B.RENUKA TEJASWINI

KEYLOGGER AND SECURITY

FINAL PROJECT

KEYLOGGER

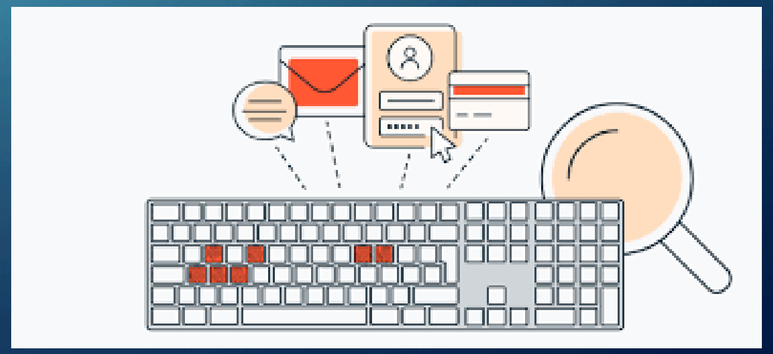
- A keylogger is a programme or tool designed to monitor and keep a tab on the “**keystrokes**” made on the user keyboard.
- This enables on compromising sensitive data like passwords etc..

AGENDA

- Problem statement
- Project overview
- Who are the end users
- Solution and its value
- Modelling
- result

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.



PROJECT OVERVIEW

- Keylogging is the action of capturing and recording keys struck on a keyboard.
- A keylogger is a program which captures and monitors all keylogs.
- Keyloggers can be both in the form of a built software program or directly downloaded onto a hardware module.

WHO ARE THE END USERS ?

- Keyloggers are used in IT organizations to troubleshoot technical problems with computers and business networks.
- Families and businesspeople use keyloggers legally to monitor network usage without their users' direct knowledge.
- Microsoft publicly stated that window 10 has a built-in keylogger in its final version "to improve typing and writing services“.

BENEFITS OF KEYLOGGER IN CS

1. **Insider threats**: The **keystroke recorder** secures confidential data from insider threats if any, along with tracking keyboard usage.
2. **RECORDED REPORTS:** Keyloggers are terrific assistance in registering the reports of the completed projects in their cloud storage for project managers to access it anytime to inspect the employees' productivity.
3. **PRODUCTIVITY TRACKER:** One of the best advantages of keyloggers is tracking employee productivity(especially in the remote work structure). A **keystroke recorder** can support maintaining the work balance for the management teams by distinguishing between the productive and non-productive workforce.

BENEFITS OF KEYLOGGER IN CS

1. **TIME MANAGEMENT:** Another positive of **keystroke recorders** is tracking the time of their employees. These keyloggers are super-efficient applications tracking the log-in, log-out time details, and the total working hours of employees. Such specifications benefit the management a lot in holding the productivity graph of the entire organization simultaneously.
2. **EMPLOYEE ACTIVITY:** Employers can monitor employee activities, total time taken to finish an assigned task, including the work approach they follow. **EmpMonitor** is the best employee monitoring software for monitoring employee activities in remote work.

MODELING

- **Threat modelling**:Threat modeling involves identifying and communicating information about the threats that may impact a particular system or network. Security threat modeling enables an IT team to understand the nature of threats, as well as how they may impact the network
- **Attack chain analysis**: The cyber-attack chain (also referred to as the cyber kill chain) is a way to understand the sequence of events involved in an external attack on an organization's IT environment.
- **Risk assessment**: A risk assessment is a systematic process that helps identify, analyze, and control hazards and risks in a situation or place.

MODELING

- **Behavioral modelling**: **Behavioral Model** is specially designed to make us understand behavior and factors that influence behavior of a System.
- **Data Theft**: One of the primary purposes of keyloggers is to steal sensitive information entered by users, such as usernames, passwords, credit card numbers, and other personal or financial data.
- **Privacy Breach**: Keyloggers compromise the privacy of individuals by surreptitiously monitoring and recording their keystrokes. This intrusion into users' privacy can lead to the unauthorized collection of personal and confidential information, undermining trust and causing psychological distress.

RESULT

- **Data Theft**: One of the primary purposes of keyloggers is to steal sensitive information entered by users, such as usernames, passwords, credit card numbers, and other personal or financial data. This stolen information can be exploited by cybercriminals for various malicious purposes, including identity theft, financial fraud, and espionage.
- **Privacy Breach**: Keyloggers compromise the privacy of individuals by surreptitiously monitoring and recording their keystrokes. This intrusion into users' privacy can lead to the unauthorized collection of personal and confidential information, undermining trust and causing psychological distress.
- To protect our devices use updated antiviruses.
- Don’t connect to public wifi.

Thank you