Keylogger with Encrypted Data Exfiltration - Project Report

Introduction

This project demonstrates a Proof-of-Concept (PoC) keylogger in Python that captures keystrokes, encrypts them using Fernet (AES), and simulates secure exfiltration by writing encoded data to a local file. A decryption utility is also included to view the logs securely.

Abstract

In cybersecurity education and red team exercises, it is crucial to understand the working of keyloggers. This project captures user keystrokes, encrypts the log, and stores it securely in an encoded format. It simulates a realistic exfiltration scenario while adhering to ethical and educational guidelines.

Tools Used

- Python 3
- pynput (for capturing keyboard events)
- cryptography (Fernet encryption)
- base64 (encoding data)
- datetime, shutil, os modules

Steps Involved in Building the Project

1. Setup keylogger using pynput to capture keystrokes.
2. Store raw keystrokes in a temporary log file.
3. Encrypt the log using Fernet when size exceeds threshold.
4. Encode the encrypted log using base64.
5. Write encoded logs to a simulated exfiltration file.
6. Create a decryptor utility to view encrypted logs securely.

Conclusion

This project provides an educational demonstration of how encryption can be integrated with logging mechanisms. It showcases secure handling and storage of sensitive data. The project reinforces the importance of ethical boundaries while exploring cybersecurity techniques.