KEYLOGGER AND SECURITY

APSSDC CYBER SECURITY FINAL PROJECT

GADI SRINUBABU

PROJECT TITLE

KEY LOGGER & SECURITY

AGENDA

- Introduction to Keyloggers and Security
- Understanding the Problem Statement
- Overview of the project
- Identifying the End Users
- Introducing Your Solution
- Highlighting the unique value proposition
- Discussing the key Modelling Approaches
- Results
- Project Github Link

PROBLEM STATEMENT

Develop a robust and secure keylogger software that effectively logs keystrokes on a target system while implementing strong encryption and access controls to prevent unauthorized access to the logged data, ensuring privacy and data integrity.

PROJECT OVERVIEW

THE keylogger monitors the keystrokes on the operating system you are using, checking the paths each keystroke goes through. In this way, a software keylogger can keep track of your keystrokes and record each one.

WHO ARE THE END USERS?

Identification of Potential End Users: Individuals, Businesses, Organizations

Understanding Their Needs and Concerns Regarding Keylogger Protection

Tailoring Solutions to Meet the Requirements of Various User Groups

Keyloggers, or keystroke loggers, are tools that record what a person types on a device. While there are legitimate and legal uses for keyloggers, many uses for keyloggers are malicious. In a keylogger attack, the keylogger software records every keystroke on the victim’s device and sends it to the attacker.

THE WOW IN YOUR SOLUTION:-

A keylogger is a program that secretly records everything you type on your computer. It can be used for good things like watching what employees do or keeping kids safe online. But bad people can also use it to steal your passwords and credit card numbers.

YOUR SOLUTION AND ITS VALUE PROPOSITION

Keyloggers are many hackers and script kiddie's favorite tools. Keylogging is a method that was first imagined back in the year 1983. Around then, the utilization of this product was uncommon and just the top examination organizations and spies could get their hands on it, yet today, it is a typical element offered by most government operative applications like TheOneSpy. Individuals use it as an opportunity to guarantee the assurance of their families, organizations, and the ones they care about.

MODELLING:-

Components of Keylogger Models:

- **Data Capture Mechanisms**: How keystrokes are captured.
  - **Polling**: Regularly checking keyboard buffer.
  - **Hooking**: Intercepting keystrokes via system hooks.
- **Data Storage and Transmission**: Methods for storing and sending captured data.
  - **Local Storage**: Data saved on the device.
  - **Remote Transmission**: Data sent to a remote server.
- **Evasion Techniques**: Methods to avoid detection.
  - **Rootkit Integration**: Embedding within the OS.
  - **Obfuscation**: Hiding code to avoid detection by anti-malware.

RESULTS:-

The best way to protect your devices from keylogging is to use a high-quality antivirus or firewall. You can also take other precautions to make an infection less likely.

PROJECT GIT-HUB:-

https://github.com/srin3/Apssdc.git