Keylogger with Encrypted Data Exfiltration

Introduction

A keylogger is a type of surveillance tool that captures every keystroke made on a system. In cybersecurity, keyloggers are often studied to understand how data breaches happen and to develop defenses. This project aims to develop a proof-of-concept (PoC) keylogger for ethical and educational purposes.

Abstract

This PoC keylogger records all keystrokes made by a user, encrypts the data using symmetric encryption with the Fernet module, and stores the encrypted logs locally. It includes a kill switch (ESC key) and simulates the process of exfiltration to a remote server by printing encoded logs to the console. The primary goal is to educate and demonstrate how keylogging attacks work while ensuring safe and ethical usage by encrypting all captured information.

Tools Used

- **Python 3.7.9** – This version of Python Programming language is used
- **pynput** – To capture keyboard inputs
- **cryptography (Fernet)** – For encrypting keystroke data
- **base64** – For safe encoded storage

Steps Involved in Building the Project

1. Set up the Python environment and installed necessary libraries (pynput, cryptography, base64).
2. Created a secret.key using the Fernet module from the cryptography library for secure encryption.
3. Captured keystrokes using the pynput.keyboard listener.
4. Encrypted each keystroke along with a timestamp and stored it in an encoded format using base64 in a local file.
5. Implemented a kill switch using the ESC key to stop the keylogger safely.
6. Simulated exfiltration of data by printing a preview of encrypted logs to the console (imitating a real-world attacker's server).
7. Maintained ethical usage by disabling all forms of direct transmission and ensuring encrypted storage only.

Conclusion

The PoC keylogger is a compact, secure, and ethical implementation suitable for understanding how real-world keylogging attacks work. The encryption and simulation ensure it is non-malicious and ideal for cybersecurity awareness, education, and training.

It also demonstrates the risks associated with keyloggers and emphasizes the importance of ethical hacking in identifying and patching such vulnerabilities. Future improvements may include screenshot capturing, real-time network transfer simulation, and stealth startup integration for better realism and educational value.

---------- End of Report ----------