IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

KEYLOG SPY

Nikhil Ingle
Computer Science and Engineering, Lovely Professional University
Phagwara, India
nickingle24@gmail.com

Shreya Agnihotri
Computer Science and Engineering, Lovely Professional University
Phagwara, India
shreyaagnihotri9634@gmail.com

Kavita Devi
Computer Science and Engineering, Lovely Professional University
Phagwara, India
kavita.27344@lpu.co.in

***Abstract*: The reason why it is called a Key Log Spy, is because of its working. Key Log Spy stands for Key Log which takes every log of a keystroke the on keyboard and Spy stands for anonymously careful observation. It's meant a such a manner that it tracks the logs of a keystroke on your monitor regularly without knowing the victim and the victim, continues to do his work without any knowledge of the program. But mostly most find out the dark side rather than finding out the bright side of things. Whereas key log spy can be used in organizations to eye on the employee's work during work from home (WFH), surveillance on children's activities, keep a record of id and passwords, or maybe use in a government agency to keep track of victim personnel computer utilization and to take expected action according to their consequences behavior. This project is made in python. This program keeps a record of the victim's keystrokes and sends it through the mail. It not only records the stroke of the keyboard but also the computer information, Network information, Clipboard and Screenshot also.**

Keywords: Keylogging, Python, IDLE, keystroke, cyber education.

I. INTRODUCTION

The key log itself defines its work which is carried key log. Key log is a program that is meant to record the stroke of a keypress on the system. It records the stroke of the f victim and stores it in files, which can be accessed by individuals or organizations who develop the program. It can also be said as malware because it can track the stroke or data entered by the victim. As this program works on the keystroke and we use our system for our personnel use as well as professional purpose, so became easy for us to record the stroke and allow us to keep cross-checking victim activities on the system, get system information (RAM, OS), Networking Information (IP address and MAC address), Clipboards saves data and screenshot. As we have understood keyboard is the prime use the of computer and uses it to use daily activities to get our work done by pressing keys. By pressing the key on the keyboard, it makes us clear about our victim activities as the keyboard interact with the system. Key logger can be used to track user activities in the virtual world, it can be used by government bodies to examine the threat from the enemy and propose the plan accordingly. This key log helps us gather information on victims' long geographical areas. The key log aims to get access to information over different moments and situations. Due to the gigantic increase of the internet, it became impossible to individual keep eye on every activity so reducing the efforts of key log help us to tackle the different scenario situation.

Due to key log, it integrates large assembling of cybersecurity attacks it allows to know the intention of the victim, whereas it infects the system in stealth mode. It can be used in cyber security education purposes to know students' right implementation, working, and prevention of key logs. If the key log is used for suspicious activity, then it can cause huge damage such as it can be used to spy on someone's activities regarding online banking and shopping. Whereas it can be in a valid environment as well as in an invalid environment it depends on the user who is using it. It can be used in the private sector, business sector, and also in state repel activities. Therefore, there are mainly two types of keylogger such as software keylogger and hardware keylogger. Hardware keyloggers are units used for keystroke work, a technique of capturing and recording laptop users' keystrokes, as well as a sensitive password they will be enforced via BIOS-level code or an alternative attached through the applet obstructed to the system and the system keyboard (input device). Whereas software keylogger is a program if it is attached to the system, it monitors the entire activities or tracks the key log press by the intended user to do this usual task by keeping him blind about the program to ensure the user is not unwholesome which can damage or harm our organization as program it sends the logs of sensitive data.

For cybersecurity education purposes to use the keylogging, to be ensuring security practice and should learn how to use it safely for education purposes only with proper guidance rather if caught using it for the malicious purpose have to face legality. If used properly it can help you to take the necessary step in the future to safeguard.

II. Overview of Keylogger

In key logger, the most important is a type of key logger used to gain information. As there exist two types of keylogger which are hardware-oriented and software-oriented, if we go hardware key logger then there, we some kind of inconvenience for us because for hardware keylogger we must be able to physically access the system. Physical devices are Universal Serial Bus (USB) stick, PS2 Personal System/2, or a wall charger that will record the keystroke and other data. But this hardware keylogger is somehow typically wired. Whereas we look at the other side which is a software-based keylogger, it is a program that can be used as spyware to track the action of the intended user. We can use it for various purposes whereas hackers might for malicious purposes use it to gain the access to your private information the type of website you visit by pressing the keys of keyboards that may include the credit card or debit card detail or it can also be used in organization by employers to monitor the employee work-related activities so that the employee working for an should not disclose the

confidential data of their organization. In software-based keyloggers sometimes you are required to access the system of the victim to individually install the program, but there exist many activities through which without physically accessing the system you can install the program into the victim's machine via phishing email. Which can capture the stroke of keys to writing the message, visit the website, enter the details of the card (debit or credit card) in short, anything you type using the keyboard. A key keylogger also be called malware is being installed onto the victim machine for some purpose that might conservative

or radical purpose, or might be installed by the organization to track the activity of employees to safeguard the organization's confidential data but it can also be installed by guardians of kids to protect their children's activities on a web browser.

This paper focuses on software-based keylogger because it is more prepotent than others. It is popular in the business world and can be easily found on the internet. Thus, the keylogger is required to acquire the OS (operating system) to record the stroke of the keys properly. There are many operating systems available in the market thus the program needs to be specifically mechanized in a such a manner that it can handle the keyboard state table(any precise physical, aesthetic, or operational configuration of the keys is referred to as a keyboard layout), kernel layer (It is at the center of the operating system which is a core that provides basic services for all other parts in the operating system) and system routine hook (the term system routine hook is used to cover a wide range of fashion used to alter or to make the logical changes in the operating system). The most common thing between a keylogger and a malware is the attack of fashion, both attack or infect the system anonymously. As most of the malware is designed in standard attack format such as develop, distribute, infecting, and execute. Without a great idea behind the keylogger, t cannot be initiated. As development phase is the unique pattern in which it is designed to accomplish the different targets of the different stages. Whereas the execution is implemented of the malware and the other contributing factor in it.

To gain access to the victim system without physically accessing it is through the Remote Keylogging. As it is a vital technique to gain information about any system type and type of broadband connection and information about the victim using the internet. A study proposed by Provos et al.

In the study of Provos et al it is stated that there are four approaches to malware placement on the internet for vast distribution are listed below: -

1) User-contributed content: - A online user publishes content to a public platform in the scenario. Malicious content placement may occur if the webmaster fails to examine content legality and validity using appropriate sanitization measures.
2) Web security mechanism: - By controlling the server content one can make changes in the code written in HTML, JavaScript, PHP, or other scripting languages and the database. Once the attacker gets the control over security mechanism, he gets the ability to control the content of the webserver and perform various activities.
3) Advertisement: - One can place the program inside the common ads hosting platform. As the advertisement readily tends to pop up and redirect to the linked page, then there is a chance of getting injected by the malicious program into the linked page.
4) Third-party widgets: - As with the advertisement the third-party widget is footing embedded link, often to external redirection to a dangerous location.

The final stage in the attack fashion is malware is being executed and depending on the keylogger implementation and environment this can happen in a variety of ways.

III. Working of Keylogger

The act of tracking and recording every keystroke entry made on a computer, regularly without the user's permission or knowledge, is known as keystroke logging. Any interplay you've got with the button on your keyboard is called a keystroke. You talk to your computer with keystrokes. Each stroke sends a signal to your computer, telling them what you want them to achieve. Thus, commands may include:

1). Name of the key used: full length of all the symbols on the command that use a keyboard.

2). Length of keypress: Enter onKeyUp/onKeyDown and OnKeyPress event handler. The order of events related to the keypress event.

KeyDown Key on its way down

KeyUp: key on its way up

3). Time of keypress: The KeyPress event occurs when the user presses and releases a key. The KeyPress event is fired when a key produces a character.

4). Velocity of keypress: Velocity sensitivity refer to how quickly or forcefully the keys are pressed. Pressure sensitivity is also known as aftertouch.

From fig 1.0 when all of this data is logged, it's as if you're listening in on a private chat. You think you're just "talking" to your device, but someone else was listening and taking notes on everything you said. We exchange a lot of very sensitive information on our gadgets as our lives become increasingly digital. Logged keystrokes can easily be used to piece together user behavior and personal information. Everything is inputted into computers, from online banking access to social security numbers. Social media, email, visiting a website and even text messages exchanged can all disclose a lot about you. Keylogger is a type of monitoring device that may be used for both personal and professional IT monitoring. Some of these applications cross the line into ethically dubious territory.

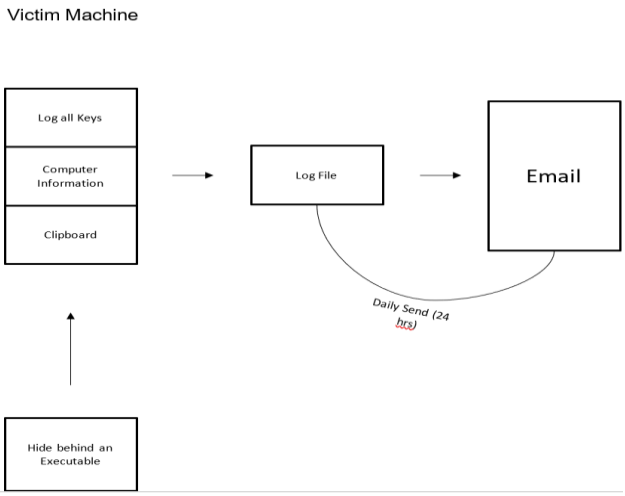

Fig 1.0

Thus in fig 1.1 other keylogger applications, on the other hand, are illegal. Regardless of the purpose, keyloggers are frequently employed without the user's knowledge or agreement, and keyloggers are frequently deployed under the premise that users will act normally.

Four variables determine whether using a keylogger is lawful, morally dubious, or criminal.

1). Is the keylogger used with explicit approval, authorization disguised in the obfuscated language in the terms of service, or no permission at all?

2). Keystrokes logging goals: is the keylogger being used to collect a user's data for an illicit purpose like identity theft or stalking?

3). Is the keylogger being used to monitor the use of the monitored product by the device owner or by the product manufacturer?

4). Keylogger use legislation dependent on location is the keylogger being used with intent and consent and in compliance with all applicable laws?

For multiple parts of the keylogger, we will be appending data to files. Before we append data to files, we must first create variables with proper extensions. Here is the variable you will need with the proper extension.

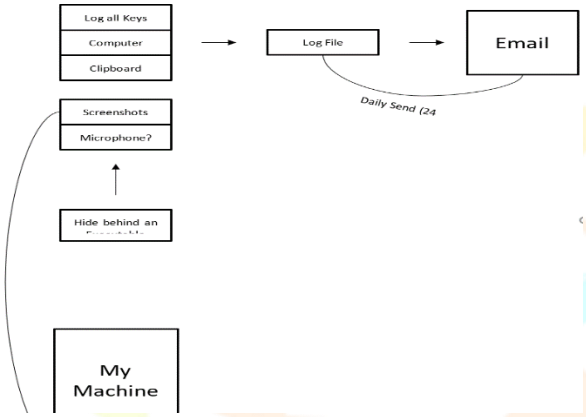

Fig 1.1

system information = "system.txt"

clipboard information = "clipboard.txt"

screenshot information= "screenshot.png"

keys information = "key_logs.txt"

we will also need 03 additional files for encryption, I simply used the filename syntax for each file.

System_information_e = 'e_system.txt'

Clipboard_information_e = 'e_clipboard.txt'

Keys_information_e = 'e_keys_logged.txt'

To log keys using python, we will be using the input module.

from input. Keyboard import key, Listener

To add email functionality, we will be using the email module.

from email. mine.multipart import MIMEMultipart

from email.mime.text import MIMEText

from email. mime.base import MIMEBase

from email import encoders

import smtplib

To gather computer information, we will use socket and platform modules.

import socket

import platform

keys ideas with socket

- The hostname= socket. The hostname () method gets the hostname
- To get the internal IP address, use a socket. gethostbyname (hostname) method

Keys ideas with platform

- To receive processor information, use the platform. Processor () method
- To get the system and version information use the platform. System () and platform. Version ()
- To get the machine information, use the platform. Machine () method

To get the clipboard information, we will be using the win32clipboard module, which is a submodule of pywin32

Import win32clipboard

Key ideas with win32clipboard

- The person may not have any writeable data for the clipboard (could have copied the image), so make sure to use a try-except block just in case the information could not be copied.
- To open clipboard, use the win32clipboard.OpenClipboard()
- To get clipboard information, use the win32clipboard.GetClipboardData()
- To close the clipboard, use the win32clipboard.CloseCLipboard()

To take a screenshot we will use the Image Grab from the Pillow Module

from multiprocessing import Process, freeze support

from PIL import Image Grab

Key ideas with Image Grab:

- The Image Grab, grab () method takes a screenshot
- To save the image, use the image variable. save () method

To ensure only one screenshot is taken at a time, add freeze support (). Use the following code below:

If __name__ == "__main__":

freeze support ()

Process (target=screenshot. Start ()

To build a timer that goes through a certain number of iterations before the keylogger ends, we will be using the timer function

Use the following process:

1. Create an iteration variable and set its value to zero (iterations = 0)
2. Create an end iteration variable which set to a certain amount of iteration before ending the keylogger (end iteration = 5)
3. Get the current time using the time. Time () function, set this equal to a variable (current Time = time. Time ())
4. Create a time iteration variable that collects the key logs for a certain period in seconds (time iteration = 15)

5. Get the stopping Time by adding the time. Time () function + time iteration to stop, set this equal to a variable (stopping Time = time. Time () _time iteration)
6. While iteration is less than (<) the ending iteration
7. If the current time is greater than (>) the stopping time

a) Take a screenshot
b) Send the screenshot to the email
c) Gather clipboard contents
d) Add 1 to the iteration variable
e) Get a new current time
f) Get a new stopping time

To encrypt files, we will use cryptography. fernet module

from cryptography. Fernet import Fernet

IV. REQUIREMENTS

Hardware Requirements:

1. Pentium Class or higher Processor

2. Minimum 64 MB RAM

3. 20 MB Free Disk Space

Software Requirements:

1. Windows XP/Vista/7/8/10 2.
2. Python IDE

V. EXISTING SYSTEM

Hardware keyloggers are bodily gadgets that accumulate the user's keystroke while they are efficiently registered, with a USB stick, PS/2 cables, or charger. As a result, hardware keyloggers can be proven most effective if attackers get real admission or access to the machine. In the emerging internet world, people store their crucial information in their system and are pretty clever to entrust their system to somebody else.

(As there do exist some software-based keyloggers that can only perform basic operations like keystrokes.)

VI. DATA COLLECTION FROM USER

They can hook the keystroke by the user whenever he uses the keyboard to press keys and also capture the computer information such as (RAM) Random Access Memory, OS (Operating System), Network Information IP address (Internet Protocol), MAC address (Media Access Control), Clipboard the data save for a temporary purpose and Screenshot it captures the current window without knowing to the client.

VII. PROBLEM STATEMENT

If the keylogger is not used adequately then there might be a risk, it can cause serious damage to the person on whom the program is initiated where it discloses the entire information of the person and be used against it to exploit him. Moreover, there might be a chance of removing software-based keylogger through antivirus. If there is an attack on a hardware-based keylogger then it is difficult to overcome.

VIII. PROPOSED STATEMENT

Before using the keylogger one must have Top to Bottom knowledge about the keylogger, and if it is used suspiciously one has to face legal issues. Hence hardware keyloggers are difficult to install, unlike software-based keyloggers. A software-based keylogger can be remotely operated from anywhere. The proposed software is readily active to get installed in the victim's machine stealthy by just clicking the link sent him to the different web page. And finally, capture all the strokes of keys and information related to the system, and networking information through email. One must have an updated antivirus installed on the system. And do not visit legit website

When used properly in the government agency help to keep track of record regarding the victim. Kind of sites they visit every day and what they communicate with each other. By using their Network information, we can easily find the geographical location of the victim with knowing them.

IX. LITERATURE REVIEW

Keyloggers are been utilized for both legitimate and illicit reasons served by keyloggers. However, keyloggers are used to gather information. Therefore, are the most famous spyware until now, (Strahija,2003).

Keylogging can also be helpful while texting, as online chat is considered a hybrid mode of communication over the internet where texting information is promoted to the other end. Research came into existence conversation as happening face-to-face, the preliminary study put up its chat service to aid Skype preparation work. A keylogger feature has been enabled in the platform, allowing you to track the time spent on each keystroke, (Giorgio Roffo, Cinzia Giorgetta, Robert Ferrario, Walter Riviera, Marco Cristani, 2014).

As there exist so many work-related stresses in the various field listed some of them are data entry, freelance transcription, and medical transcription to do their daily task. These are very stressful sometimes which leads to mood swings in the user at the work. So, to reduce that a framework is introduced which uses Convolutional Neural Network (CNN) – layers model to predict the emotion such as facial of every user while working. Whereas it tracks the speed of stroke on the key by the user for every 2-min interval of time, as a keylogger is implemented which lets us know the typing speed of the user. Thus, the result is computed using CNN (Convolutional Neural Network) model with the keylogger which predicts the user mood in seven different categories such as angry, disgust, sad, neutral, happy, surprise, and fear, and three typing speeds which are good, bad, very good. The Selenium library will then play the appropriate songs/music in several genres on the YouTube platform (background) to boost your spirit, based on your mood and typing speed fluctuations. Ensure that he/she performs better at work (for example, when she is weary or dissatisfied) or that her spirit remains boosted (such as when he/she is happy and peaceful). To carry out the task of the company, (Kshitiz Badola, Deepesh Sengar, Pooja Mudgil, 2022).

X. SENDING SECRET INFORMATION

As this program is built in a way that it stores the stroke information in a safe folder and directly sends the stroke information and other system-related information, network-related information to the intended user of the program without being able to recognize it by anybody. Thus, the task is performed in stealth mode without any notice and sends the data to the user.

XI. CRYPTOGRAPHY

Encryption fig 2.0 is the analysis of secure messaging technology that restricts access to a message's content to just the sender and intended target. The word Krypto is derived from the Greek word Krypto. This indicates that it is hidden. Hence it is closely connected to encryption, which encrypts plaintext into ciphertext, which is then re-encrypted when it arrives. Encryption also includes techniques such as microdots and merging to disguise information in photography. Ancient Egyptians were known to apply similar techniques in intricate hieroglyphs, and one of the first modern ciphers is thought to have been by Roman Emperor Julius Caesar. When it comes to cryptography is known for encryption, as it is most typically used to hide what is encrypted and decrypt email and other plaintext messages while delivering electronic data. During encryption, we used an asymmetric or private key approach. The data is encrypted with a private key and then the recipient receives both the encrypted message and private key to unlock the message.

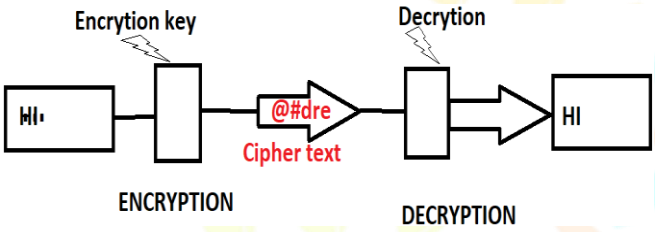

Fig 2.0

When the message is received by the recipient, he has the key to unlock the message. Therefore, we have used this method to hide the stealth conversation between us and the program. So that the victim will not be able to understand the thing.

XII. CONCLUSION

This program helps in our day-to-day life, keylogger will help us to gain data from the victim in stealth modes such as system information (RAM and OS), network information (IP Address, MAC Address), clipboard, and screenshot. Which will us to take keep on orderly victim behavior and planned accordingly. Whereas this can all so be used in to monitor the employee of the company to track his behavior about the company e.g., whether is he sharing company's confidential information to others or can it can all so be used by parents to check their kid's activity in the internet world.

XIII. REFERENCE

1. Martin Vuagnoux, S. P. (2009). Compromising electromagnetic emanation of wired and wireless keyboards. USENIX *security symposium*, 1-16.
2. Thorsten Holz, M. E. (2009). Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones. *Thorsten Holz, Markus Engelberth, Felix C. Freiling*, 1-18.
3. S. sagiroglu and G. Canbek, "Keyloggers," *IEEE Technology and Society Magazine, vol. 28, no. 3, pp. 10-17*, fall 2009.
4. *Kshitiz Badola, Deepesh Sengar, Pooja Mudgil* (2022) *Song/Music Recommendation using convolutional neural network and keylogger (Data Engineering and Communication Technology LNDECT).*
5. *Proceeding of the 16th International Conference on Multimodal Interaction Giorgio Roffo, Cinzia Giorgetta, Robert Ferrario, Walter Riviera, Marco Cristani, 2014 Statistical Analysis of personality and identity.*
6. *Aaradhya Gorrecha (2017) International Journal for Research in Emerging Science and Technology.*
7. *Ahsan Wajahat, Azhar Imran, Jahanzaib Latif, Ahsan Nazir, Anas Bilal (2019) A Novel Approach of Unprivileged Keylogger Detection International Conference on Computing, Mathematics and Engineering Technologies.*
8. *Md Bayzid, Mohiuddin Shoikot, Jafrul Hossain, Anisur Rahman (2019) Keylogger using Memory Forensic and Network Monitoring International of Computer Application.*
9. *Mehdi Dadkhah, Mohammad Davarpanah Jazi, Ana maria Ciobotaru, Elaheh Barati (2014) An Introduction to Undetectable Keylogger with Experimental Testing International Journal of Computer Network and Communication Security.*
10. *Preeti Tuli, Priyanka Sahu (2013) System Monitoring and security using Keylogger International Journal of Computer Science and Mobile Computing*