A.BHANU SAKAR

Keylogger and security

PROJECT TITLE

keylogger and security

AGENDA

1.1OUTLINE OF THE PROJECT Software Key loggers, also known as keystroke loggers, record the keys hit on a device and save them to a file, accessedby the person who deployed the malware.A key logger can be either software or hardware. A hardware keylogger is a device that connects your keyboard to your computer. Key loggers be connected directly to the keyboard and the computer through manually using one of two as approaches. PS/2 and the USP keylogger are twoexamples this method.

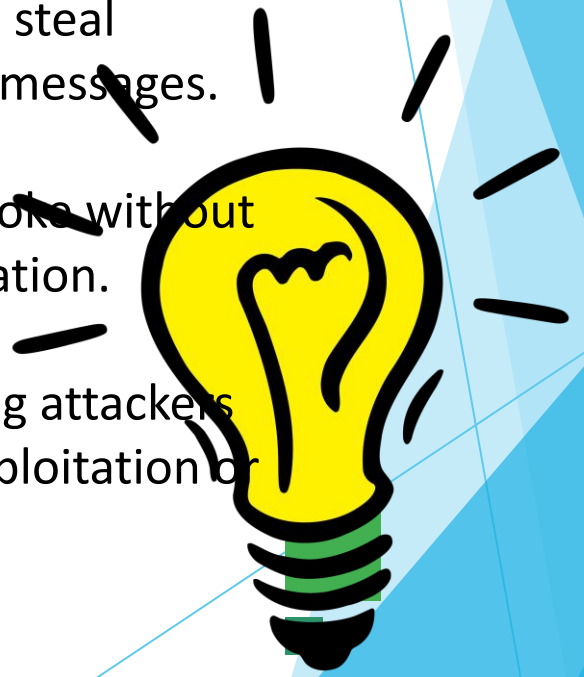
PROBLEM STATEMENT

Keyloggers pose significant security threats as they can compromise sensitive information, including passwords, credit card numbers, and personal messages. The primary concerns associated with keyloggers include:

Data Theft: Keyloggers can silently capture keystrokes, allowing attackers to steal sensitive information such as login credentials, financial data, and personal messages.

Privacy Invasion: Keyloggers invade users' privacy by recording every keystroke without their knowledge or consent, leading to potential misuse of personal information.

Malicious Intent: Keyloggers can be deployed with malicious intent, allowing attackers to remotely access and control compromised systems, leading to further exploitation or espionage.



PROJECT OVERVIEW

In this project, we aim to develop a keylogger software or hardware while ensuring robust security measures to prevent potential misuse. We will delineate the process of creating the keylogger discreetly and emphasize the significance of security considerations to safeguard against unauthorized access and ethical concerns.

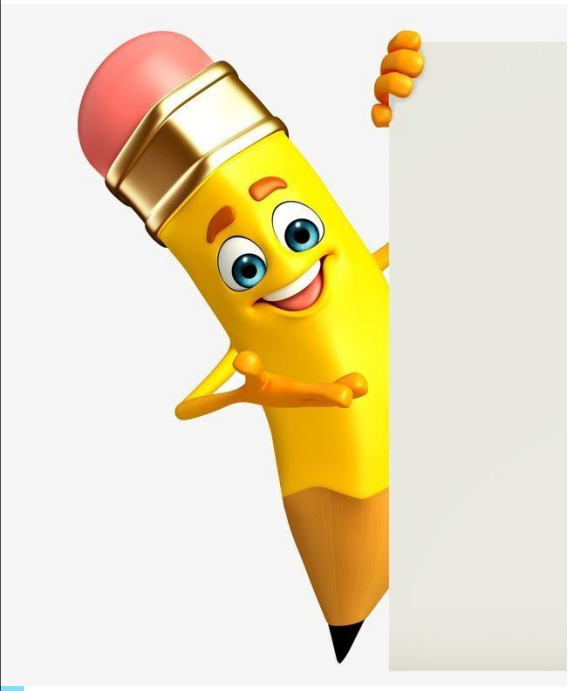
Keylogger Development:
The development phase involves crafting the keylogger software or hardware, employing is an suitable programming languages, platforms, and technologies. We will elucidate how the keylogger captures keystrokes surreptitiously and explore additional functionalities like remote monitoring and data retrieva

By implementing these security measures and adopting a proactive approach to cybersecurity, organizations and individuals can better protect themselves against the risks posed by keyloggers and other forms of malware.

WHO ARE THE END USERS?

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.

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 is an this product was uncommon and just the top examination organizations and spies could get their handson it, yet today, it is a typical element offered by most government operative applications like TheOneSpy. Individuals use it as opportunity to guarantee the assurance of their families, organizations, and the ones they care about.

THE WOW IN YOUR SOLUTION

A keylogger is a type of surveillance technology used to monitor and record each keystroke typed on a specific computer's of the keyboard. In this tutorial, you will learn how to write a an major keylogger in Python.

This tool has both legitimate and illegitimate uses. Legitimate uses can include monitoring employee productivity, parental control, and troubleshooting computer issues. However, when used unethically by hackers or script kiddies, a keylogger can capture sensitive information like login credentials, credit card numbers, and personal messages.

MODELLING

Keylogger, a tool intended to record every keystroke made on the machine and offers the attacker the ability to steal large amounts of sensitive information without the permission of the owner of the message. The primary objective of this project is to detect keylogger applications and prevent data loss and sensitive information leakage. This project aims to identify the set of mapermissions and storage levels owned by each of the applications andhence differentiate applications with proper permissions and keylogger applications that can abuse permissions. The keyloggers are detected using Black-box technique. Black-box approach is based on behavioral characteristics which can be applied to all keyloggers and it does not rely on the structural characteristics of the keylogger. This project aims to develop detection system on mobile phones based on machine learning algorithm to detect keylogger applications.

RESULTS

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