Malwares:
Keylogger and File Deleter

Dhruval Gandhi(18IT034) [1] | Nehal Patel[2]
[1,2]Smt. Kundanben Dinsha Patel Department of Information Technology,
CSPIT, Charusat University, Changa-388421, Anand, Gujarat, India
18IT034@charusat.edu.in, nehalpatel.it@charusat.ac.in

***Abstract*—Malwares are biggest threat to computers. It can compromise the security in various manners. This study shows working of malwares like keylogger, CIH file deleter. It shows how these malwares affects the target system and the information of victim is compromised.**

I. INTRODUCTION

Malware is known as malicious software. It is a computer program designed to intervene and damage different types of programs without users' concern. It is commonly transmitted over a network that affects victim's device.

Different types of malwares are there such as spyware, worms, trojans, rootkits and many more. Paper is based on study and implementing keylogger and deletion of files

Keylogger is a type of spyware that detect the user's typed keystrokes on the keyboard. It's first primary target is to anonymously record confidential information of victim's input keystrokes monitoring and then relaying those valuable information to others.

File deletion is a way of removing a file from a victim's devices by targeting specified directory. It is a CIH virus.

This study helps to understand below malwares:

1) Keylogger
2) File deletion

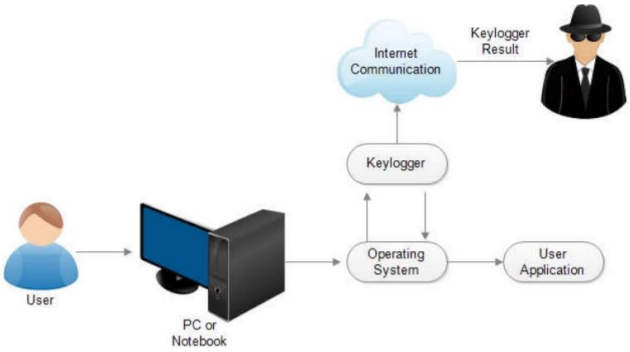
II. Work Done

1. Keylogger:

Hackers and cybercrime have discovered many methods to gain private data from your endpoint machines. Some of them are as effective as keylogging. Keylogging also known as keystroke log, is the capture of characters typed on keyboard. Data gained can have document content, user's credential, and other critical kind of information. Therefore, hacker or attacker can simply retrieve and access information.

Nowadays, Keylogging acts a critical threat to the security and solitude of our system. In this technical paper, I inspect how keylogging or keyloggers work. I studied papers, real time example of various types of keyloggers and how they differ form each other. At the end, I reached to the conclusion that how the work behind the scenes and how to implement them.

Before moving to the discovery of keyloggers, one should understand how they work, which are the types of keyloggers and how they connect with the systems.



Types of keyloggers

Keyloggers are of many types but there are two types that are majorly in use of current time.

Software keyloggers:

Keyloggers or keystroke loggers are software programs or hardware devices that track the activities of a keyboard. Keyloggers are a form of spyware where users are unknown to their actions are being recorded. Keyloggers can be used in different ways like cybercriminal may use them to maliciously gain access to your device and user's information while employers might use them to monitor employee activities. Some keyloggers can also capture your screen at random time intervals; these are known as screen recorders or screenshot taker. Keylogger software typically stores your keystrokes in a small log file, which is either accessed later or automatically emailed to the person monitoring your actions.

Hardware keyloggers:

Hardware keyloggers are being used for keystrokes logging which is a method of capturing and recording user's activity, including sensitive password. They can be implemented via a device plugged into between a computer keyboard and a computer. They log all user's activity to their internal memory.

It has benefits over software keyloggers like they can begin logging from the moment a computer is turned on and therefore the can intercept credentials for the BIOS or disk encryption software.

Implementation:

Here is how I implemented software keylogger with some additional feature. Here all the files converted to the executable file and then it will run in background on user's device

Step 1:

Software keylogger first takes place at sender side. Sender will convert it into .exe file and then sender will attach all the keylogging files and will give to the victim's side.

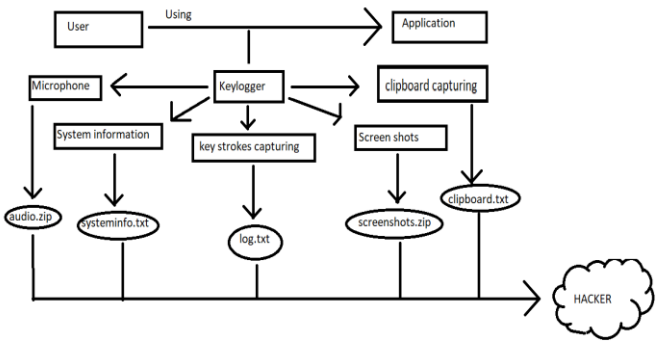
Step 2:

It is step that plays role at victim's side. Once the malware that sender has send is executed will start running at background in victim's device. It will directly go into startup folder of victim's device and start retrieving all the sensitive information of victim into the log file. It will run on victim's pc till device will shut down and will collect all their activities.

Step 3:

After collecting all functionalities when victim device will restart then all the recorded information will send to the attacker's(sender) through the mail and all recorded information will be deleted and it will start a new session.

Flowchart:



There are two files:

1) Keylogger.py

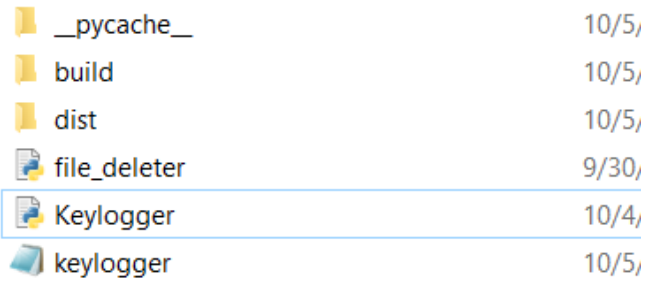
Contains all the functions of keylogger

Record keystrokes and will save into log files

2)Send_mail.py

It will send back all the recorded data to attacker via mail

It will then erase all data that has recorded into log files



Functionalities:

1) Keystrokes:

Anything that will press on the keyboard automatically save in key_log.txt file.

2) Clipboard logging:

Anything that can be copied to the clipboard will directly save in clipboardinfo.txt file.

3) Microphone recording:

It will automatically turn on mic on victim's device for specific time interval and record all voices around for limited time and will save the .wav file to specified folder.

Example: If user start their device then it will record it for 20 seconds of audio.

When send_mail will execute It will convert the folder into zip and then send it.

4) Screenshot capturing when google chrome is open:

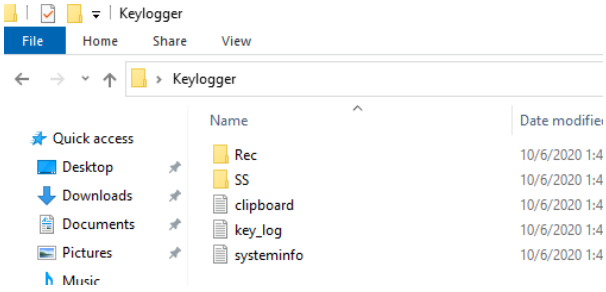
It is a feature that will take screenshot of victim's google chrome browser activity on specific time interval. Example: if browser is open then method will call and take screenshot of device screen after every 5 seconds.

After that when all these screenshots will gathered and send_mail will execute than it will convert into zip and then it will send it.

5) System information of victim's device:

System information of victim's device will save to the systeminfo.txt file.

Example: Username, Public ip, model information and all other information about device.



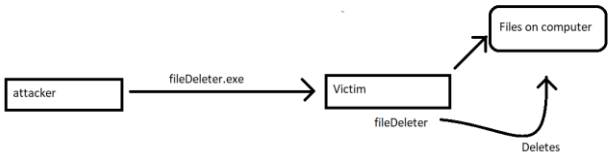
All of this functionality is implemented with the use of multithreading so that all these functionality work simultaneously and record all information.

Deletion of files:

Virus that automatically delete files on victim's device. It is one type of CIH virus. The CIH virus also known as Chernobyl virus, threatened to delete files automatically and erase the core system code or important files, folders that are kept in flash memory on the motherboard of different types of devices.

Attacker sends this malware to the victim's computer. When this malware is executed it deletes all the files on victim's computer. All the paths are predefined by the attacker. The path is set in such a way that it is present on any computer. Hence, on execution of this malware, all the important data of the victim will be lost.

Flow Chart:



III. Conclusion

Malwares like Keyloggers designed by implementing different functionality can collect all of the user's activities in order to the keystrokes, microphone, screenshot, system informationand provide attackers with useful account, identity and sensitive information. The results are storedautomatically in a dedicated path which attacker has created. On the other hand, they are tools which are useful in investigation.

File Deleter is one virus that is implemented so that it can change user's root directory by deleting files, convert your files into shortcuts, and even destroy your system and can remove all the intellectual property information files from victim's device.

IV. References

[1] https://en.wikipedia.org/wiki/Keystroke_logging
[2] https://geekflare.com/python-delete-files/
[3] https://stackoverflow.com/
[4] https://www.geeksforgeeks.org/

[5] Yahye Abukar Ahmed, Mohd Aizaini Maarof, Faud Mire Hassan and Mohamed Muse Abshir "Survey of keylogger Technologies" Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia.

[6] Tom Olzak, MBA, CISSP, MCSE "Keystrokes Logging (Keylogging)" April,2008.

[7] Nirav Bhojani "Malware Analysis", Department of Computer Science and Engineering institute of Technology, Nirma University, Ahmedabad, India.

[8] S.S.A.G CANBEK. (2009) Keylogger Increasing Threats to Computer Security and Privacy. IEEE TECHNOLOGY AND SOCIETY MAGAZINE.

[9] M. Aslam, R. N. Idrees, M. M. Baig, and M. A. Arshad, "Antihook shield against the software key loggers," in Proceedings of the National Conference of Emerging Technologies, 2004.

[10] A Survey on Automated Dynamic Malware Analysis Techniques and Tools,
http://www.seclab.tuwien.ac.at/papers/malware_survey.pdf

Malwares: Keylogger and File Deleter

ORIGINALITY REPORT

19%	18%	1%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.veracode.com Internet Source	8%
2	en.wikipedia.org Internet Source	5%
3	www.ijcst.org Internet Source	3%
4	www.softwaredelta.com Internet Source	2%
5	Submitted to Charotar University of Science And Technology Student Paper	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		