Advanced Keylogger- A Stealthy Malware for Computer Monitoring

Aarushi Dwivedi
Information Technology Maharaja Agrasen Institute of Technology
Delhi, India
aarushidwivedi07@gmail.com

Krishna Chandra Tripathi
Information Technology
Maharaja Agrasen Institute of Technology
Delhi, India
kctripathi@mait.ac.in

M.L. Sharma
Information Technology
Maharaja Agrasen Institute of Technology
Delhi, India
mlsharma@mait.ac.in

***Abstract*— Modern society is far more dependent on electronic devices than the previous generations. This dependency has both pros and cons. Although the list of pros is endless, they can easily be outweighed by one con which is being vulnerable to malicious programs. Keylogger is one such malware. Earlier, the prime focus was just limited to recording keystrokes made by a user but now are known for incorporating a multitude of features. Keyloggers are used to steal confidential information covertly and their detection is not quite simple since they execute completely in stealth mode. In this exposition, an advanced software keylogger is proposed which is compared with the existing keyloggers based on two criteria, first being the number of features incorporated and second, the CPU usage while the keylogger is being executed. The evaluation posits that the proposed keylogger contains more features with keeping the CPU usage to a minimum hence making it difficult to be detected by the user.**

Keywords*— Malware, Keyloggers, Hacking, Security, Computer monitoring

I. INTRODUCTION

In 2019, Arpanet, the precursor of the internet, celebrated its 50th anniversary. Since 1969 more than 4 billion people have access to the internet and the number of devices connected to IP addresses is more than twice as much the global residents. While the usage of the internet grows significantly, security threats also continue to rise. Downloading malicious software from the internet continues to be a major contributing factor in breach of security [1][2].

A program that aims to perform unsolicited and disorderly tasks in an operating system without the user's authorization is known as malware or malicious software. List of malware includes, but are not limited to Virus, Worm, Trojan horse, keylogger, and Spyware. All these malwares have been and continue to be a severe threat all over the world. In this exposition, the key focus is on keyloggers. They are embedded on a machine with the sole purpose of monitoring the user. Traditionally, they were used only to log keystrokes and send them to the attacker but with time, the keyloggers are becoming advanced and are incorporating a myriad of additional features such as enabling the microphone, the webcam, capturing screenshots, etc.

Keyloggers serve both legitimate and illegitimate purposes [3]. They are used by attackers to invade the privacy of users to steal confidential data however, they can also be used in daily life for sincere purposes such as child monitoring, forensic investigation, and ethical hacking, as mentioned in Table 1.

TABLE I.

Applications of keyloggers	
Legitimate	**Illegitimate**
1. Research instrument in writing activities	1. Information Gathering
2. Monitoring children	2. Illegal screen recording
3. Forensic investigation	3. Identity theft
4. Ethical hacking	4. Invasion of privacy
5. Improving employee productivity	5. Data breach
6. Backup and data recovery	

Keyloggers are on the rise due to their covert nature [4]. They execute in stealth mode and not easily detectable by antiviruses. However, there are preventive measures that can be taken to thwart keyloggers. Firewalls, anti-malware, and other such preventive applications must be downloaded. Ensuring that security patches are always updated. Applications must be downloaded from trusted sources and licensed software should be used. Another easy way to detect unwanted software is through regularly checking the CPU and memory usage of the computer.

The proposed algorithm of the keylogger in written in python. It incorporates the following features: Gathering computer information, clipboard contents, enabling the microphone, gathering Chrome data and screen capture functionality. The gathered information is sent to the attacker via email and leaves no trace.

In this paper, the implementation of a new proposed keylogger is present, along with its purpose and comparison with other existing keyloggers in terms of the incorporated features. The remainder of the exposition is as follows: Section 2 contains the related work and section 3 comprises the proposed methodology. In section 4, the result and analysis of the keylogger are discussed. Section 5 concludes the paper with future scope. References are mentioned in section 6.

II. RELATED WORK

Keyloggers have been around since the mid-1970s, created by the Soviet Union for targeting typewriters termed as "Selectric bug". Since then, keyloggers have evolved tremendously. Both in efficiency and usability, a rise has been observed in the last 10 years. Keyloggers, as the name suggests could only produce results if the keys are logged. A serious challenge was introduced when Microsoft Windows 8 was released in 2012 with a touchscreen personal keyboard

[1]. S. Moses in "Touch Interface and Keylogging Malware" investigates the abilities of keyloggers to capture keystrokes from a virtual keyboard. Further how other keyloggers respond to it are also demonstrated. In [3], A. Bhardwaj proposes that the keyloggers must be defined on two criteria: the location of execution and functionalities offered. Further, the keylogger can be either hardware-based or software-based. With new keyloggers being introduced, the detection of keylogger is also a domain that is progressing. In 2013, E. Ladakis [5] presented a stealthy keylogger with a novel approach by exploring the domain of graphics card as a substitute for hosting an environment for the keylogger to operate. Since mobile devices have now become an integral part of our lives banking services are also being provided on mobile applications. People are progressively becoming comfortable with using the application because it makes the financial process laidback. In [6], A. Kuncoro brings attention to security threats possessed by these mobile applications using keyloggers. In [7], security software is analyzed. In [8], Y. Albatain also brings attention to detection of keyloggers using Graphics Processing Units. Keyloggers are being tested against the most popular and effective software to see if keyloggers can be detected or not. In [9], Danial Javaheri proposes a new method to detect and eliminate spyware including keylogger with 93% accuracy. Various surveys are conducted every year to get a better understanding of how our data is being monitored. All major companies systematically document data of their clients and employees, the extent of which remains ambiguous. In System Monitoring and Security Using Keylogger [10], the extent, the key concepts involved, and the forces driving the adoption of keyloggers are discussed. Recently in 2019, IBM reported HawkEye[11] v9 Keylogger increasing usage. Above mentioned work clearly illustrates the keyloggers continue to an intriguing field of research [12]. An algorithm for a new advanced version of keylogger in Python is presented in this paper.

III. PROPOSED METHODOLOGY

In this paper, the proposed algorithm is written in Python programming language. The software is only for a particular victim and not for masses. The software can be sent to a victim through email or by using additional hardware such as pendrive or hard disk. The features incorporated are as follows:

- Every keystroke including special characters will be saved.
- Access to the victims' clipboard.
- Screenshots of victims' screen.
- Access to microphone.
- Computer information: RAM, OS.
- Network information: IP address, MAC address.
- Gathering chrome history information

The gathered information is sent through email and the documents are automatically deleted from the user's computer.

A. Backdoor Algorithm:

Adv_Klogger-

Step 1: A basic keylogger using Python was written in Pycharm IDE.

Step 2: A class keylogger is created. Step 3: Functions are defined.

1) All the details collected from the target machine are sent to the attacker via email.

```
Def send_email(email_id, password, attachment): server = smtplib.SMTP ("smtp.gmail.com",

587)

server.starttls() server.login(email, password)

server.sendmail(email, email, message)
```

2) This function is defined to take the screenshot of the target machine.

```
Def screenshot():

im = ImageGrab.grab() im.save(file_path + extend +

screenshot_info)
```

3) Data is recorded from the targets machine using microphone function.

```
Def microphone():

myrecording = sd.rec(int(seconds* fs), samplerate= fs, channels= 2)

sd.wait()

write(file_path + extend + audio_information, fs, myrecording)
```

4) Contents stored in the clipboard are recorded using this function.

```
Def copy_clipboard():

with open(file_path + extend + clipboard_information, "a") as f:

win32clipboard.OpenClipboard()
```

5) The keys are logged using Process_key_info() function.

```
Def Process_key_info():

try:

current_key = str(key.char)

except AttributeError:
```

6) Chrome history information is retrieved using this function.

```
Def chrome_info(): history=sqlite3.connect(os.getenv("APPDATA")+pat

h)

out = history.cursor()
```

Step 4: Convert the file into an executable.

Step 5: The file is sent to the user via email or USB device.

Step 6: Gathered information of the target machine is received via email.

B. The keyloggers used:

- Spyrix Free Keylogger: The free version of this keylogger is 50 Mb, available for Windows XP and above. The download instructions are very simple and a person who is not tech savvy can also use this. Sprix Agent is downloaded and installed on target computer. Options to choose the method of logging are provided. The free version incorporates several features such as screenshot capture, remote installation, alert keywords, etc. The term of data storage is 2 days.
- KidInspector: It is a 100 Mb leading parental control software that allows parents to monitor activities of their children. It is available for both windows and MAC. It is a paid software but available for free trial for 3 days. The trial consists of various features like capturing screenshot, monitoring of clipboard, visited websites, social networking website chats, etc. The term of data storage is 3 days.
- Free Keylogger: It is also a paid software but comes with a 7-day free trial that incorporates all the features. It is

1.6 Mb software that is available for Windows XP and above. The features include capturing chats, capturing screenshots, remote monitoring, microphone functionality and visual surveillance.

C. Simulation parameters

TABLE II.

Parameter	Value
Processor	Ryzen 5
RAM	8 gb
Operating system	Windows
Simulation Language	Python
Python version	3.8.6

D. Guidelines for testing

- Anti-virus software was turned off before downloading the keyloggers.
- Keyloggers were downloaded.
- Basic testing with keys was performed.
- User interface was judged.
- Screenshots were taken.
- CPU and memory usage were noted while the keylogger was being executed.
- Same steps were repeated for all the keyloggers.

IV. RESULT AND ANALYSIS

Software keyloggers continue to dominate hardware keyloggers.[4] In this exposition top 4 Windows based software keyloggers (2020) are compared with Adv_Klogger, which is presented in the research paper. The three keyloggers are: Spyrix free Keylogger, KidInspector Keylogger and Free Keylogger [13][14]. The basis of comparison is the features that are incorporated in the keyloggers and the CPU usage. All the keyloggers had three features in common which are logging keys, screenshot functionality and remote monitoring. Table 3. Contains detailed analysis of all five keyloggers and what all features they entail.

Fig 1. provides a visual representation of how keyloggers differ based on number of features they contain. The keyloggers are widely used and differ because of functionalities they contain. The more functions a keylogger has the more useful it is to a user or a company. As illustrated, Adv_Klogger incorporates more features than the other keyloggers.

The second parameter which is used here to compare the keyloggers is the CPU usage. One of the easiest ways to detect a malicious activity is through the CPU and memory usage. Fig 2. contains a graphical representation of keyloggers differ by their CPU usage. The data in the graph is noted by monitoring keylogger execution for a period and calculating the average of how high the usage becomes while the program is being executed. As it is clearly demonstrated that the Adv_Klogger does not show much spike in the usage and cannot be easily noticed.

TABLE III.

	Name of the keylogger	**Features**						
		Logs keys	Microphone	Screenshot	Computer information	Clipboard contents	Remote monitoring	Browser (Chrome) information
1.	Adv_Klogger	✖	✖	✖	✖	✖	✖	✖
2.	Spyrix free	✖		✖		✖	✖	
3.	KidInspector	✖	✖	✖			✖	
4.	FreeKeylogger	✖	✖	✖			✖	

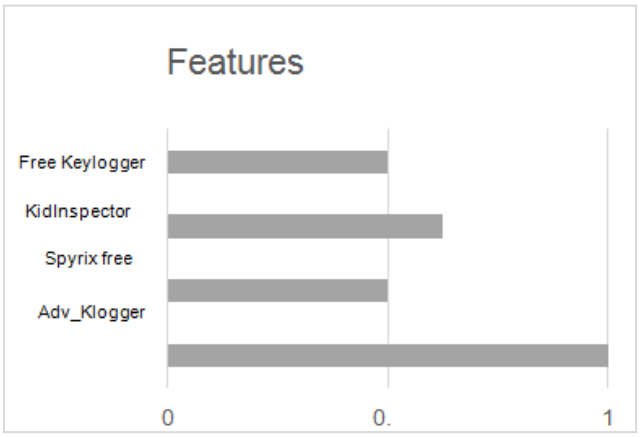

Fig. 1. Comparison based on feature

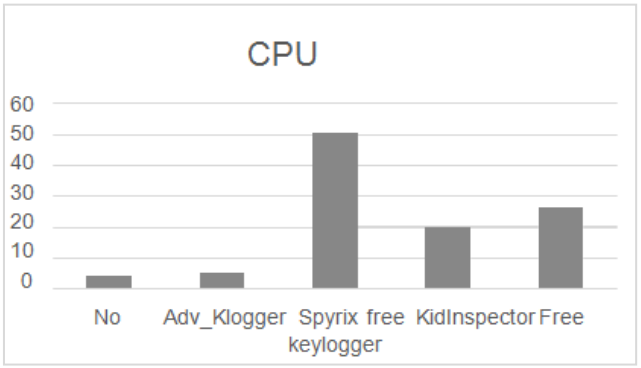

Fig. 2. Comparison based on CPU usage

REFERENCES

[1] S. Moses, J. Mercado, A. Larson and D. Rowe, "Touch interface and keylogging malware," 2015 11th International Conference on Innovations in Information Technology (IIT), Dubai, 2015, pp. 86-91.doi: 10.1109/INNOVATIONS.2015.7381520

[2] P. Tuli, P. Sahu, "System Monitoring and Security Using Keylogger", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue. 3, March 2013, pg.106 – 111.

[3] Murugan, S; Kuppusamy, K. 'System and methodology for unknown malware attack'. Second IEEE International Conference on Sustainable Energy and Intelligent System (SEISCON 2011)

[4] A. Solairaj, S. C. Prabanand, J. Mathalairaj, C. Prathap and L. S. Vignesh, "Keyloggers software detection techniques," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016, pp. 1-6, doi: 10.1109/ISCO.2016.7726880

[5] Ladakis, L. Koromilas, G. Vasiliadis, et. al.," You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger", EuroSec'13 April 14 2013, Prague, Czech Republic.

[6] A. Kuncoro, B. Kusuma, "Keylogger Is A Hacking Technique That Allows Threatening Information On Mobile Banking User", 2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia.

[7] M. Dadkhah, A. Ciobotaru, et. al, "An Introduction to Undetectable Keyloggers with Experimental Testing", International Journal of Computer Networks and Communications Security - September 2014

[8] Albabtain, Y; Yang, B. 'The process of reverse engineering GPU malware and provide protection to GPUs'. 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications, and 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, US, 2018. DOI: 10.1109/TrustCom/BigDataSE.2018.00248.

[9] Arghire, I. 'Business users targeted by HawkEye keylogger malware'. Security Week, 28 May 2019. Accessed Jan 2020.

[10] Figure 8: Comparing the proposed virtual keyboard with QWERTY and ABC keyboards. February 2020 Network Security 19 FEATURE Volume 6, 2018. DOI: 10.1109/ ACCESS.2018.2884964.

[11] A. Bhardwaj, S. Goundar, "Keyloggers: silent cyber security weapons", 2020 Network Security Volume 2020, Issue 2, February 2020, Pages 14- 19.

[12] S. Shetty. Introduction to spyware keyloggers. www.securityfocus.com/infocus/1829, 2005.

[13] "Top 10 Free keyloggers for windows"- J. Paterson

[14] Javaheri, D; Hosseinzadeh, M; Rahmani, M. 'Detection and elimination of spyware and ransomware by intercepting kernellevel system routines.' IEEE Access, Figure 7: Algorithm for the proposed virtual keyboard.

[15] Sagiroglu, Seref & Canbek, Gürol. (2009). Keyloggers Increasing Threats to Computer Security and Privacy. Technology and Society Magazine, IEEE. 28. 10 - 17. 10.1109/MTS.2009.934159..