VISVESVARAYA TECHNOLOGICAL UNIVERSITY

JNANASANGAMA, BELAGAVI - 590018

A Project Based Learning

(23MCS213)

on

Keystroke Capturing and Detection

Submitted in partial fulfillment for the award of degree of

Masters of Technology
in
COMPUTER SCIENCE AND ENGINEERING

Submitted by
Swapnali Vijay Gawade (1BG23SCS07)

Internal Guide
Dr. Rajashree Soman

Professor, Dept. of CSE BNMIT,
Bengaluru

Vidyayāmruthamashnuthe

B.N.M. Institute of Technology

An Autonomous Institution under VTU,
Approved by AICTE, Accredited as grade A Institution by NAAC.
All eligible branches – CSE, ECE, EEE, ISE & Mech. Egg. Are accredited
by NBA for academic years 2018-19 to 2020-21 & valid upto 30.06.2021
Post box no. 7087, 27th cross, 12th Main, Banashankari 2nd Stage, Bengaluru- 560070, INDIA
Ph: 91-80- 26711780/81/82 Email: principal@bnmit.in, www. bnmit.org

Department of Computer Science and Engineering

2023 – 2024

B.N.M. Institute of Technology

An Autonomous Institution under VTU,
Approved by AICTE, Accredited as grade A Institution by NAAC.
All eligible branches – CSE, ECE, EEE, ISE & Mech. Egg. Are accredited
by NBA for academic years 2018-19 to 2020-21 & valid upto 30.06.2021
Post box no. 7087, 27th cross, 12th Main, Banashankari 2nd Stage, Bengaluru- 560070, INDIA
Ph: 91-80- 26711780/81/82   Email: principal@bnmit.in, www. bnmit.org

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Vidyayāmruthamashnuthe

CERTIFICATE

Certified that the project work entitled "Keystroke capturing and detection" carried out by **Ms. Swapnali Vijay Gawade (USN:1BG23SCS07),** are bonafide student of I Semester, BNM Institute of Technology in partial fulfillment for the award of Masters of Technology in COMPUTER SCIENCE AND ENGINEERING of Visvesvaraya Technological University, Belagavi during the year 2023-24. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The Project-based learning report of Digital Image Processing and Computer Vision Subject has been approved as it satisfies the academic requirements in respect of project work.

Dr. Geetha S
Professor
Department of CSE
BNMIT, Bengaluru

Dr. Chayadevi M L
Professor and Head
Department of CSE
BNMIT, Bengaluru

Dr. Krishnamurthy G.N
Principal
BNMIT,
Bengaluru

Name **Signature**

Examiner 1:

Examiner 2:

ACKNOWLEDGEMENT

The success and final outcome of this project required a lot of guidance and assistance from many people and we are extremely privileged to have got this all along the completion of my project.

I would like to thank **Shri. Narayan Rao R Maanay**, Secretary, BNMIT, Bengaluru for providing excellent academic environment in the college.

I would like to sincerely thank **Prof. T. J. Rama Murthy**, Director, BNMIT, for having extended his support and encouragement during the course of the work.

I would like to sincerely thank **Dr. S. Y. Kulkarni**, Additional Director, BNMIT, for having extended his support and encouragement during the course of the work.

I would like to express my gratitude to **Prof. Eishwar N. Maanay**, Dean, BNMIT, Bengaluru, for his support and encouragement.

I would like to thank **Dr. Krishnamurthy G.N**, Principal, BNMIT, Bengaluru, for his constant encouragement.

I express my in-depth, heartfelt, sincere gratitude to **Dr. Chayadevi M L**, Professor and H.O.D, Department of Computer Science and Engineering, BNMIT, Bengaluru, for her valuable suggestions and support.

I express my in-depth, heartfelt, sincere gratitude to **Dr. Rajashree Soman**, Project Coordinator, Professor, BNMIT, Bengaluru, for her valuable suggestions and support.

Swapnali Vijay Gawade
(1BG23SCS07)

Table of Contents

ABSTRACT

Keyloggers are a type of computer malware that records keystroke events on the keyboard and saves them to a log file, allowing it to steal sensitive data like passwords. Malicious software captures usernames, PINs, and passwords as a result. Without drawing the user's attention, the hacker Keyloggers possess a big threat to both Transactions such as commercial and personal i.e., E-commerce, online banking, email chatting, and other similar activities are examples of online activities. An attacker can collect valuable data without entering into a strong database or file server using this method. The main purpose of keyloggers is to tamper with the chain of events that occur when a key is pressed, and information is displayed on the screen as a result of the keystroke. Keyloggers can be used for both lawful and illegitimate objectives, depending on the user who is utilizing it. Keyloggers for systems, i.e., for identifying fraudulent users, can be used by system administrators. Keyloggers can help a computer forensics analyst examine digital files more effectively. Keyloggers are extremely useful for keeping track on ongoing criminal activity.

LIST OF FIGURES

LIST OF Tables

CHAPTER 1

1.1 INTRODUCTION

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.

An infamous keylogger attack uses a type of malware called DarkHotel. Hackers target unsecured Wi-Fi at hotels and prompt users to download the software. Once downloaded, DarkHotel acts as a keylogger and reports keystrokes to the hackers. After a certain number of recorded keystrokes, DarkHotel deletes itself from the device. That way, it doesn't remain on a device for too long and can avoid detection.

It's important to protect yourself from keylogger attacks used by malicious users. Because keyloggers can record and quickly identify sensitive information, they are a significant threat to cybersecurity. To protect yourself, it's important to know what keyloggers are, how to prevent an attack and how to remove a keylogger if you are attacked.

Personal information is lucrative to cybercriminals, and cybercriminals use various strategies to try to gain access to your sensitive data. Spyware is one kind of cybersecurity risk where a malicious user attempts to gather information about a user to cause harm. Cybercriminals often use a keystroke logger as spyware to track a user's actions without their knowledge.

1.2 PROBLEM STATEMENT

A keylogger is a type of software or hardware that records keystrokes on a computer or device. While keyloggers can serve legitimate purposes, such as monitoring children's internet activity or tracking employee computer usage, they are often associated with malicious intent, such as stealing sensitive information like passwords or credit card numbers.

Software Key loggers, also known as keystroke loggers, record the keys hit on a device and save them to a file, which is then accessed by 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. Keyloggers can be connected directly to the keyboard and the computer through manually using one of two approaches. PS/2 and the USP keylogger are two examples of this method.

1.3 OBJECTIVE

The purpose of this application is to keep tracks on every key that is typed through the keyboard and send it to the admin through the mail server in the time set or given. It provides confidentiality as well as data recovery to all the IT infrastructures in need.

In many companies now-a-days data security and data recovery is the most important factor. So there are many cases where data recovery is required. For these kinds of problems keylogger is one of the best solutions which is often referred to as keylogging or keyboard capturing. Keyboard capturing is the action of recording the keys stroke on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Using keylogger application users can retrieve data when working file is damaged due to several reasons like loss of power etc.

This is a surveillance application used to track the users which logs keystrokes; uses log files to retrieve information. Using this application, we can recall forgotten email or URL. In this keylogger project, whenever the user types something through the keyboard, the keystrokes are captured and mailed to the mail id of admin without the knowledge of the user within the time set.

CHAPTER 2

LITERATURE SURVEY

KEYLOGGER IN EDUCTION

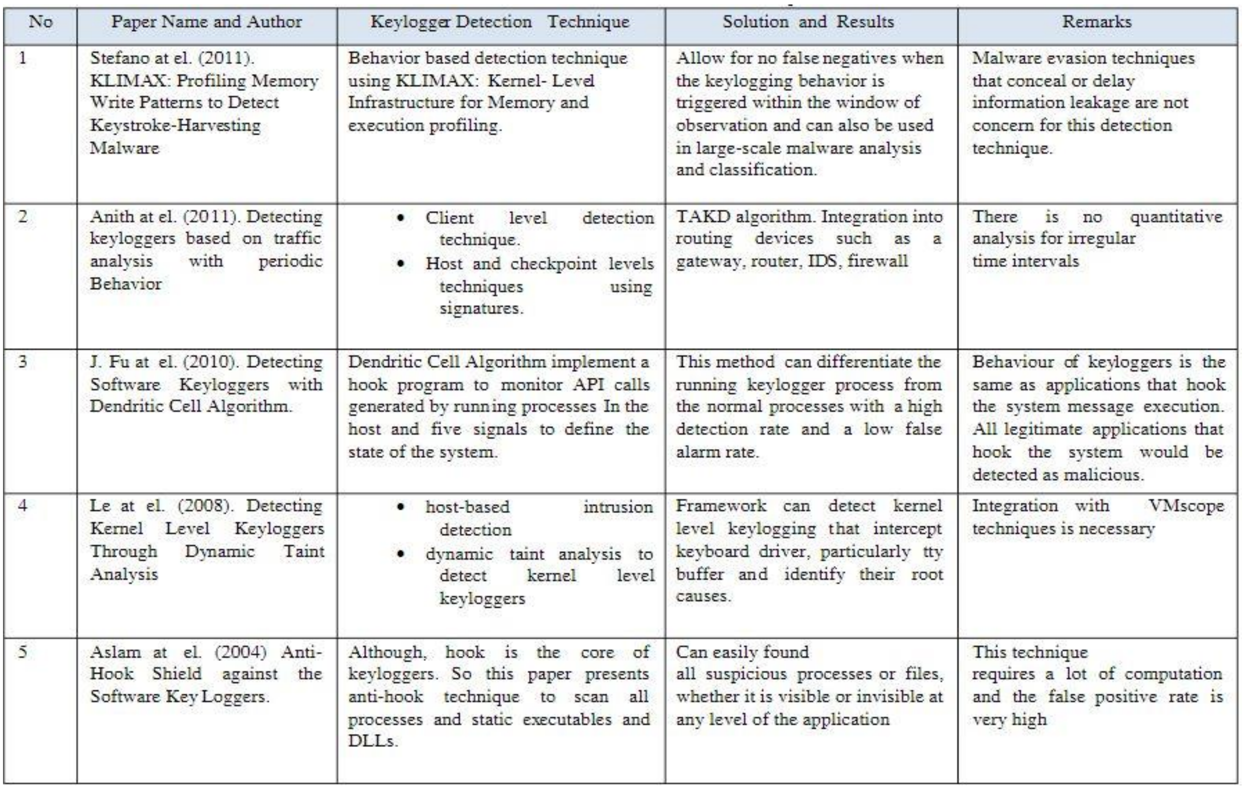
As online education platform is increasing, keylogger can inspire to do hard work. There may be students who will do their daily work to impress teacher by using internet source. Knowing they're being watched will be a motivator to work diligently. Keyloggers can be used during practical examination in order to prevent from copying

KEYLOGGER IN INDUSTRY

Reduces Corruption & Ensure Accurate Report:

A. You'll get accurate and detailed reports regarding employee activities if you install a software keylogger. You can feel confident that your personnel are just doing their best.

B. Users are at risk because keyloggers can record passwords and other personal information entered through the keys. This can lead to the invasion of secret passwords, bank account information, online identities, and social network login.



No	Paper Name and Author	Keylogger Detection Technique	Solution and Results	Remarks
1	Stefano at el. (2011). KLIMAX: Profiling Memory Write Patterns to Detect Keystroke-Harvesting Malware	Behavior based detection technique using KLIMAX: Kernel- Level Infrastructure for Memory and execution profiling.	Allow for no false negatives when the keylogging behavior is triggered within the window of observation and can also be used in large-scale malware analysis and classification.	Malware evasion techniques that conceal or delay information leakage are not concern for this detection technique.
2	Anith at el. (2011). Detecting keyloggers based on traffic analysis with periodic Behavior	• Client level detection technique. • Host and checkpoint levels techniques using signatures.	TAKD algorithm. Integration into routing devices such as a gateway, router, IDS, firewall	There is no quantitative analysis for irregular time intervals
3	J. Fu at el. (2010). Detecting Software Keyloggers with Dendritic Cell Algorithm.	Dendritic Cell Algorithm implement a hook program to monitor API calls generated by running processes In the host and five signals to define the state of the system.	This method can differentiate the running keylogger process from the normal processes with a high detection rate and a low false alarm rate.	Behaviour of keyloggers is the same as applications that hook the system message execution. All legitimate applications that hook the system would be detected as malicious.
4	Le at el. (2008). Detecting Kernel Level Keyloggers Through Dynamic Taint Analysis	• host-based intrusion detection • dynamic taint analysis to detect kernel level keyloggers	Framework can detect kernel level keylogging that intercept keyboard driver, particularly tty buffer and identify their root causes.	Integration with VMscope techniques is necessary
5	Aslam at el. (2004) Anti-Hook Shield against the Software Key Loggers.	Although, hook is the core of keyloggers. So this paper presents anti-hook technique to scan all processes and static executables and DLLs.	Can easily found all suspicious processes or files, whether it is visible or invisible at any level of the application	This technique requires a lot of computation and the false positive rate is very high

Table 2.1 Survey on Keylogger

2.1 INFERENCE FROM LITERATURE

To notice keyloggers more clearly, it is critical for an individual to have a firm grasp on the fundamentals of what keyloggers are, how they are implemented, and the various approaches to them. To respond to these kinds of questions, we'll go over the various types of algorithms that have been developed so far to solve the problem, as well as the disadvantages of each system.

Key logging is a safety tradeoff technique that should be feasible from a variety of perspectives. When an attacker gains physical access to your computer, they can wiretap the physical hardware, such as the keyboard, to capture the user's valuable information. This technique is totally reliant on some real-world phenomena, such as sound transmission from a client's composition or the electromagnetic propagation of a remote console. Keyloggers are used for both legal and illegal reasons

Example : Attackers commonly use keyloggers to steal private information from individuals or businesses. Many credit card details have previously been hacked by criminals using keyloggers.

CHAPTER 3

MODLE IMPLEMENTATION

3.1 Technical Specification

HARDWARE REQUIREMENTS:

Operating system: Windows and Linux specified

RAM: 512MB (minimum requirement)

Hard Disk: 1GB working space (minimum requirement)

SOFTWARE REQUIREMENTS:

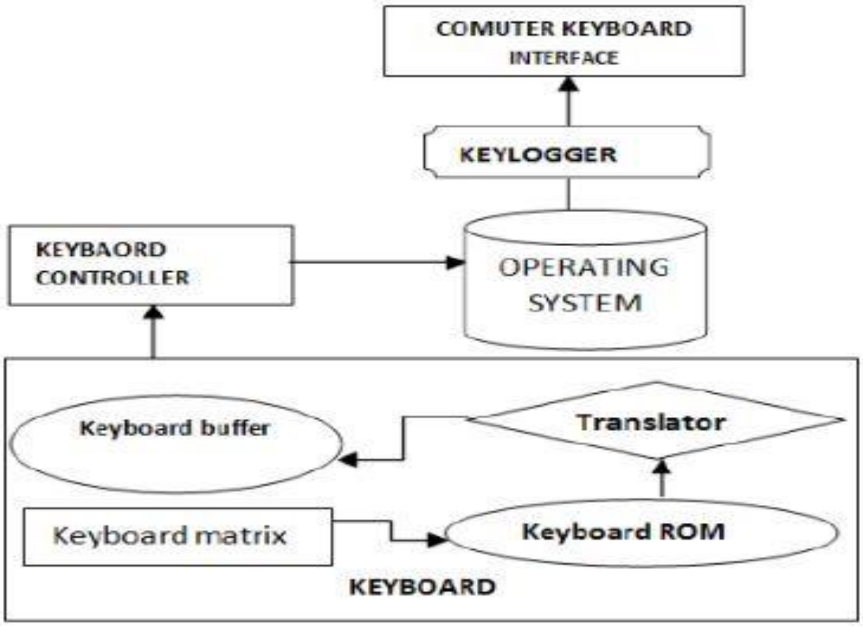
Languages : Python Tools : PyCharm, Python 3.8.0

Technology : Advanced programming using Python

3.2 Proposed System

Keyboard is primary target of most common keyloggers; it consists of matrix of circuit with keys also known as key matrix, there are many different types of key matrix depending on keyboard manufactures. However, the circuit closes key matrix when the user presses key, then keyboard processor and ROM detect this event. The processor translates the circuit location to a character or control code and sends to keyboard buffer.

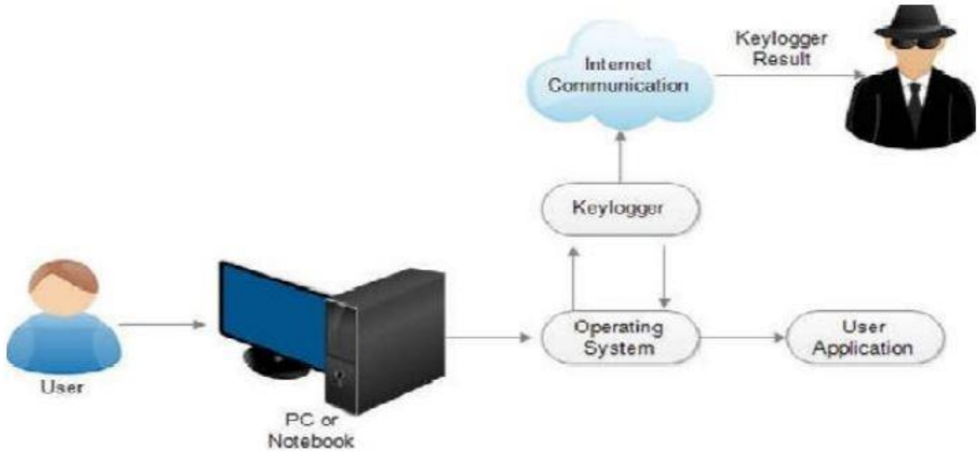
The computer's keyboard controller receives the incoming keyboard data and forwards it to the windows operating system. Data travelling between operating system and computer keyboard interface is, intercepted by keylogger. Thus the message flow is not transferred into next hook procedure.



Fig(3.2) Implementation Of Proposed System

3.3 Design and Implementation

The fundamental goal of keyloggers is to intercept any two links in the chain of events that occurs between when a key is hit and when data about a certain keystroke is presented on the monitor. Surveillance video, a hardware bug in the keyboard, cables, or the computer itself, intercepting input/output, substituting the keyboard driver, the sensor driver in the keyboard stack, able to intercept kernel functions by any means possible (substituting addresses in system tables, splicing function code, etc.), intercepting DLL functions in user mode, and, finally, requesting information from the keyboard using standard documented methods can all be used to achieve this.



Fig(3.3) System Flow Diagram of Keylogger

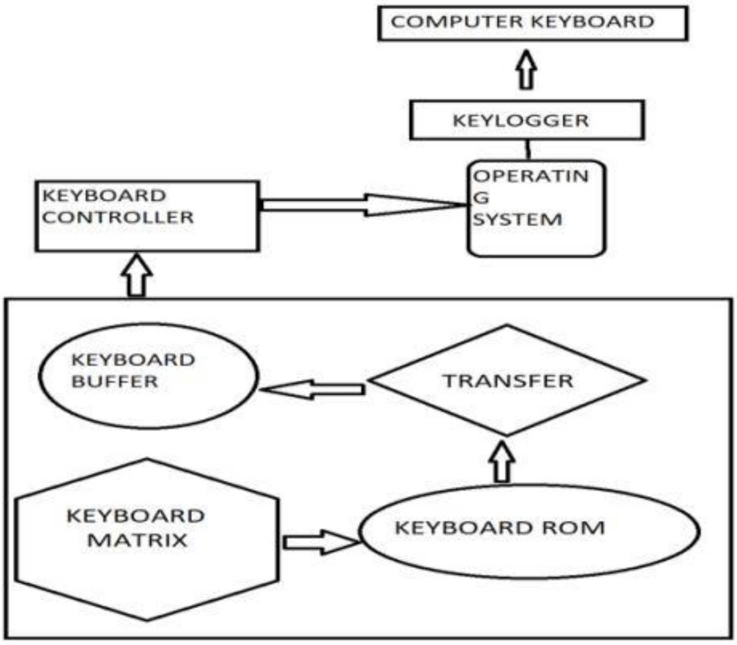
CHAPTER 4

METHODOLOGY

Most frequent keyloggers target the keyboard; it comprises of a circuit matrix A key matrix, often known as a key database, is a database that contains keys. Depending on the keyboard manufacturer, there are many distinct types of key matrix. When the user pushes a key, the circuit closes the key matrix, which is detected by the keyboard processor and ROM.

The circuit location is converted to a message or control code by the CPU, which is subsequently delivered to the keyboard storage. The computer's keyboard controller receives and transmits incoming keyboard data to the Windows operating system. The data that travels between the operating 8 system and the computer keyboard interface is captured by a keylogger.

4.1 Architecture of Keylogger



Fig(4.1)Architecture of Keylogger

1. OBSERVING USER DATA

The capability that will be required to capture keystrokes and mouse events will be activated. The capacity will capture what the client is typing in the console as well as the mouse click. It will snap a screenshot of the title of the current window. As a result, the proprietor of the product will examine all of their information without understanding who the client of the framework is.

2. SENDING SECRET INFORMATION

The software has two options for saving log information: one is to put it in a hidden folder, and the other is to send the log files directly to the software's owner's email address.

3. MAKE THIS SOFTWARE IN STEALTH MODE

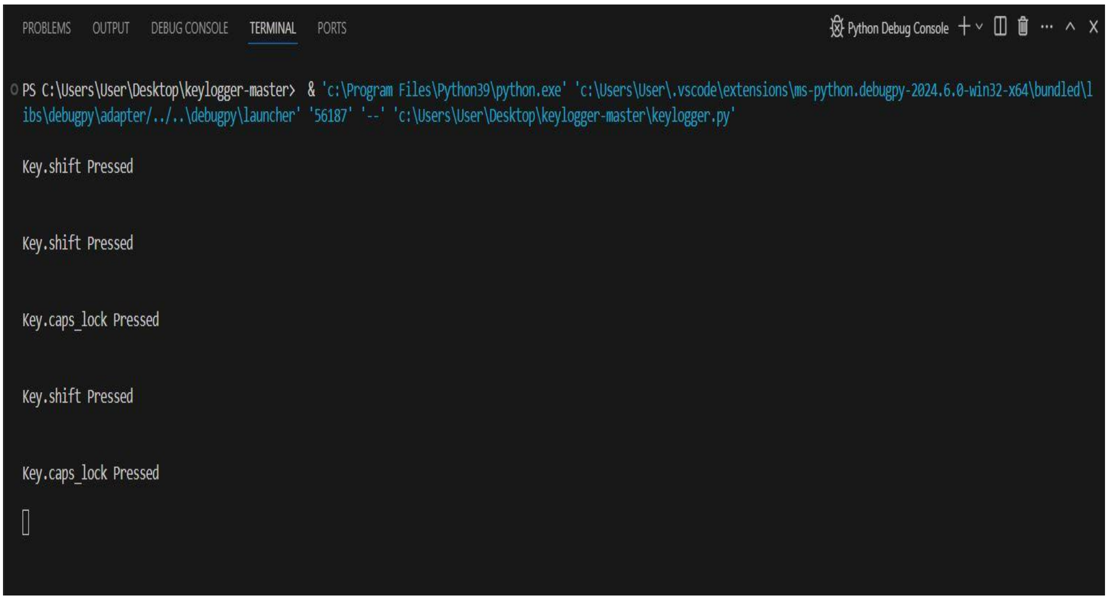
One major feature of the software is that it operates in stealth mode. Generally, this mechanism will hide the keylogger software first from owner, but it will ensure that the software is always on and recording all keystrokes.

CHAPTER 5

RESULTS

Keyloggers span a wide range of topics, including keylogger design and implementation, legal and ethical issues, real coding, and current activity in this field. This project is especially encouraging hands-on exposure to software security programmers. Keyloggers are an important part of today's cybersecurity education.

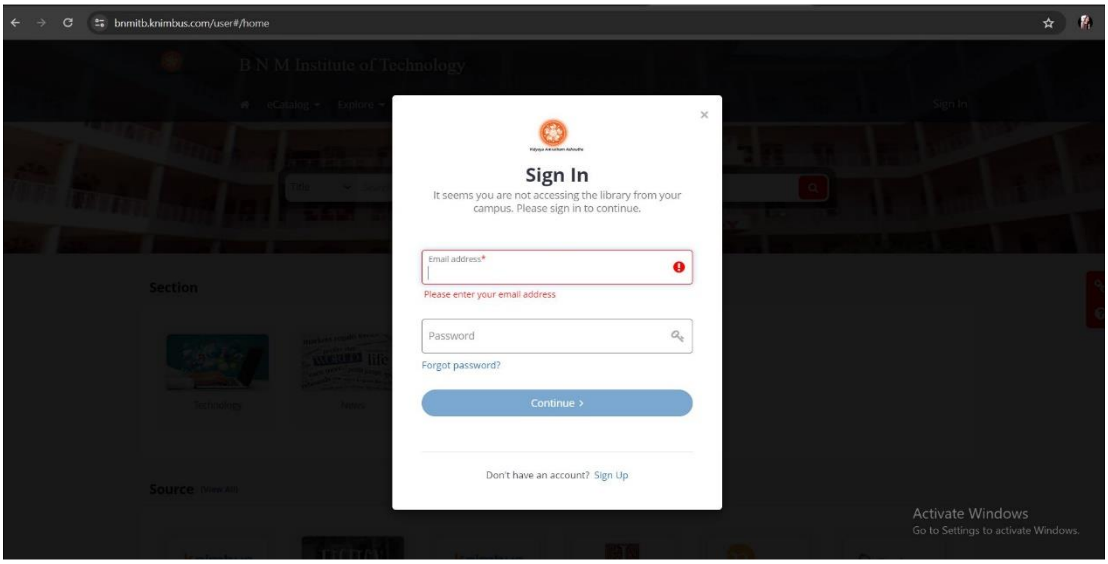
Image(5.1) visualize that the program is initiated and is in running state. Here the user activities are captured.



```
PS C:\Users\User\Desktop\keylogger-master>  & 'c:\Program Files\Python39\python.exe' 'c:\Users\User\.vscode\extensions\ms-python.debugpy-2024.6.0-win32-x64\bundled\l
ibs\debugpy\adapter/../..\debugpy\launcher' '56187' '--' 'c:\Users\User\Desktop\keylogger-master\keylogger.py'

Key.shift Pressed


Key.shift Pressed


Key.caps_lock Pressed


Key.shift Pressed


Key.caps_lock Pressed
```

Image(5.1)Program is in running state

Image(5.2) Captures the activity performed in the browser and logs in into file



bnmitb.knimbus.com/user#/home

B N M Institute of Technology

Sign In

It seems you are not accessing the library from your campus. Please sign in to continue.

Email address*

Please enter your email address

Password

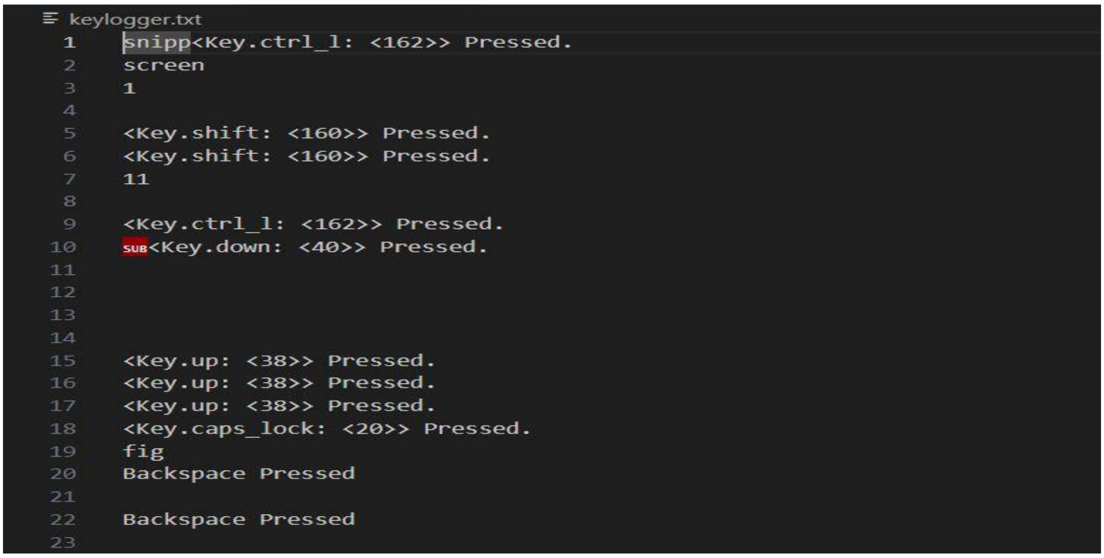
Don't have an account? Sign Up

Activate Windows

Go to Settings to activate Windows.

Image(5.2) Activity of the browser is in process

Image(5.3) Captures the keys pressed. Analysis the ASCII code of respective key and maintains it in a text file.



keylogger.txt

```
snipp<Key.ctrl_l: <162>> Pressed.
screen
1

<Key.shift: <160>> Pressed.
<Key.shift: <160>> Pressed.
11

<Key.ctrl_l: <162>> Pressed.
SUB<Key.down: <40>> Pressed.




<Key.up: <38>> Pressed.
<Key.up: <38>> Pressed.
<Key.up: <38>> Pressed.
<Key.caps_lock: <20>> Pressed.
fig
Backspace Pressed

Backspace Pressed

```

Image(5.3) Events of Keystrokes is recorded in file

CONCLUSION

Keyloggers are sophisticated tools that can access not only the platform, but also the user's private information like their name, password, pin, card and bank statement. While some keyloggers are utilized in a legal manner, the creators of many keyloggers do so unlawfully. The most frequent keylogger types and strategies used to hide themselves while subverting a user's PC were examined in this study. In addition, we looked at the present situation of keyloggers and the methods through which they spread Finally, we looked into existing detection methods and made some recommendations for prevention.

REFERENCES

[1] C.-C. C. Chieh-Ning Lien, "Keylogger Defender," UCLA Computer Science Department, Los Angeles, CA 90095, USA, 2015.

[2] C. a. Solms, "Implementing Rootkits to address operating system vulnerabilities," presented at the. Academy of computer science and software engineering, Universtiy of Johannesburg. Johannesburg, South Africa., 2011

[3] S. S. a. Anith.”Detecting keylogger based on traffic analysis with periodic behavior”PSG College of Technology, Coimbatore, India.2011

[4] Y. L. Jun Fu, Chengyu Tan,Xiaofei Xiong, "Detecting Software Keyloggers with Dendritic Cell Algorithm," presented at the 2010 International Conference on Communications and Mobile Computing, Wuhan University, 2010.

[5] M. Aslam, R. N. Idrees, M. M. Baig, and M. A.Arshad, “Antihook shield against the software key loggers,” in Proceedings of the National Conference of Emerging Technologies, 2019.

[6] A. R. P. Kalpa Vishnani, and Radhesh Mohandas, "An In-Depth Analysis of the Epitome of Online Stealth: Keyloggers; and Their Countermeasures," Dept. of Computer Science & Engg, National Institute of Technology Karnataka, Surathkal, Srinivasnagar, Mangalore - 575025, India, 2010.

[7] Y. L. Jun Fu, Chengyu Tan,Xiaofei Xiong, "Detecting Software Keyloggers with Dendritic Cell Algorithm," presented at the 2020 International Conference on Communications and Mobile Computing, Wuhan University