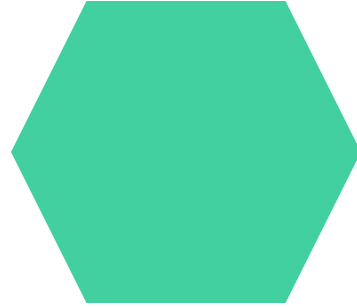


# Final Project



VICTOR RICHARDS



# PROJECT TITLE



## KEYLOGGERS



# AGENDA

## KEYLOGGERS

**The agenda for the presentation on keyloggers includes an overview of what keyloggers are and how they operate, the various types of keyloggers (software and hardware), their legitimate and malicious uses, detection and prevention strategies, and the legal and ethical considerations surrounding their use. The presentation aims to educate the audience on the risks associated with keyloggers and provide practical advice on safeguarding against them.**



# PROBLEM STATEMENT



**The problem statement is that the key logger can be detected using antiviruses. Installation of hardware key logger is difficult without the knowledge of the owner of the system. The solution to the above existing problem is that we can build a software key logger instead of hardware key logger.**




# PROJECT OVERVIEW

**Key logger can be implemented in different ways. They may be software-based, where a program is installed on a computer to capture keystrokes, or hardware-based, involving physical devices connected between the keyboard and the computer. Some advanced key logger can also capture screenshots, log mouse clicks, and monitor other activities.**



**It's important to note that the use of key logger without the consent of the individual being monitored is generally considered unethical and, in many cases, illegal. Privacy laws and regulations vary by jurisdiction, and individuals have the right to know and consent to being monitored.**



# WHO ARE THE END USERS?



**End users of keyloggers include cybercriminals who use them for malicious purposes such as stealing sensitive information, employers who may use them to monitor employee activities for productivity or security reasons, and law enforcement agencies that deploy keyloggers for surveillance and investigative purposes. Additionally, individuals might use keyloggers for personal monitoring, such as keeping track of their own device usage or, in some cases, to monitor family members.**



# YOUR SOLUTION AND ITS VALUE PROPOSITION



**Everyone should keep their password and personal data safe. Keyloggers can make destroy everything the data of details. 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.**

# 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 keyboard. In this tutorial, you will learn how to write a 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 permissions and storage levels owned by each of the applications and hence 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 precautions to make an infection less likely.**

**Keylogging results in the capture of every keystroke made on a device, potentially leading to the theft of sensitive information like passwords, credit card numbers, and personal communications. This data can be exploited for financial gain, identity theft, or unauthorized access to confidential systems.**