KEY LOGGER

Presented By:

NAME: Madhan N

COLLEGE: priyadarshini Engineering College

DEPATREMENT: computer science and engineering

OUTLINE:

- Introduction
- Problem statement
- System development approach
- Algorithm
- Result (output image)
- 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.

PROBLEM STATEMENT:

- In today's digital age, security and surveillance have become increasingly important. One significant aspect of digital security involves monitoring and recording user activity on computing devices. To address this need, we propose the development of a keylogger software solution.

SYSTEM DEVELOPMENT APPROACH

- Deploying a keylogger system requires careful planning and consideration to ensure its effectiveness, security, and ethical usage. Here's a step-by-step deployment approach:

Select Deployment Method:

- Choose the appropriate deployment method based on the target devices and your deployment environment.
- Deployment methods can include manual installation, remote deployment, or integration into existing software systems.
- **Deployment Plan:**
- Develop a deployment plan outlining the steps and timeline for deploying the keylogger system.
- Consider factors such as user training, communication, and support during the deployment process.

ALGORITHM

1. Initialize the keylogger system, setting up necessary variables and data structures.
2. Continuously monitor keyboard input using platform-specific APIs or low-level keyboard hooks.
3. Process each keystroke to extract relevant information such as the key pressed, timestamp, and any modifiers
4. Log the processed keystrokes to a secure file or database
5. Implement stealth mechanisms to ensure that the keylogger operates silently without detection.
6. Configure the keylogger to start automatically upon system boot-up.
7. Securely manage encryption keys to protect the confidentiality and integrity of the encrypted data.
8. Provide configurable options for users to customize keylogger settings, such as logging frequency or target applications

RESULT(OUTPUTIMAGE)

CONCLUSION

- In conclusion, the development and deployment of a keylogger present both technical challenges and ethical considerations. Keyloggers serve various purposes, from legitimate use cases such as parental control and employee monitoring to potentially malicious activities like unauthorized data collection.
- While designing a keylogger algorithm, it's essential to prioritize security, privacy, and ethical usage. The algorithm should be capable of stealthy operation, securely logging keystrokes, and encrypting logged data to prevent unauthorized access. Additionally, considerations such as cross-platform compatibility, error handling, and user configuration options contribute to the effectiveness and usability of the keylogger


THANK
YOU