**Development and Detection of Keyloggers for Windows Operating System**

**CDAC, Noida**

**CYBER GYAN VIRTUAL INTERNSHIP PROGRAM**

**Submitted By:**

PORIKA SANIYA

Project Trainee, (May-June) 2024

**BONAFIDE CERTIFICATE**

This is to certify that this project report entitled **Development and Detection of Keyloggers for Windows Operating System** submitted to CDAC Noida, is a Bonafede record of work done by **Boda sruthilaya** under my supervision from 06-06-2024 to 25-06-2024.

(Signature) (Signature)

HEAD OF THE DEPARTMENT SUPERVISOR

**Declaration by Author(s)**

This is to declare that this report has been written by me/us. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. I/We aver that if any part of the report is found to be plagiarized, I/we are shall take full responsibility for it.

Name of Author(S) – **PORIKA SANIYA**

**TABLE OF CONTENTS**

1. [Introduction](https://docs.google.com/document/d/1uJ3cHOgW28jXpBUGNB919CJ9Us-EeoKS/edit#heading=h.gjdgxs)
2. [Domain of the Project](https://docs.google.com/document/d/1uJ3cHOgW28jXpBUGNB919CJ9Us-EeoKS/edit#heading=h.30j0zll)
3. [Expected Outcome](https://docs.google.com/document/d/1uJ3cHOgW28jXpBUGNB919CJ9Us-EeoKS/edit#heading=h.1fob9te)
4. Suggested Tools/Techniques to be Used
5. Implementation
6. Conclusion

### Introduction :-

This project involves both the development of a keylogger for the Windows operating system and the creation of detection mechanisms to identify and mitigate keylogger activities. The implementation phase will focus on creating a keylogger application capable of capturing keystrokes on a Windows system, utilizing various techniques such as hooking into the keyboard input events. The detection phase will involve researching and implementing methods to identify keylogger behavior, including signature-based detection, heuristic analysis, and monitoring system processes for suspicious activity.

**Domain of the Project :-**

**Cybersecurity - Keylogging**

**Expected Outcome :-**

The expected outcome of this project includes:

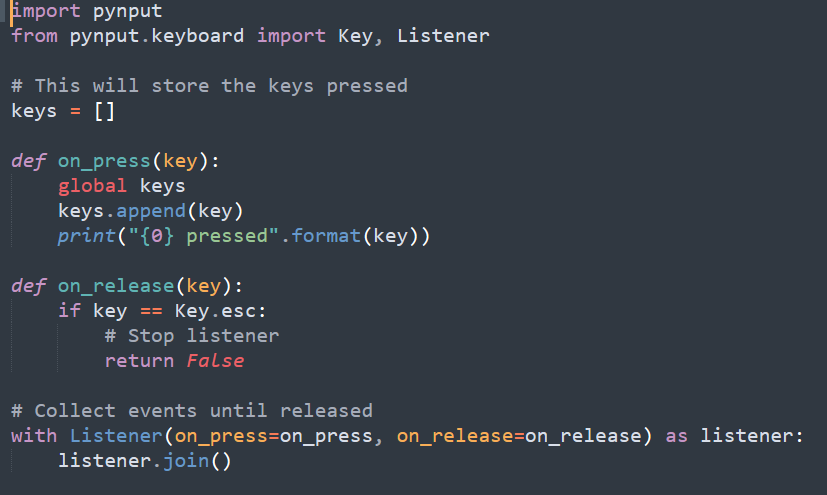
1. Development of a functional keylogger application for the Windows operating system.
2. Implementation of effective detection mechanisms to identify and mitigate keylogger activities.
3. Detailed documentation, including a project report outlining the implementation process, detection methodologies, and evaluation results.

**Suggested Tools/Techniques to be Used :-**

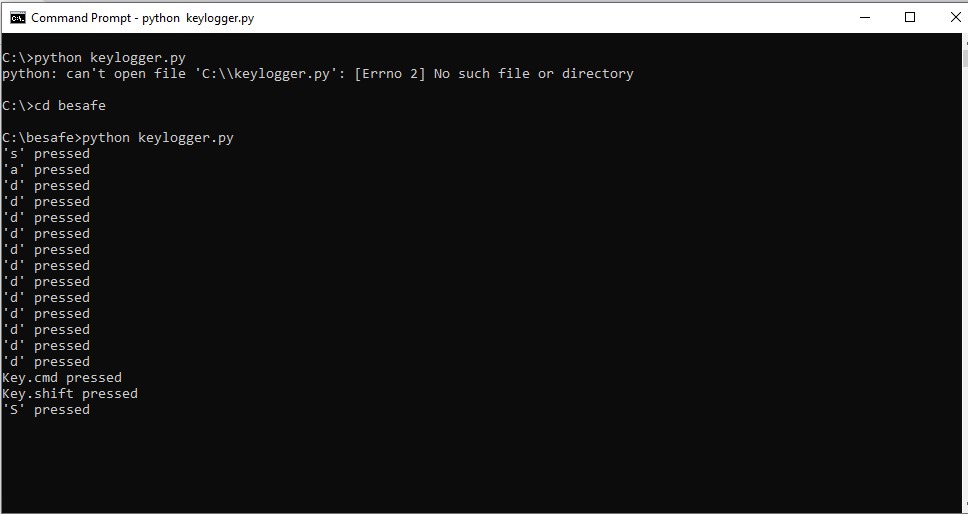
* **Programming Languages:** C++, Python
* **System Monitoring Tools:** Process Explorer, Sysinternals Suite
* **Detection Techniques:** Signature-based detection, Heuristic analysis
* **Testing:** Antivirus software for testing detection capabilities

**Implementation :**-

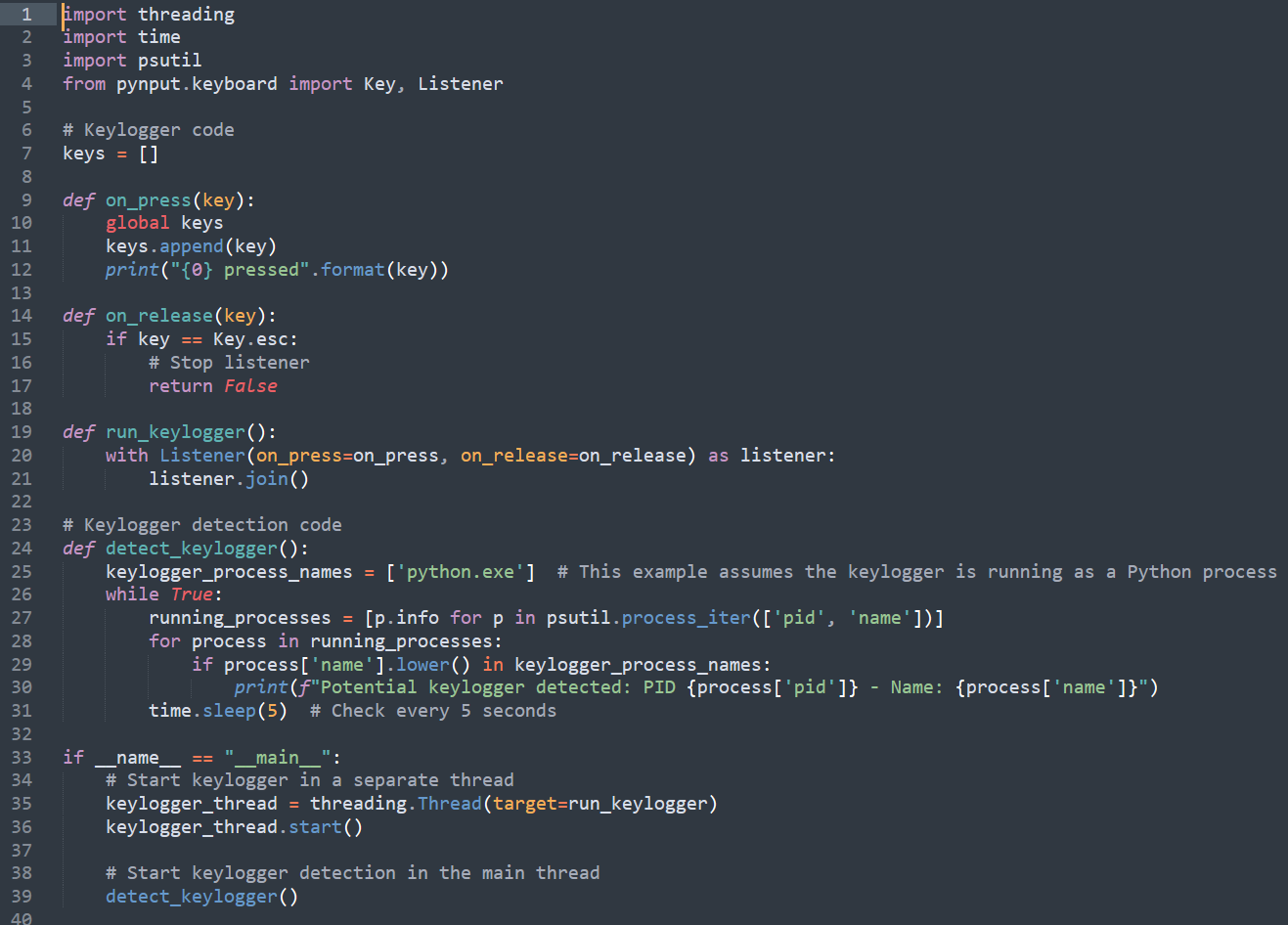
KEYLOGGER –



OUTPUT :-



DETECTION OF KEYLOGGER :-



OUTPUT :-



### Conclusion :-

This internship project offers a comprehensive exploration of both offensive and defensive aspects of cybersecurity related to keyloggers. Interns will gain hands-on experience in software development, system monitoring, and cybersecurity techniques, culminating in a detailed understanding of keylogger threats and protection strategies.

**ACKNOWLEDGEMENT**

I am deeply grateful to CDAC Noida for providing me with the opportunity to participate in the Cyber Gyan Virtual Internship Program. This experience has been invaluable in advancing my knowledge and skills, particularly through the project on "Development and Detection of Keyloggers for Windows Operating System."

I would like to extend my heartfelt thanks to the Cyber Gyan Virtual Internship Program team members for their collaboration and support. Their guidance and assistance have greatly enriched my internship journey and contributed significantly to the successful completion of this project.

PORIKA SANIYA

BTech-EE

NIT SILCHAR

**References :-**

1. "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory" by Michael Hale Ligh, Andrew Case, and Jamie Levy
2. "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig
3. "Windows Internals, Part 1: System architecture, processes, threads, memory management, and more" by Pavel Yosifovich, Mark Russinovich, Alex Ionescu, and David A. Solomon
4. "Detecting and Defending Against Keyloggers"-Article by SANS Institute