Keylogger with Encrypted Data Exfiltration

# Introduction

The project 'Keylogger with Encrypted Data Exfiltration' aims to build a proof-of-concept keylogger that not only captures user keystrokes but also encrypts the logged data and simulates its exfiltration to a remote server. The primary objective is to understand the techniques used in advanced persistent threats while maintaining ethical constraints.

# Abstract

A keylogger is a tool designed to record the keys struck on a keyboard. In this project, we take it one step further by encrypting the logged data using Fernet symmetric encryption and simulating the transmission of this data to a mock server running on localhost. This setup demonstrates how sensitive data can be exfiltrated covertly in real-world attack scenarios. This project is conducted in a controlled environment strictly for educational and ethical learning purposes.

# Tools Used

- Python  
- pynput (for capturing keystrokes)  
- cryptography.fernet (for encryption)  
- socket (for simulated exfiltration)  
- datetime (for timestamping keystrokes)

# Steps Involved in Building the Project

1. Captured keystrokes using the pynput module to monitor keyboard input.  
2. Buffered and timestamped keystroke data for processing.  
3. Encrypted the buffered data using the Fernet class from the cryptography module.  
4. Stored the encrypted logs locally in a secure text file.  
5. Simulated data exfiltration to a server running on localhost via a socket connection.  
6. Implemented a startup persistence script to auto-run the keylogger on system reboot.  
7. Added a kill switch using the ESC key to terminate the logger safely.

# Conclusion

The Keylogger with Encrypted Data Exfiltration project effectively demonstrates how keylogging can be carried out securely and covertly. By encrypting logs and using mock exfiltration, it highlights critical cybersecurity concepts such as data confidentiality, persistence, and ethical boundaries. This project serves as a practical learning tool for understanding the importance of securing input systems and preventing unauthorized access to sensitive data.