Capstone Project
Keylogger Detection
by
Team

Nathanael A Thomas (E23MCAG0068), Austin Devodass (E23MCAG0059), Shobit Jain (E23MCAG0089)
Department of computer Science Engineering, Bennett University

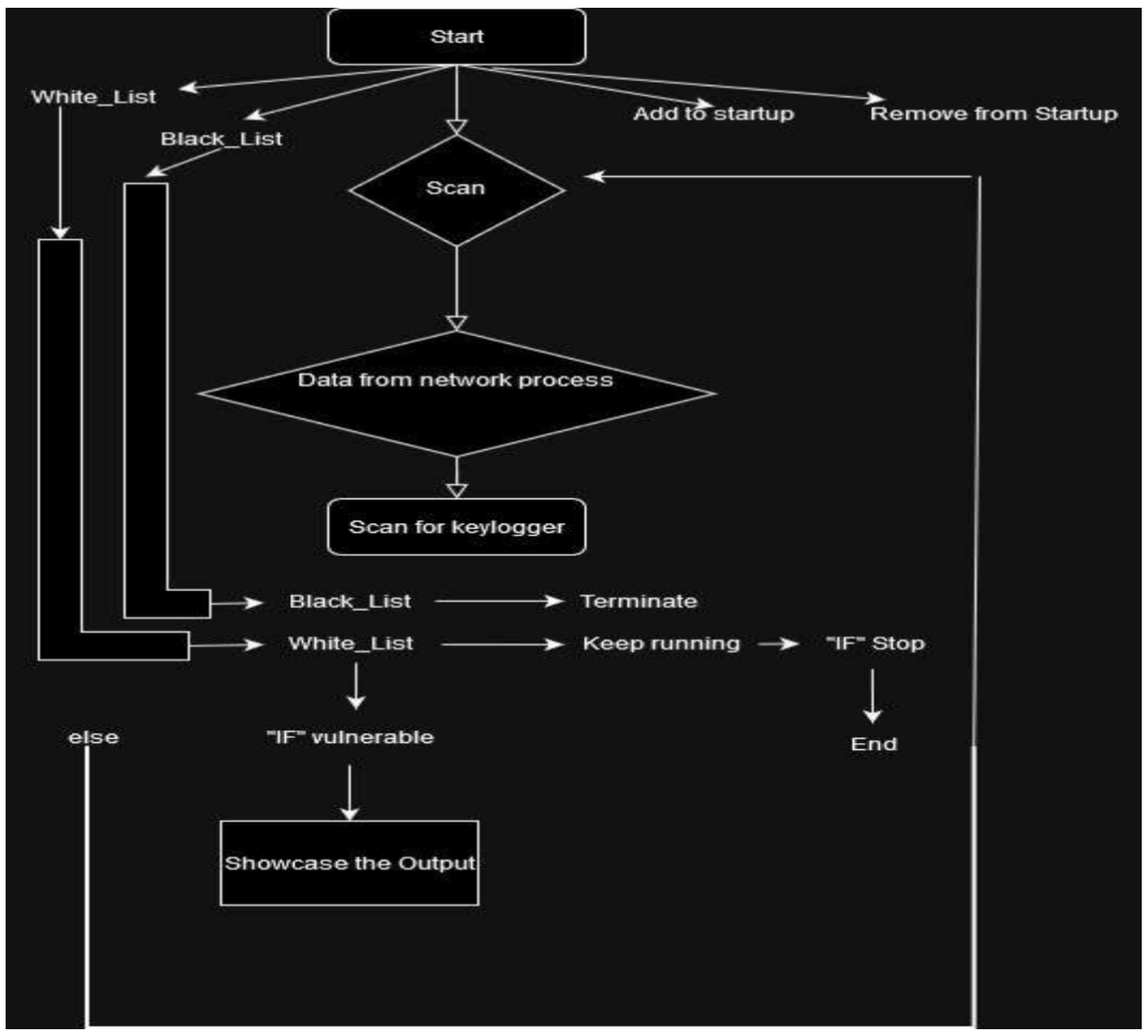
Abstract

Our objective is to develop a highly effective system for detecting keyloggers,which are malicious software designed to record keystrokes. By utilizing cutting-edge algorithms and continuous monitoring, we are dedicated to strengthening cybersecurity, safeguarding privacy, and thwarting data breaches in personal and organizational environments.

Introduction

The spread of malicious software in today's digital environment is a serious danger to cybersecurity. Keyloggers are particularly sneaky among these threats, covertly recording keystrokes and compromising confidential data. The repercussions of keylogger assaults, which can affect both persons and companies, can be dire and include identity theft and financial fraud. Because of this, creating efficient keylogger detection systems is essential to preventing these attacks and preserving the integrity of digital environments. The goal of this project is to develop a strong keylogger detection system that can recognize and stop malicious keylogging activity in order to meet this urgent demand.

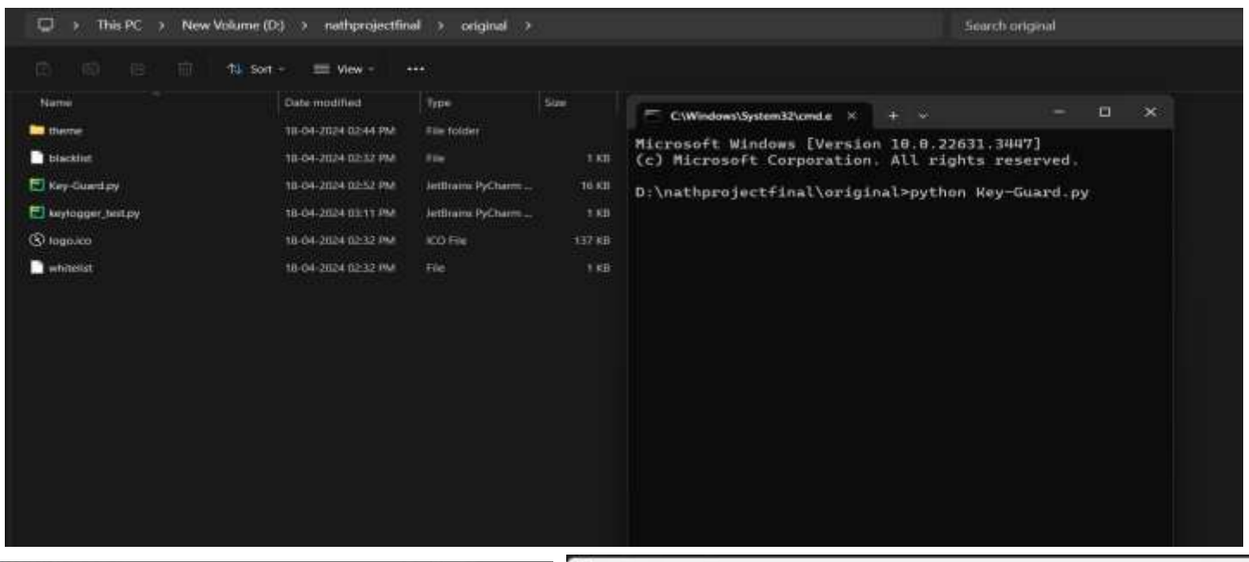
Proposed Method

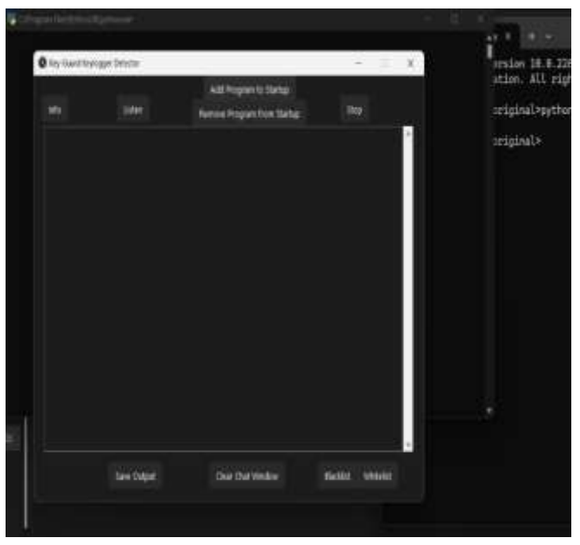


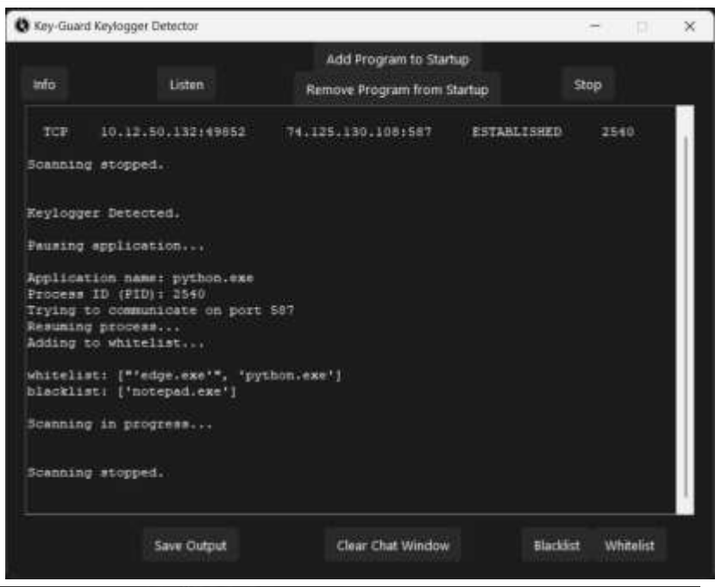
- Start: This is the beginning of the program.
- Add to Startup/Remove from Startup: This function controls whether the program itself is added to or removed from a list of programs that automatically run when the computer starts up.
- Black List/White List: These lists contain programs that the scanning function will reference. Programs on the whitelist are considered safe and those on the blacklist are considered unsafe.
- Scan: This function scans the computer for signs of keyloggers.
- Data from network process: This refers to the data that the program collects while scanning the computer system.
- Scan for Keylogger: This function analyzes the data collected during the scan to identify potential keyloggers.
- Black List: If the program finds something suspicious during the scan, it will check the blacklist to see if it matches a known keylogger.
- White List: If the program finds something suspicious during the scan, it will check the whitelist to see if it's a program that is considered safe.
- Terminate: If the program detects a keylogger that is not on the whitelist, it will terminate the program.
- Keep Running: If the program detects an unfamiliar program but it is on the whitelist, or if nothing suspicious is found, the program will keep running.
- Showcase the Output: This function displays the results of the scan.

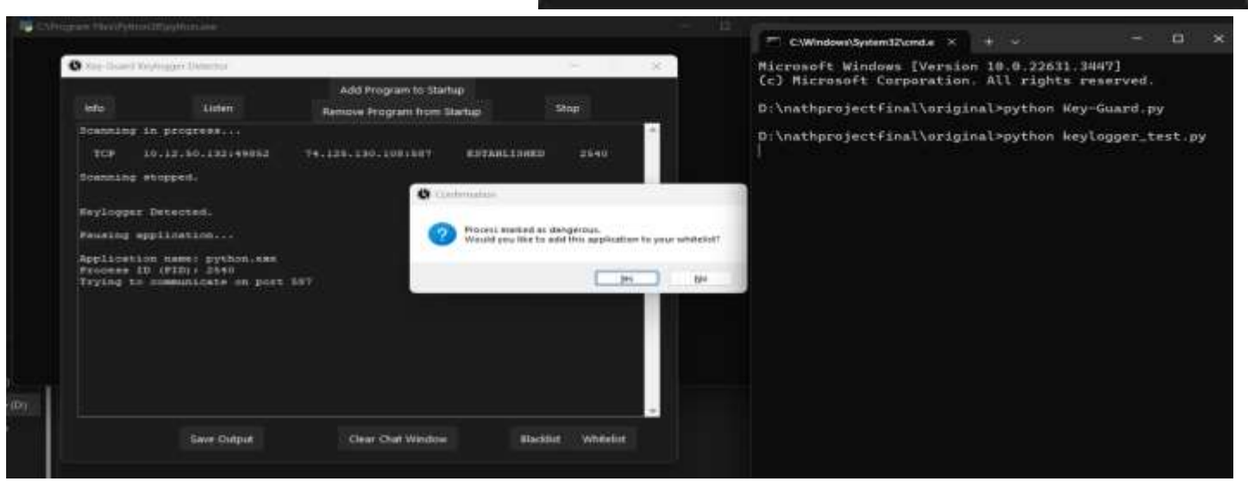
Experimental Results and Discussion

We evaluated the functionality of our keylogger detection tool experimentally using a test keylogger. The outcomes were overwhelmingly favorable, as our detection program achieved a 100% detection rate by accurately detecting the keylogger in each and every case. The outcomes of the experiment confirm that our keylogger detection program is reliable and effective in stopping malicious keylogging activities. Our technology shows potential in protecting against keylogger threats and preserving the security of digital environments, as it can detect the test keylogger with 100% accuracy.









Conclusions

To sum up, the development of a keylogger detection system has been a highly successful project of ours, producing an impressive 100% detection rate in keylogger identification. This result demonstrates how well our solution protects against unauthorized keyboard logging activity, improving cybersecurity for both individuals and enterprises.

GitHub & Video Link

Video Link - https://youtu.be/-ab__unrh3U?si=7nn4cd0fVQ_yLjRO
GitHub Link - https://github.com/Nathanaelxn/KEY-GUARD

References

- https://www.researchgate.net/profile/Ana-Maria-Ciobotaru/publication/266743342_An_Introduction_to_Undetectable_Keyloggers_with_Experimental_Testing/links/
- 57bc297008ae51eef1f61559/An-Introduction-to-Undetectable-Keyloggers-with-Experimental-Testing.pdf
- https://ieeexplore.ieee.org/abstract/document/7726880
- https://www.researchgate.net/profile/Yahye-Abukar/publication/309230926_Survey_of_Keylogger_Technologies/links/59a00619aca27237edba3c12/Survey-of-Keylogger-Technologies.pdf

Team No. - 01