2021 5th International Conference on Information Systems and Computer Networks (ISCON)
GLA University, Mathura, India. Oct 22-23, 2021

Analysis and Implementation of Novel Keylogger Technique

Mayank Srivastava
Department of CEA,
GLA University
Mathura (UP), India
mayank.srivastava@gla.ac.in

Anjali Kumari
Department of CEA,
GLA University
Mathura (UP), India
anjali.kumari_csf18@gla.ac.in

Krishan Kant Dwivedi
Department of CEA,
GLA University
Mathura (UP), India
krishan.dwivedi_csf18@gla.ac.in

Sakshit Jain
Department of CEA,
GLA University
Mathura (UP), India
sakshit.jain_csf18@gla.ac.in

Vrishti Saxena
Department of CEA,
GLA University
Mathura (UP), India
vrishti.saxena_csf18@gla.ac.in

2021 5th International Conference on Information Systems and Computer Networks (ISCON) | 978-1-6654-0341-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISCON52037.2021.9702433

***Abstract*—Keystroke logging, also known as keystroke or keyboard scanning, is a way to record the keys that are being typed on the keyboard, by the user's computer or keyboard, so that the keyboard user does not know that their details are being tracked. Data can be gained by someone using the login system. Some programs themselves are legal, and are created to track the use of employer's computer. Key logging is also used to learn keystroke power or human-computer interconnection. Many methods for key chain are available, which are software or hardware based methods or acoustic crypt-analysis. In this paper, we have proposed a key logger that captures the keystrokes of the victim as well as the running applications on which the victim might be working, and stores it in an encrypted form in a file, which is further uploaded on the server after every hour. It also records extra information of the victim like it's IP address, MAC Address, and Username. The software runs on a stealth mode, that is it uses very low RAM. It re-launches itself as soon as the system starts. The keystrokes are stored in an encrypted form in the file and then uploaded on server, which is later downloaded and decrypted by the attacker.**

Keywords - Server , Key Stroke Capturing , Encryption , Security

I. INTRODUCTION

Keylogger or keystroke recorder is a program that is designed to detect and record every key pressed by the victim [1]. It is one of the oldest and basic type of malware. It detects and document all the data that the victim upload on an internet site or application and deliver it to the attacker. Cyber Attackers use keystroke recorder to take private or business details for example bank details, which can be sold and used for gaining benefits. On the other hand, it also has authentic application among enterprises to resolve different problems, enhance client experience and proctor employees' activity. Law-enforcement authorities and secret services also practice the key logging for surveillance purposes [2].

Key loggers obtain data and send it to the third person - either in the criminal, judicial or Information Technology department. Key logger is a program that use algorithmic rules that record keystrokes for pattern matching and other mechanisms [3]. The volume of information gathered via key logger program may differ. The most basic key logger can only pick-up keystrokes on a single internet site or app. Advanced key logger are the one that can document every key the victim has pressed in any application or website, in addition to the data that victim has copied and pasted. [3]

Other versions of key logger - particularly those that indicate mobile phones - in order to document information like call logs and call recordings, personal and business messages (like SMS), GPS location, screenshots and microphone recordings and camera pictures as well. Key loggers can be categorized as hardware-based and software-based key logging [3]. Hardware-based key logger can be constructed between the keyboard connector and the system's port. Software-based applications could be either complete programs, tools, or malicious software corrupting the system or computer unknowingly.

Information captured by key loggers can be transferred to the attackers through electronic mail or by uploading the documented data to pre-determined internet sites, or private FTP servers. Sometimes a key logger comes tied up with a bigger cyber-attack which helps the attacker to log all the keystrokes pressed by the victim. The world's first key logger was used by the Soviet Union, to record IBM's typewriters that was being used by ambassadors in Moscow, in 1970s. Nowadays, key logger used as a eavesdropper is a popular tool for illegal purpose to record business details for example bank details, account details, credit or debit card details and private details like personal or business mails, userID and password, personal address, or delicate business data procedures or industrial estate. The attacker can then trade that stolen data or utilize it in the framework of a major cyber-attack subject to the data that the attacker has gathered and its criticality in the market [3].

Let's take a scenario that a key logger is capable of recording the click of a main server database keys of a huge enterprise. The attacker is now capable of obtaining the control of laptops and mainframe servers which ultimately produce enormous volumes of information that the attacker is able to now fabricate. Keyloggers don't harm the system itself like other malware or software [4]. But they are very dangerous for victim's as they can be used to retrieve credentials and information like passwords and user id's that are inputted by the keyboard. Because of keylogger the

attacker can gain information of victim's like email address, PIN codes, account numbers user names, online play accounts, email passwords etc. [5].

Once the attacker has victim's credentials, he/she can easily do malicious activities like accessing the play account of the victim or transferring money from the user's account. Unfortunately gaining access to victim's credentials can be very serious unlike losing a few dollars. Keyloggers can be used as a spy tool in industrial and political fields, access to potentially sensitive trade data and seperate government resources that could jeopardize security of the government organizations [5].

Keyloggers, social Engineering are the most widely used methods of cyber-attacks. People that know about security and its importance can easily defend themselves from these things by ignoring spam mails and by keeping their personal information away from suspicious websites. However, it is very difficult for victims to fight keyloggers, as it is often not possible for the user to have a keylogger installed on his machine. The keyloggers are progressing- they keep a track of visited websites of the victim and are only accessible by clicking buttons on websites that have a particular interest in cyber attacking [6].

Recently there is a dramatic increase in different types of malicious programs with keylogging performance [6]. No internet accessing user is safe for cyber criminals, irrespective of your place anywhere in world or any organization where we work [7].

II. RELATED WORK

In this section, we will elaborate the various categories of keyloggers currently available in the world.

Software-based keylogger: As the name suggest these keyloggers mainly target the software running on a system / computer and capture keystrokes from them Keyloggers can be for Monitoring and Spying. Often Corporates use Keyloggers to monitor the working of their employs and also to see what resources they are using. In places like cyber cafes the owner an install keylogger software to spy on their costumers and steal Credentials and Confidential information. [1]

Hypervisor-based: A keylogger can stay logical on a malware hypervisor that works under the OS, which is untouched. This is the trick by which it seems like a visible machine.The example based on this concept is Blue Pill.[2]

Kernel-based: This type of software based keylogger obtains ROOT Access in this way they remain hidden in the OS. Kernel based keylogger holds the keystrokes to pass through the OS's Kernel. This method becomes hard for both reading and writing [5]. They are used as "rootkits" which alter the OS kernel by which they gain unauthorized access of the hardware. Kernel keylogger may act as a "Keyboard Driver" and get keystrokes as they are typed and ready to go to the OS [2].

Memory Injection based: Memory Injection Keyloggers perform keylogging by substituting the memory tables linked with application functions. The do this by Placing memory tables or by pushing it directly in the memory. Trojans like Zeus and SpyEye use these kinds of methods to achieve their goal [8].

Hardware-based keylogger: Hardware Keyloggers work on a Hardware level(layer) to catch the keystrokes. They are software independent [8]. The implementation of hardware based keyloggers can be done through BIOS firmware or simply by a plugging a device between a Computer and Keyboard device. They have an internal memory to save the keystroke log [1]. Advantage of hardware keylogger over software one is that they capture the keystrokes the instant a computer turns on. Means they record every keystrokes from the beginning. In this way they can also capture BIOS Password [1].

Acoustic keylogger: Acoustic keyloggers analysis the sound of clicking buttons one by one. Special equipment is required to listen to user audio to type. The same microphone is used for long term recording distance, so this microphone is used to take the keyboard noise from a hundred feet or a workplace

Wireless keylogger: The wireless keylogger uses Bluetooth transmission methods data included in the log file up to 100M. The main purpose of this wireless keylogger is to capture packet transferred from a wireless keyboard that uses 27 MHz RF encrypted RF connection sent touch keys character. However, the bad news is this wireless keylogger requires a closed receiver / antenna compared to the target location function

USB based keylogger: In USB Keylogging method we use a USB Device to capture the keylogs in between the keyboard and the System. The Keystrokes are saved inside the internal memory of the drive. To do this we only have to plug the USB device in between USB port and USB Keyboard [9].

III. PROPOSED METHODLOGY

In this section we will describe the various features of our keylogger and technology used in making it. We have explained how those features are important, what role they play and how they helped in the development of our keylogger.

Stealth Feature/Trojan Horse: A trojan Horse is a malware that appears to be useful to the victim at first sight. But when the target download and install that malicious program on his/her computer then the program works fine but in background does all the malicious stuff like Key logging, spying, cookie stealing, file deletion, change of environment variables etc. [10]. Trojan Horse works in stealth mode takes less memory and computer processing in order to manipulate the user. It remains silent but does all the malicious work in the background. The Key Logger program is in form of an executable(.exe) format, it acts like a Trojan horse. Initially the software may look like it has been used for utility purposes, but originally it’s a Key Logger. The executable takes very less disk Space(22kb) and consumes less Processing power and memory [10].

Running Application Logs: The key logger also gathers the information about what the user is doing by storing the Names Running Applications in a file. The Traditional key loggers used store only the keystrokes which is a raw our keylogger also captures the running application on the target system to make our data more meaningful.

Encryption and Decryption: The content inside Keylog Files and Process Log Files are encrypted. It’s important because if the user access these files then he/she may not be

able to understand that what the file is all about. The Key Log and Running app log files names are also random, without any extension. We use different algorithm for encrypting content of Keylogs file and Process Log File. For Key Log We use our self-made encryption algorithm called **"White Space"** encryption algorithm. In which we replace the ASCII codes with the "White Space Characters". It's a substitution algorithm.

Uploading Files On Server: The Key Log Files and The Process Log Files Get Uploaded On Attacker's FTP Server. The Files get uploaded every hour. If, by any chance, the internet connection gets lost then whenever the connection gets restored the files will be uploaded to the server.

Auto Start: Our Application will automatically start if the system reboots, because it registers itself at the start up app list. So our app will never stop or crash unless until the user does something.

A. Encryption Algorithm Working

Encryption is a method by which information or some data is hidden by converting it in some secret code by which the true meaning of the information remains hidden.

In our keylogger we use 'The White Space Encryption Algorithm' for encryption , which is substitution cipher method.

Substitution cipher method is the method in which the characters of the normal or plain text are substituted by some other character via means of a key. For example with a shift of 5, A would be replaced by F, B would become G, and so on.

- MATHEMATICAL REPRESENTATION

The method can be represented with the help of modular arithmetic by transforming the letters into numbers. For Example A = 0, B = 1,…, Z = 25.

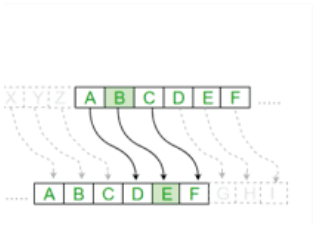
Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x+n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x-n) mod\ 26$$

(Decryption Phase with shift n)



For substitution of characters of the plaintext our keylogger uses "White Space Characters".

These characters are exceptional as they are not visible, which means if we encrypt a paragraph with "White Space Characters" and paste it in any Text Editor then they will not be visible i.e. a plain or blank space will be showed. For example, the character " " called Space is not visible but exists in a paragraph, similarly we use the 'White space' characters to substitute our plain or normal text.

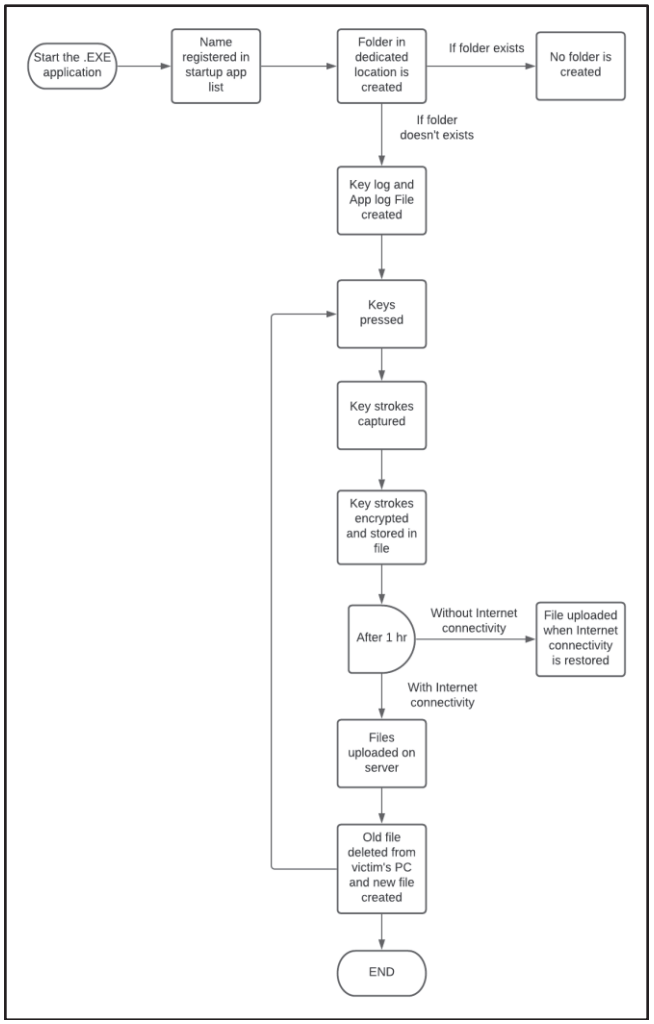


Fig. 1. Key Logger Flowchart

This way the encrypted text will be shown as a blank document to the user, in case they get suspicious of our keylogger activities. We can also use this algorithm to encrypt data inside the network packets. The person monitoring the network will find nothing inside the packets as the data encrypted by our algorithm appears as blocks of empty spaces.

Key Feature: Most of the substitution algorithm available can only substitute alphabets and not integers or special characters. But, our algorithm can encrypt all types of characters i.e. alphabets, integers and special characters.

In our algorithm we have mapped "White Space Characters" only for numbers as the algorithm encrypts the characters with their ASCII code (which are integers) of the key pressed by the user. For Example: ASCII CODE of character "e" is 69, so we substitute the integers "6" and "9" with the "White space Character". "6" is substituted with Unicode "8202"and "9" is substituted with Unicode "8192".

6 ⟶ 8202 and 9 ⟶ 8192

So after encryption character "e" whose ASCII CODE is "69" becomes " ", a white space character. We are substituting integers with white spaces because every character can be represented in form of integers and therefore we will require only nine "white space characters" values for substitution of all the characters like alphabets and special characters.

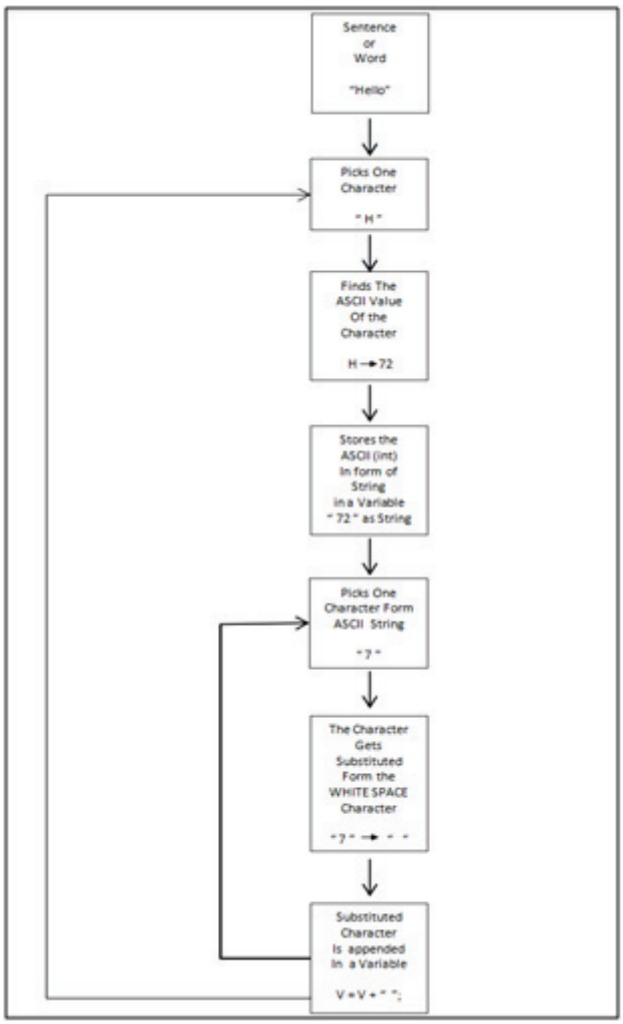


Fig. 2. Encrytion Algorithm Flowchart

IV. EXPERIMENTAL RESULTS

For experimental purpose we tested our key logger by the following steps below.

Fig. 3. Credentials Of The User

In Figure 3, we see that the user has visited an online banking website of SBI BANK and entered their credentials as follows, **Username = "anyuserNAME"** and **Password= "PASSWORD12"**. In the back-end, our keylogger application is continuously running and storing every keystroke of the user along with application/site they opened using timestamp.

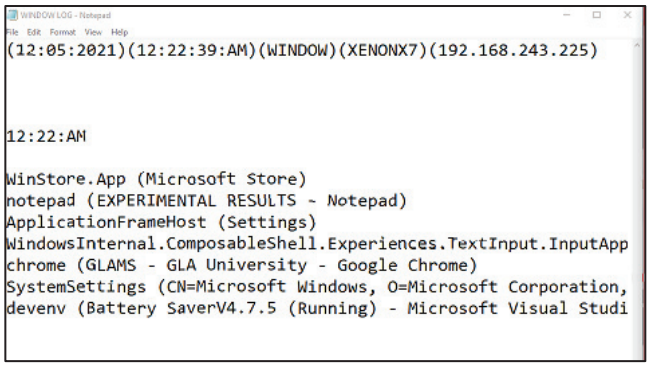


Fig. 4. Application Log File

In Figure 4, we see an application log file. This file is created in the user's PC which stores and keeps the log of all the applications that they have worked on and all the websites they have visited along with the timestamp i.e. the time when the user visited that particular website or the application they used.

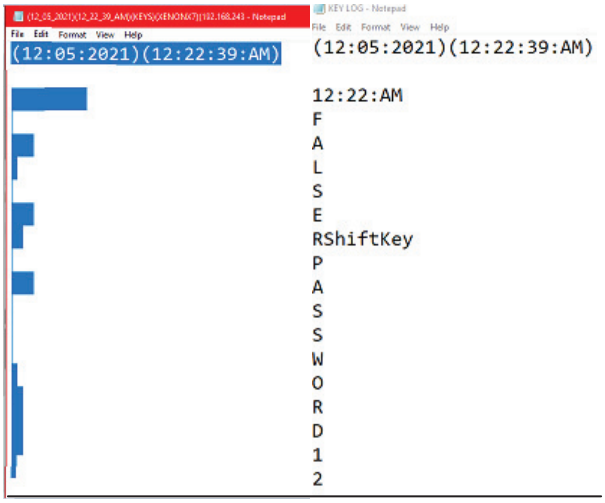


Fig. 5. KEYSTROKE LOG FILE

In Figure 5, we see a Keystroke Log file. This file is also created in the user's PC that captures and stores all the keystrokes of the user along with timestamp, which later helps the attacker to find which keys were used on which application or site so that the attacker can find the associated username and password. Both files are encrypted. So, even if the victim opens this file then the files will appear as a blank document to the user making the file undetectable.

The (left part) of Figure 5 shows the encrypted keystrokes of the user and the (right part) shows the decrypted keystrokes. Now, both encrypted files are uploaded on the attacker's personal server. The name of uploaded files on the server is as follows: "victim's system's name+date+time+ip-address" this helps the attacker to identify the system and time period of the file created.

Fig. 6. DECRYPTOR

In figure 6, we see a decryptor application which we use to decrypt and open the files on the server. We open the decryptor, copy the file path to the decryptor window and decrypt the files. Now the attacker can view the decrypted files and with the help of the timestamp, find the time period when the SBI site was used in Figure:04 and then with the help of other file i.e., the key log file, can find the username as "anyuserNAME" and the password as "PASSWORD12" as we can see in Figure:03

A. Comparison Of Algorithms

In our encryption algorithm, we substituted the characters with white space Characters. So, the file that is created while capturing the keystrokes can be seen as an empty file. So, even if the target discovered that log file of captured keystrokes, he/she will not be suspicious of any malicious activities occurring in his/her system and think of it as a blank file. On the other hand, if we use caesar cipher encryption algorithm, the file will contain characters and the victim can become suspicious and the file could be detected by them, which will eventually lead to the chances of getting caught.

If we used a preexisting algorithm say "Caesar Cipher" for encryption, and if the user discovered the log file then he/she may be able to decrypt the contents of the file via any Online Caesar Cipher Decryption Website. Because Caesar Cipher is a public and widely used algorithm, everyone knows the process of Decryption. The Encryption Algorithm made by our team is not public and if the user finds that the contents inside the file are encrypted, it will be impossible for the user to decrypt it or perform any sort of crypt-analysis because the encryption/decryption is with us and private.

The Encryption algorithm we designed uses "Substitution" method. Most of the Substitution Algorithm in the market (like: Caesar Cipher , Hill Cipher ,Enigma Cipher) is capable of Encrypting only Characters Form A to Z , they are incapable of encrypting Numbers and Special Characters. Our "White Space" Substitution Encryption Algorithm is Capable of encrypting any Character or String containing Alphanumeric Characters.

V. CONCLUSION

Key logger invade and surpass all the system's controls. It is convenient to use and control, giving attacker access to credentials to an advantageous account, full access to all resources and intellectual assets' details. Contrarily, it is a very helpful analytical tools for legal uses as well. Controlling key logging technologies within your organization is not the same as controlling other threats and tools, which require secure understanding. The key is to know that they exist, to understand how they are used, and to use detection methods, with the detection of a key logger and part of the content in your accounting system.

REFERENCES

[1] Parth Mananbhai Pate,Prof. Vivek K. Shah,"Analysis and Implementation of Decipherments of KeyLogger", INDIAN JOURNAL OF APPLIED RESEARCH,Volume-5 Issue-1,pp. 53-55, January 2015.

[2] Yahye Abukar Ahmed, Mohd Aizaini Maarof, Fuad Mire Hassan ,and Mohamed Muse Abshir, "Survey of Keylogger Technologies",International Journal of Computer Science and Telecommunications,Volume-5, Issue-2,pp. 25-31, February 2014.

[3] C. G. S.Ortani, and Crispo."Bait your Hook: A novel Detection technique for keylogger". University of Trento, Via Sommarive.Trento, Italy.2010.

[4] Preeti Tuli,Priyanka Sahu,"System Monitoring and Security Using Keylogger",International Journal of Computer Science and Mobile Computing,Volume-2 ,Issue-3,pp.106-111,March 2013.

[5] "Welcome to System Management Wiki 2014",wikidot.com; smwiki2014.wikidot.com.

[6] O. Zaitsev." Skeleton keys: the purpose and applications of keyloggers"2009.

[7] Disha H. Parekh, Nehal Adhvaryu, Vishal Dahiy,"Keystroke Logging: Integrating Natural Language Processing Technique to Analyze Log Data",International Journal of Innovative Technology and Exploring Engineering (IJITEE),Volume-9 Issue-3,pp. 2028-2033,January 2020.

[8] A. Davis, "Hardware keylogger Detection," Smith Square London, 2007.

[9] Shetty, S. (2005, April). Introduction to spyware keyloggers. SecurityFocus. Retrieved 27 March 2008 from http://www.securityfocus.com/infocus/1829.

[10] R. Venkatesh and R. K. Sekhar, "User Activity Monitoring Using Keylogger," Asia Journal of Information Technology, volume-15, issue-23, pp. 4758-4762, 2015.

[11] Devashree Kataria , Manan Kalpesh Shah , S Bharath Raj , Priya G ,"Real Time Working of Keylogger Malware Analysis", International Journal of Engineering Research & Technology (IJERT), Volume-09, Issue-10,pp. 569-573,October 2020.

[12] Tom Olzak, "KeystrokE Logging", www.researchgate.net,April 2008 https://www.researchgate.net/publication/228797653_Keystroke_logging_keylogging.

[13] Aaradhya Gorecha,"Cyber Security–KEYLOGGERSComparison of Detection Techniques & Its Legitimate Use",International Journal of Engineering Research & Technology, Volume-4,Issue-11,pp. 10-13, November 2017

[14] Wilson, T. V. & Tyson, J. (2008)." How computer keyboards work". HowStuffWorks.com. Retrieved 2011 from http://computer.howstuffworks.com/keyboard.htm

[15] Robbert van der Steeg,"Create a Simple, Hidden Console Keylogger in C# Sharp ",null-byte.wonderhowto.com,January 2012; https://null-byte.wonderhowto.com/how-to/create-simple-hidden-console-keylogger-c-sharp-0132757/

[16] Preeti Tuli, -System Monitoring and Security Using Keylogger‖ International Journal Of Computer Science and Mobile Computing, Volume 2, Issue. 3, pg.106 – 111. March 2013.

[17] "SpyEye Targets Opera, Google Chrome Users". Krebs on Security. Retrieved 26 April 2011

[18] Andrew Kelly (2010-09-10). "Cracking Passwords using Keyboard Acoustics and Language Modeling" (PDF).

[19] Sarah Young (14 September 2005). "Researchers recover typed text using audio recording of keystrokes". UC Berkeley NewsCenter.

[20] O. Zaitsev." Skeleton keys: the purpose and applications of keyloggers"2009

TABLE I. WORKING STATUS OF OUR KEY LOGGER ON DIFFERENT VIRTUAL KEYBOARD

Virtual Keyword Name	Download Link	Status
Windows on Screen Keyboard	"Windows in-buit"	**Working**
Free Virtual Keyword	https://freevirtualkeyboard.com/	**Working**
Touch-it Virtual Keyword	https://download.cnet.com/Touch-It-Virtual-Keyboard/3000-2072_4-75598528.html	**Working**
Ghost press	https://schiffer.tech/ghostpress.html	**Working**
Hot Virtual Keyword	https://hotvirtualkeyboard.com/	**Working**