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

Keylogger for Windows using Python

Santripti Bhujel[1], Mrs. N. Priya[2]

[1]Student, [2]Assistant Professor,

[1,2]Master of Computer Application, Jain (Deemeed-to-be University), Bangalore, Karnataka, India

ABSTRACT

The proposed point Keylogger which is likewise called as keystroke logger is a product that tracks or logs the key struck on your console, regularly in a mystery way that you have no clue about that your activities are being observed. Most of the people tend to see only bad side of this particular software but it also has legitimate use. Aside from being utilized for vindictive purpose like gathering account data, Visa numbers, client names, passwords, and other private information, it can be used in office to check on your employees, at home to monitor your children's activities and by law enforcement to examine and follow occurrences connected to the utilization of PCs. The project will be completely based on Python where I will make use of pynput module which is not a standard python module and needs to be installed. The software that I am going to build should monitor the keyboard movement and stores the output in a file. To elevate the project I will also add a feature where the logs will be directly sent to the e-mail.

KEYWORDS: *key logging, keystroke, hooking, root kits*

How to cite this paper: 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: www.ijtsrd.com/papers/ijtsrd37991.pdf

IJTSRD37991

I. INTRODUCTION

Key logging program also known as keyloggers is a kind of malware that has capability to maliciously track input of the user from the keyboard in aim to retrieve private information. Keyloggers thus cause a major threat to business and personal activities of kind like transactions, online banking, email and chat. The keyboard is the prime target as it allows keyloggers to retrieve user input to the system as it is the most common way user interacts with a computer. There are two types of keyloggers that exists in market, a software keylogger and a hardware keylogger among which software keylogger are widely used and are easy to plant and cause substantial damage. 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).

The fundamental goal of keyloggers is to meddle in the chain of occasions that happen when a key is squeezed and when the information is shown on the screen because of a keystroke. Keylogger can be used for legitimate as well as illegitimate purposes, it basically depends on user who is using it. System administrators can use keyloggers for systems, i.e. for detecting suspicious users. Keyloggers can effectively assist a computer forensics analyst in the examination of digital media. Keyloggers are especially effective in monitoring ongoing crimes. Keystroke loggers can be used to capture and compile a record of all typed keys. Keyloggers can at times be utilized as a spying instrument to bargain business and state-possessed organization's information. Attackers can utilize keylogger to gain admittance to the clients' private and delicate data, they can exploit the separated information to perform online cash exchange the client's record or different vindictive stuff.

II. LITERATURE REVIEW

To recognize keyloggers all the more conceivably, it is significant for an individual to get a handle on top to bottom information about what keyloggers really is, how they are implemented, and understand different approach to it. To response this kind of queries we will discuss about different kind of algorithm proposed so far to overcome the problem and also the drawbacks of those proposed system.

Key logging is a security trading off procedure which should be possible from multiple points of view. When an attacker gain physical access to your computer devices they can wiretap the physical hardware like keyboard to collect the valuable data of the user. This strategy is totally reliant on some actual properties, either the sound transmission created when a client is composing or the electromagnetic spread of a remote console (Martin Vuagnoux, 2009).

External keyloggers or hardware keyloggers are small electronic device which is placed in between keyboard and motherboard, this procedure requires the attackers to have a physical access to the system which they are intended to compromise. Keyloggers are executed on the focused on machine to record client's keystrokes logging movement lastly giving over those private information to outsider (Thorsten Holz, 2009).

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, (Strahija, 2003).

A malicious programs having keystroke logging feature using an example of real-time online banking system. On the off chance that any of the capacities of the framework were erroneously actualized, they can conceivably give an assailant to get an admittance to a client's ledger. The loophole of this assaults may be removed without problems if the gadget continually ask for a completely new set of characters or alphabets whether or not login is a success. As the examination depend on individual positions and now not at the particular styles of character which are permitted inside the verification code, allowing codes to incorporate a more prominent assortment of characters could now not eliminate the weakness, in spite of the fact that it would perhaps improve security in different regards. He likewise suggested that expanding the allowable lengths of verification codes could drowsy down the assault, yet could now not change the straightforward situation. In synopsis, the central issue is that enemy of key logging frameworks executed in this particular way adequately invalidate their entire reasoning(S. P. Goring, 2007).

III. EXISTING SYSTEM

Hardware keyloggers is a physical device like USB sticks, a PS2 cable, or a wall charger which captures keystrokes of a user while they are logged into the system. Hence, hardware keyloggers can be installed only and only if an attacker gain physical access to the targeted system. In today's date when a person store all his important data in his system, he is wise enough not to give his system to anyone other than people he knows closely. Thus, implementation of a hardware keyloggers are really difficult.

IV. PROBLEM STATEMENT

Keyloggers are a genuine danger to clients and the clients' information, which is considered exploitative movement. The problem statement is that the keyloggers can be detected using antiviruses. Installation of hardware keyloggers is difficult without the knowledge of the owner of the system.

V. PROPOSED SYSTEM

The solution to the above existing problem is that we can build a software keyloggers instead of hardware keyloggers. The proposed model provides the solution that reduces the difficulties while installing the keylogger in the target system. Since, software keylogger can be installed remotely and does not need any physical access of the target system. Proposed software is efficient enough to get installed in targeted system by itself when the user for example clicks the malicious link sent to him through mail or any social media and finally captures all the keystrokes of the user while he is logged into the system, saves the logs in a folder or sends the log directly to the mail address of the third party.

VI. REQUIREMENTS

Hardware Requirements:

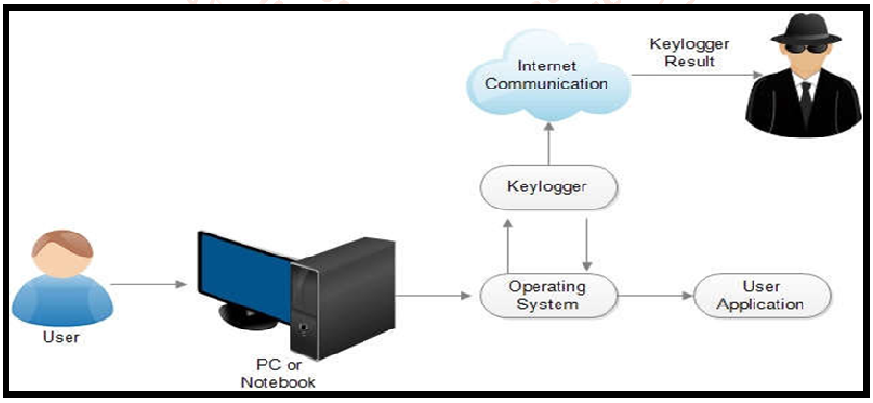
1. Pentium Class or higher Processor
2. Minimum 64 MB RAM
3. 20 MB Free Disk Space

Software Requirements:

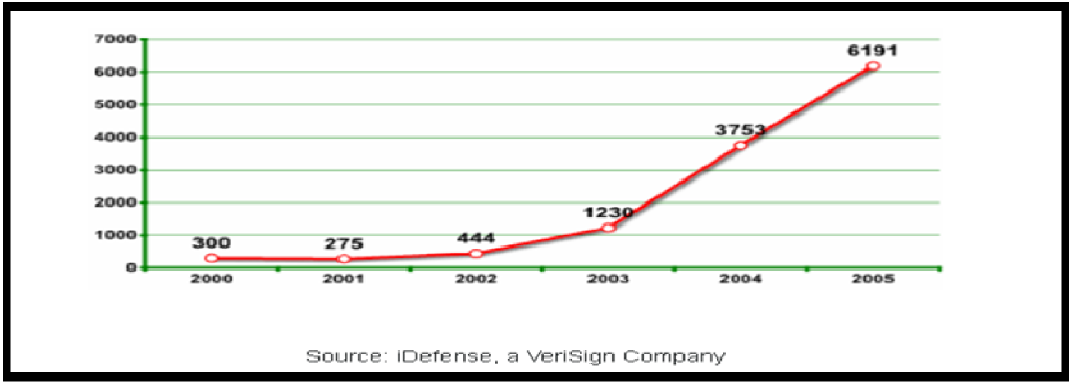
1. Windows XP/Vista/7/8/10
2. Python IDE

VII. IMPLEMENTATION

7.1. SYSTEM FLOW DIGRAM

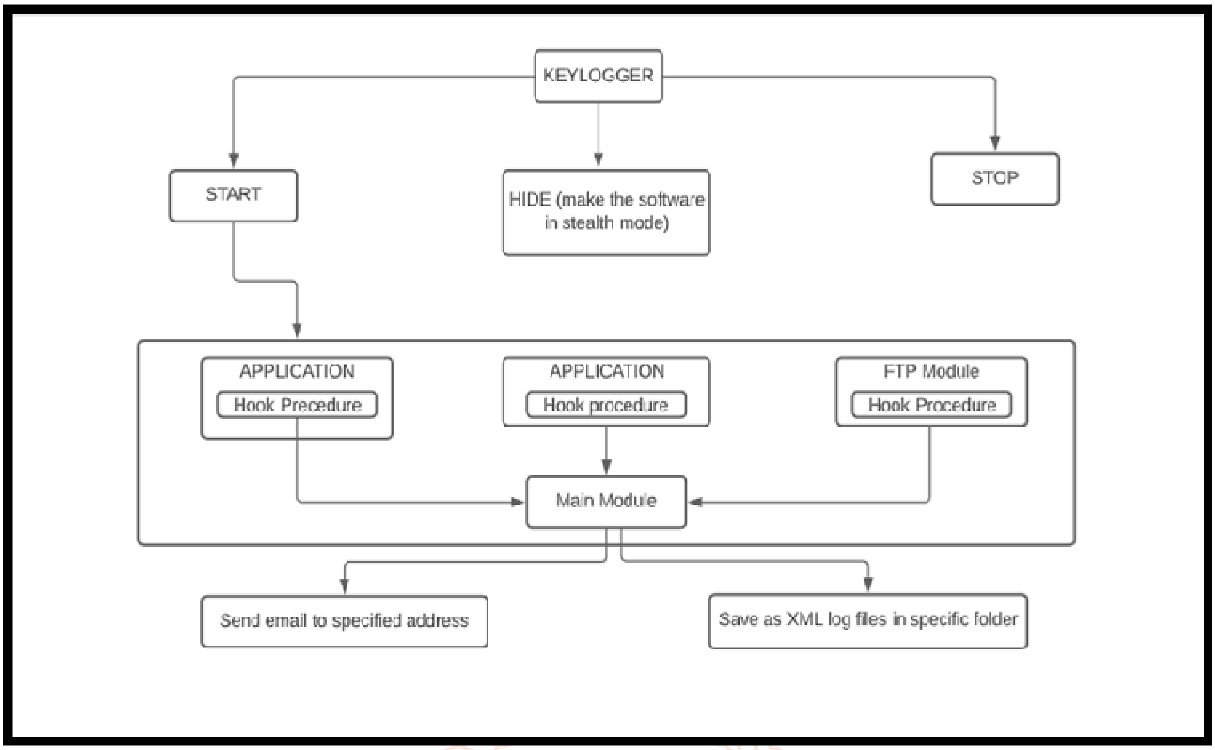


7.2. Increased use of keyloggers by cyber criminals-



Source: iDefense, a VeriSign Company

VIII. SYSTEM ARCHITECTURE


KEYLOGGER
START
HIDE (make the software in stealth mode)
STOP
APPLICATION
Hook Precedure
APPLICATION
Hook procedure
FTP Module
Hook Procedure
Main Module
Send email to specified address
Save as XML log files in specific folder

8.1. OBSERVING USER DATA

The capacity that is expected to catch the keystrokes and mouse occasions will get initiated. The capacity will get what clients is composing in the console and furthermore catch the mouse click. It will take the screen capture of the current window title. Consequently, without knowing the client of the framework all their information will be checked by the proprietor of the product.

8.2. SENDING SECRET INFORMATION

The software provides two methods, first one is to save the log information in a specific hidden folder or to send the log files directly to the mail of the owner of the software.

8.2 MAKE THIS SOFTWARE IN STEALTH MODE

The software provide one important feature that makes the software in stealth mode. Basically, this function will hide the keylogger software from the owner but will make sure that the software is up and running all the time and is capturing all the keystrokes.

IX. CONCLUSION

The product can play out the proposed work like a fundamental keylogger does to get all secret data from client of the framework by getting their keystrokes occasions and mouse clicks without the information on the client. So client of the framework is ignorant of things occurring in foundation. The software is able to monitor data and store the data in a specific folder or send the data to the owner's mail id. The software is also able to hide itself from the owner if the system while it runs in background. Thus, I accept that my methodology extensively increases current standards for observing the information and gathering it for either lawful or unlawful reason.

References

[1] Martin Vuagnoux, S. P. (2009). Compromising electromagnetic emanations of wired and wireless keyboards. *USENIX security symposium*, 1–16.

[2] S. P. Goring, J. R. (2007). Anti-keylogging measures for secure internet login: an example of the law of unintended consequences. *Computers & Security*, 1-9.

[3] Strahija, N. (2003, February 8). *Student charged after college computers hacked*. Retrieved from Xtrix security: http://www.xatrix.org/article2641.html

[4] 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.