International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

Survey on Security Detection Techniques Using Keylogger

Shreya Jaiswal[1], Prof. B. Jana[2]

[1]Research Schaller, SHEAT Group of Institutions, Varanasi, India

[2]Professor and head, SHEAT Group of Institutions, Varanasi, India

ARTICLEINFO

Article History:

Accepted: 05 Sep 2023

Published: 16 Sep 2023

Publication Issue

Volume 9, Issue 5

September-October-2023

Page Number

209-215

ABSTRACT

Keyloggers are kind of a rootkit malware that catch composed keystroke occasions of the console and save into log record, hence, it can capture delicate data, for example, usernames, PINs, and passwords, in this manner communicates into vindictive assailant without pulling in the consideration of clients. Keyloggers present a significant danger to deals and individual exercises such as E-business, internet banking, email talking, and framework information base. Antivirus programming that is ordinarily used to identify and eliminate known Keyloggers. Nonetheless, it can't recognize obscure Keyloggers. This paper presents an outline of Keyloggers programs, types, qualities of Keyloggers and philosophy they use. At last we will break down the current discovery procedures, and investigate a few proactive methods.

Keywords – Keyloggers, Rootkit Malware, Obscure Keyloggers, Antivirus Programming, Proactive Methods

I. INTRODUCTION

Cybercriminals have come up with many methods to commit malicious activities on user's system or network system with the objective of stealing sensitive information or personal data. Cybercriminals and hackers make use of key logging apps or software to steal passwords and confidential information. Keystroke logging, which is also called as key logging is used to records keystrokes that are entered on a keyboard. Passwords, PINs, credit card numbers, confidential texts and other information can be recorded and retrieved by a cybercriminal when typed on a keyboard of a hacked computer.

Key logging can be used by hackers for all kinds of criminal purposes. Hackers can easily get access to the banking accounts, Email accounts and other login account credentials by stealing password and lock owners out. The information they get can be used to steal money and to blackmail the owner. It can also be done by known person to deceive friend, colleagues at work and family members. The hacker can use this information as part of identity theft schemes to blackmail the owner for profit gain.

Keystroke logging is activity monitoring program that records the keys pressed of a keyboard and mouse clicking and save to a log file. It can be easily used to fetch the sensitive data like PINs, passwords, bank

details and other credential information without the knowledge of user and transmit into malicious attackers [1]. It can be major threat because we cannot identify the presence of Keyloggers on our system as it runs in background and also it does not appear in task manager in windows operating system.

The revolutionary capabilities of Internet have changed the way how we share files and information, send electronic mails, message exchange. The advancement in technology have large influence in our life. Internet has become a multidisciplinary tool. More than 40 percent of the world's population is connected to the internet according to internetlivestatus.com. Cyber criminals commit malicious activities to capture the confidential information from user's system without cracking into user's database or file server. Malware, which is also called as malicious software is any code or program which is written by hackers with the intent to cause damage to a system without the user's consent.

There are various types of malwares like viruses, Trojans, ransom ware, spywares, rootkit, botnets, etc. They harm the computer system or network by performing various functions like monitoring the user's activity without their consent, deleting and hiding sensitive data, data theft, etc. Keylogger is one of malware rootkits that record the user's activity without their knowledge [2].

Keyloggers can record whatever you do on your computer. The modern Keyloggers are highly sophisticated and more and more difficult to detect by anti-virus programs and anti-malware tools in the market. Keylogger detection and prevention is a challenging task for security managers. Unlike traditional viruses and worms, advanced Keyloggers are present which are near to impossible to detect.

Keylogger is basically a particular type of spyware that can record everything you type on your keyboard. Although it is a common tool for corporations, the information technology department of the corporation uses the key logging software for troubleshooting purpose or it is also used to keep an eye on employee's suspicious activity. Nevertheless, the major concern about Keyloggers is when some third party are behind them. When the third party breach our computer system, we don't know what type of Keylogger it is, and it can steal any kind of password we have entered, periodic take screen shots of the screen, record the web pages we have viewed, any instant messaging sessions, sent Emails, confidential financial information and then send all that data to the third parties. The sent data can be used by third parties for criminal purposes. Keyloggers is mainly categorized into two major categories-hardware Keylogger and the software Keylogger. Hardware Keylogger are easy to use as they are placed in the internal hardware of the computer itself or it can be secretly inserted in between the CPU and the keyboard wire. But to plant the hardware Keylogger, the cybercriminal has to have physical access to the computer system while no one is watching.

Unlike hardware Keyloggers, software Keyloggers can be easily introduced on victim's system. That is the main reason why software Keylogger is much more common. It doesn't harm the hardware of the system but it is definitely a threat to for business and personal activities. Before going deep into the study of key logging, we should have the knowledge of keyboard functioning and how they interface with other devices.

II. RELATED WORK

Malware recognition is frequently examined as being static or dynamic; static depends on mark discovery that requires malevolent mark present in the archive. The greatest disservice of this method is that it has nothing to do against novel Keyloggers. Dynamic location should be utilized to recognize key logging malware; conduct based identification was actualized. As Keyloggers consistently use Windows snares, Aslam et al.[3] examined subterranean insect snared shield that utilizes by hailing program that snared framework schedules that consistently focused by Keyloggers; However, it is simple for Keylogger designers to avoid

this location strategy by utilizing various techniques to log the client exercises other than utilizing Set Windows Hooked however.

Dynamic based location procedures or conduct based was proposed by Martignoni et al. [4] indicated the semantic hole between undeniable level conduct and their low-level agent PC, and accomplished generally for the exceptional layered engineering. This methodology is accustomed to demonstrating semantic hole through underlying hierarchic. Their model finder utilize dubious conduct component as contribution with framework expansive cycle execution for checking, so hailing dubious movement is perceived if an interaction's action intently coordinates the conduct particulars. In the interim Ortoline et al. [6] implemented Black-box way to deal with recognize the most well-known Keyloggers. Their model depended on conduct of the Keylogger by methods for keystroke to the I/O design shaped by Keyloggers.

A significant number of the powerful discovery instrument being executed and investigated, however it is difficult to identify Keyloggers precisely. Sreenivas et al. [7] recognized Keylogger by utilizing TAKD calculations that can undoubtedly incorporated into routine gadgets, for example, switch, door, firewall, IDS, etc. to improve its key logging identification. TAKD calculation fused peculiarity based recognition component and log based procedure to beat the issue of mark based identification.

Another helpful identification component is Taint information examination structure utilizes a host-based Intrusion Detection System (IDS) to corrupt, screen, and inspect the console information at the console gadget driver level. This structure plans to distinguish portion level Keyloggers that alters the ordinary progression of control information in the console drive to separate keystroke information occasions and afterward send back to the aggressor. Subsequently extraction happens while information goes along the chain of console gadget driver in the part [5].

Table 1 Summary of some related work

No	Paper Name and Author	Keylogger Detection Technique	Solution and Results	Remarks
1	Stefano at el. (2011). KLIMAX: Profiling Memory Write Patterns to Detect Keystroke-Harvesting Malware	Behavior based detection technique using KLIMAX: Kernel-Level Infrastructure for Memory and execution profiling.	Consider no bogus negatives when the keylogging conduct is set off inside the window of perception and can likewise be utilized in enormous scope malware investigation and order.	Malware avoidance procedures that disguise or defer data spillage are not worry for this discovery strategy.
2	Anith at el. (2011). Detecting keyloggers based on traffic analysis with periodic Behavior	Client level detection technique. Host and checkpoint levels techniques using signatures.	TAKD algorithm. Incorporation into directing gadgets, for example, gateway, router, IDS, firewall	There is no quantitative examination for unpredictable time spans
3	J. Fu at el. (2010). Detecting Software Keyloggers with Dendritic Cell	Dendritic Cell Algorithm implement a hook program to monitor API calls generated by	This method can differentiate the running Keylogger process from the normal processes with a high	Conduct of Keyloggers is equivalent to application s that snare the framework

	Algorithm.	running processes In the host and five signals to define the state of thesystem.	detection rate and a low false alarm rate.	message execution. All authentic applications that snare the framework would be distinguished as vindictive.
4	Le at el. (2008). Detecting Kernel Level Keyloggers Through Dynamic Taint Analysis	Host-based intrusion detection. dynamic taint analysis to detect kernel level Keyloggers	System can distinguish bit level keylogging that catch console driver, especially cushion and recognize their underlying drivers.	Integration with VMscope techniques is necessary
5	Aslam at el. (2004) Anti-Hook Shield against the Software Key Loggers.	Although, hook is the core of Keyloggers. So this paper presents anti-hook technique to scan all processes and	Can without much of a stretch found every single dubious interaction or documents, regardless of	This procedure requires a ton of calculation and the bogus positive rate is extremely

Working of Keyboards

Keyboard plays a pivotal role in Keyloggers. The keyboard contains microprocessor and controller circuitry. The controller circuitry is called as key matrix. It is basically a grid of circuits. Different keyboard manufacturers use different types of controller circuitry in their keyboard [8]. However, key codes remain the same. Whenever the user enters or hold a key, then the microprocessor recognizes and forward it to keyboard buffer given statement as shown in figure1.

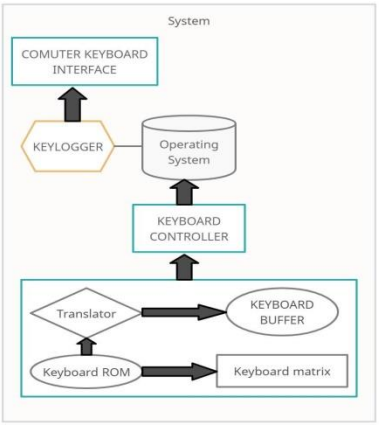

Figure 1 Block diagram of Keylogger working

The Keylogger intercept the data which is travelled between keyboard and operating system. Hence the information flow is not transferred into next hook procedure [9]. The keyboard connected with other devices using wired connection such as PS2 standard or a wireless connection such as USB connector which is more common nowadays. Now we have the understanding of keyboard operation, next let us look into the working of keylogging.

Working of Keylogger

The work of Keylogger is to sniff out the keystrokes without affecting the working of computer systems. Keylogger consists of hardware tools or software tools or the combination of both in order to capture the data or information which get stored in the log system.

The two major flavors of Keyloggers are hardware-based or software-based Keylogger. Hardware- based Keyloggers can be embedded in the CPU port, or as an unnoticeable plugin between the CPU and the keyboard so that it can interpret all the signal sent from keyboard. But the major problem is the physical presence of cybercriminal is required in order to connect the hardware Keylogger to the system. Unlike hardware-based Keyloggers, software types are easy to introduce and to install on the user's device without

making much effort. That's the only reason software Keyloggers are much preferable.

Software-Based Keylogger

A software Keylogger is just a piece of code or a program that hooks into the OS and interrupts keypress events. For that to happen all we need to do is install a global keyboard hook. Thus, whenever the keys are pressed, it will get stored as a log file in the system without the user's knowledge.

We can download the log files as text files, or add FTP (File Transfer Protocol) credentials to send this log file to the third parties to FTP server or we can also email it to the attacker given statement as shown in figure2.

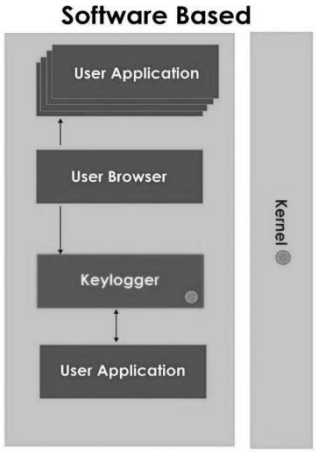

Figure 2 Software Based Keylogger Description

Hardware-Based Keylogger

A hardware-based Keylogger is plugged in between the keyboard and the CPU box via a PS/2 or USB connection. It contains key matrix which monitor a keyboard's USB or PS/2 connection, filters keystroke data, and record the data to the internal memory.

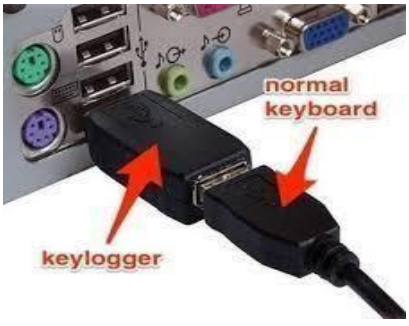

Figure 3 Representation of Hardware Based Keylogger

They don't depend upon any software being installed as they function at hardware level in a computer system. The hardware Keyloggers cannot be detected by the software running on the computer like anti-virus software and security scanners. Unlike software Keylogger, it does not require any driver or any kind of software to work. Its installation is easy and can be done in a few seconds.

These kinds of Keyloggers are used only with desktop computers or the systems which include a separate keyboard connected by a cable. We can easily notice them. On the other side, if we don't detect them then there is little, we can do about them since the computer is not even aware, they are there. Sometimes the spy agencies and the like use similar devices to check the system or web activities for a reason Representation in figure3.

Detection of Keylogger infection

Keyloggers taint PC framework similarly that other malware does. These Keyloggers get introduced on a framework when we click on record connections which get through an obscure source or address. The cybercriminals or aggressors utilize social designing or phishing methods. The connections we get can come to us by some obscure spam Email address, through an instant message from an irregular number, a spam message, through some tainted or unreliable site, by introducing some noxious programming. Likewise, it doesn't come alone. The other malwares alongside the Keylogger bring into the framework by a similar Trojan which likewise harm the framework and exceptionally powerless against the framework and the security of the information. More often than not, the equipment Keylogger is presented in the framework by some known individual or in the event that somebody accesses our opened PC framework.

In a large portion of the cases, the client couldn't say whether there is any Keylogger in foundation. Likewise, we can casualty to Keyloggers when we present any free programming, administrations or apparatuses. These can undoubtedly pollute our PC frameworks. At times, the casualty gets an admonition which alert about a contamination on our framework. More often than not, the Keyloggers are concealed in the sites we visit when riding the web [11].

In some cases, it additionally gives a proposal to fix an infection by downloading a free antivirus application. Around then, it would be better close all windows or the program we use without clicking. It is consistently a decent practice to abstain from clicking anything which comes from an obscure source.

Additionally, we should remember that Keylogger works out of sight. Thus, it is difficult to discover that each key we have squeezed and all our movement is recorded and shipped off the outsiders or it very well may be utilized for some coercing or unlawful reason.

Some Keyloggers work to record each program, site or window that we open on our PC framework. In the event that we are dynamic web clients, the vast majority of our web file requests, the destinations we visit consistently or some other web development can be recorded.

There are number of methods of presenting Keylogger in our gadget. Some third individual can straightforwardly introduce them and make them run in foundation or, in all likelihood we can download it unconsciously from the noxious website which is tainted. They are additionally a lot of routes out there to introduce a Keylogger into the far off framework. Keyloggers could undoubtedly keep away from the web access limitation by controlling the sites and they use it to convey the recorded information [10].

They have both moral and exploitative applications. These days, there are enormous number of situations where the malignant projects are utilized for criminal operations, for example, spam messages which may incorporate potential dangers, for example, infections, worms, content to run Keyloggers or exercises like fraud, data robbery and security penetrate. Frequently there are circumstances where cybercriminals take another person's work and offer it as their own.

For the most part, Keyloggers are presented by malware, yet they additionally have legal applications where they may likewise be introduced by managers who need to screen their representatives, guardians who need to watch out for their youngsters' action or desirous mates. In Information Technology Department of each partnership, a Keylogger is an extraordinary device to keep up the security of the PC frameworks over the organization. In organization, the log records are created for each framework and just the administrator and the top of the information security office has the admittance to investigate it if important. Some Keyloggers have the element to advise the administrator when there is some ill- conceived conduct in the framework as shown in figure 4, which represents the increasing incidents of cyber-attack over the years [12].

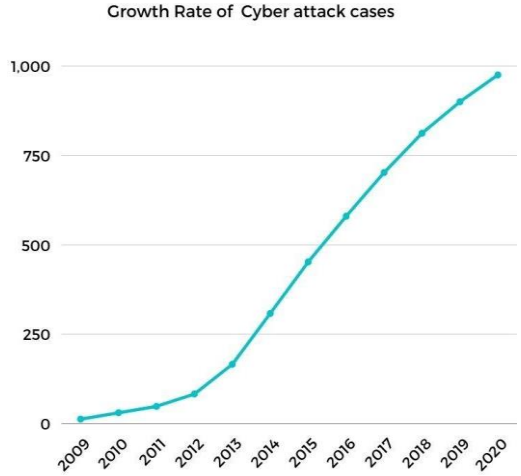

Figure 4 Shows cases of cyber-attack over the years

III.PREVENTION TECHNIQUE

There are different ways to check if the malicious Keyloggers hide on our computer system and steal some confidential or security related information such as passwords, PINs, or bank accounts.

There is some anti-malware software which can help in detecting and removing Keyloggers. The other way is to examine the running process via the Task Manager in Windows OS to check for some unusual .exe processes that are running in the background. Also, we should check all the start-up entries for anything unusual. Some Keyloggers which enter through browsers, are generally called browser Keyloggers. We should uninstall that browser and install a fresh new version.

Hardware Keyloggers are plugged at the end of our keyboard's wire in between CPU and wire. If you are some really important person or perhaps you are working on some confidential and important data,

might be someone professional spying on you. In such cases, you should backup your data, wipe your PC and reinstall operating system. We should take the necessary precautions to make sure our PC isn't invaded by hackers or cybercriminals. We should prefer a system with proactive protection to detect any malicious program or activity. The best way is to use virtual keyboard. By using virtual keyboard, they cannot steal our credentials [13]. Also, we should avoid entering any personal information on suspicious websites.

The presence of Keylogger doesn't affect computer working and if it is sending data to a network or a third party, it disguises itself as normal files or traffic. There are Keyloggers present which can reinstall themselves if the user is able to find it and remove it. We can observe in a number of ways if there is some unusual activity like there could be a slowdown or the system is not working properly or slowing down the processes. The best way to protect our computer systems from Keyloggers is to scan our system regularly with some antivirus programs or anti- malware tools. Another protection measure against a Keylogger is to detach the system from the internet connection when you see any unusual activity in the PC.

Antivirus software are not beneficial against Key loggers, they are unable to detect key logging software. We can stop Keyloggers by using keyboard encryption program which generally encrypts keystroke data and route it directly to the web browser or desktop through a secure medium that is invisible to Keyloggers.

Merits of Keylogger

- In IT firms it plays a prominent role to troubleshoot technical or network issues.
- In security agencies it is used to track suspect and collect evidence, which helps in preventing major national threats.
- It helps an individual who wants to track all the information in his personal computer in case someone uses it.
- It plays a very helpful role for parents to track their children activities on the computer.

Demerits of Keylogger

- Use of Keylogger is directly a matter of concern about the computer privacy.
- When Keylogger detection is done by malicious users they specifically read out login data such as names and passwords, and transmit them to unauthorized third parties.
- Keyloggers are the ideal devices for modern undercover work or for getting to private corporate information. They can harm business connections, monetary standing, and notoriety therefore, they can even reason an association to break significant bits of enactment, for example, the Data Protection.

IV.CONCLUSION

In this paper, we discussed about the keystroke logging, characteristics of Keylogger and different type of Keyloggers available. We also explored different ways Keylogger spread themselves. Finally, we analyzed how to detect a Keylogger and discussed some prevention techniques for Keylogger spyware attack capable of stealing the credential and confidential data from the victim's computer system. Our main aim is to be aware of the existing threats, how to recognize them and take the countermeasures against them

V. REFERENCES

[1] Working of Keyloggers available at http://securelist.com/analysis/publications/36138/keyloggers-how-theywork-and-how-to-detect-them-part-1.

[2] C.a.Rajendra. "Keylogger in Cybersecurity Education". Rechester Institute of Technology, Rechester, New York, USA.

[3] 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.

[4] E. S. L. Martignoni, M. Fredrikson, S. Jha, and J. C. Mitchell, “A layered architecture for detecting malicious behaviors,”.Heidelberg.2008

[5] C. Y. D. Le, T. Smart, and H. Wang, “Detecting kernel level keyloggers through dynamic taint analysis, " College of William & Mary, Department of Computer Science, illiamsburg, 2008.

[6] C. G. S.Ortani, and Crispo. “Bait your Hook: A novel Detection technique for keylogger”. University of Trento, Via Sommarive.Trento, Italy.2010.

[7] S. S. A. Anith. “Detecting keylogger based on traffic analysis with periodic behavior,” P.S.G. College of Technology, Coimbatore, India. 2011

[8] Davis, Andy. “Hardware Keylogger Detection,” White paper (2007).

[9] Wilson, T. V. & Tyson, J. (2008). “How computer keyboards work”.HowStuffWorks.com. Retrieved 2011 from. http://computer.howstuffworks.com/keyboard.htm.

[10] Overview of detecting key loggers: http://wwwsandboxie.com/

[11] gphandlahdpffmccakmbngmbjnjiiahp/https://www.ijcst.org/Volume5/Issue2/p5_5_2.pdf

[12] https://purplesec.us/resources/cyber-security-statistics/

[13] www.researchgate.net/publication/228797653_Keystroke_logging_keylogging

Cite this article as :

Shreya Jaiswal, Prof. B. Jana, "Survey on Security Detection Techniques Using Keylogger", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 5, pp.209-215, September-October-2023.