KEYSTROKE LOGGER FOR TARGETED ATTACKS

A PROJECT REPORT

Submitted by

ANURAG(18BCE0302)

anurag.2018@vitstudent.ac.in

CHIRAG BADHAL(18BCE0304)

chirag.badhal2018@vitstudent.ac.in

NADEEM KAISAR(18BCE0353)

nadeem.kaisar2018@vitstudent.ac.in

Slot – G2

Computer Science and Engineering

NOVEMBER 2020

ABSTRACT

Keystroke logging, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A **keystroke recorder** or **keylogger** can be either software or hardware..A key-logger is a tool that hackers use to monitor and record the keystrokes you make on your keyboard. Whether they're installed on your operating system or embedded into the hardware, some key- loggers can be very difficult to detect.

KEYWORDS:

Keyboard ,Software,Hardware

1.INTRODUCTION:

Key-loggers collect information and send it back to a third party, whether that is a criminal, law enforcement or IT department. The amount of information collected by keylogger software can vary. The most basic forms may only collect the information typed into a single website or application. More sophisticated ones may record everything you type no matter the application, including information you copy and paste.

Data captured by key-loggers can be sent back to attackers via email or uploading log data to predefined websites, databases, or FTP servers. If the key-logger comes bundled within a large attack, actors might simply remotely log into a machine to download keystroke data.

Police can use the key-loggers to keep a track of the suspects of a particular case as a lot of people are now active on electronic devices like phones and PC.Organisations making confidential projects can include a key-logging feature in order to keep a track of the systems to which the project has been delivered. Any detected anomaly can be dealt accordingly.Parents can use this feature on the devices of their children (under 18 years) to keep a track if they are visiting some restricted sites.Corporate key-logging, such monitoring software can useful in testing, debugging and user experience.IT can use keystroke data to help identify and fix user issues, assist with security and compliance efforts, and possibly provide additional forensic information in the wake of a security incident. They can also be used to flag potential insider threats, monitor employee productivity, or ensure corporate IT assets are only being used for work purposes.

2.LITERATURE SURVEY:

In her paper Hemitha pathak[1] described that malware is used to disturb system process, collect sensitive data and gain access to systems . Detecting and preventing malware attack is very important area under discussion in cyber world as malwares can badly affect computer operation. The keylogger spyware is exceptionally risky for those systems which are involved in transaction processes daily. The keystrokes of keyboard got recorded by keylogger and are then sent to intruder through email. It is very important to valuable information like account numbers, ATM's PIN code, passwords etc

Key loggers[2] are implanted on a machine to intentionally monitor the user activity by logging keystrokes and eventually delivering them to a third party. While they are seldom used for legitimate purposes (e.g., surveillance/parental monitoring infrastructures), key loggers are often maliciously exploited by attackers to steal condential information.

Keylogger is one of malware rootkits that intercepts the user's typed keystroke on the keyboard. Mr Hasan[3] wrote that the first primary target of the keylogger is to secretly record confidential information of user's input through keystroke monitoring and then relaying this valuable information to others . The keyboard is the focal method of inputting textual and numerical information on the computer through typing. Therefore, an attacker can simply retrieve and access important information with the help of logging keystrokes. Generally, there is no intelligence built-in keylogger, but logs offer information about every single keyboard event and applications that users clicked or typed.

This paper[4] presents an introduction of key loggers with explaining the different types and comparison of different detection techniques overview. Also how one of these technique which could be used for keeping to keep a watch on the children web activites to guarentee their protection from online predators and dangers. And also organizations can also use this technique to monitor their employee's activity on internet

Keyloggers [5] are implanted on a machine to intentionally monitor the user activity by logging keystrokes and eventually sending them to a third party. While they are sometimes used for legitimate purposes (i.e. child computer monitoring), keyloggers are often maliciously exploited by attackers to steal confidential information. Many credit card numbers and passwords have been stolen using keyloggers , which makes them one of the most dangerous types of spyware. Keyloggers can be implemented as tiny hardware devices or more conveniently in software.

Keylogger programs attempt to retrieve confidential information by covertly capturing user input via keystroke monitoring and then relaying this information to others, often for malicious purposes.This[6] paper presents a case for incorporating keylogging in cybersecurity education. First, the paper provides an overview of keylogger programs, discusses keylogger design, implementation, and usage, and presents effective approaches to detect and prevent keylogging attacks. Second, the paper outlines several keylogging projects that can be incorporated into an undergraduate computing program to educate the next generation of cybersecurity practitioners in this important topic. Cyberwarfare[7] is observed very frequently as always some or the other country is targeting to ruin its enemy country by hacking confidential data from vital computer systems. This has led to dangerous international conflicts. Hence, to avoid illicit entry of other than military person or a government official several tools are being used today as spyware. Keyloggers are one of the prominent tools which are used in today's world to obtain secret or confidential data of a legitimate and contradictory a malicious user too. These keyloggers are advantageous and taken up positively for monitoring employee productivity, for law enforcement and the search for evidence of the crime.

The development of technology as described by robbi[8] is very fast, especially in the field of Internet technology that at any time experiencing significant changes, The development also supported by the ability of human resources, Keylogger is a tool that most developed because this application is very rarely recognized a malicious program by antivirus, keylogger will record all activities related to keystrokes, the recording process is accomplished by using string matching method. The application of string matching method in the process of recording the keyboard is to help the admin in knowing what the user accessed on the computer

Cyber Crime[9] has become a major threat to integrity of data owned and maintained by any organization or individual. One of the easiest ways to collect information from a system is by using a keylogger which tracks down the keyboard strokes, either using a Software-based keylogger or using a hardware-based keylogger. Though hardware-based keyloggers can be easily identified most of the times, the software-based keyloggers can pose a great threat if not detected timely. For this, a software called an anti-keylogger can be installed on the system which would track the use of any keylogger. The paper presents one such anti-keylogger named 'KeyLog Detector' which will not only display the list of suspected processes, but will also allow the user to modify, add to or delete from the names of existing suspected processes list apart from generating a system command to terminate the same

It[10] is likely that about one out of many l argee companies systematically monitors the computer , internet, or email use of its users employees. There are over hundred's different products available t oday that will let organizations see what their users do at w ork on their "personal" computers, in their email, and on the internet. But what do such numbers really mean ? What does company monitoring of user/employee email, internet, and computer usage actually look l i e? What sorts of things can an organization/compa ny see users do at their computers, and what sorts of computer activities are currently invisible to work place monitoring? This admittedly document attempts to propose, as concretely as possible what "Informationa l Flow" on internet and computer usage looks like: it s extent, the key concepts involved, and the forces driving its adoption. The keylogging program logs all keyst rokes (aka Keystroke Logging) along with the name o f the application in which the keystrokes were entered. U sing keylogger we prevent the miscellaneous use of system. Using this we capture all information in tedx and image form. Key Terms: Email monitoring, Internet monitoring, Computer monitoring, Chats/IM is monitoring, Network monitoring, Document monitoring, Web site m onitoring, Productivity monitoring, keylogging

3. Proposed Method (or) System Design

PROJECT PHASE 1:

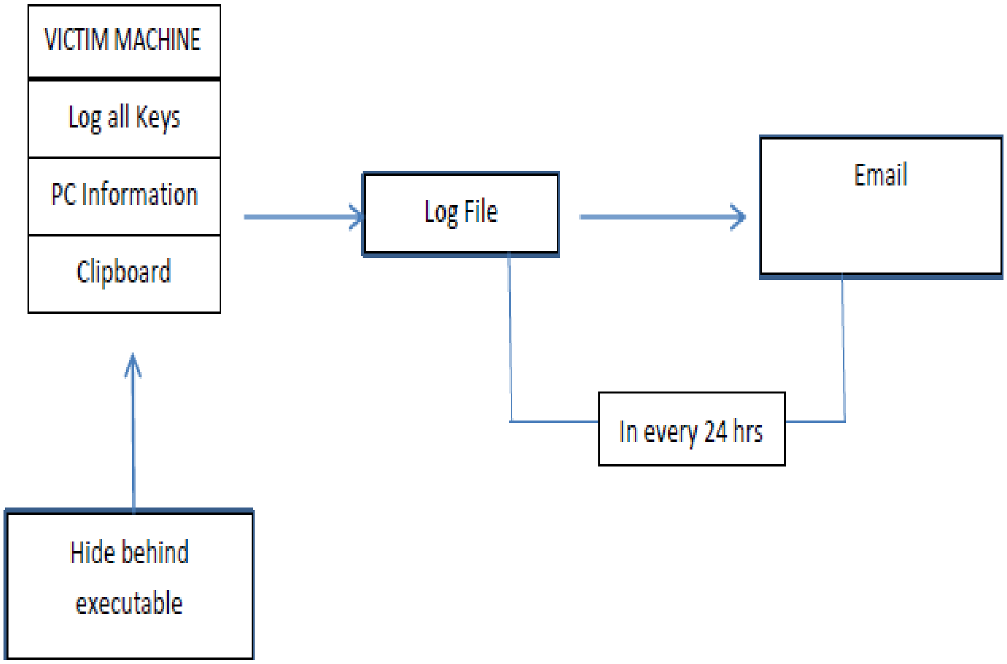


FIG 1

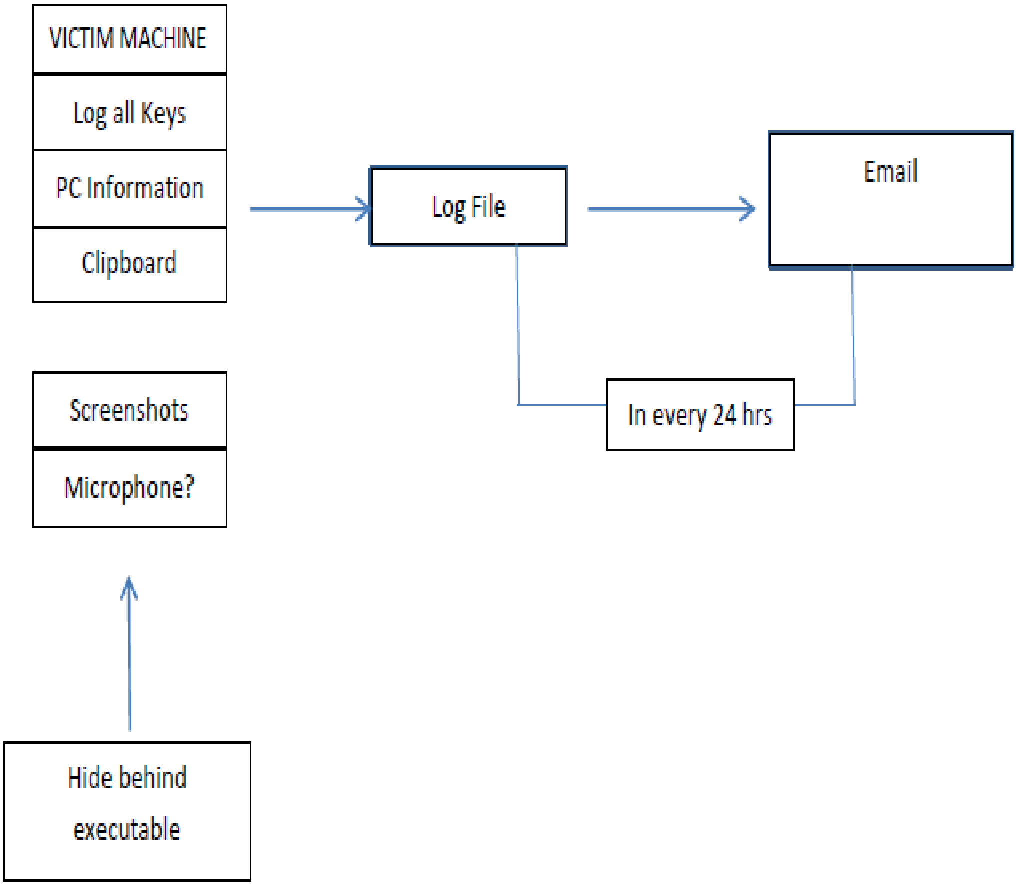
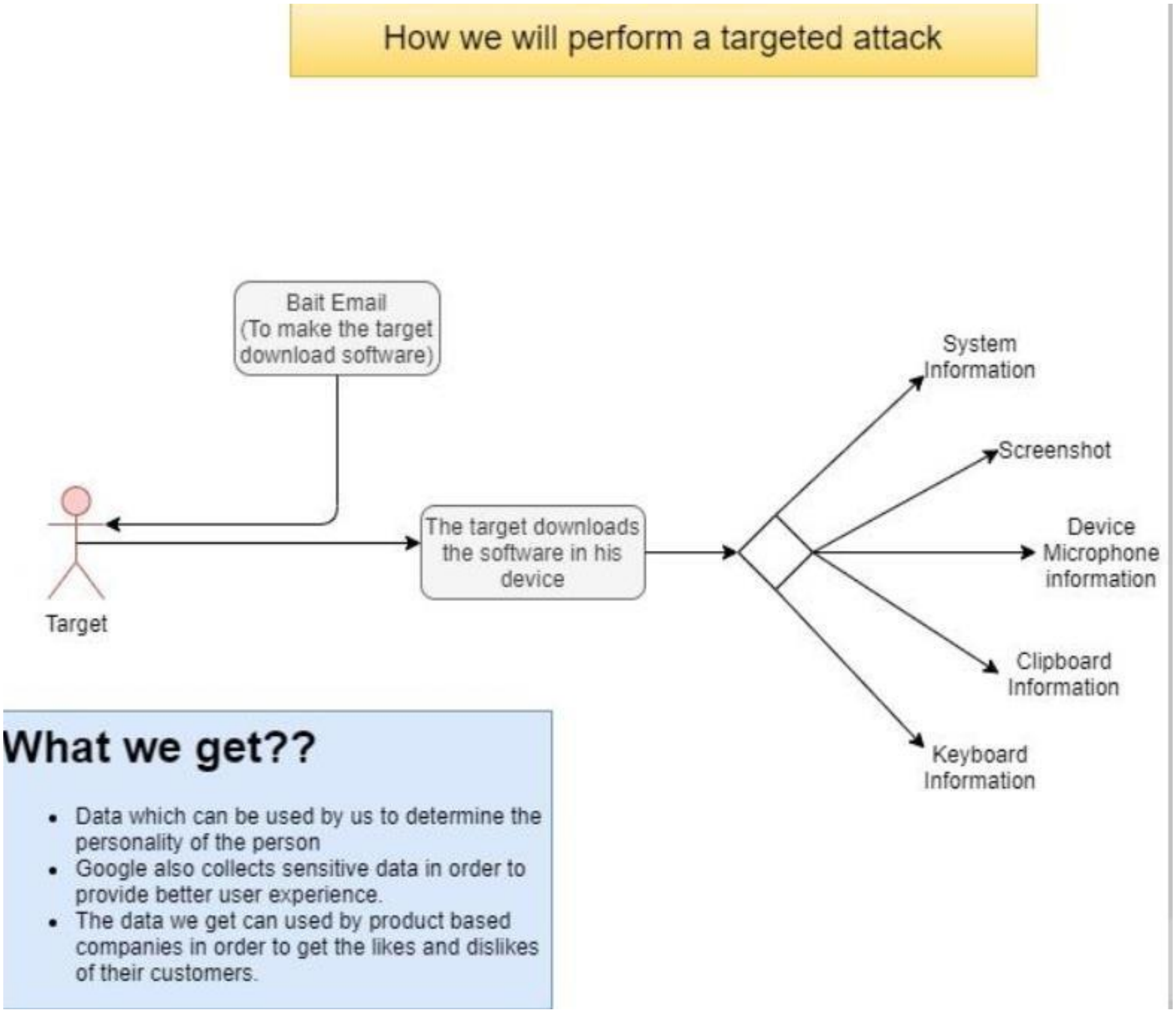


FIG 2

We have completed both the phases of the project.

3.1 Techniques/Algorithms

3.1.1 Flow Diagram


How we will perform a targeted attack
Bait Email (To make the target download software)
Target
The target downloads the software in his device
System Information
Screenshot
Device Microphone information
Clipboard Information
Keyboard Information

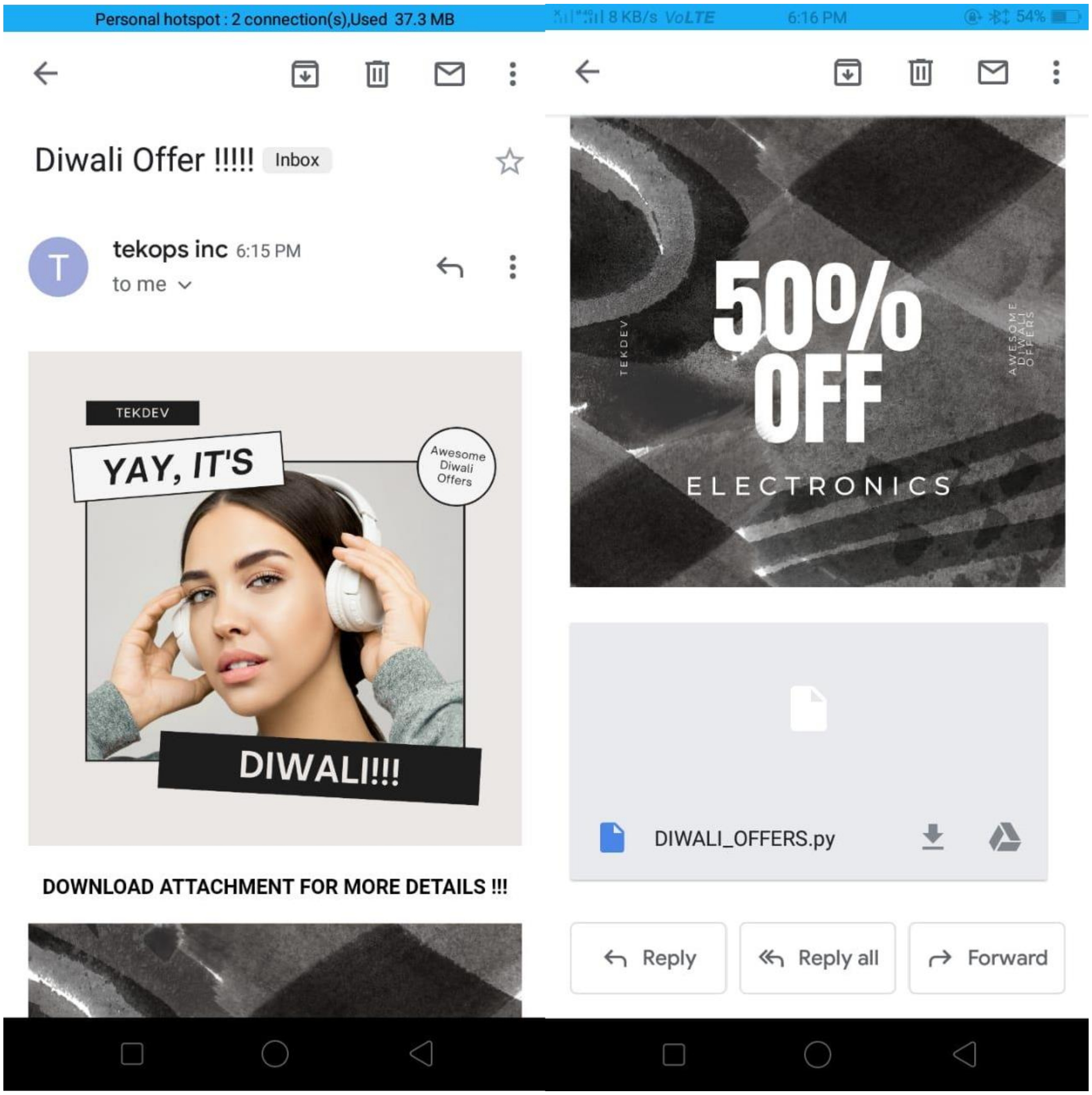
What we get??

- Data which can be used by us to determine the personality of the person
- Google also collects sensitive data in order to provide better user experience.
- The data we get can used by product based companies in order to get the likes and dislikes of their customers.

FIG 3

The bait email can be sent as any offer on some brands. Thus we can convince our target to download the key-logger software and thus we get into the targets device.

3.1.2 Bait Email



Personal hotspot : 2 connection(s),Used 37.3 MB

Diwali Offer !!!!! Inbox

tekops inc 6:15 PM
to me

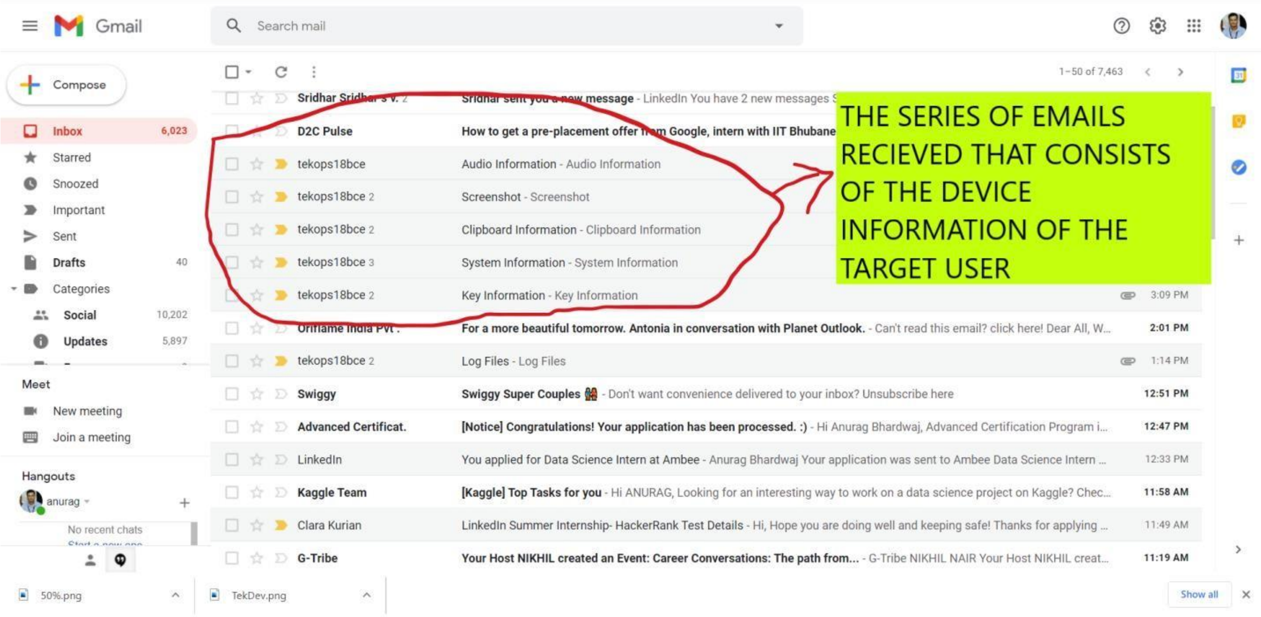
DOWNLOAD ATTACHMENT FOR MORE DETAILS !!!

DIWALI_OFFERS.py

FIG 5

4. EXPERIMENTAL RESULT AND ANALYSIS:

4.1 Email of Log Files

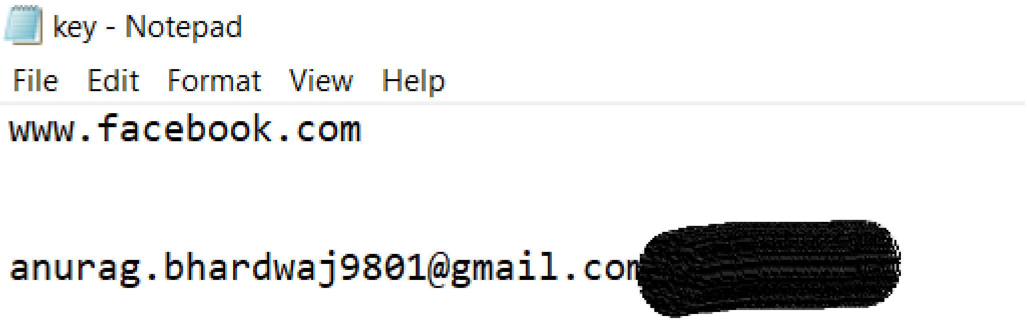


Sridhar Sridhar's V. 2	Sridhar sent you a new message - LinkedIn You have 2 new messages S	
D2C Pulse	How to get a pre-placement offer from Google, intern with IIT Bhubane	
tekops18bce	Audio Information - Audio Information	
tekops18bce 2	Screenshot - Screenshot	
tekops18bce 2	Clipboard Information - Clipboard Information	
tekops18bce 3	System Information - System Information	
tekops18bce 2	Key Information - Key Information	3:09 PM
Oriflame India Pvt .	For a more beautiful tomorrow. Antonia in conversation with Planet Outlook. - Can't read this email? click here! Dear All, W...	2:01 PM
tekops18bce 2	Log Files - Log Files	1:14 PM
Swiggy	Swiggy Super Couples 👫 - Don't want convenience delivered to your inbox? Unsubscribe here	12:51 PM
Advanced Certificat.	[Notice] Congratulations! Your application has been processed. :) - Hi Anurag Bhardwaj, Advanced Certification Program i...	12:47 PM
LinkedIn	You applied for Data Science Intern at Ambee - Anurag Bhardwaj Your application was sent to Ambee Data Science Intern ...	12:33 PM
Kaggle Team	[Kaggle] Top Tasks for you - Hi ANURAG, Looking for an interesting way to work on a data science project on Kaggle? Chec...	11:58 AM
Clara Kurian	LinkedIn Summer Internship- HackerRank Test Details - Hi, Hope you are doing well and keeping safe! Thanks for applying ...	11:49 AM
G-Tribe	Your Host NIKHIL created an Event: Career Conversations: The path from... - G-Tribe NIKHIL NAIR Your Host NIKHIL creat...	11:19 AM

THE SERIES OF EMAILS RECIEVED THAT CONSISTS OF THE DEVICE INFORMATION OF THE TARGET USER

FIG 5

4.1.1 Keyboard Information

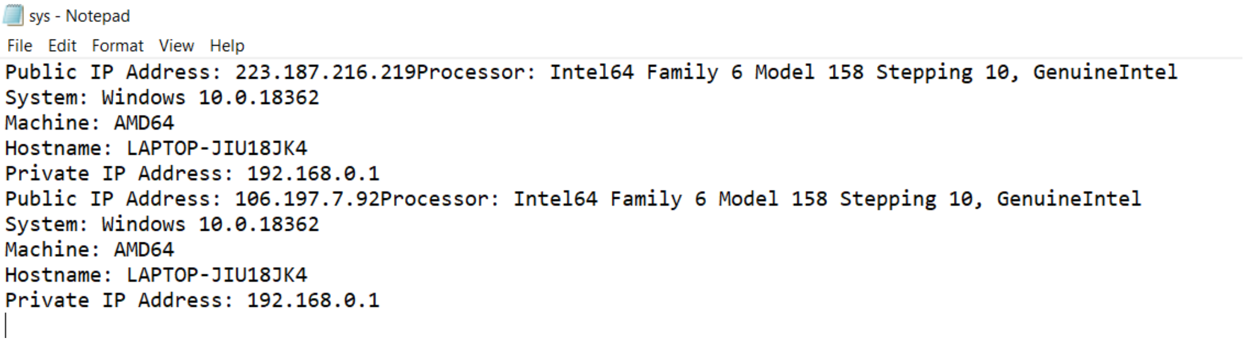


```
www.facebook.com


anurag.bhardwaj9801@gmail.co[redacted]
```

FIG 6

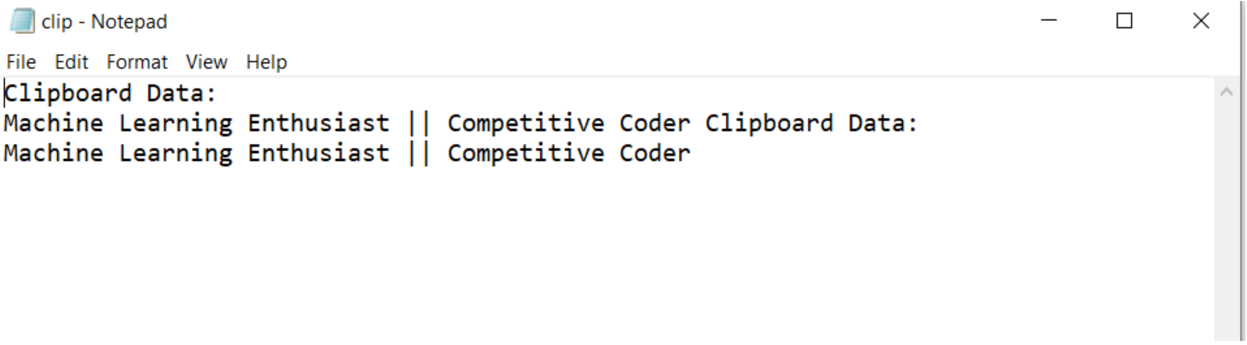
4.1.2 System Information



```
Public IP Address: 223.187.216.219Processor: Intel64 Family 6 Model 158 Stepping 10, GenuineIntel
System: Windows 10.0.18362
Machine: AMD64
Hostname: LAPTOP-JIU18JK4
Private IP Address: 192.168.0.1
Public IP Address: 106.197.7.92Processor: Intel64 Family 6 Model 158 Stepping 10, GenuineIntel
System: Windows 10.0.18362
Machine: AMD64
Hostname: LAPTOP-JIU18JK4
Private IP Address: 192.168.0.1
```

FIG 7

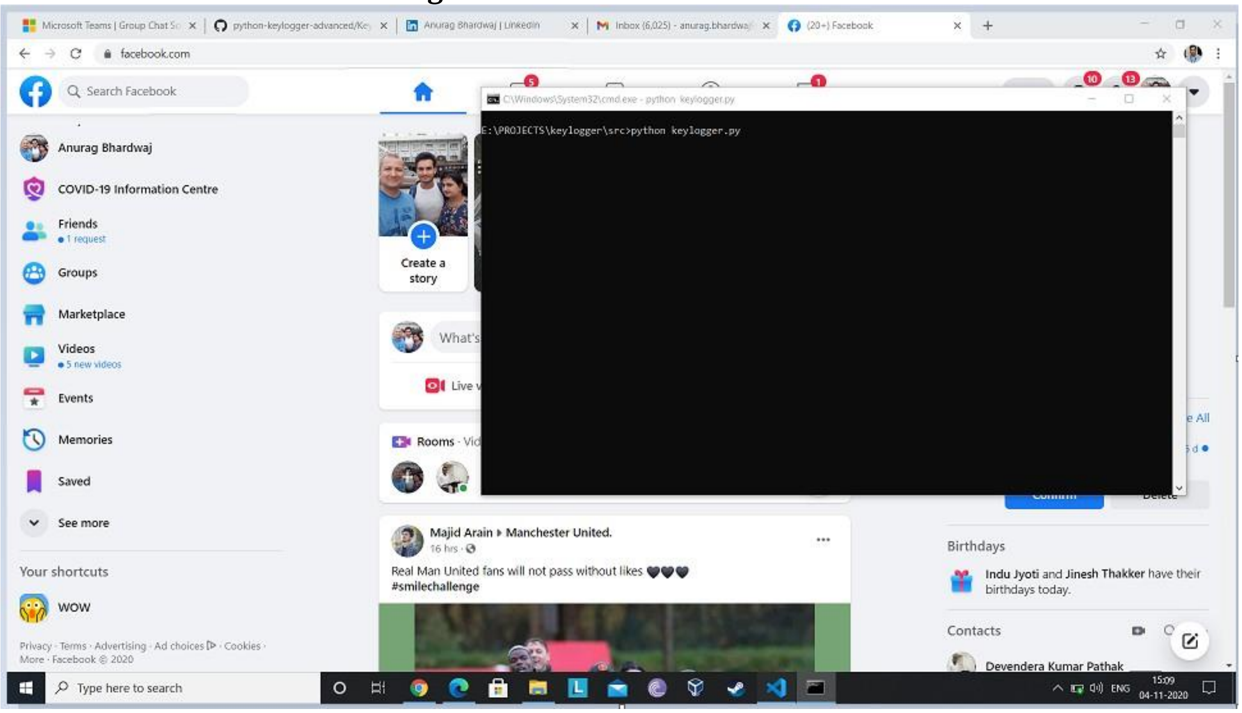
4.1.3 Clipboard Information



```
Clipboard Data:
Machine Learning Enthusiast || Competitive Coder Clipboard Data:
Machine Learning Enthusiast || Competitive Coder
```

FIG 8

4.1.4 Screenshot of Device Foreground



Microsoft Teams | Group Chat So
python-keylogger-advanced/Ke
Anurag Bhardwaj | LinkedIn
Inbox (6,025) - anurag.bhardwaj
(20+) Facebook
facebook.com
Search Facebook
C:\Windows\System32\cmd.exe - python keylogger.py
Anurag Bhardwaj
COVID-19 Information Centre
Friends
1 request
Groups
Marketplace
Videos
5 new videos
Events
Memories
Saved
See more
Your shortcuts
WOW
Privacy · Terms · Advertising · Ad choices · Cookies · More · Facebook © 2020
Create a story
What's
Live v
Rooms · Vid
Majid Arain ▸ Manchester United.
16 hrs
Real Man United fans will not pass without likes 🖤🖤🖤 #smilechallenge
Birthdays
Indu Jyoti and Jinesh Thakker have their birthdays today.
Contacts
Devendera Kumar Pathak
Type here to search
ENG
15:09
04-11-2020

```
E:\PROJECTS\keylogger\src>python keylogger.py
```

FIG 9

4.1.5 Device Audio

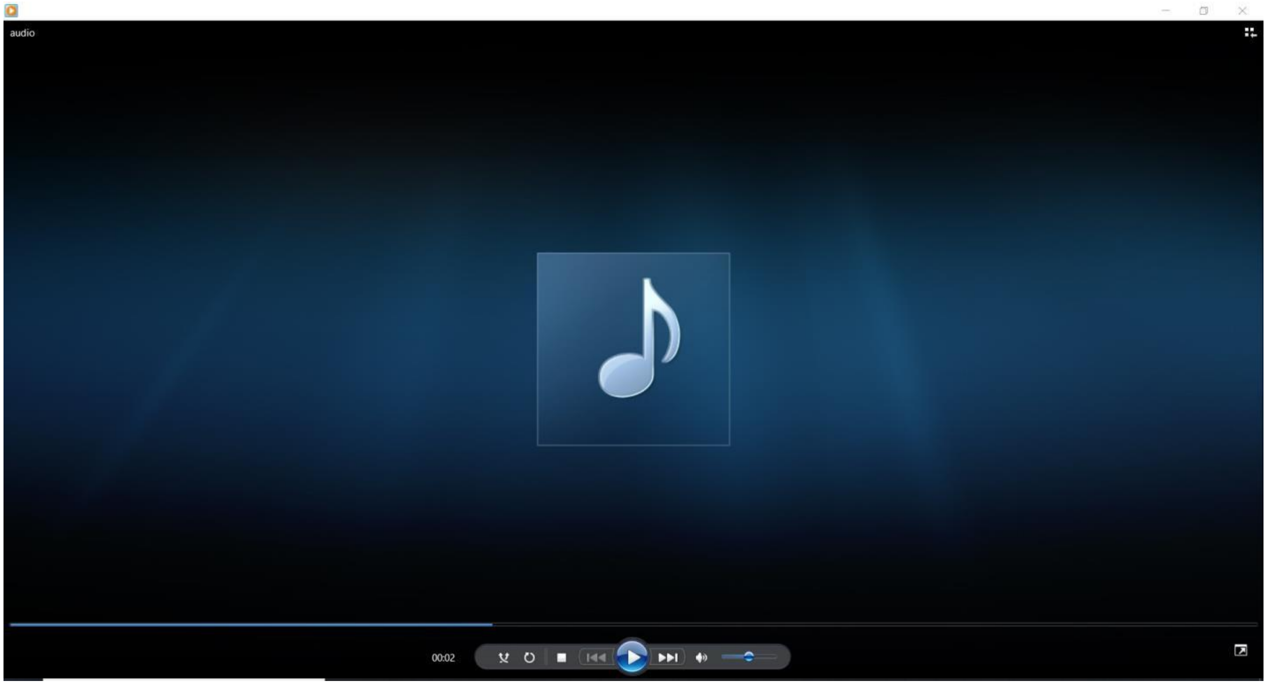


FIG-10

5. CONCLUSION:

Hence with the end of this project we hereby conclude that we have successfully implemented Key-Logger along with the implementation of the important and required features that we proposed in our project initially such as microphone and screen shot keylog. Our main of the project was to collect information and send it back to a third party. In our keylogger the Data captured by the key-loggers can be sent back to attackers via email.

Since keylogger have a bad reputation as the users confidential data such as user name,password, and pin can be recorded by the use of keylogger. But at company level, key loggers can be used to check the employees web activity and also for domestic purpose parents can keep a check on their children web activities.

6. FUTURE ENHANCEMENT:

1. In future we will make the key-logger more versatile and more invisible for the user.
2. We will try making key-logger automated so that it is not required to start manually. It will do all the work by itself
3. We will make a time schedule for the key-logger so that it can monitor the user periodically.

References

[1]A Survey on Keylogger: A malicious Attack BY Hemita Pathak, Apurva Pawar, Balaji Patil Published on April 2015

[2] Analysis and Implementation of Decipherments of KeyLogger BY Parth Mananbhai Patel and Prof. Vivek K. Shah Published on January 2015

[3]Survey of keylogger Technologies BY Yahye Abukar Ahmed1 , Mohd Aizaini Maarof2 , Fuad Mire Hassan3 and Mohamed Muse Abshir4 Published on february 2014

[4]Cyber Security – KEYLOGGERS Comparison of Detection Techniques & Its Legitimate Use By Aaradhya Gorecha published on November 2017

[5]Bait Your Hook: A Novel Detection Technique for Keyloggers Stefano Ortolani, Cristiano Giuffrida1, and Bruno Crispo published in 2010

[6] Keyloggers in Cybersecurity Education Christopher A. Wood1 and Rajendra K. Rochester Institute of Technology, Rochester, New York, USA

[7] Keystroke Logging: Integrating Natural Language Processing Technique to Analyze Log Data Disha H. Parekh, Nehal Adhvaryu, Vishal Dahiya

[8] Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm Robbi Rahim1, Heri Nurdiyanto, Ansari Saleh, Dahlan Abdullah, Dedy Hartama and Darmawan

[9]Cyber Crime Combating Using KeyLogDetector tool by Mahak arora ,kamak kumar sharma

[10] System Monitoring and Security Using Keylogger by Preeti Tuli, P. Sahu Published in 2013