IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12336

Keylogger

Allamsetti Baladithya[1], Dr.Rengarajan A[2]

Student, MCA, Jain (Deemed-to-be-University), Bengaluru, India[1]

Professor, MCA, Jain (Deemed-to-be-University), Bengaluru, India[2]

Abstract: A keylogger is a type of software or hardware device that enables the recording of all keystrokes made on a computer or mobile device keyboard. Essentially, it allows for the monitoring and tracking of user activity, which can be used for security and surveillance purposes. Keyloggers have both legitimate and illegitimate uses. For example, some organizations use them to monitor employee activity, while others use them to steal sensitive information such as login credentials, credit card numbers, and other personal data. Unfortunately, keyloggers can be used for malicious purposes, as well, which means they can pose a significant security risk to individuals and organizations alike. One of the primary challenges with keyloggers is their ability to operate surreptitiously. They are designed to work in the background, without drawing any attention to themselves, and typically do not exhibit any visible signs of their presence. As a result, they can be challenging to detect and remove from an infected system.

Keywords: Keylogger, hooking, signature-based, malware rootkits, anomaly based, OS, API.

I. INTRODUCTION

Keyloggers are a type of rootkit malware that can secretly intercept a user's keystrokes on a keyboard. These programs are primarily designed to capture and record sensitive information entered by users, such as passwords, credit card numbers, and personal identification numbers. By logging keystrokes, attackers can easily access and exploit confidential information without the user's knowledge or consent. Because the keyboard is a primary method of inputting textual and numerical information on a computer, keyloggers can easily retrieve and access valuable information by logging keystrokes. Although keyloggers do not possess any inherent intelligence, they are able to record every single keyboard event and application that the user interacts with. This allows attackers to obtain critical information such as passwords, user IDs, document contents, and other sensitive data without needing to crack database or file server.

Nowadays, keylogging poses a serious threat to the security and privacy of computer systems. These programs are typically designed to operate in a stealthy manner, making them difficult to detect by many antivirus software programs. As a result, users often have no way of knowing whether or not they are being monitored by a keylogger, leaving them vulnerable to identity theft and other forms of cybercrime. This paper provides an overview of the different types of keyloggers, how they are injected into a system, and current detection techniques. Section 2 discusses the mechanics of how keyloggers work, while Section 3 outlines related work in the field. Section 4 categorizes different types of keylogger software, and Section 5 evaluates the methodology of developing keylogger software systems. Finally, Section 6 analyzes current detection techniques for software keyloggers and proposes proactive steps that can be taken to prevent keylogger attacks. The methodology employed by keyloggers varies widely depending on the type and characteristics of the program. For example, some keyloggers may use system hooks to capture keystrokes, while others may employ kernel-level rootkit techniques to hide their presence on a system. Some keyloggers may even use remote access tools (RATs) to gain control of a victim's computer and capture keystrokes.

A real-time example of a keylogger attack is the case study of Blackberry. In 2016, the company suffered a major security breach that compromised the personal data of millions of users, including their email addresses, passwords, and other sensitive information. The attack was reportedly carried out using a keylogger that was able to bypass the company's security measures and evade detection for an extended period. Current detection techniques for keyloggers include heuristic analysis, behaviour-based analysis, and signature-based analysis. However, these methods are often ineffective against new or unknown keyloggers, which can use sophisticated evasion techniques to avoid detection. As a result, proactive measures such as using virtual keyboards, two-factor authentication, and regularly updating software and security protocols can help prevent keylogger attacks and protect sensitive information from theft. In summary, keyloggers are a type of malware that can surreptitiously capture a user's keystrokes and transmit sensitive information to an attacker. They pose a significant threat to the security and privacy of computer systems, and detecting them can be challenging. As such, it is essential that users remain vigilant and take proactive measures to protect their personal information from keylogger attacks.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12336

II. LITERATURE REVIEW

Keyloggers have both legitimate and illegal applications. Attackers often use keyloggers to obtain sensitive information belonging to individuals or organizations. With the aid of keyloggers, attackers have previously compromised the credit card details of many individuals. This makes keyloggers one of the most dangerous forms of spyware to date, according to Strahija (2003).

A malicious program with keystroke logging feature can be a threat to online banking systems. Any errors in implementing the system's functions can potentially give an attacker access to a user's bank account. To prevent such attacks, the system could ask for a completely new set of characters or alphabets every time a user logs in, regardless of whether the login is successful. However, the vulnerability cannot be eliminated merely by allowing codes to include a greater variety of characters, as the attack is based on individual positions, not specific character patterns. Increasing the allowable length of verification codes may slow down the attack, but it will not change the fundamental situation. In conclusion, implementing anti-keylogging systems in this manner effectively nullifies their entire purpose, according to S. P. Goring in 2007.

To effectively detect and prevent keyloggers, it is important for individuals to have a comprehensive understanding of what keyloggers are, how they are implemented, and the various approaches used to combat them. This paper aims to provide an overview of different algorithms proposed to address the problem of keylogging, as well as the limitations of these proposed systems. Keylogging is a compromising security technique that can be executed in various ways. One such way is when attackers gain physical access to a user's computer device and wiretap the physical hardware, such as the keyboard, in order to collect valuable data. This method relies on the actual physical properties of the hardware, such as the sound transmission generated when a user types, or the electromagnetic radiation emitted by a wireless keyboard (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).

Software keyloggers continue to dominate hardware keyloggers. In this exposition top 4 Windows based software keyloggers (2020) are compared with Adv_Klogger, which is presented in the research paper. The three keyloggers are: Spyrix free Keylogger, KidInspector Keylogger and Free Keylogger. The basis of comparison is the features that are incorporated in the keyloggers and the CPU usage. All the keyloggers had three features in common which are logging keys, screenshot functionality and remote monitoring. Contains detailed analysis of all five keyloggers and what all features they entail. provides a visual representation of how keyloggers differ based on number of features they contain. The keyloggers are widely used and differ because of functionalities they contain. The more functions a keylogger has the more useful it is to a user or a company. As illustrated, Adv_Klogger incorporates more features than the other keyloggers. The second parameter which is used here to compare the keyloggers is the CPU usage. One of the easiest ways to detect a malicious activity is through the CPU and memory usage contains a graphical representation of keyloggers differ by their CPU usage. The data in the graph is noted by monitoring keylogger execution for a period and calculating the average of how high the usage becomes while the program is being executed. As it is clearly demonstrated that the Adv_Klogger does not show much spike in the usage and cannot be easily noticed.

III. HOW KEYBOARD WORKS

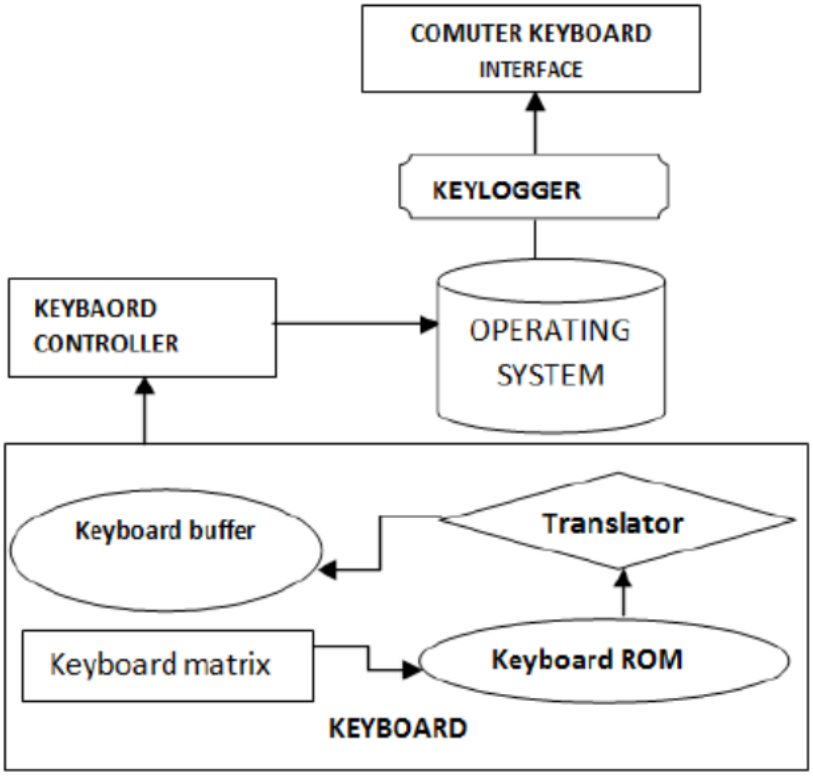
Most keyloggers target the keyboard as it is the primary input device of a computer. The keyboard is made up of a key matrix, which is a circuit with keys arranged in a grid pattern. Depending on the manufacturer, there are different types of key matrices. When a user presses a key, the circuit is closed and the keyboard processor and ROM detect this event. The processor then translates the circuit location to a character or control code and sends it to the keyboard buffer. The keyboard buffer stores the input characters until they are processed by the operating system or application.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12336



[Fig. 1 : Shows how Keyboard works]

As the user types on the keyboard, the input data is sent to the computer's keyboard controller for processing. The controller then sends the input data to the operating system for further processing. This data exchange process between the keyboard and the operating system can be intercepted by keyloggers, enabling them to capture all input data. The keylogger sits between the keyboard and the operating system, and is able to capture the input data before it is passed on to the operating system. This allows the keylogger to capture every keystroke entered by the user.

Types of Keyloggers

There are various types of keyloggers, which can be classified into four main categories based on their method of data capture: hardware, acoustic, wireless intercept, and software keyloggers. Although these categories have different methods of capturing information, they all share a common characteristic of saving sensitive data and information in a log file.

Hardware keylogger

A hardware keylogger is a physical device that can be attached to the computer's keyboard to capture keystrokes. The keylogger is connected between the keyboard and the computer through one of two connection methods. The first method is to directly connect the keylogger between the keyboard and the computer, as is the case with PS/2 and USB keyloggers. This allows the keylogger to intercept all keystrokes before they reach the computer's operating system.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12336

[Fig 2: shows keylogger of PS/2]

Another method of keylogging is wireless intercept, which involves intercepting wireless signals between a keyboard and a receiver. This type of keylogger requires specialized equipment and is more difficult to implement than other types of keyloggers. Software keyloggers, on the other hand, are programs that can be installed on a computer to capture keystrokes and other activities. They can be more difficult to detect than hardware keyloggers, as they do not require physical access to the computer. Each type of keylogger has its own unique set of advantages and disadvantages, depending on the specific situation in which it is being used. However, they all share the common trait of capturing and saving sensitive data and information in a log file.

Wireless keylogger

A wireless keylogger is a type of keylogger that uses Bluetooth interfaces to capture data and transfer it to a log file, typically up to a distance of 100 meters. Its main objective is to intercept packets transmitted from wireless keyboards that use a 27 MHz RF connection of encrypted RF transported keystroke characters. However, the downside is that this type of keylogger requires a receiver/antenna that is relatively close to the target area of work.

[Fig 3 : Bluetooth-accessible keylogger]

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12336

Software keylogger

Software keylogger is a type of keylogger that intercepts the data between the keyboard and the operating system, records keystroke events, and then sends the data to the attacker who installed it. The majority of keyloggers are software-based, as they can easily be installed on a target system. Windows operating system has various event mechanisms, such as the keyboard driver, which translates keyboard events into Windows messages, like WM_KEYDOWN, and places them into a message queue. The operating system then sends these messages to the active window's message queue. The active window's thread polls this queue and sends the message to the window procedure.

IV. RELATED WORKS

Malware detection methods can be categorized as either static or dynamic. Static detection relies on signature detection to detect known malicious software, but it is not effective against new, unknown keyloggers. Dynamic detection, on the other hand, can detect keylogging malware through behavioural-based techniques. Researchers have proposed various dynamic detection techniques, such as behavioural-based detection, semantic gap modelling, and black-box approaches. However, accurately detecting keyloggers remains a challenge.

One proposed detection mechanism is the Taint data analysis framework, which 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 modify the normal flow of control data in the keyboard driver to extract keystroke data events and transmit them back to the attacker.

To address the limitations of signature-based detection, Aslam et al. discussed an ant-hooked shield that flags programs that hook system routines targeted by keyloggers. Martignonietal. proposed a dynamic-based detection technique that models the semantic gap between high-level behaviour and their low-level computer representation, achieving largely unique layered architecture. Sreenivas et al. developed TAKD algorithms that can be easily integrated into routine devices to improve keylogging detection, while Le et al. proposed a detection model that detects keyloggers by examining the flow of data in the kernel

Impact of Keyloggers

Keyloggers are malicious programs that are specifically designed to capture all keystrokes entered by users on their computer keyboards. They can easily obtain sensitive information such as passwords, personal details, and financial information. Unlike viruses and worms, keyloggers can run on a system undetected for a long time, sharing the same resources with legitimate programs. They come in different types and forms, but they all pose a great threat to user privacy and security. One of the biggest challenges with keyloggers is that they can remain hidden even when doing a directory listing of hidden files. They are also capable of intercepting and decrypting information passed through the internet, allowing attackers to easily access sensitive data. To tackle this issue, security experts are now focusing on kernel keyloggers which target the operating system kernel using hooking mechanisms. Therefore, software keyloggers have become a major concern for users and organizations alike.

V. METHODOLOGY : KEYLOGGER SYSTEM

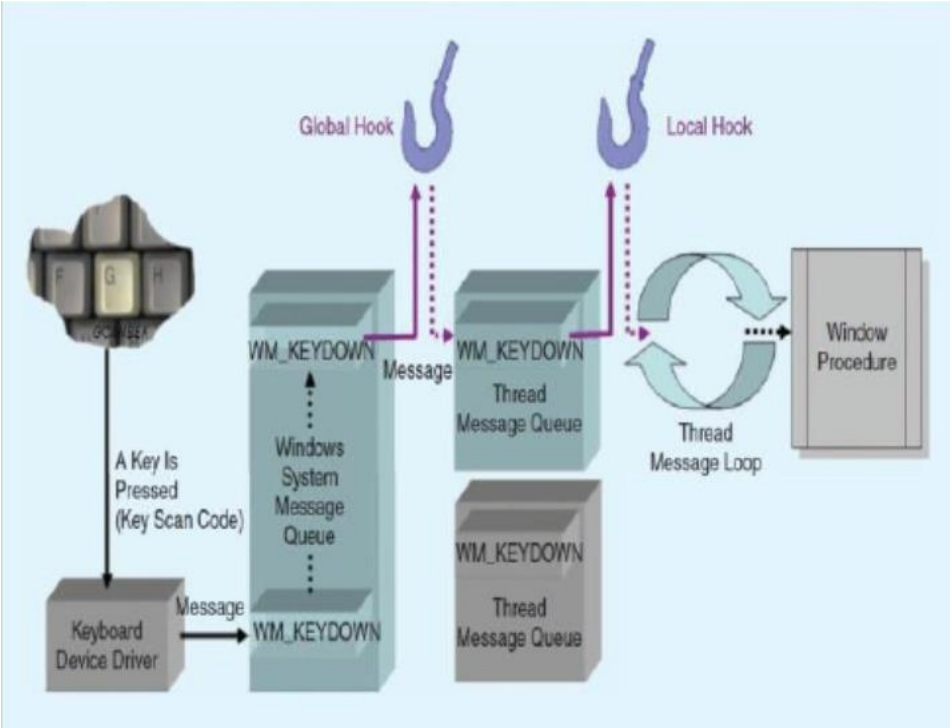
There are various methods for developing keylogger systems, and three of the main ones are the Windows Keyboard Hook method, the Keyboard State Table method, and the Kernel-Based Keyboard Filter Driver method. Among these, the Windows Keyboard Hook method is a widely used technique that leverages the operating system's functions to enable hook-based keyloggers to monitor keyboard activity. This method involves the OS recording any key presses and registering the application that performs the monitoring, after which any message passing through the mechanism is first approved by the monitoring application before being delivered to its original target. Due to its effectiveness, this technique is commonly employed by keyloggers for capturing keystrokes.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12336



[Fig.4 : shows Block diagram hook mechanism]

Windows message hooks can be classified into two types: global hook and local hook. The former checks system-wide messages, while the latter monitors application-specific messages. Keyboard hook is a type of local hook that can read all keyboard messages and pass them to the next hook procedure in a chain. It can also modify the original message and interrupt the flow of the message by not passing it to the next hook procedure.

On the other hand, the Keyboard State Table method employs a table that contains the status of 256 virtual keys. This table is used by applications that utilize a window interface to determine the states of the key, whether it is up or down. For example, when a key is pressed with Ctrl or Shift key, the GetKeyboardState API function can be used by keyloggers to expose the keystroke information. They can also add their thread to the top-level of thread message loop of the window using the AttachThreadInput API.

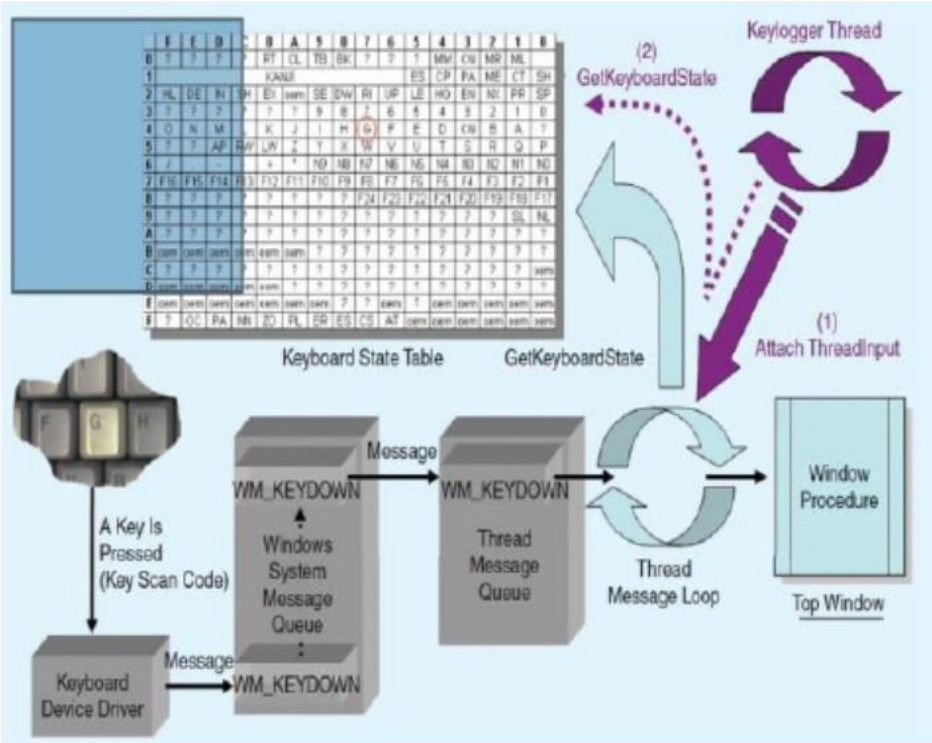
In summary, there are two main methods for developing keylogger systems: Windows Keyboard Hook method and Keyboard State Table method. While the former uses hooks to monitor keyboard messages, the latter uses a table to determine the status of virtual keys. Both methods can be employed by keyloggers to capture keystroke information and expose it to unauthorized third parties.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12336



[Fig.5 : shows keyboard stat table method]

Compared to other keylogging methods, the Kernel-Based Keyboard Filter Driver method operates at the kernel level of the operating system, making it more difficult to detect. However, to install this type of keylogger on a target machine, the user must have administrator privileges. Once installed, the keylogger is able to intercept keystrokes and data before they even reach the operating system, as it has been installed as a keyboard filter driver.

This method of keylogging is particularly stealthy, as it operates at such a low level of the system and can capture data in real-time without being detected. However, due to the level of access required to install this type of keylogger, it is typically used by advanced attackers or insiders with access to the target system.

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 information 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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12336

VI. ANALYZING CURRENT DETECTION TECHNIQUES

The detection and prevention of malware is not foolproof, particularly in cases where rootkits have modified the operating system. As such, various keylogger detector techniques have been developed, including both application-based and kernel-based methods, as well as proactive techniques.

Application-based keylogger detectors are designed to detect spyware keyloggers specifically in Microsoft Windows, which is used by the vast majority of personal computers. Hook-based and signature-based techniques are used to detect these keyloggers. Hook-based techniques rely on system message-handling mechanisms and observe keystroke data passing between hook procedures, allowing for the detection of a keylogger interception. This technique is widely used and has been implemented in HookFinder and System Virginity Verifier. Signature-based techniques, on the other hand, rely on file signatures to monitor modifications of files such as dynamic linked libraries and registry entries that are inserted into the system by keyloggers. Application keyloggers whose signatures are found in the database are flagged as malicious.

Behavior-based detection is another important category of detection method. Instead of looking for specific file signatures, this technique scrutinizes the behavior of the application. However, this method has a high false positive rate due to the fact that new keyloggers often exhibit behaviors of stealthiness and mimic legitimate applications, making it possible for them to evade detection.

VII . CONCLUSION AND FUTURE RESEARCH

Keyloggers pose a significant threat to users' sensitive data, such as login credentials and banking information. While some keyloggers serve legitimate purposes, many are created and used maliciously. This article explores the various types of keyloggers and the tactics they employ to remain undetected on a user's system. Additionally, it examines the current state of keylogging technology and highlights both detection and prevention techniques.

Preventing and detecting keylogging technology is similar to protecting against other forms of malicious code or threats. It involves maintaining awareness, monitoring regularly, and implementing layered defenses. It is critical to understand the threat posed by keyloggers, how they operate, and the various methods used to detect and mitigate them. Organizations should incorporate keylogger detection and countermeasures as part of their incident response plan.

Future work may involve improving the TAKD algorithm, which is based on traffic analysis and periodic behavior that has a fixed time interval for communication between source and destination. For example, an attacker may choose to communicate every 15 minutes. Enhancements to this detection algorithm may provide more accurate quantitative analysis for irregular time intervals.

VIII. REFERENCES

[1] In 2005, Chieh-Ning Lien from the UCLA Computer Science Department in Los Angeles, USA, published a paper titled "Keylogger Defender" which discussed techniques for detecting and preventing keyloggers from infiltrating computer systems.

[2] In 2011, Solms presented a paper on implementing rootkits as a defense mechanism against vulnerabilities in operating systems at the Academy of Computer Science and Software Engineering at the University of Johannesburg in South Africa.

[3] Aslam et al. presented a paper at the National Conference of Emerging Technologies in 2004, which discussed an antihook shield designed to protect against software keyloggers.

[4] In 2008, Martignoni et al. proposed a layered architecture for detecting malicious behaviors, which could be used to identify keyloggers on computer systems.

[5] Le et al. from the College of William & Mary's Department of Computer Science in Williamsburg, USA, presented a paper in 2008 that discussed a technique for detecting kernel-level keyloggers using dynamic taint analysis.

[6] Ortani and Crispo from the University of Trento in Italy proposed a novel detection technique for keyloggers in 2010, which involved baiting the keylogger with fake keystrokes and analyzing its response.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12336

[7] Anith from PSG College of Technology in Coimbatore, India, presented a paper in 2011 which discussed detecting keyloggers based on traffic analysis and periodic behavior.

[8] Rajendra from the Rochester Institute of Technology in New York, USA, wrote a paper on the use of keyloggers in cybersecurity education.

[9] Olzak from Erudio Security, LLC published a paper in 2008 on keystroke logging and keylogging, which discussed the risks posed by keyloggers and techniques for detecting and removing them.

[10] Canbek from Istanbul Technical University in Turkey published a paper in 2009 titled "Keylogger Increasing Threats to Computer Security and Privacy," which highlighted the growing threat posed by keyloggers to computer security and privacy.

[11] Dedicated 2Spyware maintains a list of keyloggers and provides resources for their removal, as of September 2007.

[12] Zaitsev published a paper in 2009 titled "Skeleton Keys: The Purpose and Applications of Keyloggers," which discussed the use of keyloggers in different scenarios and the risks associated with their use.

[13] Vishnani and Mohandas from the National Institute of Technology Karnataka in India published a paper in 2005 that provided an in-depth analysis of keyloggers and their countermeasures.

[14] The website Securelist provides information on how keyloggers work and techniques for detecting them, as of September 2009.

[15] Aickelin and Al-Rubaiee from the University of Nottingham in the UK presented a paper in 2008 on detecting bots based on keylogging activities.

[16] Shetty presented data on operating system market share in 2007, which can help in understanding the potential impact of keyloggers on different operating systems.

[17] Rutkowska presented a paper in which she defined a roadmap for malware detection on Windows systems using a tool called the System Virginity Verifier.

[18] Yin et al. presented a paper in 2007 on a system called Panorama, which captures system-wide information flow for malware detection and analysis.

[19] CastleCops provides a list of freeware antirootkit tools that can be used to detect and remove keyloggers from computer systems.

[20] Mathur from Purdue University in Indiana, USA, published a survey of malware detection techniques in 2007, which included information on detecting keyloggers.