Internship Project Report

Project Name: Encrypted Keylogger with Telegram Exfiltration

Developer: Shubham Dongare

Internship Company: Elevate Labs

Introduction

This report presents the development of a keylogger with encrypted data exfiltration, created as part of an internship project. The objective was to simulate a real-world scenario where sensitive keystroke data is captured, encrypted, and sent to a remote server (Telegram bot), demonstrating both ethical hacking and programming skills.

Abstract

The project involves creating a proof-of-concept keylogger in Python. It captures keystrokes, encrypts the data, stores it temporarily, and sends it to a Telegram bot for remote monitoring. Key features include auto-start persistence, encrypted log management, screenshot capture, and bot commands such as /activate, /deactivate, /status, and /exit.

Tools Used

- Python
- pynput (for keystroke capture)
- cryptography (for encryption)
- base64 (for encoding)
- threading and time (for scheduling)
- requests (for Telegram integration)
- os, shutil, sys, winreg (for system interaction and persistence)

Steps Involved in Building the Project

1. Set up Telegram bot and retrieve bot token and chat ID.
2. Create a separate script to fetch the chat ID dynamically.
3. Implement keystroke logger using pynput.

4. Store logs locally in rotating log files.

5. Encrypt log content and send to Telegram.

6. Auto-delete logs after sending.

7. Capture screenshots every minute and send them similarly.

8. Add bot commands to control keylogger remotely.

9. Implement kill switch (Ctrl+Shift+Q).

10. Add persistence by adding script to Windows startup via registry.

Conclusion

This project successfully demonstrates the development of a secure, encrypted keylogger with real-time exfiltration using a Telegram bot. It combines ethical hacking principles, scripting, encryption, and automation to provide a powerful learning experience in cybersecurity. All actions were conducted within a safe and ethical framework.