CAPSTONE PROJECT

KEYLOGGER IN SECURITY

Presented By:

1. Student Name: S.Mahalakshmi
2. College Name: A.V.C. College of Engineering
3. Department: Information technology

edunet foundation

OUTLINE

- **Problem Statement** (Should not include solution)
- **Proposed System/Solution**
- **System Development Approach** (Technology Used)
- **Algorithm & Deployment**
- **Result (Output Image)**
- **Conclusion**
- **References**

PROBLEM STATEMENT

- **Project problem statement for keylogger Problem Statement:**
- In today's digital age, where cybersecurity threats loom large, one of the significant concerns is the proliferation of keyloggers, stealthy software tools designed to monitor and record keystrokes on a user's computer without their knowledge. Keyloggers pose a severe threat to individuals and organizations they can capture sensitive information such as passwords, credit card details, and other personal data, leading to identity theft, financial loss, and privacy breaches.

PROPOSED SOLUTION

- Keyloggers are malicious software that can be a serious threat. Here are some proposed solutions to protect yourself from keyloggers:
- **Prevention:**
- **Anti-virus and Anti-malware software:** Install and keep up-to-date reputable antivirus and anti-malware software that can detect and remove keyloggers.
- **Be cautious with downloads and attachments:** Only download files and open attachments from trusted sources. Be wary of clicking on links in emails, even if they appear to be from someone you know..
- **Detection:**
- **System behavior changes:** Unusual slowdowns, new programs running in the background, or unexplained browser activity can be signs of a keylogger infection.
- **Anti-keylogging software:** There are specific anti-keylogging programs that can detect and block keyloggers.
- **Regular security scans:** Regularly scan your system with your antivirus and anti-malware software to detect any potential threats.
- **Recovery:**
- **Boot into Safe Mode:** If you suspect a keylogger infection, boot your computer into Safe Mode. This will only load the essential programs needed to run your system, making it easier to identify and remove the keylogger.
- **Security software scan:** Run a full scan with your antivirus and anti-malware software in Safe Mode.
- **Change passwords:** Once you've removed the keylogger, change all your passwords for online accounts, especially financial accounts and email.
- **Additional Tips:**
- **Be mindful of public computers:** Avoid entering sensitive information on public computers, as they may be infected with keyloggers.
- **Keep your software updated:** Always update your operating system, applications, and web browser to the latest versions to patch security vulnerabilities that keyloggers might exploit.

SYSTEM APPROACH

The "System Approach" section outlines the overall strategy and methodology for developing and implementing the rental bike prediction system. Here's a suggested structure for this section:

- System requirements:100 MB free disk space. Pentium II processor or higher. 512 MB RAM.
- Library required to build the model:
- pynput
- mSpy
- Tkinter
- jsonlib

ALGORITHM & DEPLOYMENT

Step 1: Install the Required Library

- Ensure that you have the keyboard library installed in your Python environment. Open your command prompt or terminal and execute the following command

Step 2: Importing the Necessary Libraries

- Begin by importing the keyboard library at the beginning of your Python script. This library will enable us to work with keyboard inputs. Insert the following line of code

Step 3: Define the Log File

- Specify the name and location of the log file where the keystrokes will be saved. In this example, we'll use 'keystrokes.txt' as the file name. Feel free to modify it as desired. Add the following line of code

Step 4: Create the Key Press Event Function

- Define a function that will handle the key press events. This function will be called whenever a key is pressed.

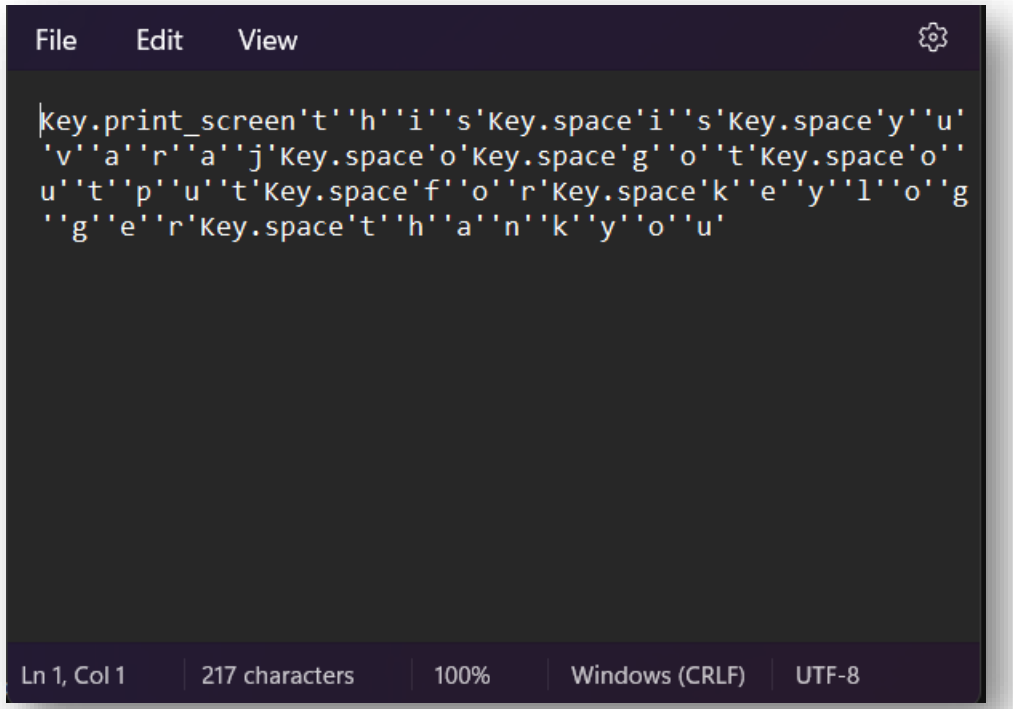
Step 5: Register the Key Press Event

- Register the 'on_key_press' function to be called whenever a key is pressed. This will enable our code to capture the keystrokes. Add the following line:
- keyboard.on_press(on_key_press)

Step 6: Run the Code

- Save your Python script with a '.py' extension (e.g., 'keylogger.py'). Open your command prompt or terminal, navigate to the directory where the script is located, and execute the command:

RESULT



edunet foundation

CONCLUSION

- In conclusion, keyloggers pose a serious threat to your online security. However, by implementing a layered approach that combines preventative measures, detection techniques, and a recovery plan, you can significantly reduce your risk. Remember, vigilance is key. Stay informed about the latest cybersecurity threats and maintain good security hygiene by keeping your software updated, using strong passwords, and practicing caution when online. If you suspect a keylogger infection, don't hesitate to seek help from a professional. By taking proactive steps, you can safeguard your sensitive information and navigate the digital world with greater confidence.

REFERENCES

- Here are some general references on online security that you can consult for more details:
- National Institute of Standards and Technology (NIST) Cybersecurity Framework: https://www.nist.gov/cyberframework
- Cybersecurity & Infrastructure Security Agency (CISA) Shields Up program: https://www.cisa.gov/shields-up
- Kaspersky Lab - What is Keystroke Logging and Keyloggers?: https://www.kaspersky.com/resource-center/definitions/keylogger

THANK YOU

edunet foundation