Borneo International Journal eISSN 2636-9826; Vol. 6 (1); 2023; 33-43
Published by *Majmuah Enterprise*
www.majmuah.com

Keylogger: The Unsung Hacking Weapon

ADI BADIOZAMAN BIN RUHANI, MOHAMAD FADLI BIN ZOLKIPLI
School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: adryunosuke@gmail.com, m.fadli.zolkipli@uum.edu.my| Tel: +601137150046, +60177247779 |

Received: February 21, 2023
Accepted: February 24, 2023
Online Published: March 01, 2023

Abstract

This paper provides an overview of keyloggers as a tool for hacking and the potential threats they pose to individuals and organizations. It explores the history of keyloggers, the types of keyloggers, how they work, and the different techniques used to detect and prevent keylogger attacks. The paper discusses the different types of keyloggers that exist, including hardware and software keyloggers, and explains how they can be used to steal sensitive data. The study also outlines the detection and prevention techniques used to combat keylogger attacks, such as anti-virus software, network traffic analysis, and biometric authentication. The effectiveness of each method is discussed, along with its limitations. The paper emphasizes the need for increased awareness and education on the risks of keylogger attacks and the importance of implementing best practices for information security. It also provides a literature review on keylogger attacks and discusses the future trends in combating keylogger threats, such as advanced encryption techniques, enhanced biometric authentication, and Threat Intelligence solutions. The study concludes that keylogger attacks are a growing threat and that organizations and individuals need to take necessary steps to protect their sensitive data. Overall, this paper serves as a comprehensive guide to understanding keyloggers as a tool for hacking and the measures that can be taken to prevent and detect keylogger attacks.

Keywords: keylogger, keystroke, malware, cybersecurity, threats, countermeasures

1. Introduction

Hacking attacks can occur on physical security, operating system, network, application and smartphone through various techniques such as social engineering, phishing, Denial-of-Service (DoS), SQL injection, Man-in-the-Middle (MitM) attack, password cracking and malicious programs (malware).

According to the data from (AV-Test, 2023), there have been 1,239,639,278 malware detections since 1984, and 8,637,398 new malware detections have been reported just in 2023. More than 450,000 brand-new malicious software programmes and potentially unwanted programmes (PUA) are logged daily, evaluated, categorised, and saved. The risk of this malware threat can no longer be avoided in the age of the borderless world, where numerous device types are connected and data exchange occurs frequently. In cyber-attacks, (Al-masalha *et al*., 2020) classifies malware as Syntactic attack which is considered a software application installed on a system without the user's consent for the purpose of stealing data. When talking about malware, the majority of us only mention Trojan horses, computer viruses, worms, ransomware, and adware but do not realise that keyloggers also fall under the same umbrella.

Keystroke logging was not created in the internet era, according to (Ingersoll, 2013; Interscan, n.d.) of its history. The most popular electric typewriter in the world was actually bugged by the Russians employing keystroke recorders as early as the middle of the 1970s, it was just been discovered. The Soviets were able to successfully install them in at least thirteen IBM Selectric computers located in the American embassy and consulate buildings. These machines could transmit radio bursts of encrypted keystrokes that were then delivered straight to the Kremlin. The bugged typewriters employed a technique known as "keystroke logging," which is the same term for a similar "listening" computer programme hackers and spies use to read a user's traffic.

It is concerning to see incidents of theft of private or sensitive data popping up all over the place. Keystroke logging also referred to as keylogging, is a technique used to capture keystrokes made on a keyboard. When entered on a compromised computer's keyboard, passwords, PIN codes, and other private data can be gathered and retrieved by a cybercriminal. (Tove, 2022) stated that according to a Symantec report, approximately 50% of malware is employed to gather personal information rather than cause computer damage. In line with that, Kaspersky Labs has detected over 300 different kinds of keyloggers, and the SANS Institute believes that roughly 10 million PCs in the United States are infected with keylogging malware. These figures demonstrate that keyloggers are a very prevalent type of malware that is becoming more and more popular.

Anti-virus software and anti-malware solutions are finding it increasingly difficult to identify the sophisticated recent keyloggers. Unlike conventional viruses and worms, enhanced keyloggers exist and are nearly difficult to detect, making keylogger detection and prevention a tough challenge. The main issue with keyloggers, though, is when a third party is responsible for them. This third-party breaches into the computer system and steals all kinds of information before sending it to other parties that can utilise it for illegal activities (Proactive *et al.*, 2021).

There have been several measures put in place, including the use of technology to identify and prevent it as well as the enforcement of laws and policies. That strategy, but, hasn't yet been able to resolve this problem. In this study, we concentrate on investigating keyloggers, one of the malware risks, in order to comprehend attacks and countermeasures. This study offers an overview of keylogger attack methods, defensive strategies, and emerging approaches. The purpose of this paper is to increase public awareness about keylogger intrusions and to encourage more research in this area by both the industry and academia. The rest of the paper is structured as follows: Section 2 presents an overview, Section 3 summarizes the different types of keylogger threats and approaches being studied, Section 4 describes the traditional methods currently being used to defend against keylogger threats, Section 5 outlines the future trend in countering keylogger threats which includes a strong defence concept, and finally, Section 6 presents the conclusions and highlights future work.

2. Overview

This study uses a historical review method to demonstrate familiarity with contemporary developments and to determine the most likely directions for further study. As our main sources, we searched the following databases for research papers: ACM Digital Library, EmeraldInsight, Elsevier - Scopus, Elsevier: ScienceDirect, Google Scholar, ScienceGate, and ResearchGate. The chosen research articles mostly were released between 2018 and 2023. Keyloggers have become a major threat to computer security in recent years. The use of keyloggers has increased due to the ease of installation and their effectiveness in stealing sensitive information. Keyloggers can be either hardware-based or software-based, with the latter being more prevalent. Software keyloggers can be installed on a target system through malicious software downloads or phishing attacks. They are generally easier to develop and detect compared to hardware keyloggers (Engineering, 2020)

A keylogger is a type of malware (hardware or software) that has the ability to log each keystroke entered on an infected device. The keylogger is capable of recording private information. As a result, it poses a serious risk to cybersecurity since it enables cybercriminals to access private data without authorization and utilise it for nefarious objectives like identity theft, financial fraud, or other destructive acts. An instrument called a keylogger may record keystrokes made on a keyboard automatically and because of this, an attacker can employ this method to access private information in a secured database without having to break into the house (Darus *et al*., 2022).

Several detection and prevention methods have been proposed to mitigate keylogger attacks, including the use of antivirus software, firewalls, and network traffic analysis. However, with the constant evolution of keyloggers, these methods are not foolproof, and new techniques need to be developed to counter these threats. On the Internet, there are two intriguing incidents related to keyloggers. There are two reports, one from 2020 and the other from 2013, that show keyloggers have been in use for a long. In the article from Malwarebytes, it is discussed how the COVID-19 pandemic in 2020 would lead to an increase in keylogger assaults. It details how fraudsters are utilising the pandemic as a means of dispersing malware and stealing private data. According to the article, keylogger attacks are among the most prevalent COVID-19 scams, and they can spread via email phishing schemes, malicious websites, and infected software.

Keylogger attacks have been used to steal private data from automated teller machines (ATMs) and point-of-sale (POS) terminals in 2013. According to the report, keyloggers are intended to collect keystrokes and steal private data like passwords and credit card numbers. According to the article, keyloggers are growing in popularity among cybercriminals because they make it easy for attackers to obtain information from several victims with little effort. This demonstrates that the threat posed by keyloggers should not be disregarded based on the rare examples of incidents that do occur. It can have a significant effect on the victim just by employing this "little weapon." Recent research has focused on the use of artificial intelligence and machine learning to detect and prevent keylogger attacks. For example, natural language processing can be used to analyse keylog files to identify suspicious keywords and phrases. Biometric authentication, such as facial recognition and fingerprint scanning, can also be used to prevent keylogger attacks by eliminating the need for passwords.

3. Keylogger Threats

Keylogger is a type of technology used to monitor and record the keystrokes made on a computer or mobile device. Keyloggers can either be software-based or hardware-based. They are often used by hackers to steal sensitive information, or to monitor activities. It is important to be aware of the risks and to take measures to protect from keyloggers used maliciously.

3.1 Concept

Keyloggers are designed to record keystrokes by obstructing the information flow between the time a key is pressed and the time the keystroke is visible on the screen. A variety of techniques can be used to achieve this, including video surveillance, hardware flaws in keyboards or computers, input/output interception, changing the keyboard driver or filter driver, interfering with kernel functions, manipulating DLL functions, and using conventional techniques to gather information from the keyboard. The concept of keylogger breaks down into two definition which is Keystroke Logging and Keylogger Tools (Prajapati *et al*., 2020). Keystroke logging is the process of tracking and recording every key entered on a computer, usually without the user's knowledge or consent. A keystroke is any action taken on the keyboard, which serves as the means of communication between the user and the computer. The information recorded during keystroke logging includes the length of time a key was pressed, the timing of the press, the speed, and the name of the key used. This information can be very revealing, like listening in on a private conversation. With the increasing use of digital devices, a large amount of sensitive information is shared, making keystroke logging a serious concern.

Keylogger Tools are devices or programs designed to track and record every keystroke made on a computer. These tools can either be hardware or software, and they log the information from every keystroke into a text file that can be accessed later. Some keyloggers can also record data from the copy-cut-paste clipboard, calls, GPS location, microphone or camera footage. Although keyloggers have legitimate uses for personal or professional IT monitoring, some uses fall into an ethically questionable grey area, while others are clearly criminal. Regardless of the use, keyloggers are often used without the full knowledge or consent of the user, with the assumption that the user will behave normally.

3.2 Types

In the modern world, keyloggers come in many different varieties. Keystroke loggers can be broadly classified into two categories, as described in the overview. In **Figure 1**, the types are represented diagrammatically (Parekh* *et al*., 2020).

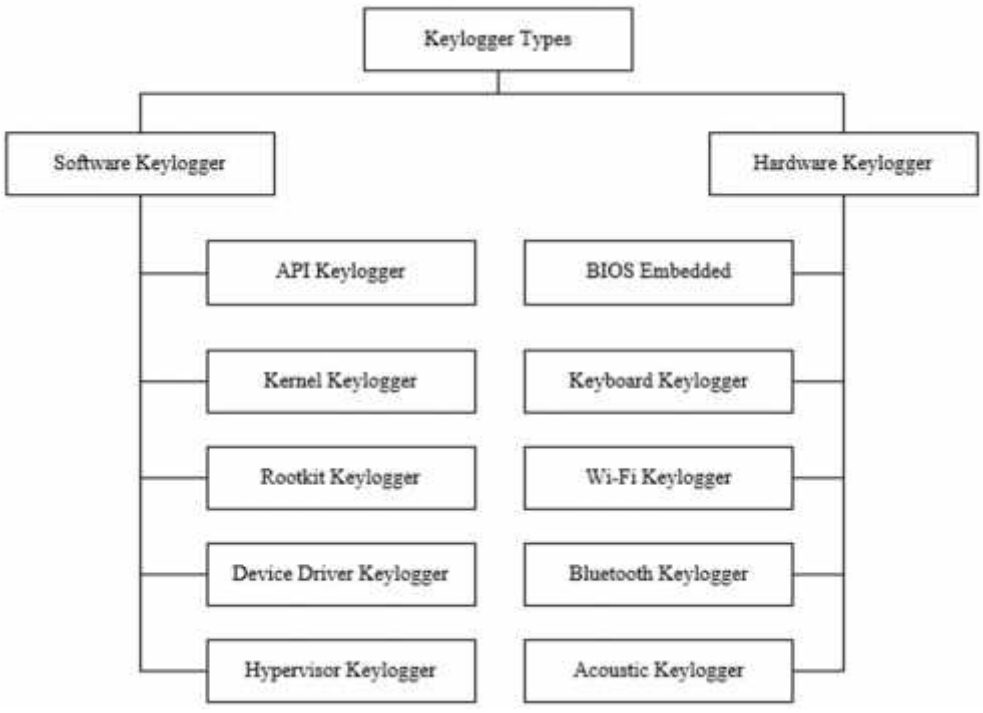

Figure 1: Types of keylogger (Parekh* *et al*., 2020)

API-based software keyloggers capture keyboard or keypad inputs within an active application by intercepting its APIs. These keyloggers operate like a normal application and do not leave any evidence of malware. The keystrokes can be recorded and stored, including key presses, releases, or both (Tian *et al*., 2017). Kernel-based software keyloggers are programs that gain access to the core of the operating system and capture the key presses that go through it. These keyloggers, with their root access, are extremely well-hidden and nearly impossible to detect. Applications without root access cannot spot them at all. A kernel-level software keylogger can function as a device driver for the keyboard, providing the same services as the original device driver, but also storing the keystrokes for the attacker (Engineering, 2020).

The term rootkit refers to a type of software that penetrates a system and intercepts system functions. It can hide its presence by concealing processes, files, folders, and registry keys. Some rootkits install their own drivers and services within the system. Although relatively uncommon, rootkit software keyloggers are the most dangerous type of keylogger as they have the ability to capture a set of functions responsible for processing messages or text input. This includes functions such as GetMessage, TranslateMessage library, and PeekMessage user32.dll, which allow the rootkit to monitor messages obtained by GUI applications. With the use of these methods and functions, rootkit software keyloggers can easily intercept messages and data (Zaitsev, 2010).

A software keylogger known as a "device driver" intercepts and records each keystroke made on the keyboard by acting as the keyboard's device driver. It is challenging to spot this kind of keylogger since it is integrated into the operating system and has root access. The keylogger offers the same functionality as the genuine keyboard device driver, but it additionally records and transmits keystrokes to the attacker. Device driver keyloggers can hide their existence and carry out their operations without the user realising it since they have root access. The phrase "hypervisor" refers to computer software, sometimes known as a "virtual machine monitor," that builds and oversees virtual machines (VMM). Theoretically, an operating system instance on a computer or mobile device might be captured by a hypervisor, which would then virtualize all of the devices and files on the system. Because of the potential for keyboard logging or interception caused by this virtualization, a rootkit is necessary to install the virus (Engineering, 2020).

A BIOS-embedded hardware keylogger is a type of keylogger that is installed directly onto the motherboard of a computer system (Witczyńska, 2019). It operates at the BIOS level, meaning that it is undetectable by most software-based security solutions, and it is capable of logging keystrokes before the operating system even loads. Since the keylogger is embedded in the hardware, it is difficult to detect and remove without physical access to the computer. A keyboard keylogger is a type of hardware keylogger that is specifically designed to capture and record keystrokes made on a keyboard. It is a small device that can be easily installed between a keyboard and a computer, or it can be built into a keyboard itself (Barankova *et al*., 2020). Once installed, the keyboard keylogger silently records every keystroke made on the keyboard and stores the information in its internal memory or sends it to a remote location for later retrieval. This type of keylogger is difficult to detect and can be a serious threat to privacy and security, as it can capture sensitive information.

A hardware keylogger that transmits keystrokes typed on a keyboard to a remote server using Wi-Fi is known as a Wi-Fi keylogger. It can be a stand-alone device or an internal card inside a computer and enables cybercriminals to monitor keystrokes remotely without having to physically access the system. This method is advantageous for attackers because the captured data is transmitted via Wi-Fi (Charan *et al*., 2023), allowing them to access it from anywhere, making it an effective and discreet tool for cybercrime. Hardware keylogger can records keystrokes and sends them to a remote device using Bluetooth technology. It is usually disguised as a legitimate Bluetooth device, such as a keyboard or mouse, and can be planted on a target computer to capture sensitive information. The captured data can then be retrieved by the attacker at a later time. Bluetooth keyloggers can be difficult to detect because they do not require a physical connection to the computer and can operate from a distance (Prajapati *et al*., 2020).

An acoustic keylogger is a type of hardware keylogger that captures the sound of keystrokes instead of recording the electrical signals that are sent to a computer when a key is pressed. This type of keylogger uses a small microphone or other audio recording device to capture the sound of the keystrokes being typed on a keyboard. The captured audio can then be converted back into text using automated speech recognition software. Acoustic keyloggers are difficult to detect, as they do not require any special software or drivers to be installed on the target system, making them a particularly insidious form of keylogging attack (Monaco, 2018).

Referring to (Prajapati *et al*., 2020), the technical comparison between software and hardware keyloggers is shown in **Table 1**.

Software Keylogger	Hardware Keylogger
i. Software keyloggers are programs that keep track of what's being typed on a keyboard.	i. A hardware keylogger is a small, 4cm memory chip that is integrated into a keyboard.
ii. The information recorded by software keyloggers is often saved in log files.	ii. It records the keystroke data on this memory chip.
iii. This information can later be retrieved or sent automatically via email to the person who's monitoring the activity.	iii. The stored information can be viewed using software that is included in the package with the hardware keylogger.
iv. Software keyloggers can either be installed by hackers to gather information from their victims, or by someone like a parent to monitor the internet activity of their children.	iv. Companies often use hardware keyloggers to monitor their employees' computer usage.
v. The presence of a software keylogger can be detected by anti-malware or anti-spyware software.	v. Anti-malware or anti-spyware software cannot detect hardware keyloggers.

Table 1: Technical comparison keylogger categories (Prajapati *et al*., 2020)

When talking about which keylogger category poses the most threat, it depends on the circumstance and the keylogger's intended usage. Both software and hardware keyloggers can be used maliciously, however because hardware keyloggers can get around anti-malware and anti-spyware software, they might be seen as more dangerous. Because they are physically installed into the computer, hardware keyloggers are more challenging to find than software keyloggers, which can be detected and removed by anti-malware software. However, software keyloggers may be more adaptable and adjustable, which in some circumstances may increase their effectiveness.

3.3 Threats Approach

Keylogger malware's dissemination and use are important to the creation and evolution of the programme. Distribution of keyloggers remotely is essential for remote infection to occur. Currently, keyloggers can be distributed through a number of different techniques on the internet. Keyloggers can be distributed on the internet in four primary ways: through adverts, third-party widgets, user-contributed content, and web server security procedures (Prajapati *et al*., 2020). Advertisements can be a common host for malware because third parties can inject malicious content into the chain of redirections. Third-party widgets are embedded links that can be redirected to harmful locations. User-contributed content can be malicious if the webmaster doesn't properly check the legality and validity of the content. Web server security mechanisms can prevent malware placement by controlling server content, but if an attacker gains control of these mechanisms, they can manipulate the content on the website to their advantage.

The distribution of malware is typically a precursor to an infection. This can occur through the exploitation of web applications and by tricking individuals through social engineering techniques. "Drive-by-downloads" is a term used to describe the automatic download and execution of malicious software when a person visits a compromised website (Provos *et al*., 2007). The malware distribution is carried out by exploiting vulnerabilities in the browser using malicious code that will activate system routines or shell commands on the target computer to download the malware. If the machine doesn't have any security vulnerabilities, the attacker may resort to social engineering techniques (Thornburgh, 2004) to trick the user into downloading the malware. The final stage of the attack is for the keylogging malware to start running, which can happen in various ways, depending on the design and context of the keylogger.

Additionally, further analysis (Zenebe *et al*., 2019) of system exploits revealed that password crackers, RATs (Remote Administration Tools), tools that exploit buffer overflows, and keylogger tools are among the most commonly shared tools among hackers in Dark Web. The research results from (Ryan *et al*., 2022) indicate that the usage of Keystroke Dynamics is on the rise for various purposes, such as accessing platforms through typing behaviour and continuous monitoring for suspicious activity. However, the authentication method using Keystroke Dynamics can be vulnerable to exploitation if an attacker successfully records and copies the target user's typing pattern. Keylogging is a common way to capture and record a user's typing patterns without their knowledge, but it is not an easy task for an attacker to install

a keylogger on a victim's computer. It may require the attacker to create malware, trick the victim into running a harmful program, or have physical access to the computer to manually install the keylogger.

A study by (Bojovic *et al*., 2019) showed that USB has become the primary port for connecting computers. Its programmability makes it an easy way for hardware and operating system developers to create products and firmware. However, this ease of use also increases the risk of vulnerabilities due to its simple plug-and-play nature. In the paper (Almazaydeh *et al*., 2017) identified the BadUSB attack as being high-risk due to its ability to emulate a keyboard or network card. This device can present itself as both a flash drive and a keyboard, enabling the introduction of malicious software. The host computer is unable to scan the firmware, making it impossible for antivirus software to detect this threat (Tian *et al*., 2015).

According to (Gazzari, 2021), wearables are designed to gather and process information for the user's benefit and are often worn for the majority of the day, collecting data that may contain traces of sensitive activities. Human-centric sensors embedded in smartwatches and other wearables pose risks for keylogging, as they may collect data that can be used to infer keystrokes and potentially attack multiple devices the user interacts with while wearing the device. As these devices are often connected to mobile devices or operate independently, users may not remove them when engaging in sensitive activities such as typing on a physical keyboard. Therefore, the sensor data collected by wearables can reveal everything that has been typed on a personal, work, or any other device, which makes them a potential target for cybercriminals.

4. Defending Against the Silent Threats

In the 21st century, keyloggers have become a rapidly growing type of unauthorized software that is used for gathering private information without the consent of users. This is achieved by recording all the keystrokes made by a user using an unprivileged program running in the user space. These keystrokes are then saved in a log file or an FTP server. The lack of system protection, such as outdated antivirus software and firewalls, makes it easy for keyloggers to be planted and executed. The design of keyloggers is based on factors such as the infection medium, the type of target machine, and the lifetime of the keylogger. It has been reported that the growth of keyloggers has been seen in various types of criminal activities.

4.1 Detection Methods

Detection methods to deal with keylogger threats can include: regular system scans and updates of antivirus software, usage of anti-spyware and anti-malware tools, monitoring of network traffic and system logs, implementing firewalls and intrusion detection systems, and practicing safe browsing habits.

4.1.1 Use of Antivirus Software

Antivirus software works by scanning computer's files and processes for known signatures of malware, including keyloggers. When a keylogger is detected, the antivirus software will either delete the malware or quarantine it so that it can no longer cause harm. Antivirus software can also monitor computer in real-time for suspicious activity that may indicate a keylogger is present, such as changes to system files or unusual network traffic. Additionally, many antivirus software packages have the ability to automatically update their virus definitions, which means they will always be up-to-date in detecting new keylogger threats. However, in recent times, keyloggers have become a significant concern as they often go undetected by antivirus software as they use the system resources together with genuine programs (Riahi Manesh & Kaabouch, 2019).

4.1.2 Monitoring of System Logs

Monitoring system logs can be a useful tool in detecting keylogger threats as it records all activities on a computer system. Logs can reveal the presence of keylogger malware by detecting unusual system activity, such as unexpected incoming network traffic or unusual process execution. This can indicate that sensitive information is being stolen, recorded, or transmitted. Some sources suggest regularly monitoring system logs for anomalies and using tools to analyse and alert on potential threats. For example, according to a study by the Institute of Electrical and Electronics Engineers (IEEE), "system logs are a rich source of information for detecting unauthorized activity." The study also suggests that tools such as intrusion detection systems (IDS) and security information and event management (SIEM) software can help to monitor and analyse system logs for signs of keylogger malware.

Another study by the SANS Institute highlights the importance of log analysis in detecting keylogger threats. The study states, "log analysis can be a valuable tool in the identification and removal of keyloggers." By regularly monitoring

system logs and analysing them for suspicious activity, organisations can reduce the risk of keylogger malware infections and prevent the theft of sensitive information.

4.1.3 Network Traffic Analysis

Network Traffic Analysis is a method of detecting keylogger threats by monitoring and analysing network traffic for any suspicious activities or patterns. This process involves the use of specialized tools, such as intrusion detection systems (IDS) and security information and event management (SIEM) systems, to inspect network traffic in real-time and identify any anomalies or malicious activity. Network Traffic Analysis can detect keylogger threats by examining the data being transmitted over the network and identifying any unusual patterns of activity (Ahmed, 2019), such as large amounts of data being transmitted at once, changes in network behaviour, or unusual connections to remote servers. This analysis can detect keyloggers, evaluate their scope and the data collected, leading to prevention of further attacks and minimizing the damage.

However, from the study conducted by (Bayzid *et al*., 2019), it was found that real-time monitoring of the network can offer a means of quickly detecting any malicious processes in operation, which in turn can help with their removal, though there is currently no definitive method for eliminating keyloggers.

4.2 Prevention Methods

Prevention methods in countering keylogger attacks refer to steps taken to stop the attack from happening in the first place. These methods aim to create an environment that makes it difficult for the attacker to install or use a keylogger on a target system. Some common prevention methods include regularly updating anti-virus software, installing firewalls, keeping software up-to-date, and avoiding suspicious or untrusted email attachments or downloads. Other measures include using encryption to protect sensitive data, setting strong passwords, and training users to be aware of social engineering tactics that might trick them into downloading a keylogger. By taking these steps, organisations and individuals can reduce their risk of falling victim to keylogger attacks and protect their sensitive information.

4.2.1 Regular Software Updates

Regular software updates can prevent keylogger attacks by fixing vulnerabilities in the software that can be exploited by attackers to install keyloggers. Software updates often include patches for security vulnerabilities that have been discovered, so updating software as soon as updates are available can help to stay protected from potential attacks (Assunção, 2019). Additionally, software updates can also bring new security features and improvements that can further strengthen the defence against keyloggers and other types of malicious software. By staying up-to-date with software, it can help prevent keylogger attacks and reduce risk of falling victim to identity theft, financial fraud, and other malicious activities.

4.2.2 Biometric Authentication

Biometric authentication is a method of identity verification that uses biological traits, such as fingerprints, facial recognition, iris recognition, voice recognition, and others, to identify a person. In the context of keylogger attacks, biometric authentication can prevent keyloggers from stealing sensitive information because the biometric data is unique to each person and cannot be captured or replicated by a keylogger. The biometric authentication process involves using specialized hardware, such as a fingerprint reader or a webcam, to capture the biometric data and compare it to the data stored in a secure database. But the limitation in implementing this technique is that biometric authentication systems can be expensive (Sidhardha & Deepthi, 2020).

4.2.3 Firewall Configuration

Firewall configuration can prevent keylogger attacks by controlling incoming and outgoing network traffic based on predefined security rules. The firewall can be configured to block or allow specific types of traffic, such as traffic from known malicious IP addresses or traffic that contains certain keywords. This helps to prevent keyloggers from transmitting sensitive information over the network (“Trends and Applications in Information Systems and Technologies,” 2021).

5. Future Trend in Combating Keylogger Threats

The future trend to counter keylogger threats is shifting towards advanced technologies such as artificial intelligence and machine learning. Encryption techniques are also becoming more popular as a means of preventing keylogger

attacks. Biometric authentication, such as fingerprint and facial recognition, is also increasingly being used as a preventive measure. With the ever-evolving threat landscape, it is important to stay informed and implement multi-layered security measures to protect against keylogger attacks.

5.1 Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) are emerging as a crucial aspect of future trend in combating keylogger threats. The use of AI and ML can help in improving the accuracy and efficiency of identifying and defending against keyloggers. These technologies can help in detecting anomalies and deviations in the system that may indicate the presence of keylogger. They can also aid in monitoring and analysing the keystrokes in real-time to detect any suspicious activity and prevent it from happening. AI and ML can also be used in creating and updating signatures for detecting new and evolving keyloggers. As keyloggers continuously evolve, traditional security measures may become obsolete, but with the use of AI and ML, the security systems can keep up with these changes and detect new keylogger threats. Additionally, AI and ML can also help in strengthening the overall security posture by providing an additional layer of defence and reducing the risk of keylogger attacks.

(Parekh* *et al*., 2020) presents a new idea of using keylogger logs and analysing them with natural language processing techniques. The logs captured through a keylogger called Refog were used to demonstrate the concept. The authors tokenized and lemmatized the logs to identify the type of user. The uniqueness of the study is the use of artificial intelligence, specifically natural language processing, to analyse the keylogger logs. This approach helps to reduce CPU utilization time and provides insights into a user's communication patterns and sentiments. This study also highlights the benefits of using keyloggers as a tool for understanding user behaviour and improving security. AI and ML are becoming an indispensable part of future trend in combating keylogger threats and have a tremendous potential to improve the security systems by detecting and preventing keylogger attacks.

5.2 Advance Encryption Techniques

The idea behind encryption is to convert plaintext into an unreadable ciphertext using an encryption algorithm and a secret key. When the ciphertext is intercepted by a keylogger, it is of no use as it cannot be deciphered without the secret key. The AES Encryption Algorithm is a very strong encryption algorithm that utilizes a 128-bit fixed data block, and is a Symmetric Algorithm used to prevent unauthorized access to content (Rai *et al*., 2022).

In the future, we can expect more advanced encryption techniques to be developed that are specifically designed to counter keyloggers. For example, encryption algorithms that use multiple keys or that change the encryption key with every keystroke can make it harder for keyloggers to capture the plaintext information. Additionally, the use of end-to-end encryption in communication channels, such as instant messaging or email, can also reduce the risk of keylogger attacks. Thus, to address the issue of keylogger threats, the future may involve utilizing encryption methods such as post-quantum cryptographic (PQC) algorithms, which are resistant to attacks from quantum computers (Kanad Basu, Deepraj Soni, Mohammed Nabeel, 2019).

5.3 Enhanced Biometric Authentication

In the future, biometric authentication is expected to become more widely used in the security industry, especially in the context of keylogger threats. The technology can be used to secure personal and financial information, prevent identity theft, and prevent unauthorized access to sensitive systems and data. Additionally, biometric authentication can be used in combination with encryption techniques to provide a multi-layer security system that is highly resistant to keylogger attacks. In a study, (Kim & Mun, 2022) has presented a multi-level authentication system based on blockchain technologies like DID (decentralised identity) technology and biometric recognition technology that ensures both security and integrity.

5.4 Exchange of Threat Intelligence

Exchange of threat intelligence involves the sharing of information related to cybersecurity threats and attacks between different organisations, typically within a specific industry or sector. This sharing can include details about specific threats or attacks, as well as tactics, techniques, and procedures (TTPs) used by hackers. The exchange of threat intelligence can help organisations to identify and respond to threats more quickly and effectively, as well as improve their overall cybersecurity posture. It can also help to foster greater collaboration and cooperation between organisations in the fight against cybercrime.

According to (Tounsi & Rais, 2018), as businesses continue to migrate to the cloud, indicators of compromise (IOC) are also evolving. The need for a business to better safeguard its data is increased by the ease of access to it, its connections to email accounts, online applications, and documents stored on a number of platforms, including cloud systems and mobile devices. In this context, threat intelligence (TI) offers various benefits. Among of these benefits include the ability to selectively distribute TI data, identify new malware and stealth cyberattacks, and issue early warnings.

5.5 Joint Efforts to Combat Keylogger Threats

Joint efforts to combat keylogger threats involve collaboration among different parties, including security researchers, software vendors, and end-users. This approach recognizes that keyloggers are a complex and evolving threat that requires a coordinated effort to counter effectively. Collaboration may involve sharing information about new threats, developing and disseminating best practices for prevention and detection, and working together to develop new technologies to counter keyloggers. Therefore, this can be utilized by taking advantage of the social trends in the use and advancement of cyberspace, such as varying local priorities in global technological progress, growth in online communities, cooperation, and exchange of information (Malik *et al*., 2019). By working together, these groups can enhance the overall effectiveness of their efforts and more effectively protect against this persistent and growing threat.

5.6 Importance of User Awareness

User awareness is crucial in countering keylogger attacks because keyloggers often rely on social engineering techniques to trick users into downloading or installing the malware. By being informed and vigilant, users can avoid falling prey to these attacks, and take measures to protect their devices and personal information. Additionally, users should be encouraged to practice good password hygiene, such as using strong, unique passwords and enabling two-factor authentication, to minimize the potential impact of keylogger attacks. General awareness and attentiveness are the strongest defences against hardware keyloggers. Users should regularly check their hardware for updates, alterations, and the presence of any keyloggers (Blåfield, 2020). Overall, raising awareness about keylogger threats and providing education and training to users is an essential step in preventing and mitigating the damage of these attacks.

5.7 Importance of Following Best Practices for Online Safety

Following best practices for online safety is crucial in countering keylogger threats, as it can prevent keyloggers from being installed on a system in the first place. Best practices include keeping software and security programs up to date, avoiding suspicious emails and links, using strong and unique passwords, and enabling two-factor authentication. By following these practices, users can significantly reduce the risk of falling victim to keylogger attacks and other forms of cybercrime. It is also important for organisations to provide regular training and education to their employees on best practices for online safety to ensure that they remain vigilant and informed about potential threats. According to (Kara, 2020), enhancing people's awareness is one way to reduce dealing with harmful situations. Information security is primarily concerned with two aspects: (1) comprehension of information security behaviours; and (2) acting in accordance with recommended practises.

6. Conclusions

In conclusion, keyloggers are one of the most dangerous and widely used hacking tools in the modern digital world. With the ever-increasing reliance on technology and the internet, individuals and organisations have become increasingly vulnerable to the threat posed by keyloggers. The ability of these programs to covertly record and transmit sensitive information, such as login credentials and other private data, makes them a powerful weapon in the hands of hackers. In order to effectively combat this threat, it is important for individuals and organisations to take proactive steps to protect themselves.Ultimately, by staying vigilant and taking the necessary precautions, individuals and organisations can safeguard against the threat posed by keyloggers and other hacking tools. Overall, this paper serves as a comprehensive guide to understanding keyloggers as a tool for hacking and the measures that can be taken to prevent and detect keylogger attacks. It is also intended that researchers would utilise this paper as a resource to generate ideas for the subsequent study, especially regarding the future trend of keylogger threat and future prevention.

Acknowledgements

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

References

Ahmed, B. (2019). Keylogger Detection using Memory Forensic and Network Monitoring Keylogger Detection using Memory Forensic and Network Monitoring. *International Journal of Computer Applications*, *177-No.*(October), 17–21.

Al-masalha, H., Hnaif, A. A., & Kanan, T. (2020). Cyber-Crime Effect on Jordanian Society. *Int. J. Advance Soft Compu. Appl*, *12*(3), 123–139.

Almazaydeh, L., Zhang, J., Wu, P., Wei, R., Cheng, Y., & Elleithy, K. (2017). Bad USB MITM: A Network Attack Based on Physical Access and Its Practical Security Solutions. *Computer and Information Science*, *11*(1), 1. https://doi.org/10.5539/cis.v11n1p1

Assunção, P. (2019). A Zero Trust Approach to Network Security. *Proceedings of the Digital Privacy and Security Conference 2019*, *10.11228/dpsc.01.01*, 99. https://privacyandsecurityconference.pt/conference2019/Proceedings_Digital_Privacy_and_Security_Conference_2019.pdf#page=65

AV-Test. (2023). *Malware Statistics & Trends Report | AV-TEST*. AV-Test. https://www.av-test.org/en/statistics/malware/

Barankova, I. I., Mikhailova, U. V., & Lukyanov, G. I. (2020). Software development and hardware means of hidden usb-keylogger devices identification. *Journal of Physics: Conference Series*, *1441*(1). https://doi.org/10.1088/1742-6596/1441/1/012032

Bayzid, M., Shoikot, M., Hossain, J., & Rahman, A. (2019). Keylogger Detection using Memory Forensic and Network Monitoring. *International Journal of Computer Applications*, *177*(11), 17–21. https://doi.org/10.5120/ijca2019919483

Blåfield, T. (2020). *DIFFERENT TYPES OF KEYLOGGERS Mitigation and risk relevancy in modern society* (Issue May). Tampere University.

Bojovic, P. D., Basicevic, I., Pilipovic, M., Bojovic, Z., & Bojovic, M. (2019). The rising threat of hardware attacks : USB keyboard attack case study. *JOURNAL OF IEEE SECURITY & PRIVACY, November*. https://doi.org/10.13140/RG.2.2.27801.47205

Charan, B. S. V., Kulkarni, L., & Karad, V. (2023). Survey On Micro-Controller Based Bad USB Attacks. *Positive School Psychology*, *7*(1), 965–974.

Darus, M. Y., Azizi, M., & Ariffin, M. (2022). Enhancement Keylogger Application for Parental Control and Monitor Children ' s Activities. *Journal of Positive School Psychology*, *6*(3), 8482–8492.

Engineering, C. P. (2020). Types of Keyloggers Technologies – Survey. *ICCCE 2020 Proceedings of the 3rd International Conference on Communications and Cyber Physical Engineering*, 11–22.

Gazzari, M. (2021). My (o) Armband Leaks Passwords : An EMG and IMU Based Keylogging Side-Channel Attack. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *5*(4).

Ingersoll, G. (2013). *Russia Turns to Typewriters for Secrets*. Business Insider. https://www.businessinsider.com/russia-turns-to-typewriters-for-secrets-2013-7

Interscan, Q. (n.d.). *Soviet Spies Bugged World's First Electronic Typewriters*. QCC Interscan. Retrieved February 6, 2023, from https://web.archive.org/web/20131220110339/http://www.qccglobal.com/news/first-keystroke-logger.php

Kanad Basu, Deepraj Soni, Mohammed Nabeel, and R. K. (2019). NIST Post-Quantum Cryptography- A Hardware Evaluation Study. *IACR Cryptology EPrint Archive*, *2019*(2), 1–16. https://eprint.iacr.org/2019/047.pdf#page=22&zoom=100,0,442

Kara, M. (2020). information security awareness scale (MISAS). *Emerald Online Information Review*, *45*(2). https://doi.org/10.1108/OIR-04-2020-0129

Kim, S., & Mun, H. (2022). Multi-Factor Authentication with Randomly Selected Authentication Methods with DID on a Random Terminal. *Applied Science*, *12*(2301), 1–13.

Malik, J., Gandhi, R., Vishwavidyalaya, P., Malik, J. K., & Choudhury, S. (2019). A Brief Review on Cyber Crime-Growth and Evolution. *Pramana Research Journal*, *9*(3), 242–278. https://www.researchgate.net/publication/340756419

Monaco, J. (2018). SoK: Keylogging Side Channels. *Proceedings - IEEE Symposium on Security and Privacy*, *2018-May*, 211–228. https://doi.org/10.1109/SP.2018.00026

Parekh*, D. H., Adhvaryu, N., & Dahiya, D. V. (2020). Keystroke Logging: Integrating Natural Language Processing Technique to Analyze Log Data. *International Journal of Innovative Technology and Exploring Engineering*, *9*(3), 2028–2033. https://doi.org/10.35940/ijitee.c8817.019320

Prajapati, V., Kalsariya, R., Dubey, A., Mehta, K., & Patil, P. M. (2020). Analysis of Keyloggers in Cybersecurity. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *8*(October), 466–474.

Proactive, M., Suitable, I., Enterprises, C., Sun, J., Liu, C., & Yuan, H. (2021). Keylogger Detection and Prevention.

Journal of Physics: Conference Series, *2007*(1). https://doi.org/10.1088/1742-6596/2007/1/012005

Provos, N., McNamee, D., Mavrommatis, P., Wang, K., & Modadugu, N. (2007). The ghost in the browser analysis of web-based malware. *1st Workshop on Hot Topics in Understanding Botnets, HotBots 2007*.

Rai, S., Choubey, V., Suryansh, & Garg, P. (2022). A Systematic Review of Encryption and Keylogging for Computer System Security. *Proceedings - 2022 5th International Conference on Computational Intelligence and Communication Technologies, CCICT 2022*, *July*, 157–163. https://doi.org/10.1109/CCiCT56684.2022.00039

Riahi Manesh, M., & Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Computers and Security*, *85*, 386–401. https://doi.org/10.1016/j.cose.2019.05.003

Ryan, C., Siahaan, P., & Chowanda, A. (2022). Spoofing keystroke dynamics authentication through synthetic typing pattern extracted from screen recorded video. *Journal of Big Data*, *8*. https://doi.org/10.1186/s40537-022-00662-8

Sidhardha, P. N., & Deepthi, D. (2020). TEXT-BASED SHOULDER SURFING AND KEY LOGGER RESISTANT GRAPHICAL PASSWORD. *Journal of Engineering Sciences*, *11*(3), 214–223.

Thornburgh, T. (2004). Social engineering: The "dark art." *2004 Information Security Curriculum Development Conference, InfoSecCD 2004*, 133–135. https://doi.org/10.1145/1059524.1059554

Tian, D., Bates, A., & Butler, K. (2015). Defending against malicious USB firmware with GoodUSB. *ACM International Conference Proceeding Series*, *7-11-Decem*, 261–270. https://doi.org/10.1145/2818000.2818040

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*(2), 445–461. https://doi.org/10.1688/JISE.2017.33.2.10

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers and Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Tove, M. (2022). *What Are Keyloggers And How Can You Protect Yourself?* https://vpnoverview.com/internet-safety/malware/keyloggers/

Trends and Applications in Information Systems and Technologies. (2021). In R. Alvaro, A. Hojjat, D. Gintautas, M. Fernando, & R. C. Ana Maria (Eds.), *Advances in Intelligent Systems and Computing: Vol. 1365 AIST*. Springer. https://doi.org/10.1007/978-3-030-72657-7_12

Witczyńska, K. (2019). Effective protection of information systems and networks against attacks in the era of globalization. *Logistics and Transport*, *41*(1), 51–56. https://doi.org/10.26411/83-1734-2015-1-41-6-19

Zaitsev, O. (2010). Skeleton keys: The purpose and applications of keyloggers. *Network Security*, *2010*(10), 12–17. https://doi.org/10.1016/S1353-4858(10)70126-4

Zenebe, A., Shumba, M., Carillo, A., & Cuenca, S. (2019). Cyber Threat Discovery from Dark Web. *EPiC Series in Computing*, *64*, 174–183.