International Journal of Innovative Research in Engineering
Volume 3, Issue 6 (November-December 2022), PP: 98-100.
www.theijire.com **ISSN No: 2582-8746**

Advanced Key logger Using Python

Ritesh Yadav[1], Piyush Kumar[2] , Shivam Prajapati[3], Nidhi Sharma[4], Shailesh Patel[5]
[1,2,3, 4]Institute of Technology and Management, Gida, Gorakhpur,India.
[5]Assistant Professor, Institute Of Technology And Management, Gida, Gorakhpur, India.

How to cite this paper:
Ritesh Yadav[1],Piyush Kumar[2] , Shivam Prajapati[3] , Nidhi Sharma[4] , Shailesh Patel[5]. **"Advanced Key logger Using Python",** IJIRE-V3I06-98-100.

Abstract: *A key logger is sometimes known as a system monitor or a keystroke recorder. Every keystroke made on a certain data input device may be monitored and recorded using a technology called keystroke that is commonly used in police operations. Cybercriminals frequently employ key logging as a spyware tool to acquire personally identifiable information, login information, and critical corporate data. Keystroke is used to track employee performance to monitor their laptop use, parents to monitor their children's internet use, device owners to look for potentially illegal conduct on their devices, or law enforcement to analyse incidents involving laptops. Various degrees of morality or acceptability might be attached to the procedure..There are many different key logging methods, including those based in software and hardware. Although key loggers are simple to spot, they can result in illicit transactions once they have infected our machine. Malware assaults that steal data are commonplace today. This essay provides an overview of various password attack types, analyses key logger attack prevention and detection methods, and suggests some preventative steps to lessen malware attacks and personal data detection.*

Key Word: *Key logger, Keyboard, Cryptography, Cipher text, Encryption, Decryption, Hardware Key logger, Software Key logger.*

I.INTRODUCTION

Malware is the process of disturbing system like collect sensitive data and gain access to systems [1]. Ancient authentication systems wont to defend access to on-line services (such as passwords) square measure prone to attack by the introduction of a keystroke faller to the service user's pc [2]. Detecting and preventing malware attack is very important in cyber world as malwares can badly affect computer operation. Once an hacker got access to private userdata, he/she can easily make money transfer from user account to un trusted account. The private data can have manyconsequences which can prove to be more hazards than particular individual's financial loss. We can summarize malware as program intentionally developed for damaging computer specifically those have internet connection [3]. Key loggers square measure a significant threat to users and therefore the user's information, as they track the keystrokes to intercept passwords and different sensitive data type written in through the keyboard. this provides hackers the good thing about access the PIN codes and account numbers, passwords to on-line searching sites, email id's, email logins and different hint etc. when the hackers get access to the user's private and sensitive information, they can take advantage of the extracted data to perform online money transaction the user's account. Key loggers will typically be used as a spying tool to compromise business and state-owned company's information. the most objective of key loggers is to interfere within the chain of events that happen once a secret is ironed and once the information is displayed on the monitor as a results of keystroke. A key logger can be done by introducing a wiring or a hardware bug in the keyboard, to achieve video surveillance, terminating input/output, or by also implementing the use if a filter driver in the keyboard stack. Exploiting the user's keyboard in generalised, documented methods to obtain information. The log file created by the key logger may be sent to the required receiver. Some key loggers programs will record any email addresses that you just have used and URL's of any websites that you just visit. There square measure two different root kit ways employed by hackers: masking in kernel mode and masking in usermode. during this paper we tend to specialise in the literature survey that is said to key logger, its types, interference detection of key logger attacks and its varied applications.

II.LITERATURE SURVEY

Cyber warfare is a fairly common occurrence since every time, one government or another tries to destabilise another by stealing private information from crucial computer systems. Dangerous international conflicts have resulted from this. In order to prevent unauthorised entry of anyone who is not a member of the military or a government official, spyware is currently being deployed on many tools. Key loggers are one of the common techniques used in the modern world to gather private or sensitive information from both trustworthy and dishonest users. These key loggers are helpful and widely used for law enforcement, crime scene investigation, and employee productivity tracking. While its bad uses include passwords and data theft, they are illegal.

Fig-Keyboard of Key logger

III.METHODOLOGY

Key logger is a program that was used to secretly monitor and log all the keystrokes in a computer system. This program can be installed in a computer system or by sending the .jpg file or email to the user's system. If the user clicks this type of images or emails their system gets hacked. For example, if the key logger sending the random image related prize, if the user clicks the image or typing their personal details they got hacked. This Section covers an over view that how the key logger & keyboard works. Key logger attack does that when unknown app or APK runs background of our system, when we type something in our system or if we visit any websites or if we type the bank account details that will be sent to the hacker. By using this master key the hacker can access all the information that they need. Key logging can be two types they are hardware based key logging and software based key logging . A hardware based key logger, small device that serves as a connector between the computer and the keyboard. In this type, a piece of hardware that was inserted somewhere between computer and along keyboard's cables. A software key logger is like remote access it allows to access locally recorded data from the remote location. There are some methods to be followed and used for communication: uploading the data to a website, database or FTP server, periodically emailing data to a predefined email address, wirelessly transmitting data through an attached hardware system, software enabling remote login to your local machine [11]. Some software key loggers capture information when any of the keyboard key pressed as input. The sentence or word or anything when copied to clipboard it will be captured. Randomly timed screenshots of computer the screen of computer will be logged. The windows API allows programs to request text value of some control like password that typed for any forms it will be captured. Keyboard plays an important role in key logger. Keyboard is the main target for key loggers. Keyboard has sequence of key matrix and it also called as circuit matrix. When the particular key is pressed, the keyboard controller notes that which key is pressed and ROM record the events.

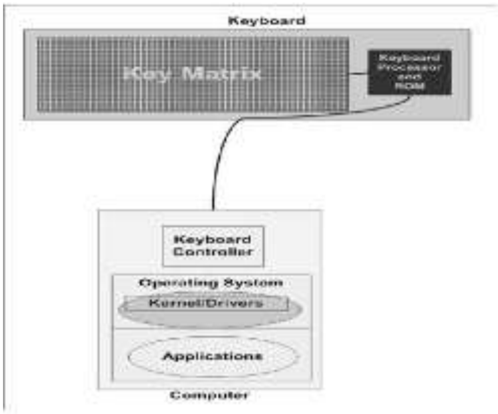

Fig- shows the working of keyboard

It sends the event to operating system and it also sends the code to keyboard buffer. The data travelled between the operating system and computer keyboard is interrupted by key logger. Whenever the key is pressed by user, every time the key logger will be noticed. By recording the each and every key that was pressed by the user. The key logger can hack the particular users system and so that hacker can get database and bank details of that particular user. Hacker can send stolen passwords or database to other intruder.

- Key loggers can be installed when a user clicks on a link or opens an attachment/file from a phishing mail.
- Key loggers can be installed through webpage script. This is done by exploiting a vulnerable browser and thekeystroke logging is launched when the user visits the malicious website.

IV. SYSTEM DESIGN

The process of recording (logging) the keys pressed on a keyboard is known as keystroke logging (usually when the useris unaware). Computer and business network technical issues are investigated using these apps. Although it can be used for bad purposes like stealing passwords, it is more frequently used to monitor network traffic. A keylogger is installed by a hacker using a Trojan virus as the delivery vehicle. However, a hacker will try two distinct techniques to get into your computer before one is downloaded onto it. And you must participate in both scenarios. The first technique entails phishing is the practise of impersonating an official corporation email in order to get passwords and credit card information. Sometimes, these emails have attachments that, when clicked, silently download applications into yourmachine. To use the second method, the hacker first conducts background research on the target person in an effort to identify a flaw in their online behaviour. If a hacker learns that the victim frequently visits porn sites, the hacker can create an email that contains a bogus coupon for a membership to a premium erotic website. The victim has a good possibility of downloading the bogus attachment and inadvertently installing the keylogger because this technique targetsa particular interest of the victim .

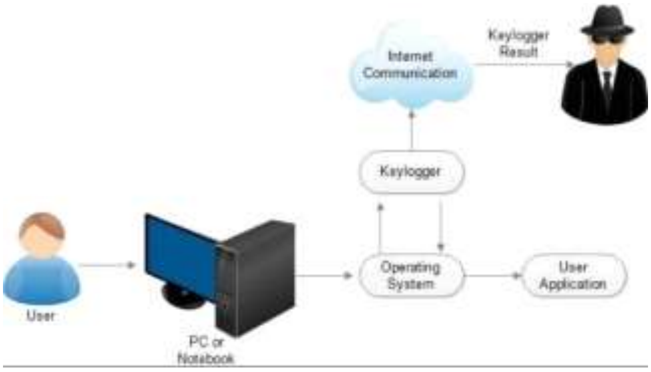

Fig. Key logger Process in User Activity

V.CONCLUSION

With the advancement of technology and the widespread use of computers in both private and public settings, key logger devices—both hardware and software—present a serious risk of cyber interception. The key logger is a malicious programme that can read and gather information from the keyboard and is difficult to detect. As a result, this review essay is a comprehensive reference to all you need to know about key logger software. It's not always simple to tell if a key logger is installed on your device. The only way to spot hardware key loggers is to examine the keyboard's interior as well as the connections that connect to it. Once you've located the gadget, take it out manually . Thus, this is all the information you need to know about key loggers.

References

1. *https://www.ntiva.com/cyber-security-services/*
2. *https://enterprise.xcitium.com/what-is-a-keylogger/*
3. *https://www.researchomatic.com/literature-review-20382.html*
4. *https://www.veracode.com/security/keylogger*
5. *Cyber Security – KEYLOGGERS Comparison of Detection Techniques & Its Legitimate Use Aaradhya GorechaInformation Technology Department SVKM NMIMS MPSTME, Shirpur, Maharashtra, India.*
6. *Malware Definition Available at http://en.wikipedia.org/wiki/Malware.*