Encrypted Keylogger — Internship Project Report

Author: Abhinav Tiwari

Project Type: Educational Proof-of-Concept (PoC) — Internship Project
Date: October 24, 2025
Organization: Elevate Labs

Introduction

This project is an educational proof-of-concept (PoC) that demonstrates the capabilities of a keylogger while emphasizing ethical considerations and cybersecurity awareness. The tool is designed for research and educational purposes to help security professionals understand keylogger behaviour and develop effective countermeasures.

Abstract

The Encrypted Keylogger PoC is a sophisticated yet controlled implementation that showcases keylogging techniques, data encryption, and system persistence. Built with Python, it serves as a valuable resource for cybersecurity education, penetration testing training, and defensive strategy development. The project includes built-in ethical safeguards to prevent misuse and ensure responsible implementation.

Language Used

- **Python 3.x**: Core programming language
- **pynput**: For keyboard event monitoring
- **cryptography**: For data encryption (Fernet)
- **requests**: For HTTP communication
- **psutil**: For process monitoring
- **logging**: For system logging and debugging

Steps Involved in Building the Project

1. **System Design**
   - Planned the modular architecture
   - Defined core components and their interactions
   - Established ethical guidelines and constraints

2. **Core Development**
   - Implemented key capture functionality using `pynput`
   - Added encryption for all stored data
   - Created configuration management system
   - Developed utility functions for common operations

3. **Persistence Mechanism**
   - Implemented Windows registry modification
   - Added startup persistence
   - Included stealth features for educational demonstration

4. **Security Features**
   - Added encryption for all sensitive data
   - Implemented kill switch functionality
   - Included application whitelisting/blacklisting
   - Added runtime limitations

5. **Testing & Validation**
   - Unit testing of individual components
   - Integration testing
   - Security validation
   - Performance optimization

6. **Documentation**
   - Code documentation
   - User guide
   - Technical specifications
   - Ethical usage guidelines

Conclusion

The Encrypted Keylogger PoC successfully demonstrates key cybersecurity concepts while maintaining strong ethical boundaries. The project serves as an excellent educational tool for understanding both offensive and defensive security techniques. Through this implementation, we've gained valuable insights into:

- Malware behaviour and detection
- System security mechanisms
- Data protection techniques
- Ethical considerations in security research

This project underscores the importance of responsible security research and the need for robust defensive measures against keyloggers and similar threats. Future enhancements could include multi-platform support, advanced evasion techniques, and more sophisticated detection mechanisms.