© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 03 | NCASIT- 2022 | April 18th 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

Monitoring Users' Activity Using Keylogger Application

Disha Pahuja, Prerna Sidana,
Sunit Basak, Neelabh Kulshreshtha,

Department of Computer Science and Engineering,

Manav Rachna International Institute of Research and Studies

Sector-43,Faridabad,Haryana,India

pahujadisha2000@gmail.com, prernasidana@gmail.com,
sunit.basak2000@gmail.com, neelabh31@gmail.com,

***Abstract*— Keyloggers are a subtype of PC malware that records keystroke developments on the keyboard and saves them to a log document, permitting it to gather touchy data, for example, usernames, PINs, and passwords, which it then, at that point, ships off an antagonistic aggressor without causing to notice itself. Keyloggers are a genuine risk to corporate and individual exchanges, including web based business, web based banking, email visiting, and framework information bases. As opposed to different types of unsafe software like infections and worms, keyloggers partner with or share framework assets like CPU and memory with substantial applications, permitting them to work undetected on the framework however long they need to without drawing the consideration of clients. Keyloggers arrive in an assortment of shapes and sizes, yet they all address a genuine risk to client security and protection. Indeed, even while leading a registry posting of stowed away documents, it's hard to differentiate them from working framework records. Besides, they can unscramble data communicated over the web and give it to the aggressor. Keylogger is broadly utilized in the space of network protection, explicitly for satisfying the reason for severe checking and observation in enormous associations. This paper grandstands the working of a keylogger alongside its many highlights, for example, gathering targets' PC data, assembling the substance that are duplicated in the clipboard, gathering sound documents which are identified from the objective's receiver, taking screen captures, etc.**

***Keywords*— Keylogger, Software, Keystrokes, API**

I. INTRODUCTION

A keylogger records each keystroke composed on the keyboard by associating with the application programming connection point (API). It records data like as usernames and passwords, Mastercard data, sites visited, programs utilized, screen captures, etc in a document. [3] Keylogger just screens the framework utilizing keystroke logs and sends current realities to the administrator through the mail server. In such occurrences, keyloggers give the best choices, for example, IT associations might communicate their concerns by seeking after the wrongdoer whose exhibition is dissolving that of the entire firm, elderly folks might help to such an extent that they might keep track on their kids' exercises, and a particular individual's exercises can be followed by saving passwords for quite a long time media stages. Most importantly, a keylogger is probably the best utilization of moral hacking rudiments. Utilizing this, certain safeguards might be taken to keep individual data from falling under the control of complete outsiders. A keylogger is a sort of software that tracks or logs all the keys that a client pushes on their keyboard, for the most part stealthily so the client of the framework is uninformed that their exercises are being noticed. It's otherwise called a keyboard captor. These are both moral and gainful. Managers can introduce them to screen their laborers' PC utilization (Fig.1), expecting them to achieve their positions as opposed to lingering via web-based media. [7] A keylogger is a sort of software that tracks or logs all of the keys that a client pushes on their keyboard, for the most part covertly so the client of the framework is ignorant that their exercises are being noticed. It's otherwise called a keyboard captor. These are both moral and gainful. Businesses can introduce them to screen their laborers' PC use, expecting them to achieve their positions as opposed to stalling via web-based media.

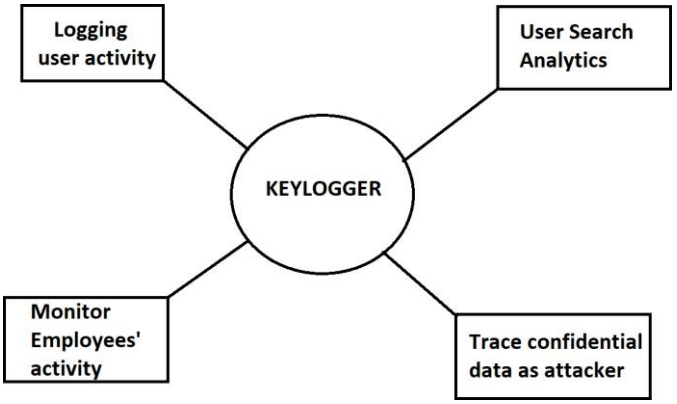

Figure 1: Functions of a keylogger

II. LITERATURE REVIEW

Electronic devices are essentially more significant in current life than they were in past ages. This association offers the two benefits and impediments. Even though there are a few benefits, one hindrance, being presented to pernicious applications, may effortlessly eclipse them. One kind of malware is keylogger. Beforehand, the essential spotlight was simply on catching a client's keystrokes, however they are currently noted for consolidating a wide scope of usefulness.

Keyloggers are utilized to remove touchy data imperceptibly, and they are hard to distinguish since they work completely in covertness mode. It represents a huge test for clients since it very well might be utilized to catch passwords and other sensitive information composed through the keyboard. Therefore, cybercrime is on the ascent. Fraudsters can get account numbers and PIN codes for electronic installment frameworks, just as usernames, email locations, passwords, etc. It can likewise be valuable in examinations of human-PC collaboration. There are for sure an assortment of keylogging strategies, both equipment and software based. Software-based keyloggers are PC applications that work with the software on the objective machine.

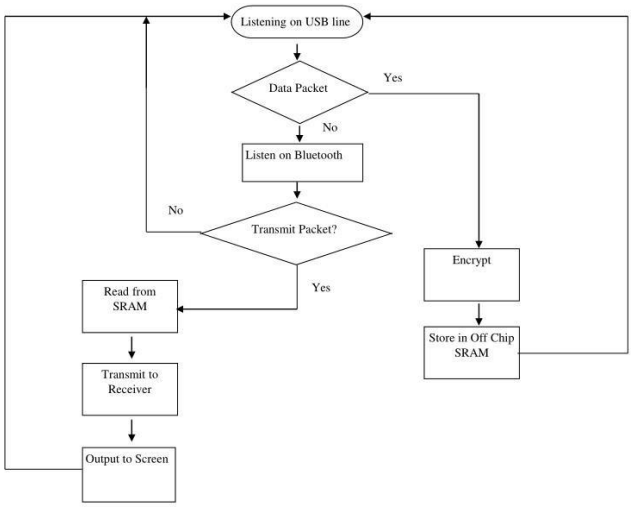

Figure. 2: Workflow representation of software keylogger

In view of the privileges needed to run, software-based keyloggers are isolated into various gatherings. In kernel space, a keylogger with full advantages will work and unprivileged keyloggers work in client space. Software keyloggers require a very much created disease instrument to guarantee legitimate establishment, for instance, an internet browser exploit.[6] Most keyloggers share a typical execution strategy known as snaring, however each keylogger will carry out it in an alternate manner relying upon the setting for which the keylogger is required. The essential objective of snaring is to catch the ordinary control stream and change data returned by an objective framework schedule.

API-based keyloggers associate with a running application's keyboard APIs. As an ordinary piece of software rather than infection, the keylogger registers keystroke occasions. Each time the client pushes or delivers a key, the keylogger gets an occasion. It is simply recorded by the keylogger. Get the condition of the async key and the forefront window.

These schedules are utilized to acquire the current window titles, keyboard occasions, and mouse occasions. To make preparations for obscure keyloggers, a software-based enemy of keylogger is utilized. [8]It will gather all dynamic cycles on the PC and contrast them with the executable records of the software; assuming they match, all dynamic cycles of the predetermined software will be ended. Thus, keylogger running in secrecy mode will likewise get shut.

III. METHODOLOGY

The main focus will be on Software Keyloggers and endeavor to create akeylogger that will gather the client's keyboard sources of info and store them in a text document. All keystrokes, mouse clicks, applications, windows, website pages, email sent and got, visit talks, framework occasions, reports printed, document use, and screen captures are recorded by the keylogger.

API-based keyloggers intercept the signals delivered by each keypress to the software you're typing into. APIs enable software developers and hardware makers to communicate in the same "language" and connect with one another. API keyloggers silently intercept and retrieve keyboard APIs and perform logging of each keystroke in a digital document file.

To guarantee the appropriate establishment, software keyloggers require an all around created disease strategy, like an internet browser weakness. Most keyloggers utilize a pervasive execution approach known as snaring, which is carried out diversely relying upon the climate where the keylogger is required. [5] Snaring's essential goal is to block customary control streams and alter data returned by an objective framework system.

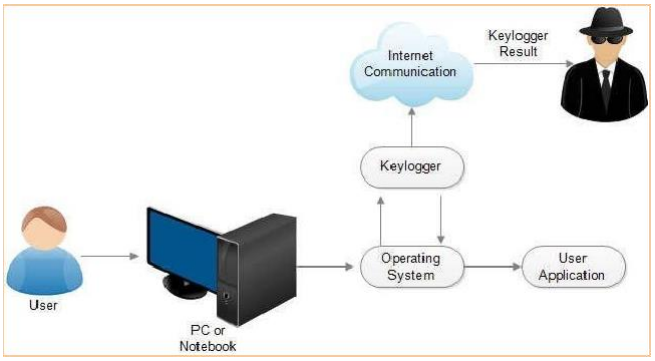

Figure 3: Methodology of a keylogger: Diagrammatic Representation

Functions which receive notification of events are called filter functions; they differ from each other by which events they can intercept. In order for Windows to call a filter function, the function must be bound to a hook (for instance, to a keyboard hook).Binding one or more filter functions to a hook is called “setting a hook”.

Our Keylogger’s main objective is to monitor the user’s activity wherever the user is using the keyboard to input any type of information from entering important credentials to copying the content to the clipboard, every activity will be monitored.

IV. WEB ARCHITECTURE

The keyboard is the essential objective of most normal keyloggers. It comprises a grid of circuits with keys[1]. This grid is known as a key lattice. There are various kinds of key grid relying upon the assembling of the keyboard. Be that as it may, the circuit shuts the key lattice when the client presses a key, then, at that point, keyboard processor and ROM distinguish these occasions.

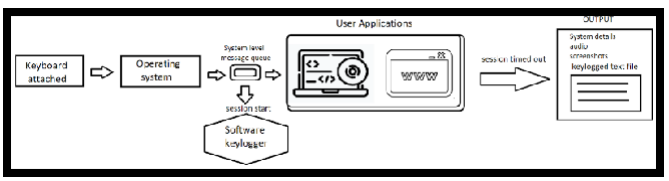

Figure 4: Web-based architecture of API-based Keylogger

The processor translates the circuit location to a character or control code and sends it to the keyboard buffer. The computer's keyboard controller receives the incoming keyboard data and forwards it to the windows operating system. Data travelling between the operating system and computer keyboard interface is intercepted by keylogger.[11] The data source can be from any sort of existing user applications, search activity on web browsers or even pressing of those keys which do not depict a visual output (shift key, tab key, alt key, esc key). All the keystrokes are apparently recorded as a part of a specific duration, known as a session. The output, consisting of proof of the monitored activity, also includes the details of the device on which the session of keylogger was started. Finally the data is sent to an email ID that is included in the keylogger software itself.

IV IMPLEMENTATION

Our keylogger application is programmed in python, the programming language. To program a keylogger, there is a primary set of modules included that play a key role in the implementation so that our purpose of building keylogger isfulfilled (Fig.5).

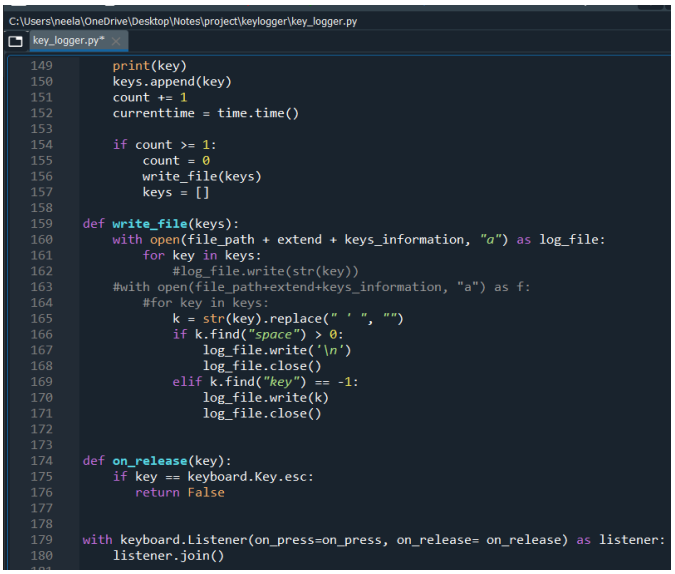

Fig. 5a Source code of keylogger (input)

Figure 5b: Implementation of API-based keylogger

A. email.mime: Creating email and MIME objects

The substance administrator generally replaces its usefulness in the new API, though in different applications, these classes might in any case be significant, even in non-inheritance code. A message object structure is frequently acquired by sending a document or some message to a parser, which parses the substance and returns the root message object. You may, be that as it may, make a whole message structure without any preparation, just as individual Message objects, the hard way. Truth be told, you might broaden a current design by adding extra Message objects, moving them around, etc. This results in an exceptionally easy to understand climate for cutting and parting MIME messages.

1) *class email.mime.base.MIMEBase(_maintype, _subtype, *, policy=compat32, **_params)*

This is the basic class for all MIME-specific Message subclasses. Normally, you won't make instances of MIMEBase, though you may. MIMEBase is primarily supplied as a useful foundation class for more specialised MIME-aware subclasses.

2) *class email.mime.multipart. MIMEMultipart (_subtype='mixed',boundary=None, _subparts=None, *, policy=compat32, **_params)*

This is a subclass of MIMEBase that fills in as a delegate base class for multipart MIME messages. Discretionary _subtype is set to blend as a matter of course and could be utilized to show the message's subtype. The message article will be given a Content-Type header of multipart/subtype. A MIME-Version header will be embedded too.

The multipart limit string is an elective limit. At the point when None is utilized (the default), the boundary is figured out just when it is needed (for instance, when the message is serialized).

3) *class email.mime.text.MIMEText(text, _subtype = 'plain', _charset = None, *, policy=compat32)*

The MIMEText class, a subclass of MIMENonMultipart, is utilized to build MIME objects of the principle type text. The payload string is addressed by _text. The minor kind is _subtype, which is set to plain of course. The person set of the text is provided as a contribution to the MIMENonMultipart work Object() { [native code] }; assuming that the string incorporates just ascii code focuses, it defaults to us-ascii; in any case, it defaults to utf-8. The _charset boundary takes a string or a Charsetobject as a contention.

B) email.encoders : Encoders

This module is part of the legacy (Compat32) email API. In the new API the functionality is provided by the *cte* parameter of the set_content() method.

This module is deprecated in Python 3. The functions provided here should not be called explicitly since the MIMEText class sets the content type and CTE header using the *_subtype* and *_charset* values passed during the instantiation of that class.

When creating Message objects from scratch, you often need to encode the payloads for transport through compliant mail servers. This is especially true for *image/** and *text/** type messages containing binary data.

The email package provides some convenient encoders in its encoders module. These encoders are actually used by the MIMEAudio and MIMEImage class constructors to provide

default encodings. All encoder functions take exactly one argument, the message object to encode. They usually extract the payload, encode it, and reset the payload to this newly encoded value. They should also set the *Content-Transfer-Encoding* headeras appropriate.

A. Features of keylogger

Following are the main features of our keylogger:

1. Basic keylogger - The keylogger will store all the keystrokes in a text file. Most frequent keyloggers target the keyboard; it comprises of a circuit matrix containing keys, also known as a key matrix; there are many different types of key matrix depending on keyboard manufacturers. When the user presses a key, the circuit closes the key matrix, which is detected by the keyboard processor and ROM.[11] The CPU converts the circuit location into a character or control code, which is then sent to the keyboard buffer. The keyboard controller on the computer accepts incoming keyboard data and sends it to the Windows operating system.

Keylogger captures information going between the working framework and the PC keyboard interface. Accordingly, the message stream isn't moved to the following stage. Software keyloggers record keystrokes, save a duplicate to a nearby (regularly scrambled) log document, and along these lines send the information to the working framework. Everything seems typical to the unwary client (Fig.6).

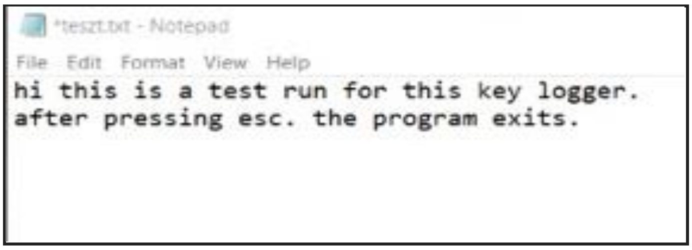

Figure 6a: Text file created after implementation of keylogger

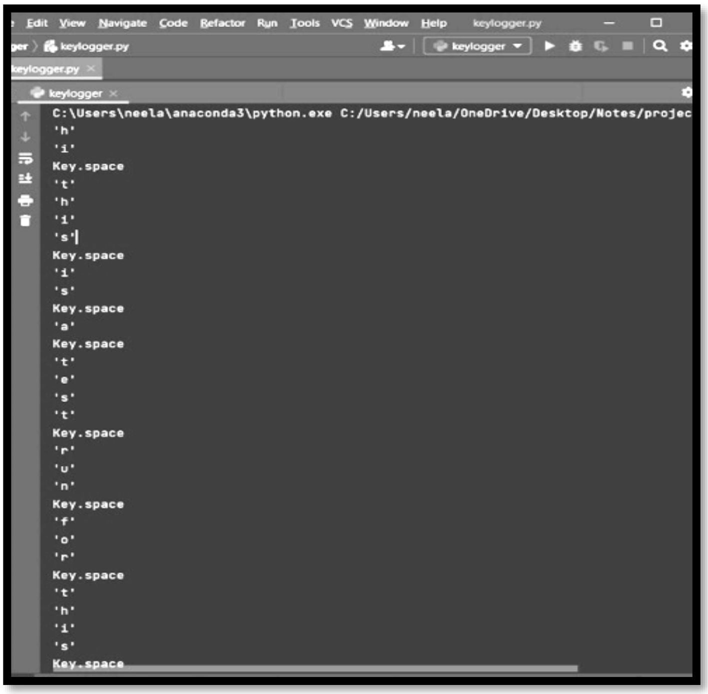

Figure 6b: Basic Keylogger implementation in python

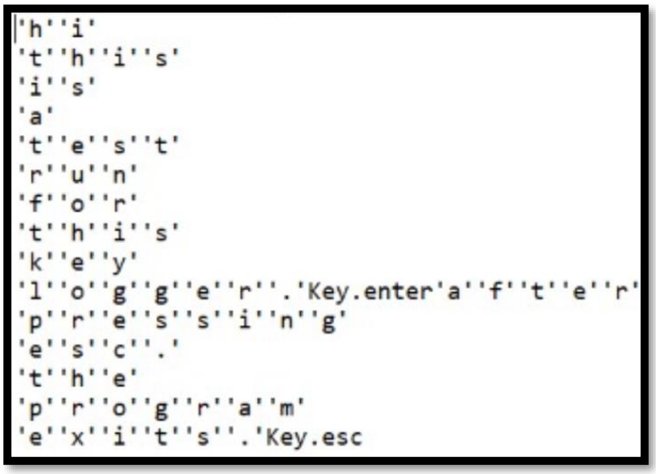

Figure 7: Output file after one session is completed

2. Email functionality- It will send an email to the mentioned email ID with the saved text file as an attachment. In this programme, there are two options: store monitored data and transmit monitored data via e-mail. Any choice is available to us, like to save the gathered data in a certain folder at a specific time interval. The collected data can be sent to a certain e-mail address at a specific time period. As a result, third parties will have access to user keystrokes and mouse events. Cyber thieves have access to personal information such as bank passwords, pin numbers, and usernames in this method.

Figure 8: The output files and device information sent on the mentioned email

3. Getting computer information- Along with the text file it will also send the targets' device information. The device information will include information like the IP address of the user, processor information, model information, hostname of the device and private IP address of the device. This information will also be sent in the email to remotely access it (Fig.9).

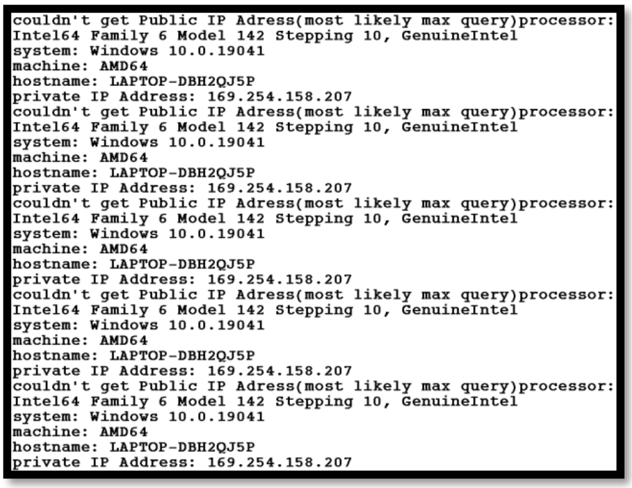

Figure 9: Device information collected with completion of each session

Gathering clipboard content- Anything that can be copied to the clipboard is captured. Data may be readily shared between programmes or inside an application since all applications have access to the clipboard. The Sniff function compares the current clipboard data to the previous known contents (using the built-in clipboard variable). If they vary, something new has been copiedto the clipboard, so the contents are appended to the log file and time stamp it (Fig.10).

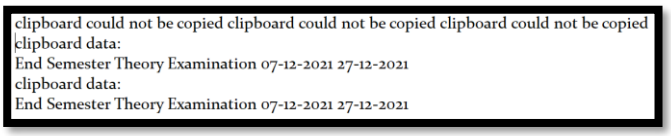

Figure 10: Capturing of the clipboard content

Collecting audio from the microphone- It will also collect the audio files of the target's device. The keylogger will gather all the audio files present in the target's device and will store them in
.wav extension file. The contents stored in the .wav file will also be sent as an attachment with the email.

4. Take screenshots- The keylogger will take screenshots of targets' activity and will save it. All running programs, the list of open windows, or the current active window may all be shown in a single screenshot. If there was a chat, you'll see the names of the other parties as well as their actual responses (which a simple keyboard logger won't be able to record). If a password was used, you'll be able to identify which app or account the password belonged to. In addition, you'll be able to see which applications they're using, even if they're portable or run from a flash drive.

V. CONCLUSION

Electronic gadgets are significantly more important in modern life than they were in past generations. This reliance offers both advantages and disadvantages. Although there are several advantages, one disadvantage, being exposed to malicious programmes, might easily overshadow them. One type of malware is keylogger. Previously, the primary focus was just on capturing a user's keystrokes, but they are now noted for combining a wide range of functionality. Keyloggers are used to steal sensitive information invisibly, and they are difficult to detect since they operate entirely in stealth mode. Users must keep their software up-to-date to avoid keylogging attacks, and it is recommended that they maintain a strong password policy for their computers.

It is recommended that self-running files on externally connected devices such as USBs be disabled, and that copying data to and from external computers be restricted. [12] By doing so, threats may be reduced. Many software keyloggers are used by many organizations for monitoring purposes. A keylogger is a type of software that tracks or logs all of the keys that a user presses on their keyboard, generally invisibly so that the user is unaware that their activities are being watched. It's sometimes referred to as a keyboard capturer. These are both legal and practical. Employers can install them to monitor how their staff use their computers, requiring them to perform duties rather than waste time on social media. The following are some of the possible adjustments and enhancements:

1) Recording of system screen
2) Full remote cloud monitoring
3) Screenshot of immediately changed pages
4) Secure web account for data storing
5) Password Protection
6) Parental Control

VI. REFERENCES

[1] Ahmed, Y.A., Maarof, M.A., Hassan, F.M. and Abshir, M.M., 2014. *Survey of Keylogger technologies*. International journal of computer science and telecommunications, 5(2).

[2] Dwivedi, A., Tripathi, K. C. and Sharma, M. (2021) *"Advanced Keylogger- A Stealthy Malware for Computer Monitoring"*, Asian Journal For Convergence In Technology (AJCT) ISSN -2350-1146, 7(1), pp. 137-140. doi: 10.33130/AJCT.2021v07i01.028.

[3] Sivarajeshwaran, S., Ramya, G. and Priya, G., *Developing Software Based Key logger and a Method to Protect from Unknown Key loggers*

[4] Ladakis, E., Koromilas, L., Vasiliadis, G., Polychronakis, M. and Ioannidis, S., 2013, April. *You can type, but you can't hide: A stealthy GPU-based keylogger* In Proceedings of the 6th European Workshop on System Security (EuroSec). Wood, C. and Raj, R., 2010, July. *Keyloggers in Cybersecurity Education*. In Security and Management (pp. 293-299).

[5] Huseynov, H., Kourai, K., Saadawi, T. and Igbe, O., 2020, May. *Virtual Machine Introspection for Anomaly-Based Keylogger Detection* In 2020 IEEE 21st International Conference on High-Performance Switching and Routing (HPSR) (pp. 1-6). IEEE.

[6] Olzak, T., 2008. *Keystroke logging (keylogging). Adventures in Security*, April, 8, pp.1-6.

[7] Saiganesan N, Dheenadhayalan A, Arulmani M, Suresh K, 2014, *Anti-Hacking Mechanism for Keylogger using Blackbox Detection*, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCICCT – 2014 (Volume 2 – Issue 05)

[8] Tuli, P. and Sahu, P., 2013. *System monitoring and security using keylogger*. International Journal of Computer Science and Mobile Computing, 2(3), pp.106-111.

[9] Aaradhya G, 2017, *Cyber Security – KEYLOGGERS Comparison of Detection Techniques & Its Legitimate Use*, Information Technology Department SVKM NMIMS MPSTME, Shirpur, Maharashtra, India (Volume 04 – Issue 11)

[10] Wood, C. and Raj, R., 2010, July. Keyloggers in Cybersecurity Education. In Security and Management (pp. 293-299).

[11] International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470 @ IJTSRD | Unique Paper ID – IJTSRD37991 | Volume – 5 | Issue – 1 | November-December 2020 Page 566 Keylogger for Windows using Python Santripti Bhujel1, Mrs. N. Priya2

[12] SURVEY ON KEYSTROKE LOGGING ATTACKS Kavya .C 1 , Suganya.R 2 1 Student, II MSc. Computer Science, Sri Krishna Arts and Science College, Coimbatore 2 Assistant professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore.

1[13] Holz, Thorsten & Engelberth, Markus & Freiling, Felix. (2009). Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones. 1-18. 10.1007/978-3-642- 04444-1_1.

[14] Keylogging of user interaction in physical and virtual environments and its implications for honeypot analysis Stig

Arild Ysterud stigay@ifi.uio.no Network and System Administration Master's Thesis Spring 2014 .

[15] Keyloggers in Cybersecurity Education Christopher A. Wood1 and Rajendra K. Raj2 1Department of Software Engineering, Rochester Institute of Technology, Rochester, New York, USA 2Department of Computer Science, Rochester Institute of Technology, Rochester, New York, USA.