GALLA SANTOSHI RAMYA

Final Project

Keylogger & Security

A keylogger, or keystroke logger, is a type of surveillance software or hardware designed to record and log every keystroke made on a computer or mobile device. This data can be retrieved later to see what was typed, potentially revealing sensitive information like passwords, personal messages, and credit card numbers.

Security Risks

- **Data Theft**: Keyloggers can capture sensitive information such as login credentials, financial data, and personal communications.
- **Privacy Invasion**: They can be used for spying on individuals, monitoring employee activity, or unauthorized surveillance.
- **Identity Theft**: The stolen information can be used

AGENDA

1. Problem statement
2. Project overview
3. Who are the end users?
4. Solution and its value propositin

5.Results

6.Project Link

PROBLEM STATEMENT

A keylogger designed covertly record keystrokes on various platforms (Windows, macOS, Linux) with an emphasis on stealth and secure data transmission. Explore software and hardware-based methods, implement encryption, and address ethical and legal implications.

A keylogger is a type of malicious software or hardware device designed to secretly record keystrokes made on a computer or other electronic devices. Its primary objective is to capture sensitive information such as usernames, passwords, credit card numbers, and other personal or financial data typed by the user. Keyloggers operate covertly, often without the user's knowledge, and can transmit the captured data to a third party for malicious purposes

PROJECT OVERVIEW

This project aims to develop a comprehensive keylogger capable of covertly recording keystrokes on diverse platforms such as Windows, macOS, and Linux. The keylogger will emphasize stealth to operate discreetly in the background without user detection. Secure data transmission protocols will be implemented to ensure captured keystrokes are transmitted safely. The project will explore both software and hardware-based approaches to maximize versatility and effectiveness. Ethical considerations regarding privacy and legality will be thoroughly addressed throughout the development process. The ultimate goal is to enhance cybersecurity awareness and defenses against potential threats posed by keylogging techniques

WHO ARE THE END USERS?

•The end users of keylogger projects typically include:

Security Professionals and Penetration Testers: They use keyloggers to assess and strengthen the security of computer systems and networks by identifying vulnerabilities and testing defenses against potential cyber threats.

Parents or Guardians: Some install keyloggers on family devices to monitor children's online activities, ensuring their safety and protecting them from inappropriate content or interactions.

Law Enforcement and Forensic Investigators: Keyloggers assist in gathering digital evidence for criminal investigations, aiding in the prosecution of cybercrimes such as hacking, fraud, or unauthorized access.

YOUR SOLUTION AND ITS VALUE PROPOSITION

The solution consists of various components addressing keyloggers:

Detection Algorithms:

Development and implementation of algorithms to detect keyloggers on systems.

User Education:

Initiatives and materials to educate users on the risks of keyloggers and preventive measures.

Software Tools:

Creation and deployment of software tools designed to detect and remove keyloggers.

Regular Updates:

Ensuring that detection tools and educational materials are regularly updated to address new types of keyloggers.

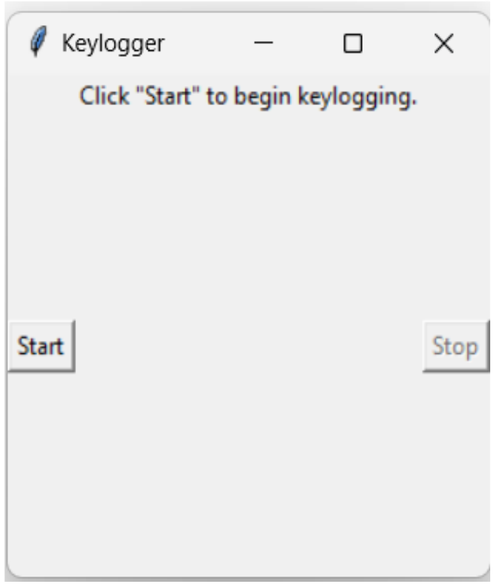
VALUE PROPOSITION

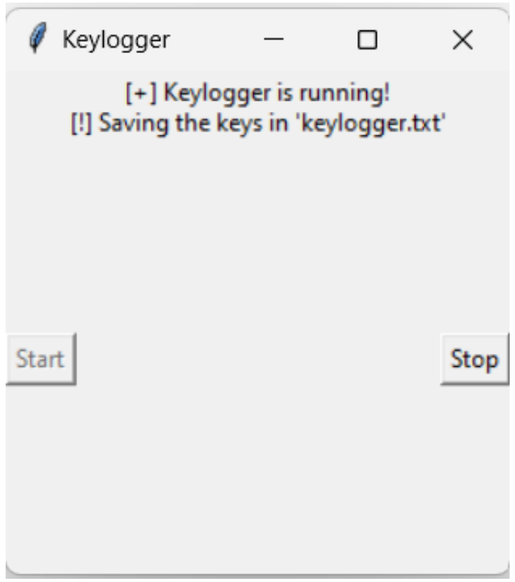
The value proposition highlights the benefits provided by the solution:

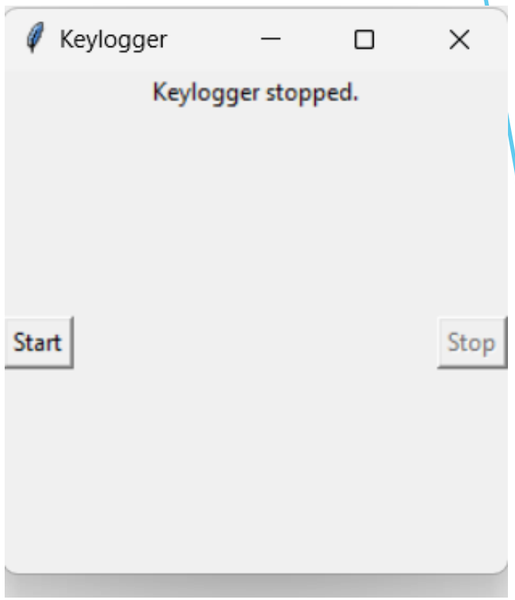
Enhanced Security:

Improved overall security for users' systems by effectively detecting and removing keyloggers.

RESULTS


Keylogger
Click "Start" to begin keylogging.
Start
Stop


Keylogger
[+] Keylogger is running!
[!] Saving the keys in 'keylogger.txt'
Start
Stop


Keylogger
Keylogger stopped.
Start
Stop

Project Link

https://github.com/ramya-225/Cybersecurity-project