Project Title:

Keylogger with Encrypted Data Exfiltration

---

1. Introduction

In the cybersecurity domain, keyloggers are often associated with malicious intent. However, understanding how they work is essential for ethical hackers, penetration testers, and forensic investigators to build defensive tools. This project demonstrates a **proof-of-concept (PoC)** keylogger that captures keystrokes, encrypts the data, and simulates sending it to a remote server in a secure and ethical environment.

---

2. Abstract

This project aims to simulate a stealthy keylogger that encrypts captured keystrokes using the **Fernet symmetric encryption algorithm**. It stores logs with timestamps, simulates data exfiltration to a local server, and includes features like **startup persistence** and a **kill switch**. This tool is intended strictly for ethical testing and education. It does not violate any system's real-time privacy or security. The exercise enhances awareness of how attackers may operate and how defenders can detect such behavior.

---

3. Tools Used

- **Python 3.x** – Core language used
- **pynput** – For capturing keystrokes
- **cryptography (Fernet)** – For AES-128 based encryption
- **base64** – For encoding encrypted data
- **socket / requests** – For simulated data exfiltration
- **os, sys, threading** – For background processes and persistence

---

4. Steps Involved

a. Keystroke Logging

Using pynput.keyboard.Listener, every keystroke is recorded and written to a buffer.

b. Encryption Module

The captured data is encrypted in real-time using a Fernet key (AES under the hood). The key is generated once and securely stored.

c. Local Log Storage

Encrypted data is logged to a file with corresponding timestamps in an obfuscated directory (e.g., .syslogs/).

d. Simulated Data Exfiltration

The system attempts to send the encrypted logs to a local Flask server running on localhost, simulating an attacker-controlled remote server.

e. Persistence and Kill Switch

On Windows, the script adds itself to startup using the registry. A keyboard combo (e.g., Ctrl + Alt + K) acts as a kill switch to stop the listener.

---

5. Conclusion

This project helped simulate a real-world keylogging and data exfiltration attack scenario, encrypted and stealthy in nature. It demonstrates how attackers may misuse legitimate libraries and OS functionalities. In a red-team/blue-team simulation, this PoC becomes a valuable resource for training and defensive development.

🔐 Ethical Disclaimer

The keylogger was tested in a controlled virtual environment, with full consent, for **educational** and **demonstration** purposes only. Any use outside such boundaries is unethical and potentially illegal.