**KEY LOGGER**

*A Project Report*

*Submitted By*

**RONAK GUPTA - 2014110620**

**ABHISEKH DASH - 2014110613**

**KRISHN SHARMA – 2014110650**

*In partial fulfilment of the requirement*

*For Project Based Learning of*

**BACHELOR OF TECHNOLOGY**

*In*

**COMPUTER SCIENCE AND ENGINEERING**

*For*

***Computer Network***

*Under the guidance of*

***Mrs. Trupti Suryavanshi***



**DEPARTMENT OF COMPUTER SCIENCE AND**

**ENGINEERING**

**BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)**

**COLLEGE OF ENGINEERING, PUNE- 43**

**2022-23**

**BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)**

**COLLEGE OF ENGINEERING, PUNE- 43**

****

**CERTIFICATE**

This is to certify that the Project Based Learning **Key Logger**, submitted **by Ronak Gupta (2014110620), Abhishek Dash (2014110613), and Krishn Sharma (2014110650)** to the Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune - 43 for the award of the degree of **BACHELOR OF TECHNOLOGY** in Computer Science and Engineering is a bonafide record of the PBL work done by him/them under my supervision.

Place: Pune *Mrs. Trupti Suryavanshi*

Date: 14 November 2022

**Index**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Title** | **Page No.** |
| **1.** | **Introduction of Key Logger** | **1** |
| **2.** | **Literature study of Key Logger** | **2** |
| **3.** | **Methodology** | **4** |
| **4.** | **Implementation Result** | **6** |
| **5.** | **Advantages and Disadvantages of Key Logger** | **8** |
| **6.** | **Application of Key Logger** | **9** |
| **7.** | **Conclusion** | **10** |

ABSTRACT

Keyloggers are type of a rootkit malware that capture typed keystroke events of the keyboard and save into log file, therefore, it is able to intercept sensitive information such as usernames, PINs, and passwords, thus transmits into malicious attacker without attracting the attention of users. Keyloggers presents a major threat to business transactions and personal activities such E-commerce, online banking, email chatting, and system database.

Antivirus software I commonly used to detect and remove known keyloggers. However, it cannot detect unknown keyloggers. This paper presents an overview of keylogger programs, types, characteristics of keyloggers and methodology they use. A case study on Blackbery is used as a real time example in this paper. Finally we will analyze the current detection techniques, and explore several proactive techniques.

**Introduction of Key Logger**

keylogger is a tool that can record and report on a computer user's activity as they interact with a computer. The name is a short version of **keystroke logger,**and one of the main ways keyloggers keep track of you is by recording what you type as you type it. But as you'll see, there are different kind of keyloggers, and some record a broader range of inputs.

Someone watching everything you do may sound creepy, and keyloggers are often installed by malicious hackers for nefarious purposes. But there are legitimate, or at least legal, uses for keyloggers as well, as parents can use them to keep track of kids online and employers can similarly monitor their workers.

The basic functionality of a keylogger is that it records what you type and, in one way or another, reports that information back to whoever installed it on your computer. (We'll go into the details in a moment.) Since much of your interactions with your computer—and with the people you communicate with via your computer—are mediated through your keyboard, the range of potential information the snooper can acquire by this method is truly vast, from passwords and banking information to private correspondence.

Some keyloggers go beyond just logging keystrokes and recording text and snoop in a number of other ways as well. It's possible for advanced keyloggers to:

* Log clipboard text, recording information that you cut and paste from other documents
* Track activity like opening folders, documents, and applications
* Take and record randomly timed screenshots
* Request the text value of certain on-screen controls, which can be useful for grabbing passwords

**Literature study of Key Logger**

Keyboard is primary target of most common keyloggers; it consists of matrix of circuit with keys also known as key matrix, there are many different types of key matrix depending on keyboard manufactures. However, the circuit closes key matrix when the user presses key, then keyboard processor and ROM detect this events. The processor translates the circuit location to a character or control code and sends to keyboard buffer.

Malware detection is often analyzed as being static or dynamic; static is based on signature detection that requires malicious signature present in the repository. The biggest disadvantage of this technique is that it has nothing to do against novel keyloggers. Dynamic detection must be used to detect keylogging malware; behavioral based detection was implemented. As keyloggers always use Windows hooks, Aslam et al. discussed ant-hooked shield that employs by flagging program that hooked system routines that always targeted by keyloggers; However, it is easy for keylogger developers to evade this detection technique by using different methods to log the user activities other than using SetWindowsHookExhowever.

Dynamic based detection techniques or behavioral based was proposed by Martignoni et al. showed the semantic gap between high-level behavior and their low-level representative computer, and achieved largely for the unique layered architecture. This approach is used to modeling semantic gap through structural hierarchic.

Their model detector use suspicious behavior mechanism as input with system broad process execution for monitoring, so flagging suspicious activity is recognized if a process’s activity closely matches the behavior specifications. Meanwhile Ortoline et al implemented Black-box approach to detect the most common keyloggers. Their model was based on behavior of the keylogger by means of keystroke to the I/O pattern formed by keyloggers.

Many of the dynamic detection mechanism being implemented and researched, but it is hard to detect keyloggers accurately. Sreenivas et al. detected keylogger by using TAKD algorithms that can easily integrated into routine devices such as router, gateway, firewall, IDS and so on to improve its keylogging detection. TAKD algorithm incorporated anomaly-based detection mechanism and log based technique to overcome the problem of signature based detection.

Another useful detection mechanism is 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. This framework aims to detect kernel-level keyloggers that modifies 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 et al.

**Impact of Keyloggers:**

A keylogger captures all keystrokes that the user types on the computer keyboard, including passwords, personal information entered into an online registration form (e.g., a mailing address or telephone number), and financial information submitted as part of an online transaction. Unlike other types of malicious program such as viruses and worms, keyloggers associate with or share the system resources such as CPU and memory with legitimate programs that running on the system undetected for as long as they require without attracting the attention of users. There are many types of keyloggers, having different forms and behaviors, but pose a great threat to user privacy and security. First, it is hard to distinguish from operating system files even when doing a directory listing of hidden files. Second, they have the ability to decrypt information passing through internet and transmit to the attacker. Therefore, security experts are now focusing on kernel keylogger which is the most difficult keylogger whose target on the kernel operating system, with the help of hooking mechanism. Thus, the following section will focus on the software keylogger.

**Working:**

Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970’s and was a hardware key logger and first software key-logger was developed in 1983.

**1. Software key-loggers :** Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.

1. **JavaScript based key logger –** It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.
2. **Form Based Key loggers –** These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as a API in running application it looks like a simple application and whenever a key is pressed it records it.

**2. Hardware Key-loggers :** These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

1. **USB keylogger –** There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire i used or shows on the keyboard.
2. **Smartphone sensors –** Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%. Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victims computer to steal the data and login details.

So key-loggers are the software malware or a hardware which is used to steal , or snatch our login details, credentials , bank information and many more. Some keylogger application used in 2020 are:

**Methodology Used**

There are two main methods to develop keylogger systems the Windows Keyboard Hook method, the Keyboard State Table method, and the Kernel-Based Keyboard Filter Driver method. First, Windows Keyboard Hook method based on operating system provides some functions to Hook-based keyloggers for monitoring the keyboard. When a key is pressed the OS records the action and registers the application itself. Later any message running in this mechanism is approved by the application before going to the original target that receives the message. Today, most keyloggers utilize this technique to capture keystrokes.

There are three distinct types of hooks related to windows message: Global hook checks system wide message and Local hook monitors application specific message. Keyboard hook is:

1) Capable of reading all keyboard messages and transfer them to the next hook procedure in a chain.

2) Able to modify the original message and pass it to the next hook procedure.

3) Talented to interrupt the flow of the message by not passing it to the next hook procedure

Second method is Keyboard State Table method which has table consists of the status of 256 virtual keys. Therefore, application that uses a window interface refers to this table. Applications normally use this table to determine the states of the key whether it is up or down. For example, when key is pressed with Ctrl or Shift key, keylogger can utilize the GetKeyboardState API functions to disclose or reveal the keystroke information, by adding its thread to the top-level of thread message loop of window using Attach- ThreadInput API.

Unlike other methods, the Kernel-Based Keyboard Filter Driver method located in the kernel level and hard to detect, but to install them on a target machine, administrator privileges are required. In this method, keylogger that has been installed keyboard filter driver before install the system’s keyboard device driver can capture the keystrokes and data even before reach the operating system.

**A. Keylogger Characteristics**

Although the main purpose of keyloggers is to keep on a user’s keyboard actions, they now have advanced capabilities that widen beyond that function. For example, they can track virtually application running on a computer. The informations keyloggers record, sense, and transmit are the following

Keystrokes on the keyboard

1) Site Monitoring

2) Chatting Monitoring

3) Program / Tracking Application

4) Recording Printing Activity

5) Clipboard recording and Monitoring

6) Recording File/folder and Monitoring Screenshots

7) E-mail Reporting

8) Password Protection and Hot Key

**B. How keyloggers spread**

Keyloggers spread in same way as the malicious programs do. Except some cases where software companies define a keylogger as a software program designed to secretly monitor and log all keystrokes. For example, jealous spouse or partner purchases keyloggers software and installs target machine to monitor the activities performing the victim. Keyloggers are mostly spread using the following methods.

1) Opening file attached and emails cause installation of keylogger.

2) When a file is launched from an open-access directory on a P2P network; a keylogger can be installed

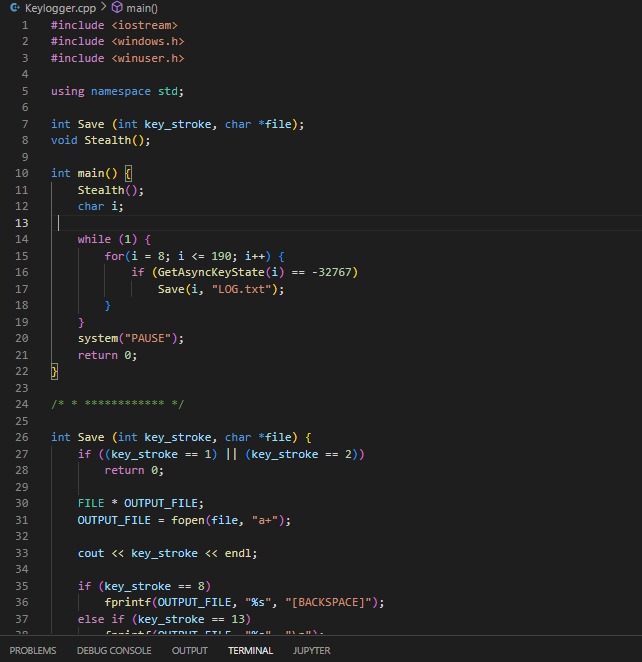
3) A keylogger can be installed via a web page script which exploits browser vulnerability. The keylogger program will automatically be launched when a user visits a infected site,

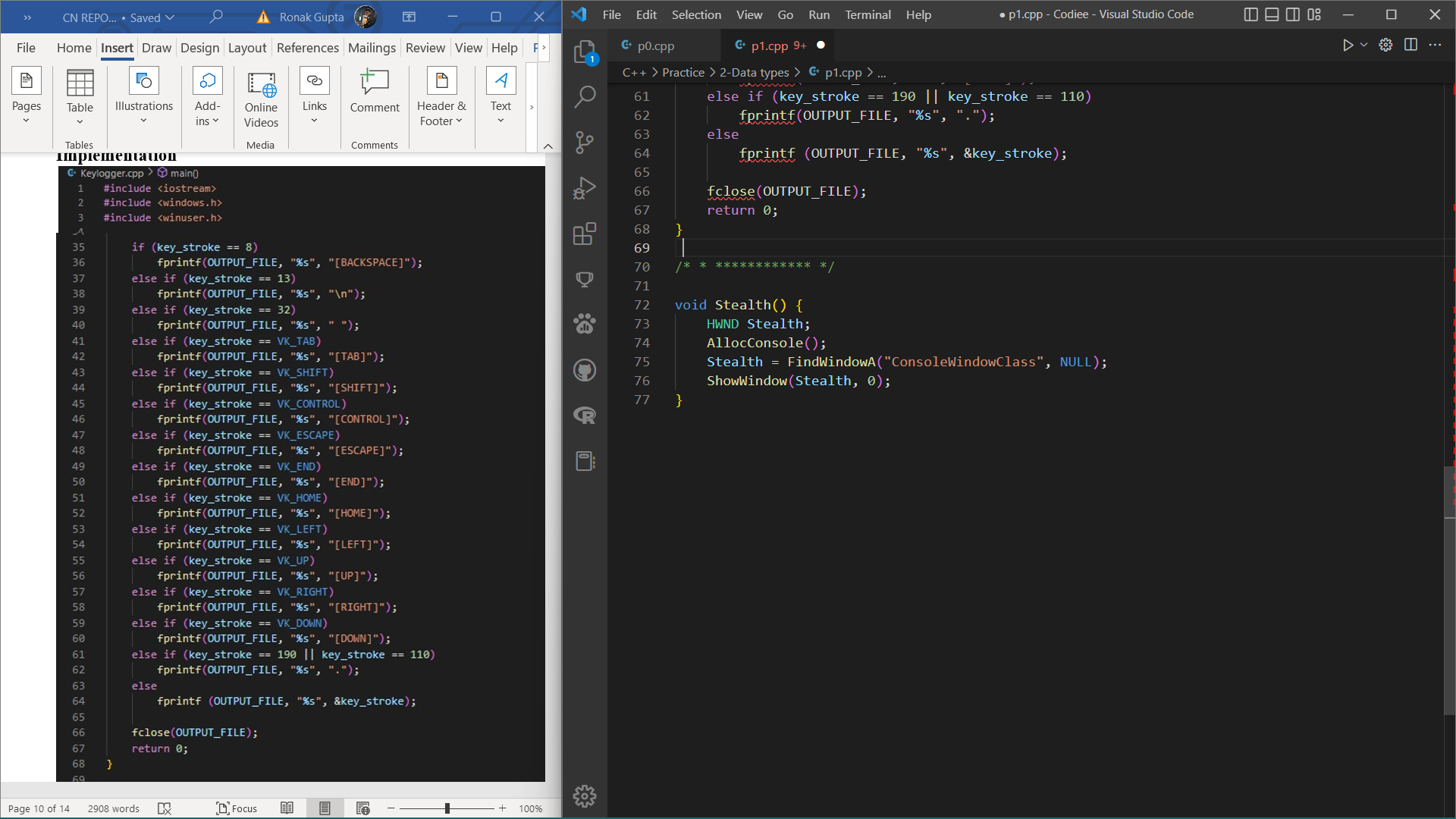
4) Another malicious program that present on victim machine can install a keylogger, if the program is able to downloading and installing other malware to the system.

**Prevention:**

1. **Anti-Key-logger –** As the name suggest these are the software which are anti / against key loggers and main task is to detect key-logger from a computer system.
2. **Anti-Virus –** Many anti-virus software also detect key loggers and delete them from the computer system. These are software anti-software so these can not get rid from the hardware key-loggers.
3. **Automatic form filler –** This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed .
4. **One-Time-Passwords –** Using OTP’s as password may be safe as every time we login we have to use a new password.
5. **Patterns or mouse-recognition –** On android devices used pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.
6. **Voice to Text Converter** – This software helps to prevent Keylogging which targets a specific part of our keyboard.

**Implementation**





Text

Description automatically generatedText

Description automatically generated

Text

Description automatically generated

**Output:**

Graphical user interface, text, application

Description automatically generated

**Advantages and Disadvantages of Keylogger**

In today’s time, people have less awareness about the computer attachment towards Computer Illegal Activity is very high. For this, Key-logger Software is very less beneficial and very harmful. for example.

**Advantage of Keylogger**

* Companies can monitor their employees on what other activities they do on the computer during work.
* To know what activities students, do in college.
* Parents can keep an eye on their children whether they are doing something wrong or they are not going towards any wrong path.
* It can have many more benefits.

**Disadvantage of Keylogger**

* Your social media account like Facebook Twitter Instagram & any other platform’s username and password can be known to anyone; I mean your account can be hacked.
* What you chatting on social media can be read by a third person.
* The most important thing is that your bank details, credit/debit / ATM card details and important passwords can go to someone else, there is a possibility of deducting money from your bank account.
* What do you use on the computer, which apps are running, will anyone know?
* If you write impotent data in Notepad, then anyone can steal it.
* What you have searched on the internet, which information you went on the website, the information can go to someone else.
* store the messages and emails.

**Application of Key Logger**

Keyloggers can be used for a variety of purposes, hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. Some keyloggers can also capture your screen at random intervals; these are known as screen recorders.

Additional application that some software keyloggers come with can capture additional information without requiring any keyboard key presses as input. They include:

1. Clipboard logging – Anything that can be copied to the clipboard is captured.
2. Screen logging – Randomly timed screenshots of your computer screen are logged.
3. Control text capture – The Windows API allows for programs to request the text value of some controls, meaning that your password may be captured even if behind a password mask (the asterisks you see when you type your password into a form).
4. Activity tracking – Recording of which folders, programs and windows are opened and also possibly screenshots of each.
5. Recording of search engine queries, instant message conversations, FTP downloads along with any other internet activities.

**Conclusion**

Keyloggers are powerful tools that cannot threat the system itself, but the user’s confidential data such as user name, password, pin and card bank. Although some keylogger are applied as legitimate way, but many keyloggers are used illegally by the creator. This paper has surveyed most common keylogger types and methods used to hide themselves while subversive user’s machine. We’ve also examined the current state of keyloggers and how they can spread. Finally, we analyzed the existing detection techniques, and outlined some prevention techniques.

Detecting keylogging technology within the organization is no different than controlling other malicious cod or threats, requiring common awareness, regularly monitoring and a layered defense. The main point is to be aware that they existing threat, recognize how they’re used, and suitable ways to detect them. Therefore, keylogger detection and countermeasure must to be part of the organization’s incident response plan.

In Future work might include enhancing TAKD algorithm which is based on traffic analysis such periodic behavior that has fixed time interval for the communication between source and destination. For example, every 15 minutes, determined by the attacker. Therefore, the result of this detection algorithm may be enhanced to achieve quantitative analysis for irregular time intervals