IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 9, September 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 9, September 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0909021 |

Keyloggers – An Overview to the Spyware

Meenakshi, Guddi Kumari, Dr. Deeptha R

B.Tech Student, Dept. of I.T., SRM Institute of Science and Technology, Ramapuram, Chennai, India

B.Tech Student, Dept. of I.T., SRM Institute of Science and Technology, Ramapuram, Chennai, India

Assistant Professor, Dept. of I.T., SRM Institute of Science and Technology, Ramapuram, Chennai, India

ABSTRACT: They retrieve all the information that is given by user. This is often used as malicious use. They will find out bank and ATM card numbers by this way. They retrieve all confidential information given by the user and send it through mail or some other medium. This is also used for some good purpose like if boss wants to check activities of his employees or if parents want to check what their children are doing. To deal with this kind of threats not only user should be made aware of this malware but students should also be educated about these types of malware.
This paper presents a case for incorporating key logger in any device. First of all this paper provides an overview of key logging discuss key stroke logging design, implementation in any device, types of key logger and its usage.

KEYWORDS: Confidential information; malware; keylogger; key stroke logging device

I. INTRODUCTION

Key stroke logging programs also known as key loggers, are a type of malware that maliciously track user input from the keyboard in an attempt to retrieve personal and private information. As nowadays computer use has been increased all of these have started online so these threats are also increasing. When we talk about key logger there are basically two types of key loggers. First one is hardware based key loggers and second one is software based key loggers. Both the types of key logger secretly captures all the keystrokes entered through the keypad of a typing device, without the consent of user.
It can affect everything including desktop or laptop keyboard as well as keypad of smart-devices. All the keystrokes get recorded in the form of logs that's why the process is called key stroke logging and the device which is doing this process it is known as key logger.
All these logs are stored in the device it can be anywhere notepad or word and then are sent to the receiver via email or some other method as set by the intruder. This is the spying technique and it can be applied to obtain both positive and negative outcome. As we know that a coin has two faces similarly a key logger has 2 uses one is malicious and one is positive use. It purely depends on user on either to use it in a positive way or negative way.

The two types of key logger:

- Hardware Key loggers: They are small or tiny device that fit in any part of the computer or laptop and detect all the keystrokes. They are attached in Wi-Fi router, under keyboard or behind the CPU to capture all the keystrokes. Nowadays there are optical key loggers that capture all the keystrokes through electromagnetic fields.

- Software Key loggers: It is non- physical technique to capture all the keystrokes. These types are more destructive than hardware key loggers because it is cannot be detected easily. These Key strokes can be installed in the operating system, root directory through any type of link or by downloading any type of files.

II. LITERATURE SURVEY

Taint data analysis framework uses a host-based Intrusion Detection System (IDS) to taint, monitor, and examine the keyboard data at the keyboard device driver level. Thisframework aims to detect kernel-level keyloggers that modify the normal flow of control data in the keyboard drive to extract keystroke data events and then transmit back to the attacker. Thus extraction occurs while data travels along the chain of keyboard device driver in the kernel. This detection model was proposed by Le etal.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 9, September 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0909021 |

Sreenivas et al detected keylogger by using TAKD algorithms that can easily integrate into routine devices such as router, gateway, firewall, IDS and soon to improve its keylogging detection. TAKD algorithm incorporated anomaly-based detection mechanism and log based technique to overcome the problem of signature based detection.

III. EXISTING SYSTEM

Current keyloggers are of 2 categories:
Hardware keyloggers and software keyloggers
Hardware Key logger is a BIOS-level firmware or via a device. All of the information that is logged by a hardware-based keylogger is stored to its own internal memory leaving no trace of its existence on the machine itself.
Similarly Software Key loggers also log the entire key from keyboard and mouse.
Drawbacks of existing System

- It does not send Screenshots.
- It does not logs special keys from the keyboard.

IV. PROPOSED SYSTEM

In proposed systemit is an advanced key logger that logs all the keys typed by the user. It is a software key logger that will send all the logs each 120 seconds. It takes screenshots and also logs special keys such as full stop, comma, exclamation marks etc.
Screenshots are taken to capture graphics-based information. Applications with screen logging abilities may take screenshots of the whole screen, of just one application, or even just around the mouse cursor. It sends logs through Gmail.
Advantages of proposed system

- Send logs each 120 seconds.
- Sends Screenshots.
- Sends log when character is greater than 20.

V. SYSTEM ARCHITECTURE

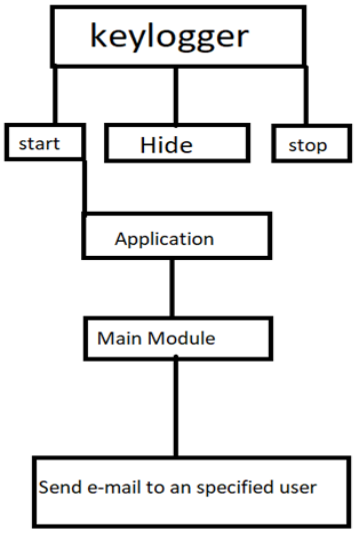

FIG.1. SYSTEM ARCHITECTURE

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 9, September 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0909021 |

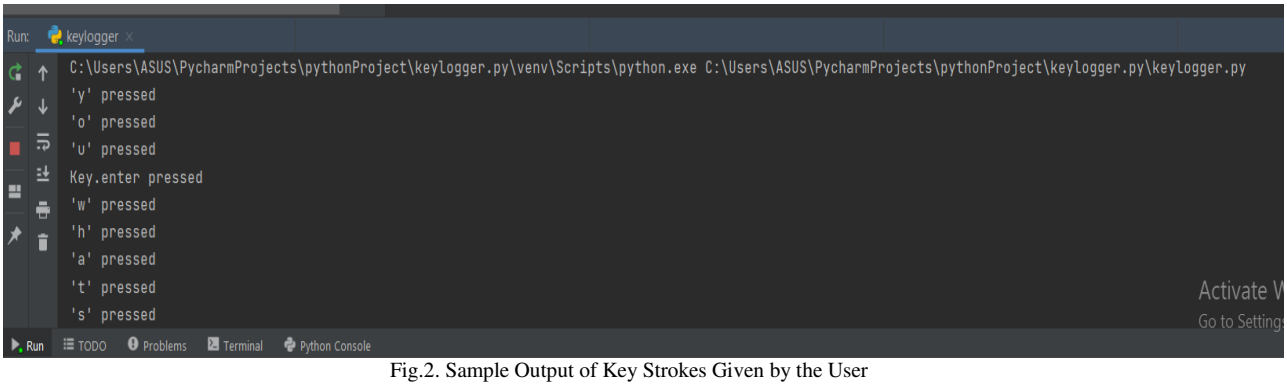

Fig.2. Sample Output of Key Strokes Given by the User

VI. MODULES

- Monitoring user data
- Sending Secret information
- Make the software in stealth mode

VII. MODULE 1 : MONITORING USER DATA

Function that is used to get all the keystrokes and mouse events start working. It will start capturing all the keystrokes or words that the user is typing and will also capture all the mouse clicks done by the user. It will use API to hook all the keystrokes.

VIII.MODULE 2: SENDING SECRET INFORMATION

We will save all the monitored data and send all the saved data through E-mail. By this way all our confidential information like bank passwords, ATM number are known by the hackers and cyber criminals.

IX. MAKE THE SOFTWARE IN STEALTH MODE

This mode is used to make the software in stealth or hidden mode. We can hide this from the owner but in running mode.

X.CONCLUSION

The main purpose of this paper is to make aware of these types of key loggers that are used by the cyber criminals. In this paper we have focused on types of key logger and uses of key logger. Then we have discussed about drawbacks of key loggers and merits of proposed system.

REFERENCES

1. G. McGraw and G. Morrisett.Attacking malicious code: A report to the infosec research council. IEEE Software, 17(5):33–44, 2000.
2. Symantec Corporation, "Viruses and risks," April 2010, http://www.symantec.com/norton/security_response/index.jsp.
3. O. Zaitsev." Skeleton keys: the purpose and applications of keyloggers"2009
4. "How they work and how to detect them Part.", http://www.securelist.com; accessed Sept. 2009
5. Youtube videos - https://youtu.be/TbMKwl11it
6. Shetty, S. (2005, April). Introduction to spyware keyloggers. SecurityFocus. Retrieved 27 March 2008 from http://www.securityfocus.com/infocus/1829

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 9, September 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0909021 |

7. Wilson, T. V. & Tyson, J. (2008). How computer keyboards work. HowStuffWorks.com. Retrieved 25 March 2008 from http://computer.howstuffworks.com/keyboard.htm

BIOGRAPHY

Dr. Deeptha Ris an Assistant Professor in the Information Technology Department, SRM Institute of Science and Technology, Ramapuram, Chennai. She received Master of Technology (M.Tech) degree in 2009 from Sathyabama University, Chennai, Tamil Nadu, India and Doctor of Philosophy (PhD) degree in 2019 from Hindustan University, Chennai, Tamil Nadu, India. Her research interests are Network Security, Software Testing, Web Services etc.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details