Keylogger Detection System

KUKKALA AKASH REDDY
Student, Dept. of Computer Science and Engineering (Cyber Security), Geethanjali College of Engineering and Technology, Cheeryal, Keesara, Hyderabad

Abstract — Keyloggers are a kind of malware that can steal passwords and other private information by recording keystroke events on the keyboard and saving them to a log file. As a result, passwords, PINs, and usernames are captured by malicious software. Without attracting the user's notice, the cybercriminal Keyloggers pose a significant risk to both Online activities include both personal and business transactions, such as online banking, e-commerce, email chat, and other related activities. By exploiting this technique, an attacker can obtain important data without breaking into a secure database or file server. Keyloggers are mostly used to alter the sequence of events that take place when a key is pushed and the information that is subsequently displayed on the screen as a result of the keystroke. Keyloggers may serve both legal and illegal purposes, based on the intentions of the person employing them. System administrators can utilize keyloggers for systems to detect fraudulent users. Keyloggers assist a computer forensics analyst in analyzing digital files more efficiently. Keyloggers are highly beneficial for monitoring ongoing criminal activities.

I. INTRODUCTION

The security and sequestration of sensitive information have become essential businesses in the modern digital world, when people, organizations, and governments rely extensively on computers and networked systems for critical tasks. The keylogger is a covert tool used by cybercriminals to cover and record keystrokes on a victim's computer, potentially compromising private information like watchwords, credit card numbers, and specific dispatches. It is one of the most pernicious and intrusive of the many dangers that lurk in the digital world. The word "keylogger" refers to a variety of malicious software and malware tools that are intended to secretly record keyboard inputs without the stoner's consent or knowledge. Keyloggers are a serious threat to both individuals and organizations since they can be used for a variety of immoral activities, such as identity theft, financial fraud, commercial surveillance, and espionage. They are an unquestionable enemy in the continuous fight for cyber security because of their capacity to function covertly, usually avoiding detection by conventional security measures. Since keyloggers are so inflexible, a lot of time and money has been spent on both comprehending their methods of penetration and creating efficient detection and mitigation techniques. To confront this widespread imminence, this multidimensional bid combines legislative measures, technological innovation, cyber security education, and collaborative efforts with diligent stakeholders. This project's main goal is to construct and create a keylogger in order to comprehend the threat and infiltration it poses. Creating an executable of the main project, which the attackers primarily employ to conceal it on the target machine, is the secondary goal. The final goal is to comprehend keylogger invasions using this executable file by combining several methods to detect, isolate, and stop possible keylogging activity in various digital contexts. The project's goal is to improve keylogger detection effectiveness by integrating Virus Total and adding antivirus features. Through the use of cloud-based Virus Total analysis and local antivirus software, the system aims to strengthen cyber security protocols by proactively detecting and eliminating keylogger risks. The goal is to safeguard sensitive user information, bolster system integrity, and contribute to comprehensive defense mechanisms against keylogging intrusions in digital ecosystems. The objective of keylogger intrusion and detection is to protect sensitive information from being stolen by malicious users. Keyloggers can record every keystroke made on a device, potentially capturing sensitive data such as credit card numbers, passwords, and other personal information. By detecting and preventing keylogger intrusions, individuals and organizations can maintain their privacy and security. Keylogger detection involves identifying and removing keylogger software or hardware that has been installed on a device without authorization. This

can be done through various methods, including antivirus software, manual inspection of active processes, and reviewing installed programs. Keylogger prevention involves taking steps to prevent keylogger installation in the first place. This can include using antivirus software, being cautious when clicking links or downloading files, avoiding public devices, and using tools such as firewalls and intrusion detection systems. By focusing on keylogger intrusion and detection, individuals and organizations can better protect themselves from cyber threats and maintain their privacy and security. The objective of keylogger intrusion and detection is to prevent and identify the installation of keyloggers, which are malicious software or hardware that record every keystroke made on a device. Keyloggers can be used to steal sensitive information like credit card numbers, passwords, and other personal data, causing significant harm to individuals and organizations.

II. LITERATURE SURVEY

1. Real Time Working of Keylogger Malware Analysis Authors: - Devashree Kataria, Manan Kalpesh Shah, S Bharath Raj, Priya G

The paper highlights the rise of malware, particularly focusing on keyloggers, as a significant concern. Keyloggers, in particular, have become increasingly problematic as most antivirus solutions struggle to detect them effectively, rendering them nearly undetectable. Antivirus software aims to prevent and remove malicious software by identifying and eliminating threats from a device. However, certain types of malwares, such as keyloggers, evade detection, posing a serious threat to user privacy and security. The paper introduces antivirus software as a defense mechanism designed to detect, prevent, and eliminate malicious software from devices. Despite its intended purpose, the focus here is on keyloggers, a specific type of malware that has become a significant concern due to its ability to evade detection by most antivirus solutions, making it extremely challenging to detect and remove them effectively.

2. Survey On Keystroke Logging Attacks Authors: - Kayak .C, Suganya.R

The Malware is the process of disturbing system like collect sensitive data and gain access to systems. Ancient authentication systems want to defend access to on-line services (such as passwords) square measure prone to attack by the introduction of a keystroke faller to the service user's pc. Detecting and preventing malware attack is very important in cyber world as malwares can badly affect computer operation. Once a hacker got access to private user data, he/she can easily make money transfer from user account to untrusted account. The private data can have many consequences which can prove to be more hazards than particular individual's financial loss. We can summarize malwares program intentionally developed for damaging computer specifically those have internet connection. Keyloggers square measure a significant threat to users and therefore the user's information, as they track the keystrokes to intercept passwords and different sensitive data type written in through the keyboard. this provides hackers the good thing about accesses the PIN codes and account numbers, passwords toon-line searching sites, email id's, email logins and different hint etc. when the hackers get access to the user's private and sensitive information, they can take advantage of the extracted data to perform online money transaction the user's account. Keyloggers will typically, be used as a spying tool to compromise business and state-owned company's information. The most objective of keyloggers is to interfere within the chain of events that happen once a secret is ironed and once the information is displayed on the monitor as a result of a keystroke.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

Existing System

Keylogger intrusion detection systems currently available in the market come in various types and functionalities. However, they face significant challenges that limit their effectiveness in combating modern cybersecurity threats.

Disadvantages

1. Limited Detection Capability: Existing systems struggle to identify all types of keylogger activities, especially those employing sophisticated techniques.

2. High System Resource Consumption: These systems often consume substantial system resources, leading to reduced performance of the host device.
3. Inadequate Adaptability to Newer Keyloggers: As new and advanced keyloggers emerge, many existing systems fail to adapt and remain effective.

PROPOSED SYSTEM

To address the limitations of current keylogger intrusion detection systems, our project aims to develop a solution tailored to the evolving cybersecurity landscape. Leveraging the knowledge and skills gained during my engineering education, the proposed system will enhance the detection and mitigation of keylogger threats.

Advantages

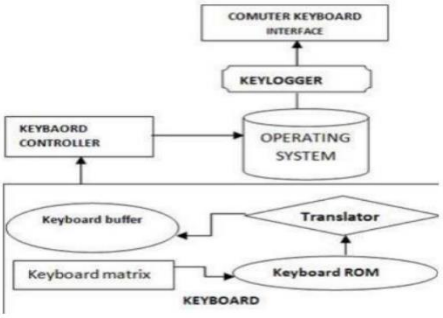
Real-Time Monitoring and Alerts: The system will offer real-time surveillance to detect keylogger activities and promptly notify users of potential threats.

Continuous Updates and Patch Management: Regular updates will ensure the system remains effective against newly emerging keylogger techniques.

Periodic Security Audits and Penetration Testing: The implementation of consistent audits and testing will help identify vulnerabilities and ensure robust protection.

IV. IMPLEMENTATION

System Architecture



A keyboard consists of a matrix of circuits overlaid with keys. This matrix of circuits, known as a key matrix, can differ between keyboard manufacturers. See Figure1. However, the key codes that are sent through the keyboard interface to a specific operating system are always the same. When the user presses a key, a circuit closes in the Key Matrix. The Keyboard Processor detects this event and captures the circuit location. Using a table stored in keyboard ROM, the processor translates the circuit location to a character or control code. Control codes are typically CTRL- or ALT- combinations. The keyboard's memory buffer temporarily stores the translated character or control code and then sends it to the computer's keyboard interface. The computer's keyboard controller receives the incoming keyboard data and forwards it to the operating system. A keyboard driver is typically used to manage this part of the process. The operating system processes the keyboard input based on the current state of the OS and applications. A keyboard interfaces with a computer via either a cable or a wireless connection. Common cable connections include the old PS2 standard and today's more common USB connector. A popular wireless connection uses a 27 MHz signal with a range of about six feet. These 50 types of connection are found in Microsoft and Logitech wireless keyboards. For solutions that require greater range, more robust wireless connections are available. These long-range connections can reach about 100.

Modules

1. Input Module

This module focuses on capturing user input to simulate keylogger behaviour for testing purposes.

Implementation of a Simple Keylogger:

Captures all keystrokes entered by the user.

2. Processing Module

This module handles the processing and transfer of captured keystroke data.

Logging Keystrokes:

Sends recorded keystroke logs to a designated email address for analysis.

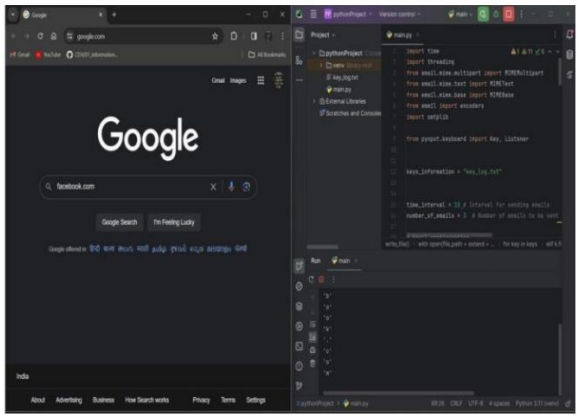
3. Output Module

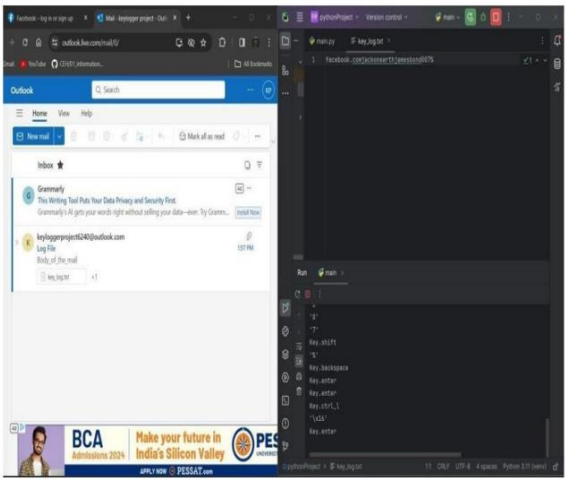
This module is designed to identify and respond to keylogger activities.

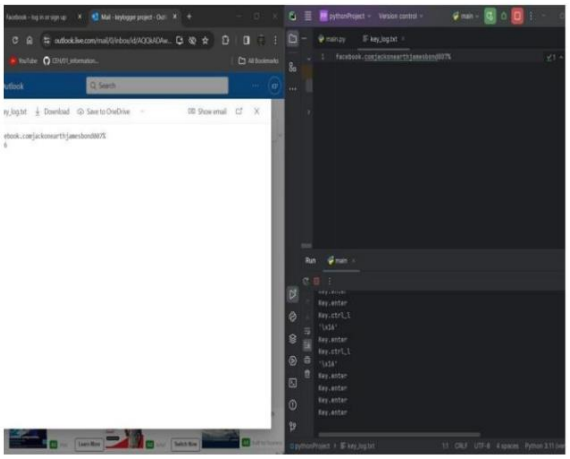
Keylogger Detection:

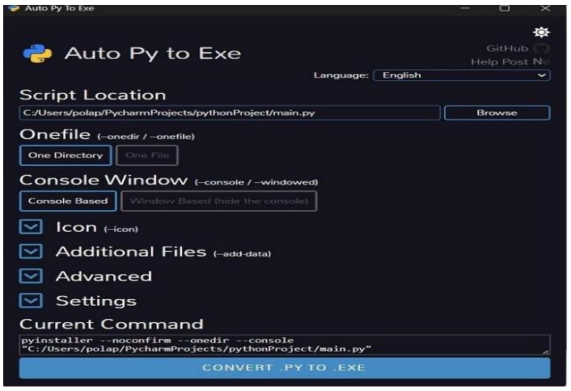
Identifies the presence of keylogging software and generates appropriate alerts or reports.

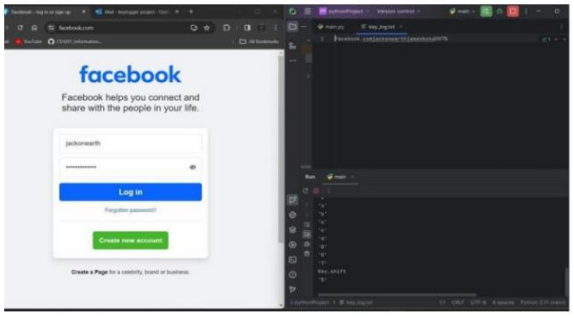
V. RESULTS

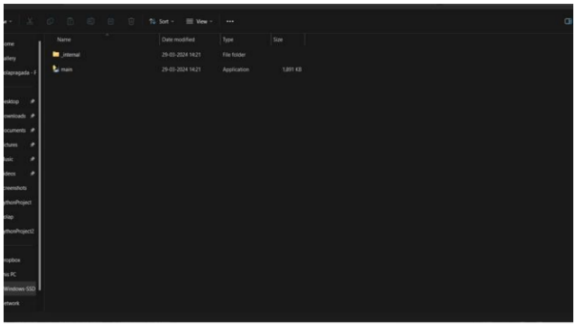

Google
facebook.com
Google Search
I'm Feeling Lucky

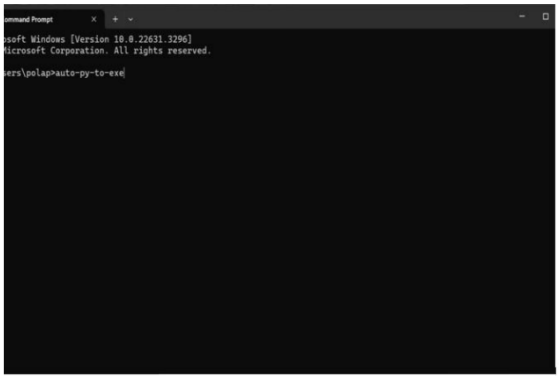

Outlook
Inbox
BCA
Make your future in India's Silicon Valley
PESSAT.com

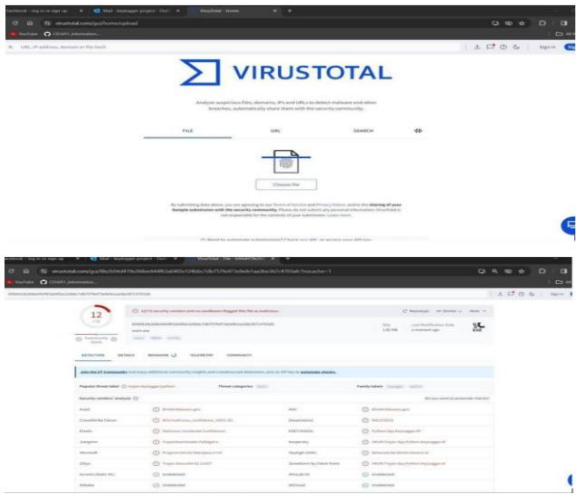



Auto Py to Exe
Language: English
Script Location
C:/Users/polap/PycharmProjects/pythonProject/main.py
Browse
Onefile (--onedir / --onefile)
One Directory
One File
Console Window (--console / --windowed)
Console Based
Window Based (hide the console)
Icon (--icon)
Additional Files (--add-data)
Advanced
Settings
Current Command
pyinstaller --noconfirm --onedir --console "C:/Users/polap/PycharmProjects/pythonProject/main.py"
CONVERT .PY TO .EXE


facebook
Facebook helps you connect and share with the people in your life.
Log in
Create new account




Command Prompt
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.
C:\Users\polap>auto-py-to-exe


VIRUSTOTAL

CONCLUSION

In conclusion, this project was completely for our understanding of the topic of Keyloggers Intrusion and Detection. The proliferation of keyloggers represents a significant threat to the security and privacy of individuals, businesses, and governments worldwide. Their ability to operate covertly and evade detection poses formidable challenges to cyber security professionals tasked with safeguarding sensitive information in an increasingly interconnected digital ecosystem.

Future enhancements

However, through ongoing research, technological innovation, and collaborative efforts across industry sectors, significant strides have been made in understanding keylogger intrusion methods and developing effective detection and mitigation strategies. By leveraging a combination of advanced security technologies, user education, and proactive security practices, organizations can bolster their defenses against keylogger related threats and mitigate the risk of data compromise and financial loss. Nevertheless, vigilance remains paramount in the ongoing battle against this pernicious form of cybercrime.

REFERENCES

[1] Ahmed, Yahye Abukar, et al. "Survey of Keylogger technologies."

[2] AISHWARYA, SANKHLA, J. O. H. N. SONIA K, and S. SUMUKH. "The Implementation and Detection of Keyloggers in a System." (2018).

[3] Bhardwaj, Akashdeep, and Sam Goundar. "Keyloggers: silent cyber security weapons." Network Security 2020.2 (2020): 14-19.

[4] Ballfield, Toni. Different types of keyloggers: Mitigation and risk relevancy in modern society. BS thesis. 2020.

[5] Constantin, Lucian. “Attack Campaign Uses Keylogger to Hijack Key Business Email Accounts.” PCWorld, 17 Mar. 2016, www.pcworld.com/article/420141/attack - campaign-useskeyloggertohijack-key- business-email-accounts.html.