KEY_LOGGER Python

Abstract

The project implements a modular keylogging and monitoring tool in Python. It captures keystrokes, clipboard data, screenshots, and active window titles, with optional secure data exfiltration via Dropbox or email. Stealth and self-destruct capabilities are included for controlled lab simulations. This tool serves as a reference for cybersecurity students and professionals to understand attack vectors and create better defensive measures.

Introduction

- Python-based keylogger for cybersecurity education.
- Demonstrates keystroke logging, clipboard monitoring, screenshot capture.
- Includes stealth and self-destruct features for controlled testing.
- Designed to strengthen understanding of attack detection and defense.

Tools Used

- Python 3.x
- pynput – Keystroke logging
- pyautogui – Screenshot capture
- dropbox – Secure data upload
- secure-smtplib – Email exfiltration
- python-dotenv – Secure credential management
- pywin32 – Windows stealth mode (optional)

Steps Involved in Building the Project

- Design modular architecture for monitoring and utilities.
- Implement keystroke, clipboard, screenshot, and window tracking modules.
- Develop Dropbox and email-based data exfiltration.
- Add stealth and self-destruct mechanisms for realistic simulation.
- Configure environment variables (.env) for secure credentials.
- Package with PyInstaller for executable testing.

Conclusion

- Project illustrates how keyloggers function for educational research.
- Helps cybersecurity students develop detection and defense strategies.
- Promotes responsible use requiring explicit permission before deployment.
- Supports controlled lab simulations to avoid legal and ethical issues.