IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁙ Impact Factor 8.102 ⁙ Peer-reviewed / Refereed journal ⁙ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124153

KEYLOGGER USING BACKDOOR

Sadia Patka[1], Ayaz sayyed[2], Syed Amanuddin[3], Mohmmed Farhan sheikh[4], OwaisQadri[5]

Assistant Professor, Anjuman College of Engineering and Technology, Nagpur, India[1]

UG Student, Department of Computer Science and Engineering, Anjuman College of Engineering and Technology, Nagpur, India[2-5]

Abstract: The proposed point Keylogger which is likewise called as keystroke logger is a product that tracks orlogs the key struck on your console, regularly in a mystery way that you have no clue about that youractivities are being observed. Most of the people tend to see only bad side of this particular software but it also has legitimate use. Aside from being utilized for vindictive purpose like gathering account data, Visa numbers, client names, passwords, and other private information, it can be used in office tocheck on your employees, at home to monitor your children's activities and by law enforcement to examine and follow occurrences connected to the utilization of PCs. The project will be completely based on Python where I will make use of pynput module which is not a standard python module andneeds to be installed. The software that I am going to build should monitor the keyboard movement and stores the output in a file. To elevate the project I will also add a feature where the logs will be directly sent to the e-mail.

Keywords: Security Analysis, Research.

I. INTRODUCTION

Key logging program also known as keyloggers is a kind of malware that has capability to maliciously track input of the user from the keyboard in aim to retrieve private information. Keyloggers thus cause a major threat to business and personal activities of kind like transactions, online banking, email and chat. The keyboard is the prime target as it allows keyloggers to retrieve user input to the system as it is the most common wayuser interacts with a computer. There are two types of keyloggers that exists in market, a software keylogger and a hardware keylogger among which software keylogger are widely used and are easy to plant and cause substantial damage. Keyloggers essentially performs two tasks that is guiding into client input stream to get keystrokes and movingthe information to a distant area (for example- mail). The fundamental goal of keyloggers is to meddle in the chain of occasions that happen when a key is squeezed and when the information is shown on the screen because of a keystroke. Keylogger can be used for legitimate as well as illegitimate purposes, it basically depends on user who is using it. System administrators can use keyloggers for systems, i.e. for detecting suspicious users. Keyloggers can effectively assist a computer forensics analyst in the examination of digital media. Keyloggers are especially effective in monitoring ongoing crimes. Keystroke loggers can be used to capture and compile a record of all typed keys. Keyloggers can at times be utilized as a spying instrument to bargain business and state-possessed organization's information. Attackers can utilize keylogger to gain admittanceto the clients' private and delicate data, they can exploit the separated information to perform online cash exchange record or different vindictive stuff.

II. METHODOLOGY

I. Research Design: Describe the design of your research, including the approach used to collect data, the methods used to analyze data, and the type of data collected.

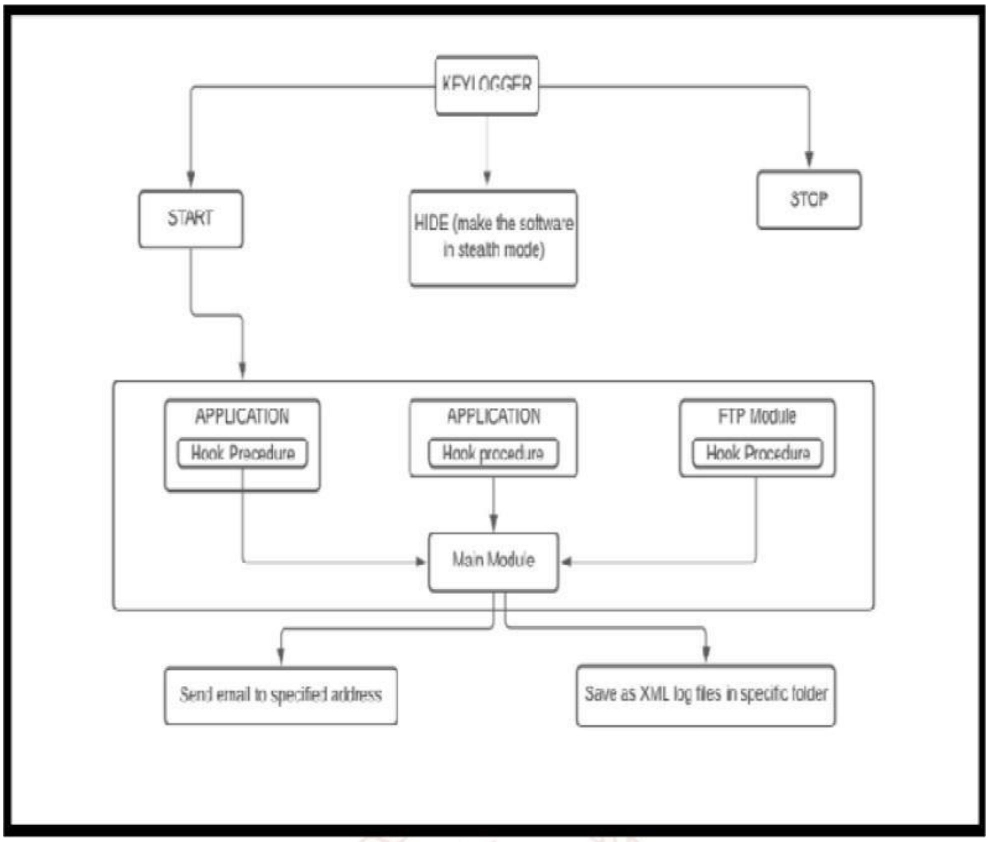
II. Data Analysis: Describe the methods used to analyze data, including the statistical tests used, the software used to analyze data, and any other tools used to analyze data.

III. Ethical Considerations: Describe the ethical considerations that were taken into account during the study, including obtaining informed consent from parents or legal guardians and protectingthe privacy and confidentiality of the participants.

IV. Data Collection: Describe the methods used to collect data, including the software used tomonitor keystrokes and any other data collected during the study.

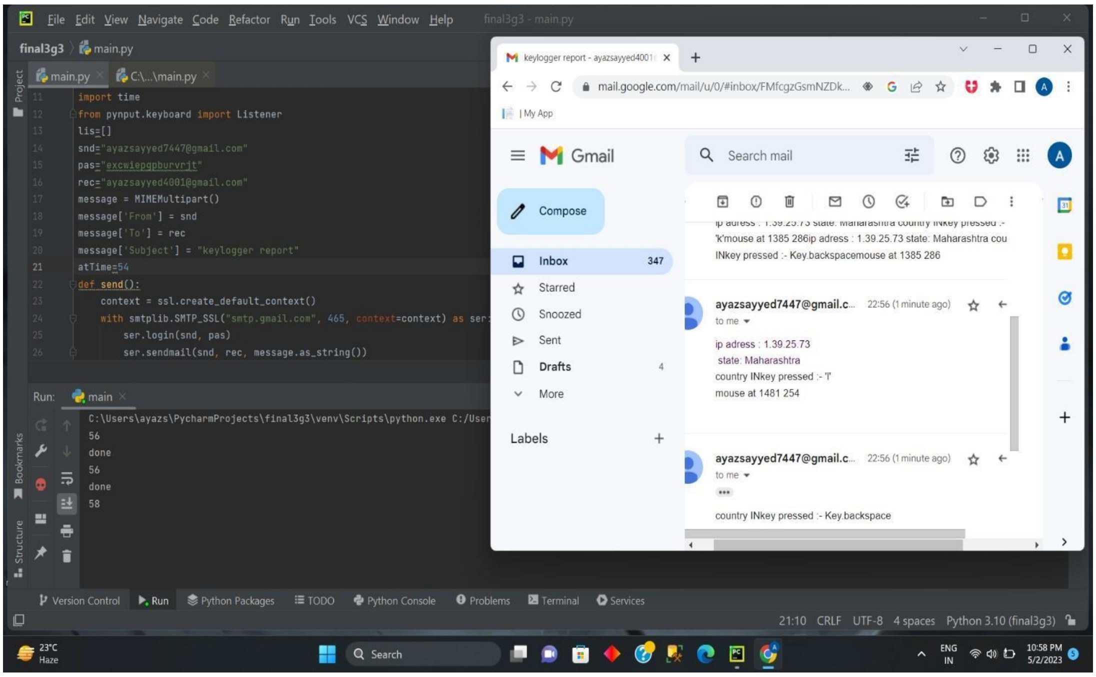
DOI: 10.17148/IJARCCE.2023.124153

III. FLOW CHART


KEYLOGGER
START
HIDE (make the software in stealth mode)
STOP
APPLICATION
Hook Procedure
APPLICATION
Hook procedure
FTP Module
Hook Procedure
Main Module
Send email to specified address
Save as XML log files in specific folder

Flow chart showing work of keylogger

IV. RESULTS AND DISCUSSION



```
import time
from pynput.keyboard import Listener
lis=[]
snd="ayazsayyed7447@gmail.com"
pas="excwiepqpburvrjt"
rec="ayazsayyed4001@gmail.com"
message = MIMEMultipart()
message['From'] = snd
message['To'] = rec
message['Subject'] = "keylogger report"
atTime=54
def send():
    context = ssl.create_default_context()
    with smtplib.SMTP_SSL("smtp.gmail.com", 465, context=context) as ser
        ser.login(snd, pas)
        ser.sendmail(snd, rec, message.as_string())
```

```
C:\Users\ayazs\PycharmProjects\final3g3\venv\Scripts\python.exe C:/User
56
done
56
done
58
```

ip adress : 1.39.25.73 state: Maharashtra country INkey pressed :-
'k'mouse at 1385 286ip adress : 1.39.25.73 state: Maharashtra cou
INkey pressed :- Key.backspacemouse at 1385 286

ayazsayyed7447@gmail.c... 22:56 (1 minute ago)
to me

ip adress : 1.39.25.73
state: Maharashtra
country INkey pressed :- 'l'
mouse at 1481 254

ayazsayyed7447@gmail.c... 22:56 (1 minute ago)
to me

country INkey pressed :- Key.backspace

Fig 1: Sample output of Keylogger

DOI: 10.17148/IJARCCE.2023.124153

In this output we can see how keylogger sent the IP address ,state ,country and keyboard and mouse event of the hacked device .The solution to the above existing problem is that we can build a software keyloggers instead of hardware keyloggers. The proposed model provides the solution that reduces the difficulties while installing the keylogger in the target system. Since, software keylogger can be installed remotely and does not need any physical access of the target system. Proposed software is efficient enough to get installed in targeted system by itself when the user for example clicks the malicious link sent to him through mail or any social media and finally captures all the keystrokes of the user while he is logged into the system, saves the logs in a folder or sends the log directly to the mail address of the third party. In the output we can see that the actions taken by the suspect can be measured and we can also get the data of the suspected person. This keylogger can also help the parents to keep an eye of theirChildrens .And also can be used by the police to trace the mobiles of thieves .

V. CONCLUSION

The product can play out the proposed work like a fundamental keylogger does to get all secret data from client of the framework by getting their keystrokes occasions and mouse clicks without the information on the client. So client of the framework is ignorant of things occurring in foundation. The software is able to monitor data and store the data in a specific folder or send the data to the owner’s mail id. The software is also able to hide itself from the owner if the system while it runs in background. Thus, I accept that my methodology extensively increases current standards for observing the information and gathering it for either lawful or unlawful reason.

REFERENCES

Here are some references for sales analysis on keylogger using backdoor:

[1] Martin Vuagnoux, S. P. (2009). Compromising electromagnetic emanations of wired and wireless keyboards. USENIX security symposium, 1–16.

[2] S. P. Goring, J. R. (2007). Anti-keylogging measures for secure internet login: an example of the law ofunintended consequences. Computers & Security, 1-9.

[3] Strahija, N. (2003, February 8). Student charged after college computers hacked. Retrieved from Xtrixsecurity: http://www.xatrix.org/article2641.html

[4] Thorsten Holz, M. E. (2009). Learning More about the Underground Economy: A Case-Study ofKeyloggers and Dropzones. Thorsten Holz, Markus Engelberth, Felix C. Freiling, 1-18.