iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** X **Month of publication:** October 2020

DOI: https://doi.org/10.22214/ijraset.2020.31925

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue X Oct 2020- Available at www.ijraset.com

Analysis of Keyloggers in Cybersecurity

Viraj Prajapati[1], Rahul Kalsariya[2], Amitesh Dubey[3], Kewal Mehta[4], Prof. Mahendra Patil[5]
[1, 2, 3, 4]*BE, Department of Computer Engineering, Atharva College of Engineering, Mumbai, India.*
[5]*HOD, Department of Computer Engineering Atharva College Of Engineering, Mumbai, India.*

Abstract: ***Keyloggers are very famous tool which are often used to harvest confidential information. One of the main reasons for this rapid growth of keyloggers is the possibility for programs running in user space to monitor all the keystrokes typed by the users of a system. They are a type of rootkit malware that attempts to retrieve confidential information by covertly capturing user input via keystroke monitoring and then relaying this information to others, often for malicious purposes, it intercepts sensitive information such as usernames, PINs, and passwords. Keyloggers thus pose a major threat to business and personal activities such as Internet transactions, online banking, email, or chat.***
To deal with such threats, not only must users be made aware of this type of malware, but software practitioners and students must also be educated in the design, implementation, and monitoring of effective defenses against different keylogger attacks. The paper provides an overview of keylogger programs, discusses keylogger design, implementation, and usage, and presents effective approaches to detect and prevent keylogging attacks. Second, the paper outlines several keylogging projects that can be incorporated into an undergraduate computing program to educate the next generation of cybersecurity practitioners on this important topic.
Keywords: Computer security, keylogging, keylogger types, software keylogger categories.

I. INTRODUCTION

Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party. Criminals use keyloggers to steal personal or financial information such as banking details, which they can then sell or use for profit. However, they also have legitimate uses within businesses to troubleshoot, improve user experience, or monitor employees. Law enforcement and intelligence agencies also uses keylogging for surveillance purposes.

Keyloggers incorporate a wide array of cybersecurity issues and provide a practical approach to understanding topics such as attacker goals, varieties of malware and their implementation, the role of malware in infecting and controlling a system, and how stealth is achieved in an infected system.

Academically, students will understand tools and mechanisms that aid in the detection and prevention of keyloggers. Commercial anti-malware programs handle common keylogging malware fairly well as they tend to be static in nature and form, but are not as effective in detecting state-of-the-art malware that employ novel stealth and behaviour mechanisms without easily recognized static signatures or patterns [15]. Whether the detection is via active system monitoring for malware memory footprints or for keylogger-like behaviour, a better approach to detecting keyloggers is needed. Ensuring that a security practitioner learns about handling keylogging malware is thus important in cybersecurity education. The rest of the paper is laid out as follows. Section 2 presents the overall perception of keylogging malware and Section 3 outlines design and implementation techniques used in keylogging. Section 4, we analyze the current software keyloggers detection techniques, and propose some proactive steps. Tools and techniques used to detect and prevent keylogging are presented in Section 5.

II. OVERVIEW

A fundamental concept behind keyloggers and similar malware is their pattern of attack. Most malware infections follow a fairly standard attack pattern that involves the sequential order of development, distribution and infection, and execution stages. The initial phase is vital to the process as any malware that is not yet implemented cannot be used by an attacker. What is unique about the development stage is that it emphasizes how the latter stages will be accomplished. Distribution and execution can both be implemented as a component of the malware and therefore are a contributing factor in its design and development. Remote keylogger distribution is a vital step for remote infection. Currently, there are many ways to distribute keyloggers using the Internet. A study shows that there are four distinct approaches to malware placement on the Internet for distribution:

©IJRASET: All Rights are Reserved

A. Advertisements. These provide a common hosting place for malware. As advertisements often tend to be redirections chained together, third parties can inject the location of malicious content into one of the nodes in the chain.

B. Third-party widgets. As with advertisements, widgets are fundamentally embedded links, often to an external Javascript function or similar entities, that can be redirected to dangerous locations.

C. User-contributed content. Here a typical web user physically uploads content to a public location. If the webmaster does an inadequate job of checking content legality and validity via appropriate sanitization techniques, malicious content placement may occur.

D. Web server security mechanisms. These mechanisms also play an important role as they can impede malware placement on web sites by controlling server content such as HTML, Javascript, PHP (or other scripting languages and applications), and database contents. Therefore, an attacker who gains control of these security mechanisms can completely control the content on the webserver and use it to her advantage.

Malware distribution is often followed by infection, which can be accomplished through both web application exploits and social engineering techniques. "Drive-by-downloads", as they are called, are forms of exploitation that involve the automatic download and execution of malicious binaries when a user visits a dangerous remote location [16]. These are accomplished by exploiting insecure browser vulnerabilities using malicious code that will invoke system routines or shell commands on the victim's computer to initiate the retrieval of the malware. The other option for the attacker trying to infect a machine that has no identifiable security vulnerabilities is to trick the user into self-infection. In other words, the attacker will employ what is referred to as "social engineering" [17] to create interest in the user to perform an action that will result in the remote retrieval of malware. The final stage in the attack pattern is for the keylogging malware to begin executing, and can occur in several different ways depending on the implementation and context of the keylogger. The implementation of these operations is discussed in the next section.

III. WORKING AND TYPES

The main idea behind keyloggers is to get in between any two links in the chain of events between when a key is pressed and when information about that keystroke is displayed on the monitor. This can be achieved using video surveillance, a hardware bug in the keyboard, wiring or the computer itself, intercepting input/ output, substituting the keyboard driver, the filter driver in the keyboard stack, intercepting kernel functions by any means possible (substituting addresses in system tables, splicing function code, etc.), intercepting DLL functions in user mode, and, finally, requesting information from the keyboard using standard documented methods.

The concept of keylogger breaks down into two definition

1) Keystroke Logging

Record-keeping for every key pressed on your keyboard.

Keystroke logging is an act of tracking and recording every keystroke entry made on a computer, often without the permission or knowledge of the user. A "keystroke" is just any interaction you make with a button on your keyboard. Keystrokes are how you "speak" to your computers. Each keystroke transmits a signal that tells your computer programs what you want them to do.[18]

These commands may include:

a) Length of the keypress
b) Time of keypress
c) Velocity of keypress
d) Name of the key used

When logged, all this information is like listening to a private conversation. You believe you're only "talking" with your device, but another person listened and wrote down everything you said. With our increasingly digital lives, we share a lot of highly sensitive information on our devices.

2) Keylogger Tools

Devices or programs used to log your keystrokes

Keylogger tools can either be hardware or software meant to automate the process of keystroke logging. These tools record the data sent by every keystroke into a text file to be retrieved at a later time. Some tools can record everything on your copy-cut-paste clipboard, calls, GPS data, and even microphone or camera footage. Keyloggers are a surveillance tool with legitimate uses for personal or professional IT monitoring. Some of these uses enter an ethically questionable grey area. However, other keylogger uses are explicitly criminal. Regardless of the use, keyloggers are often used without the user's fully aware consent and keyloggers are used under the assumption that users should behave as normal.[18]

©IJRASET: All Rights are Reserved

A. Types of Keyloggers

Mainly keyloggers are of two types: Hardware keyloggers and Software keyloggers. There are further more types in hardware and software keyloggers we will discuss them below. Though, the implementation and working of these keyloggers are different but they have one thing in common that is they capture and save confidential data and information in the log file. Keylogger tools are mostly constructed for the same purpose. But they've got important distinctions in terms of the methods they use and their form factor.

Keyloggers can come in two main forms [18]:

1) *Software Keyloggers:* Software keyloggers are computer programs that install onto your device's hard drive. Common keylogger software types may include:

a) API-based keyloggers directly eavesdrop between the signals sent from each keypress to the program you're typing into. Application programming interfaces (APIs) allow software developers and hardware manufacturers to speak the same "language" and integrate with each other. API keyloggers quietly intercept keyboard APIs, logging each keystroke in a system file. Figure 1 shows the prototype API keylogger's modules.

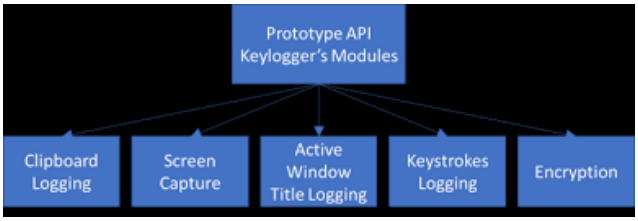


Fig.1

b) "Form grabbing"-based keyloggers eavesdrop all text entered into website forms once you send it to the server. Data is recorded locally before it is transmitted online to the web server.

c) Kernel-based keyloggers work their way into the system's core for admin-level permissions. These loggers can bypass and get unrestricted access to everything entered in your system as represented in figure 2.

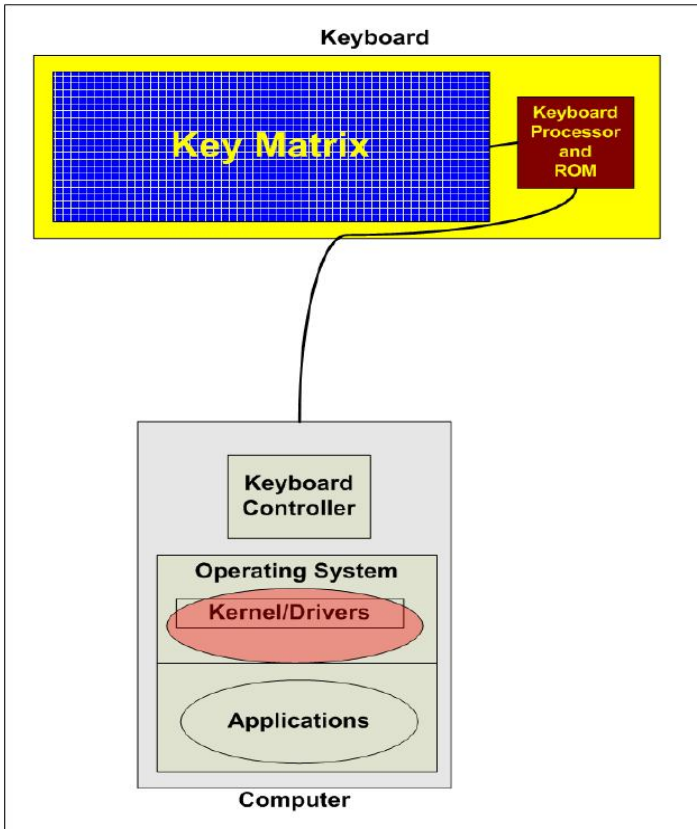


Fig.2

©IJRASET: All Rights are Reserved

2) *Hardware Keyloggers:* Hardware keyloggers are physical components built-in or connected to your device. Some hardware methods may be able to track keystrokes without even being connected to your device. The keyloggers you are most likely to fend against are:

a) Keyboard hardware keyloggers can be placed in line with your keyboard's connection cable or built into the keyboard itself. This is the most direct form of interception of your typing signals. Figure 3 shows keyboard.

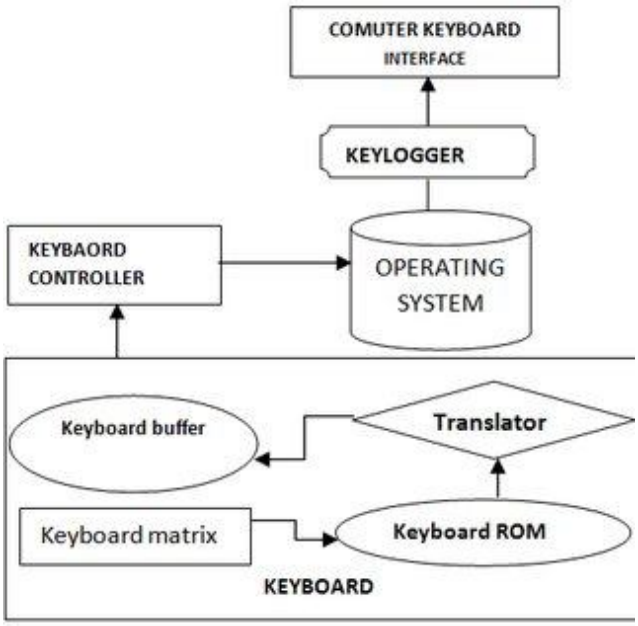


Fig.3

b) Hidden camera keyloggers may be placed in public spaces like libraries to visually track keystrokes.

c) USB disk-loaded keyloggers can be a physical trojan horse that delivers the keystroke logger malware once connected to your device. Figure 4 shows a usb keylogger attached to a keyboard.

Fig.4

©IJRASET: All Rights are Reserved

3) *Wireless Keyloggers:* Wireless keylogger exploits Bluetooth interfaces to transfer captured data to a log file up to the distance of 100M [19]. The primary target of this wireless keylogger is to intercept transmitted packet from wireless keyboard that uses 27 MHz RF connection of encrypted RF transported keystroke character. However, the bad news of this wireless keylogger needs receiver/antenna relatively closed to the target area work [20]. Figure 5 shows wifi-accessible keylogger.

Fig.5

4) *Acoustic Keyloggers:* Acoustic keyloggers are very complex and are therefore rarely used. They utilize the principles of acoustic cryptanalysis to record your keystrokes on the hardware level. No matter what keyboard you're using, each key on it has a unique acoustic signature. The differences are subtle, but individual signatures can be determined by analysing a sample through a variety of statistical methods. However, not only is this very time-consuming but the results might not be as accurate as with other types of keyloggers. [21]

B. Comparative Analysis of Software and Hardware Keyloggers

The technical comparison between software and hardware keyloggers [10] is as follows:

Software Keyloggers	Hardware Keyloggers
1. Software keyloggers are software programs that tracks the activity of a victim when a key is pressed of a keyboard	1. Hardware keyloggers is a tiny memory chip embedded in a keyboard that can be of 4cm.
2. Software keyloggers typically stores the intercepted data in a small file called log files.	2. Hardware keyloggers stores the keystroke information in a tiny memory chip.
3. The stored data can be accessed later or automatically emailed to the person monitoring the action.	3. The stored data can be browsed using a program that usually comes with the hardware keylogger package.
4. Software keyloggers can be installed by the hacker to monitor victim's data or can be installed by a person to monitor data of their relative for example, mom can install a software keylogger in their children's device to monitor internet activities.	4. Hardware keyloggers is often installed by companies to keep track of what employees do on their computer.
5. Software keyloggers can be detected by anti-malware or anti-spyware software.	5. Hardware keyloggers cannot be detected by anti-malware or anti-spyware software.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue X Oct 2020- Available at www.ijraset.com

IV. SOFTWARE KEYLOGGER CATEGORIES

There are four main categories of software keyloggers which are interrogation cycle keylogger, traps software keylogger, rootkits software keylogger and kernel mode software keylogger.

A. Interrogation Cycle Software Keylogger

Interrogation cycle software keylogger uses a number of API functions. This API function return information to int variables and during function call process custom function is used to return char [12]. These function probe keys on the keyboard. The GetAsyncKeyState function is used to determine that a key is up or down at the time the function is called when the key is pressed or released. The GetKeyboardState Copies the status of the 256 virtual keys to the specified buffer then returns the state of each key on the keyboard that is compatible with GUI applications. In order, to avoid data missing, use of high speed interrogation with 10-20 polls per second is required. Interrogation cycle software keylogger is simple and can easily detected [9].

B. Traps Software Keyloggers

This type of mechanisms works only for GUI applications to trap keystrokes as well as messages that are processed in window of other GUI application. Developing this type of keyloggers that is based on trap of hook mechanism is considered to be ideal method. The hook handling code has to be put in a DLL (Data link library) in order to install hook mechanism with the help of API functions. For example, SetWindowHookEx execute installation of an application defined hook procedure into a hook chain, and unhooks WindowHookEx helps for removal of the hook. The keylogger determines which type of message called the hook handler when SetWindowHookEx function is called. When the hook is registered first time, the GUI application receives the first message that satisfies the activation of the hook registration, and then DLL including hook code is loaded into process's address space. This determines the amount of memory allocated for all likely addresses for a computational entity, such as a device or a file [9].

C. Rootkit Software Keylogger

A rootkit is something that penetrates into the system and intercepts the system functions. It can conceal its existence of particular processes, folders, files and registry keys. Some rootkits install its own drivers and services in the system. Rootkit software keyloggers are relatively rare but are the most dangerous type of keyloggers. It captures set of function responsible for processing of messages or the inputted text processing. It has functions like GetMessage, TranslateMessage library, and PeekMessage user32.dll. This functions captures messages and surveil the messages obtained by GUI application. With the help of these methhods and set of functions it easily intercepts the messages and Data [9].

D. Kernel-mode Software Keylogger

Kernel-mode techniques that is based on tow standard principles are generally used by most of the keyloggers. The spyware to connect keyboard drive stack with the help of IOAttachDevice and IOCreateDevice function automatically after loading the operating system is provided by installing a driver-filter for the keyboard driver. However, driver filter not read or record I/O Request packets (IRPs). Also it does not intercept data about keystrokes, but target IRPs with requests for data from the KBdclass driver. After KBdclass driver finish the IRP and transfer the requested data to the IRP buffer the keystrokes information will be available. So with the help of the API function IOSetCompletionRoutine the keylogger filter has a chance to install its own termination procedure for every IRP of the IRP_MJ_READ [9].

V. DETECTION AND PREVENTION

In this section we will explore how to detect and prevent keyloggers. Till now we have traversed, the design, implementation, and use of keyloggers, i.e. , the black hat viewpoint. This section addresses the major goal of cybersecurity that is to secure the system. In this section, we survey some main classes of keylogger detector techniques. It is important for the white hat hackers to study and detect the weakness and help the software developers to fix the weaknesses before malware take advantage of it. A study of keylogger detection and prevention is thus critical for white hat hackers. Study shows that the technique of detection and prevention does not guarantee 100% especially when rootkits modify the operating system [13], [14].

Main goal of detection is to identify keyloggers that has already tainted a system on the other hand prevention focuses on not allowing keyloggers any access to a system. There are two types of method used for malware detection and analysis: static malware

©IJRASET: All Rights are Reserved

analysis and dynamic malware analysis [8]. In static analysis the malware sample is examined without actually running it whereas in dynamic analysis it involves running the malware sample and observing its behaviour. Static analysis is a process of analyzing a malware binary without actually running the code. It is generally performed by determining the signature of the binary file. The signature of the binary file is unique identification for the binary file and can be done by calculating the cryptographic hash of the file and understanding each component. These signatures are essentially sequences of machine instructions that correspond to suspicious activity performed by a program on the host machine [8]. There are two major problem with this technique is (a) the malware detection program needs to be constantly updated with new malware definitions and (b) no protection is provided against malware whose signature is not present in the repository. To overcome this, dynamic detection technique must be employed to detect keylogging malware. Dynamic analysis involves running the malware sample and observing its behaviour on the system in order to remove the infection or stop it from spreading into other systems. The system is setup in a closed, isolated virtual environment so that malware sample can be studied thoroughly without the risk of damage to your system [8]. Aslam et al [1] delineate anti-hook technique. The fact that the processes either hidden or on display uses hooks APIs for the purpose of hooking. So if we are able to scan all the processes and static executables and DLLs and detect the suspicious files or processes, which uses hooks. Anti-hook shield technique is used against software keyloggers.

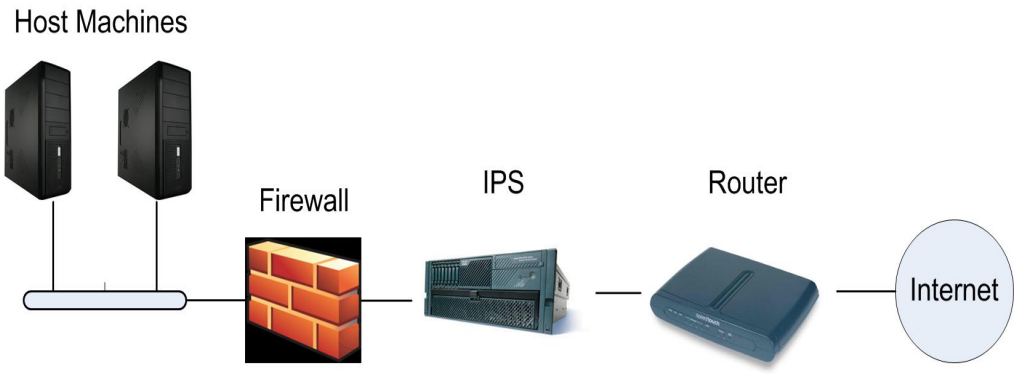
Le et al. (2008) [3] describes detection of keyloggers at kernel level through dynamic taint analysis. It is observed that kernel keyloggers usually manipulate the data flow of a keyboard driver in order to record typed keystrokes. By tainting and monitoring the keystroke data, this framework detects and analyzes any illegitimate uses of the tainted keystroke data. The technique used is host-based intrusion detection. In AU - Tian, D [2]. which is an online approach for kernel-level keylogger detection and defense. They presented LAKEED, an online defense against the kernel-level keylogger by utilizing the hardware assisted virtualization technology. The basic idea of this technique is to isolate the target kernel extension that may contain the keylogger from keyboard drivers' execution environment and then monitor their potential interactions. By comparing the runtime information with the execution baseline that is obtained by the offline analysis, the keylogger can be identified. Another detection technique for software keylogger with Dendritic Cell Algorithm implemented by Anith at el. [11] (2011). In this an immune-inspired dendritic cell algorithm (DCA) was used to detect the existence of keyloggers on an infected host machine. The basis of the detection is facilitated through the correlation between different behaviors such as keylogging, file access and network communication. It is a client level detection technique which uses host and checkpoint levels technique using signatures.

The particular computer user has to depend on existing tools and anti-malware programs to detect keyloggers on their machines as most of the dynamic detection techniques being researched, implemented and tested are still in developing stage. Rootkitrevealer [4] is an advanced rootkit detection program that helps with detection of the keyloggers, but finds it difficult to identify rootkits that hide their existence in the system as they modify privileged operating system data or memory. Anti-malware programs like Norton from Symantec and McAfee provide malware detection services. Most of these programs depend on the signature-based detection and are not able to detect unique keyloggers. Therefore, a proactive approach is needed to stop keyloggers before they infect a system. Since the main motive of the keyloggers is to retrieve confidential data. So in order to prevent potential keyloggers to infect the machines it is better to apply the following steps.[6]

1) Using one-time passwords or two step verification can help minimizing the losses.[6]

2) The anti-malware solution should be updated and maintained regularly.

3) Tools such as antivirus software, intrusion prevention systems, firewalls and routers, and even application settings. The Figure below portray the layering of such tools in an attempt to protect the host machines from malware infection.[7]



©IJRASET: All Rights are Reserved

4) Using a system with proactive protection designed to detect keylogging software.[6]

5) The most commonly used form of malware prevention is Antivirus solution as it performs critical system component scanning, real-time activity monitoring for suspicious behavior, file scanning, and network filtering or use of keylogger detection software to monitor sensitive systems like Sophos home.[5]

6) Another best method to provides suitable detection technique against both software keyloggers and hardware keyloggers is using a virtual keyboard. Since, the main target of the keylogger is the keyboard. So using a virtual keyboard instead of a standard keyboard can be useful. A virtual keyboard is a program built in Windows operating system that displays intangible keyboard on the screen. Mouse is used to press keys on the virtual screen keyboard. The figure below is a on screen keyboard of windows 10 Operating System.[6]

However, typed Keystrokes and the mouse clicking through an on-screen keyboard can easily be interrupted by a malicious program. Hence, on-screen keyboards are not reliable detection technique method of outsmarting keyloggers. In order to get rid of these keyloggers, specially designed on-screen keyboards is recommended to ensure that information transmitted through the on-screen keyboard cannot be retrieved. Some virtual keyboards also have a feature that allows a user to enter a character by hovering mouse cursor over a letter for a few seconds. Thus, the user can enter the password without even clicking the mouse button.

7) Using a key Encryption software Using a key Encryption software user can add an extra layer of security against a keystroke recorder. It encrypts the characters that a user enter on the keyboard. Thus, prevents keyloggers from logging the exact keys. So even if a keylogger is monitoring the paths the keys travel through, it can only record random characters.[5]

VI. CONCLUSION

One report issued by Symantec shows that almost 50% of malicious programs detected by the company's analysts that were used by cyber criminals to harvest personal user data [6]. According to research conducted by John Bambenek, an analyst at the SANS Institute, approximately 10 million computers in the US alone are currently infected with a malicious program which has a keylogging function [6]. Hence, it is important for cyber security professional to detect and prevent the keyloggers to spread and infect the computers. Unlike other types of malicious program, keyloggers present no threat to the system itself. Nevertheless, they can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard. Unfortunately access to confidential data can sometimes have consequences which are far more serious than an individual's loss of a few dollars. Though keylogger developers develop their products as legitimate software, but most of the keylogger are used to steal user data. In This paper we have examined the current status of the keyloggers and how they play an important role in cyber security. This paper has surveyed the working of keyloggers and the different types of keyloggers. We have also examined the categories of software keyloggers. though keylogger developers market their products as legitimate software.

VII. ACKNOWLEDGEMENT

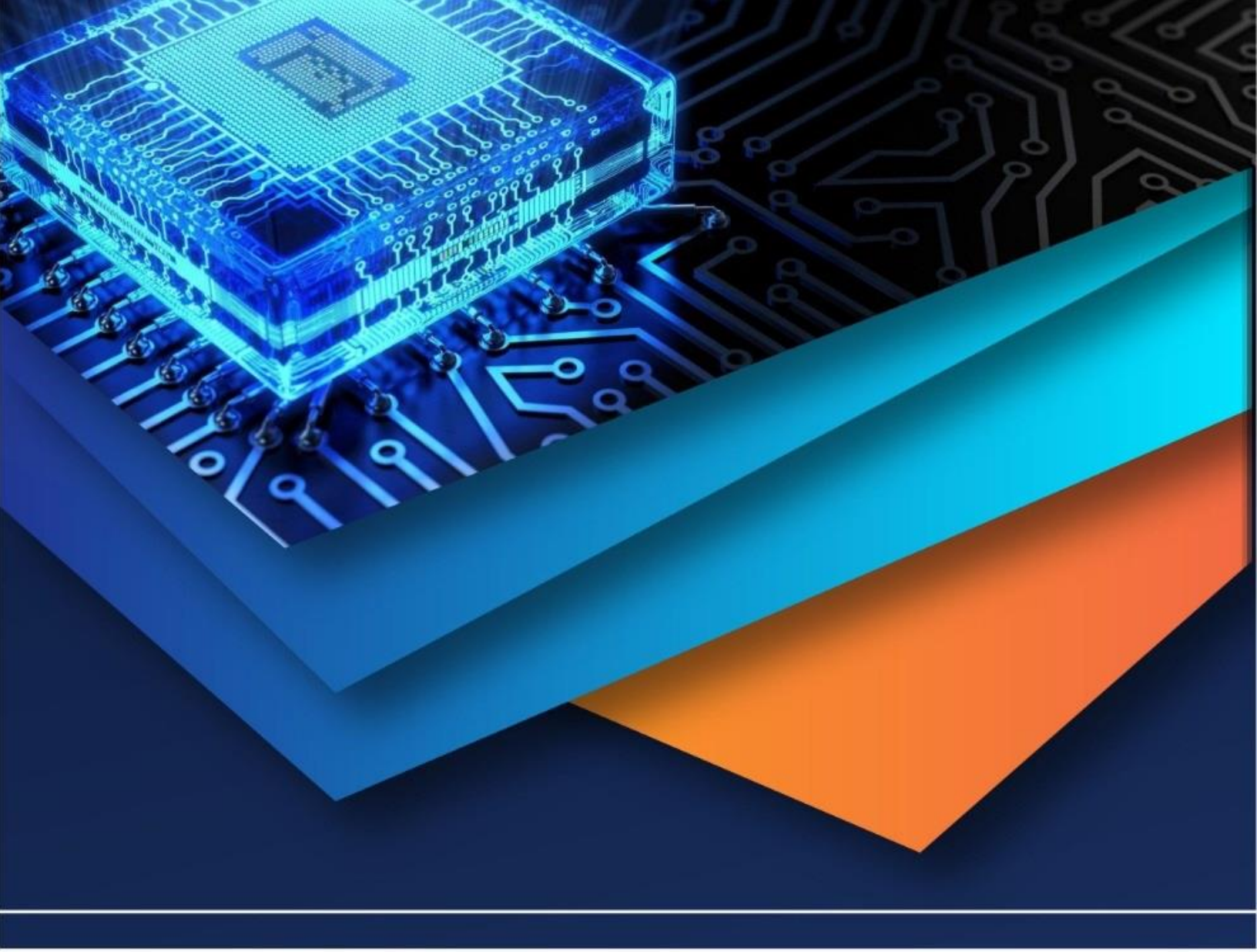
We wish to express our deepest gratitude to Prof. Mahendra Patil (H.O.D of Computer Engineering) at Atharva College of Engineering for continuously motivating us to excel in the field of Computer Engineering and for guiding us by providing reviews and the necessary technical help regarding the information presented in this document.

©IJRASET: All Rights are Reserved

REFERENCES

[1] M. Aslam, R. N. Idrees, M. M. Baig, and M. A.Arshad, "Antihook shield against the software key loggers," in Proceedings of the National Conference of Emerging Technologies, 2004.)
[2] Tian, D. & Jia, X. & Chen, J. & Hu, C.. (2017). An online approach for kernel-level keylogger detection and defense. Journal of Information Science and Engineering. 33. 445-461. 10
[3] D. Le, C. Yue, T. Smart, and H. Wang, "Detecting kernel level keyloggers through dynamic taint analysis," College of William & Mary, Department of Computer Science, Williamsburg, VA, Tech. Rep. WM-CS-2008-05, May 2008.
[4] B. Cogswell and M. Russinovich, "Rootkitrevealer v1.71," 2006 (accessed May 8, 2010), http://technet.microsoft.com /en-us/sysinternals/bb897445.aspx.
[5] Keylogger Software Definition | Common Types of Keyloggers https://enterprise.comodo.com/keylogger-software-definition.php
[6] Keyloggers: How they work and how to detect them (Part 1)., http://www.securelist.com ; accessed Sept. 2009
[7] P. Mell, K. Kent, and J. Nusbaum, "Guide to malware incident prevention and handling," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. 800-83, November 2005.
[8] Difference Between Static Malware Analysis and Dynamic Malware Analysis. http://www.differencebetween.net/technology/difference-between-static-malware-analysis-and-dynamic-malware-analysis/
[9] O. Zaitsev." Skeleton keys: the purpose and applications of keyloggers"2009
[10] What's the Difference Between Hardware Keylogger and Software Keylogger. https://www.easemon.com/whats-the-differences-between-hardware-keylogger-and-keylogger-software.html
[11] S. S. a. Anith."Detecting keylogger based on traffic analysis with periodic behavior"PSG College of Technology, Coimbatore, India.2011
[12] F. Hasani. 2011. The Secrets in the Keylogger. http://www.itknowledge24.com /the_secrets_in_keyloggers.pdf
[13] C. a. Solms, "Implementing Rootkits to address operating system vulnerabilities," presented at the. Academy of computer science and software engineering , Universtiy of Johannesburg.Johannesburg, South Africa., 2011.
[14] Baliga, L. Iftode and X. Chen, "Automated containment of rootkits Attacks, " Computers & Security, vol. 27, Issues 7-8, pp. 323-334, 2008.
[15] P. Mell, K. Kent, and J. Nusbaum, "Guide to malware incident prevention and handling," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. 800-83, November 2005.
[16] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu, "The ghost in the browser analysis of web-based malware," in HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets. Berkeley, CA, USA: USENIX Association, 2007, pp. 4–4
[17] T. Thornburgh, "Social engineering: the 'dark art'," in InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development. Kennesaw, Georgia: ACM, 2004.
[18] Working and Types of Keylogger https://www.kaspersky.co.in/resource-center/definitions/keylogger
[19] S. S. a. Anith."Detecting keylogger based on traffic analysis with periodic behavior"PSG College of Technology, Coimbatore, India.2011
[20] T. Olzak." Keystroke Logging Keylogging" Erudio Security, LLC. 2008.
[21] Zhuang, L, Zhou, F. & Tygar, J.D. (2005). "Keyboard acoustic emanations Revisited". Retrieved 2011 from http://www.cs.berkeley.edu/~zf/papers/keyboard-ccs05.pdf

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)