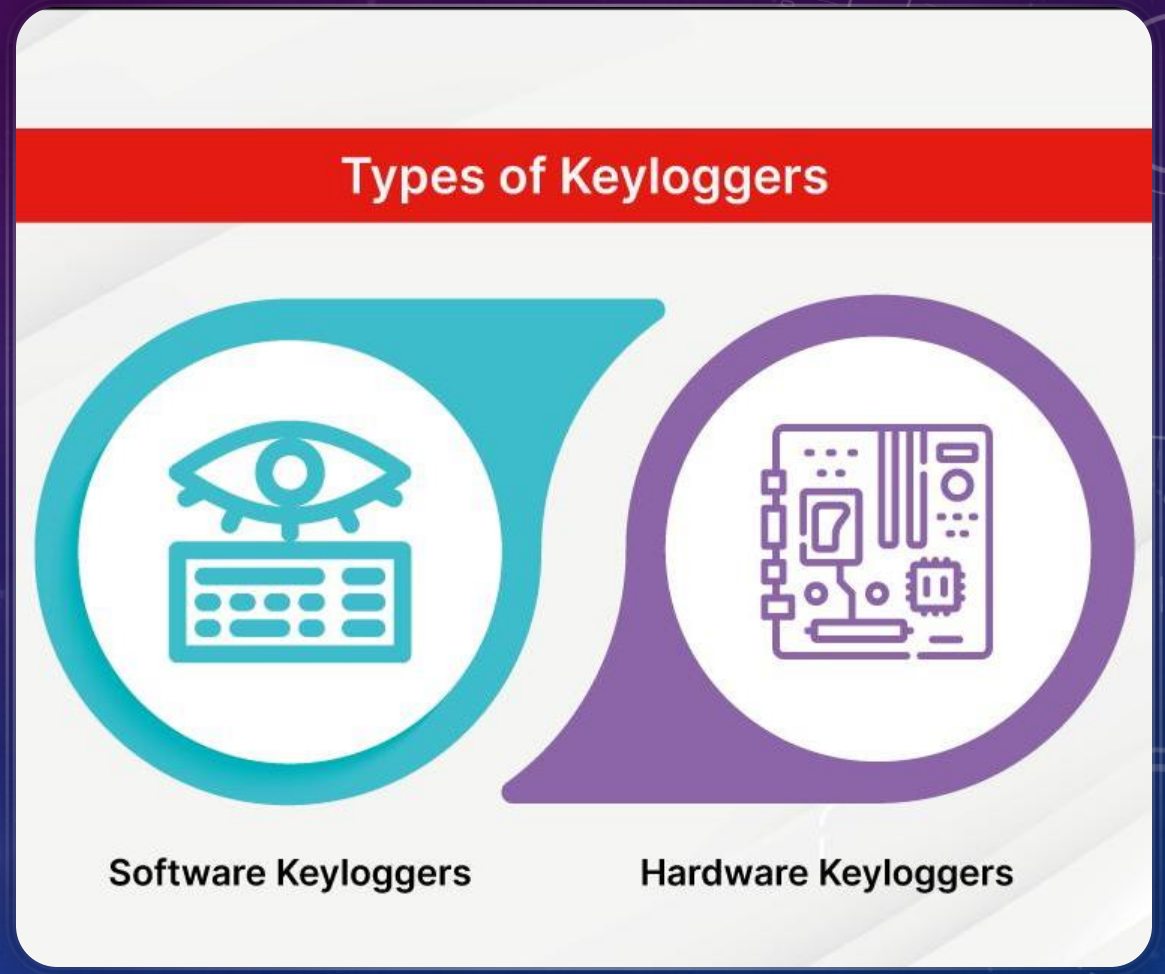


WHAT IS KEYLOGGERS:

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.

TYPES OF KEYLOGGERS:

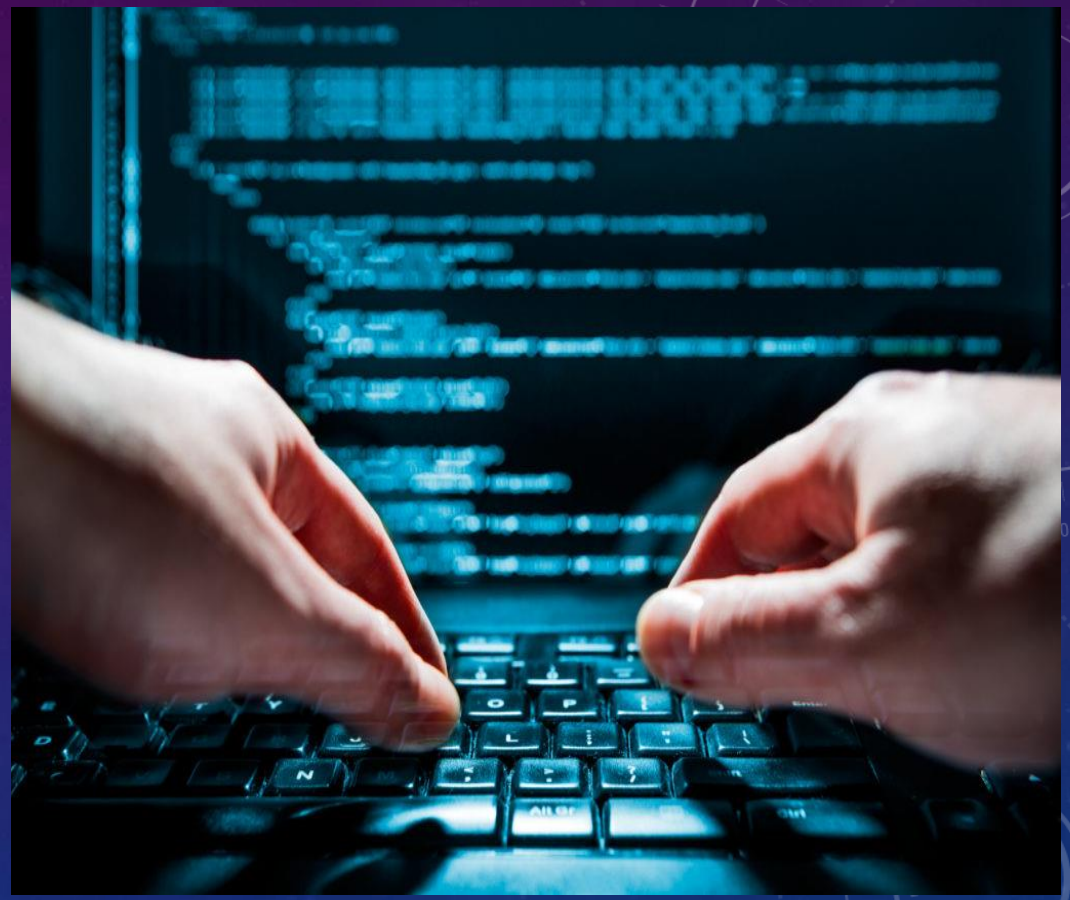
- There are two types of keyloggers:
- hardware keyloggers ,
- software keyloggers.



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:



- Software keyloggers consist of applications that have to be installed on a computer to steal keystroke 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.

KEYLOGGERS USES:

- Keyloggers are tools that can record every keystroke that you type into a computer or mobile keyboard.
- 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.
- One of the best advantages of keyloggers is tracking employee productivity(especially in the remote work structure).
- IT troubleshooting — to collect details on user problems and resolve accurately.

PROBLEM STATEMENT:

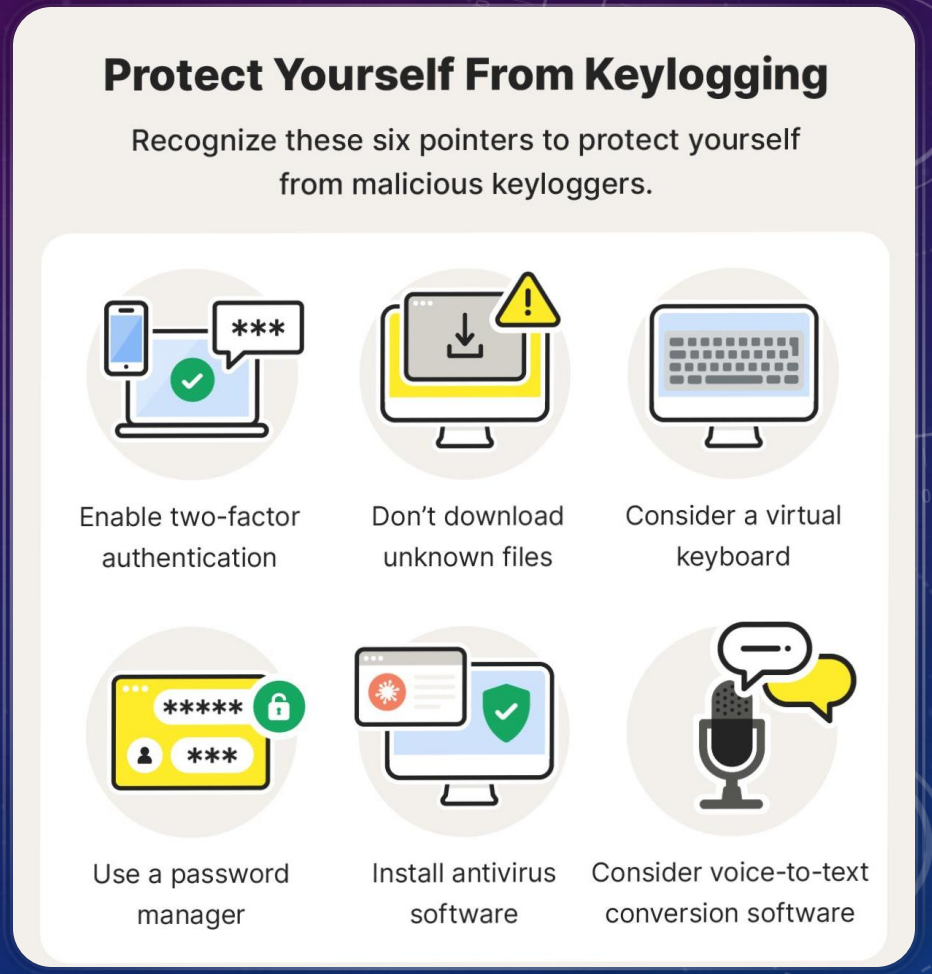
- It’s challenging to covertly install a hardware keylogger on another person’s device. To tackle this issue, We are therefore using a software keylogger that can be remotely installed on a person’s PC to resolve this problem.
- Malicious actors can deploy keyloggers to steal sensitive information, such as passwords, credit card numbers, and personal data. This information can be used for identity theft, financial fraud, or other criminal activities.
- Keyloggers are a type of malware that is downloaded onto a device through an entry point. Entry points can be infected software, emails, files or cloud programs. When keylogging software gets installed on a victim’s device, it logs every keystroke to gather login credentials and other sensitive information.

DISADVANTAGES OF KEYLOGGERS:

- 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. Keyloggers can embed themselves into the operating system of your computer.
- Yet keyboard dynamics is not without drawbacks, the most notable of which the fact that typing patterns can be erratic and inconsistent. Cramped muscles and sweaty hands can potentially alter a person's typing pattern. The type of keyboard also governs the typing patterns, which could affect verification.

EXAMPLE OF KEYLOGGERS :

- 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. Keyloggers aren't always used for illegal purposes.
- A keylogger is an example of spyware. Key PointsA keylogger is a type of spyware that records keystrokes on a computer, allowing an attacker to steal sensitive information such as passwords and credit card number.



REFERENCE:

- Keyloggers are programs that run as a background process on a computer or other device and collect keystrokes as a user types on their keyboard.
- Controlling keylogging technology within your organization is no different than managing other threats and tools, requiring common sense and a layered defense. The key is to be aware they exist, understand how they're used, and implement ways to detect them, with keylogger detection and containment part of your incident response plan.

CONCLUSION:

- Keyloggers are a potent threat to both individuals and enterprises, with the potential to cause significant harm if left undetected.
- By employers to observe employees' computer activities. By parents to supervise their children's internet usage. By device owners to track possible unauthorized activity on their devices.
- They can capture virtually every type of information entered through a keyboard.

THANK YOU !