Assignment

Mohammad Hanzala

Keylogger using C++

Cyberion

Project :

Title: Keylogger with API Integration Project

This project is a C++ application that implements a keylogger capable of capturing user keystrokes and sending them to a remote API for real-time monitoring or analysis. It uses the Windows API to hook keyboard events and libcurl for sending data over HTTP, making it both a local logger and a networked data sender.

Technology Stack :

Programming Language : C++

Server : Flask

Libraries/Tools :

- Windows API : For system-level keyboard event hooking.
- Libcurl : For making HTTP requests to the API.

Code Workflow :

1. **Main Program Initialization** : Opens the keylogging text file (keylog.txt) for appending captured keystrokes. Sets up a keyboard hook to intercept all keypress events system-wide.
2. **Keyboard Hook Procedure** : Captures keypress events and converts the virtual key codes to characters. Logs the keystrokes to keylog.txt and simultaneously invokes the Send Keystroke To API function to send the data remotely.
3. **API Communication** : Sends an HTTP POST request to the specified API endpoint with an Authorization header containing the API key.
4. **Message Loop** : Keeps the application running to continuously capture and process keyboard events.

5. Error Handling : Includes error-checking mechanisms for file handling, API communication, and hook setup failures.

Use Cases:

1. **Monitoring** : Can be adapted for monitoring keystrokes for cybersecurity research, application behavior analysis, or parental controls.

1. **Data Collection** : Provides a template for collecting keystrokes for analytical purposes, such as improving predictive text systems.

2. **Integration** : Offers a proof of concept for integrating system-level event logging with APIs for real-time monitoring.

Security and Ethical Considerations:

- This project is intended strictly for educational or ethical purposes, such as understanding the workings of keyboard hooks or designing defensive security tools.

- Deploying this tool without user consent violates legal and ethical guidelines, such as privacy laws.

- Incorporating additional features like encryption and multi-factor authentication is recommended to ensure secure handling of sensitive data.

Acknowledgment:

This project demonstrates foundational knowledge of low-level system programming, API integration, and network communication using C++. It emphasizes the importance of ethical use of such tools in cybersecurity and system analysis domains.