

**Keylogger Using Python**

A Report Submitted for Partial Fulfilment of

Course-

**Project Based Learning**

First Year Engineering Programme of SPPU, Semester-II

(2020-21)

Submitted By:

|  |  |
| --- | --- |
| Roll No. | Name of Student |
| FE20Comp084 | Sahil Bhure |
| FE20Comp086 | Shubham Deo |
| FE20Comp088 | Satya Prakash Raj |

Under the Guidance of

**Prof. Vrushali Uttarwar**

June-July 2021

**CERTIFICATE**

This is to certify that, report on **“Keylogger Using Python”** submitted by Sahil Bhure, Shubham Deo, Satya Prakash Raj of First Year Engineering Programme, is bonafide work completed in partial fulfilment of Course **Project Based Learning**.

**Prof. Vrushali Uttarwar**

**Project Guide**

**Prof. Hnnie Williams Dr. Sanjay K. Babar**

**Academic Coocrdinator Dean- FE Section**

**Dr. Vijay M. Wadhai**

**Principal**

**SYNOPSIS**

**Creating A Basic Keylogger using Python**

**Programming Language**

Introduction

A keylogger is a type of surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard. The keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. While the programs themselves are legal with many designed to allow employers to oversee the use of their computers. Keylogging can also be used to study keystroke dynamics or human-computer interaction. Numerous keylogging methods exist, ranging from hardware and software-based approaches to acoustic cryptanalysis.

Methodology

For implementation of the keylogger using python, the first step is to use the proper python IDE (such as Pycharm, Spyder, IDLE) to execute the code. Then we have to install pynput package and after import it in the code to monitor or record keystroke of our keyboard. Afterwards, we will create 'send email' module in this project itself. The user has to enter his/her email in the code. When we run the code, it will send email to the user after every 10 keystrokes.

Expected Outcomes of The Project: -

1. To understand how a Keylogger works.
2. Control and listen for mouse movements + Keyboard strokes
3. Simulate keyboard strokes using the pynput library
4. To discover the world of Ethical Hacking and Security with Python
5. To understand the Ethical and Non-Ethical uses of Keylogger

Conclusion

To conclude with the project, we get a basic knowledge about the world of ethical hacking by creating a Keylogger using Python programming language. Keyloggers are a very important tool within the computer security. Keyloggers can be dangerous too when used for hacking and for detecting attackers on the other hand.

INDEX

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO** | **TITLE** | **PAGE NO** |
| 1 | PREAMBLE | 1 |
| 2 | LITERATURE REVIEW/ THEORETICAL | 3 |
| 3 | DESIGN AND DEVELOPMENT | 5 |
| 4 | CONCLUSION | 10 |

Chapter:1

Introduction

Keyloggers are programmed to intentionally monitor the user activity by logging keystrokes and eventually delivering them to a third party. Keyloggers essentially performs two tasks that is guiding into client input stream to get keystrokes and moving the information to a distant area (for example- mail). While they are seldom used for legitimate purposes (e.g., surveillance/parental monitoring infrastructures), keyloggers are often maliciously exploited by attackers to steal confidential information. Although keylogger has some bad reputation in the world of technology because it is often linked with illegal use of the someone personal data. But it can also be used for some of the legal functions. An example can be taken as of the company security purpose, which states that web activities of workers can be checked and keylogger can be used to monitor any employee, which is suspected of being an insider threat. An inexpensive tool like keylogger can be used to save a large amount of damage of any company. Also, parents can use these to keep a check on the web activity of their children to guarantee their protection from internet as there could be misuse of that by children.

Mainly keyloggers are divided into two types Hardware keylogger and Software keylogger. Hardware key loggers are the electronic devices used for keystroke logging or capturing the information between the keyboard device and input/output port. These types of devices have an inbuilt storage where they capture the keystrokes so a person who had installed it on the system can get the information of all the activities done on that system. Software keylogger programs are made to work on the target operating systems. It collects the data travelling along the keyboard and the OS. Software keylogger intercepts the keystroke events, stores them in a remote location, and then sent to the attacker who is already having a keylogger software installed.

Chapter:2

Literature Review

In order to understand about keyloggers more clearly, it is necessary for a reader to grasp detailed knowledge about what is keyloggers, why they are so easy to implement, why countermeasures taken till know is fail to provide adequate solution for it. To answer this type of questions we will discuss about the approaches proposed so far to address the problem and why they are not satisfactory and disadvantages of these approaches. Keyloggers are used to harvest the user’s input is a privacy-breaching activity that can be done at many different levels. When physical access to the machine is available, an attacker might wiretap the hardware of the keyboard to grasp the confidential information. The use of the external keyloggers designed to depend on some physical property, either the audio emanations produced by the user typing or the electromagnetic emanations of a wireless keyboard. External hardware keyloggers are implemented as tiny device to be placed in between keyboard and motherboard, all these strategies require the attacker to have physical access to the target computer. Keyloggers are implemented on computer machine intentionally to monitor the user keystrokes logging activity and eventually delivering them to a third party. These keyloggers are seldom used for legal purposes. Keyloggers are often maliciously used by attackers to steal secret information. Many credit card passwords and numbers have been stolen using keyloggers which makes them one of the most dangerous types of spyware known to date. Keyloggers can be implemented as tiny hardware devices or more conveniently as software. Software-based keyloggers can be further classified based on the privileges they require to execute. Keyloggers implemented by a kernel module run with full privileges in kernel space. Conversely, a fully unprivileged keylogger can be implemented as a simple user-space process. Keyloggers are utilized for both lawful and illicit purposes. Keyloggers are generally utilized by assailants to take private information of an individual or an association. In past many credit card details have been compromised by attackers with the help of keyloggers. Henceforth, keyloggers are one of the most hazardous sorts of spyware till date.

Chapter:3

Design And Development

The Keylogger designed in this project is a software type keylogger made by using Python programming language. For this first we have installed Pycharm IDE (Integrated development environment), then we have installed certain libraries such as Pynput, smtplib, threading etc. The pynput library allows us to control and monitor/listen to your input devices such as they keyboard and mouse etc. The pynput**.**keyboard helps us to control and monitor the keyboard. To send emails, we use a Python development server, Mailtrap online service and a shared webhosting mail server. Simple Mail Transfer Protocol (SMTP) is a communication protocol for electronic mail transmission. Mail servers and other message transfer agents use SMTP to send and receive mail messages. Python threading allows you to have different parts of your program run concurrently and can simplify your design.

In this program we have to provide an email address on which the recorded keystrokes are sent after a specific time interval. The keystrokes are sent on the provided email until the user stops the program or turn off the system.

Keylogger

Start

Main Module

Smtplib

Threading

Pynput

Run different function Simultaneously

Connects server to send email

Record Keystrokes

Send email to specified address

Stop

Chapter:4

Conclusion

As there are always two sides of coin, just like this keylogger has some good and bad reputation. In the world of hacking, it is used to steal someone's personal information while on the other hand it is used in companies to monitor any suspicious activity that may cause serious liability to the companies benefit. But we must aware of what's installed on your computer. Use caution when surfing the internet. Keep your computers security updated.

We modelled the behaviour of a software based user-space keylogger to get all confidential information from user of the system by getting their keystrokes events and mouse clicks without the knowledge of the user. So user of the system is unaware of things happening in background.

References

Tom olzak University of Pheonix (May 2008) <https://www.researchgate.net/publication/228797653_Keystroke_logging_keylogging>

Yahye Abukar University Technology Malaysia <https://www.researchgate.net/publication/309230926_Survey_of_Keylogger_Technologies>

Santripti Bhujel, Mrs. N. Priya **"**Keylogger for Windows using Python" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.566-568, URL: <https://www.ijtsrd.com/papers/ijtsrd37991.pdf>

[Download](https://www.ijtsrd.com/papers/ijtsrd37991.pdf)