**KEYLOGGER**

Department of Computer Science, Chandigarh University shubham260602@gmail.com

**ABSTRACT**- Keyloggers are a type of rootkit malware that record composed keystroke events from the console and save into log records. As a result, it can capture sensitive information like usernames, PINs, and passwords and interact with vengeful attackers without drawing the attention of users. Keyloggers pose a serious threat to commercial and personal activities like e-commerce, online banking, email communication, and system data bases. Commonly used antivirus software for locating and removing known keyloggers However, it is unable to detect mysterious Keyloggers. This essay provides an overview of keylogger programmes, varieties, characteristics, and operating principles. Finally, we'll examine a few proactive strategies and dissect the current discovery processes.

**KEYWORD:** Keylogger, username,pasword

# 1. INTRODUCTION

Keyloggers are a type of monitoring software that records a user's keystrokes. These keystroke loggers are one of the oldest types of cyber threat, record the information you type into a website or application and send it to a third party. Keyloggers are used by criminals to steal personal or financial information, such as banking information, which they can then sell or use for profit. Keylogging is also used for surveillance by law enforcement and intelligence agencies.

The Internet's revolutionary capabilities have changed the way we share files and information, send electronic mail, and exchange messages. The advancement of technology has had a significant impact on our lives. The internet has evolved into a multidisciplinary tool. According to internetlivestatus.com, more than 40% of the world's population has access to the internet. Cyber criminals engage in malicious activities in order to obtain confidential information from a user's system without breaking into the 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.

Malware comes in many forms, including viruses, Trojans, ransomware, spyware, rootkits, botnets, and so on. They cause harm to the computer system or network by performing functions such as monitoring the user's activity without their permission, deleting and hiding sensitive data, data theft, and so on. Keylogger is a type of malware rootkit that secretly records the user's activity.

Keyloggers can monitor everything you do on your computer. Modern keyloggers are highly sophisticated and becoming increasingly difficult to detect by anti-virus and anti-malware tools in the market. Keylogger detection and prevention is a difficult task for security administrators. In addition to traditional viruses and worms, advanced Keyloggers exist that are nearly impossible to detect.

A keylogger is a 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 key logging software for troubleshooting or to keep an eye on suspicious employee activity. Nonetheless, the main concern with Keyloggers is when they are used by a third party. When a third party breaches our computer system, we have no idea what type of Keylogger it is, and it can steal any password we have entered, take periodic 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 of that data to a third party and can be used for criminal purposes.

Keyloggers are classified into two types: hardware keyloggers and software keyloggers. Hardware keyloggers are simple to use because they are embedded in the computer's internal hardware

## **2. Literature Survey**

* A. Keystroke Logging: Integrating Natural Language Processing Technique to Analyze Log Data

Disha H. Parekh, Nehal Adhvaryu, and Vishal Dahiya conducted the research. Cyberwarfare is a highly common occurrence since a hostile country is always attempting to destabilise itself by stealing sensitive information from important computer systems.

Dangerous international conflicts have resulted from this. In order to prevent unauthorised entry of anyone who is not a member of the military or a government official, spyware is currently being deployed on many tools. Keyloggers are one of the common techniques used in the modern world to gather private or sensitive information from both trustworthy and dishonest users. These keyloggers are helpful and widely used for law enforcement, crime scene investigation, and employee productivity tracking . While its bad uses include passwords and data theft, they are illegal. Today, the keylogger is perceived as a malicious attack and a security problem. Every coin, however, has two sides. Keyloggers actually assist in preventing a number of security breaches and in identifying a number of crimes committed across the internet and in other nations. This fact served as the impetus for the creation of this study, and as a result, an experimental analysis was also conducted in order to draw the conclusion that the log files from keyloggers can be used to identify a person by examining the right word patterns. This study primarily examines the area of natural language processing, processing a log file collected via keylogger software using the approach described the newspaper.

* Keylogger for Windows using Python

Mrs. N. Priya and Santripti Bhujel conducted the research. The suggested idea Keylogger, often known as a keystroke logger, is a tool that records each key you press on your console, often secretly so you are unaware that your actions are being watched. Most people prefer to just see the negative aspects of this particular programme, but it also has useful applications. In addition to being used for vengeful purposes like gathering account information, Visa numbers, client names, passwords, and other private information, it can also be used to monitor children's activities at home, in the office, and by law enforcement to look into and follow incidents involving the use of PCs. The project will be entirely written in Python, and I'll be using the pynput module, which isn't a built-in part of Python and needs to be installed. The software I'm planning to create should keep track of the keyboard strokes and record the results in a file. I'll also include a function that will send the logs directly to the email in order to advance the project.

* Keyloggers in Cybersecurity Education

Rajendra K. Raj and Christopher A. Wood conducted the research. By secretly recording user input through keyboard monitoring and then transmitting this information to others, sometimes for malicious motives, keylogger applications try to obtain confidential information. Thus, keyloggers offer a serious risk to both personal and professional activities like email, chat, online banking, and Internet transactions. Not only must users be made aware of this sort of malware, but software professionals and students must also receive training in the design, implementation, and monitoring of efficient defences against various keylogger attacks in order to deal with such threats.

* Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm

Robbi Rahim, Heri Nurdiyanto, Ansari Saleh, Dahlan Abdullah, Dedy Hartama, and Darmawan Napitupulu are responsible for the research. Technology is evolving very quickly, particularly in the area of Internet technology, which is constantly undergoing considerable changes. Keylogger is a tool that has been most developed since antivirus software very seldom identifies it as a malicious programme. Keylogger will record all activities linked to keystrokes and accomplishes the recording process by employing a string matching mechanism. The usage of the string matching approach during the keyboard recording procedure aids the administrator in understanding what the user accessed on the computer.

### 3. OBJECTIVES

* Legal Consensual Uses of Keyloggers.
* Keylogger uses that are morally and legally dubious.
* Criminal Uses of Keyloggers

### 4. PROBLEM STATEMENT

User sensitive data theft is done for a variety of nefarious reasons, including identity theft, credit card and banking fraud, software theft, and service theft, to mention a few. Key logging, also known as key eavesdropping, key harvesting, and keystroke leaking, is a technique used to do this. Keyloggers are simple to use and set up. [3] The financial loss might be significant when used for fraud-related goals as part of more complex criminal heists. Table 1.1 lists several significant keylogger-related reports of incidents. Over the years, a number of theories and strategies have been put up to address the broad issue of harmful software. However, none of the current techniques are adequate when used to address the unique issue of identifying key loggers. Signature-based solutions have limited applicability since they can easily be evaded and also require isolating and extracting a valid signature before being able to detect a new threat. [7] As we show next phase, implementation of a key logger hardly poses any challenge. Even unexperienced programmers can easily develop new variants of existing key loggers, and thus make a previously valid signature ineffective. To design and implement a exe application that works with windows operating system to capture keystrokes. The work also address the issue of malware handling in Cybersecurity.

**5. Methodology**

Keyloggers are malicious software or pieces of hardware that monitor and record your keystrokes as you type. With the use of a command-and-control (C&C) server, it takes the data and transfers it to a hacker. The hacker utilises the usernames and passwords he or she finds by analysing the keystrokes to access otherwise secure systems.

The purpose of the keylogger is to follow or monitor large groups of people, such as employees of MNCs, organisations, terrorist organisations, or suspect targets. It can also be used as a parental control to keep an eye on kids' online behaviour and prevent any cyber incidents. The goal of the proposed research project is to use numerous VMs to accomplish the suggested approach. Additionally, we intend to investigate the effects of keyloggers on laptops from any harmful websites. To track a target's keystrokes on a computer, we generate exe virus as part of our proposed solution. The victim machine will be contacted via a reverse to activate the keylogger. A shell session that is started on a connection that is initiated from a remote system is known as a reverse shell. using the Metasploit tool to incorporate Keylogger and Reverse Shell into an.exe file. transfer of an executable file via online or offline means to the target. A reverse shell session will be generated on a specific port number to the attacker's computer when the victim runs the exe file from his or her computer, without interfering with the victim's firewall. After obtaining the victim's reverse shell, we will launch the keylogger script. Afterward, each keystroke made by the victim will be logged. . We'll dump the keystroke data last. The victim's computer receives the info we spilled, and the attacker's computer

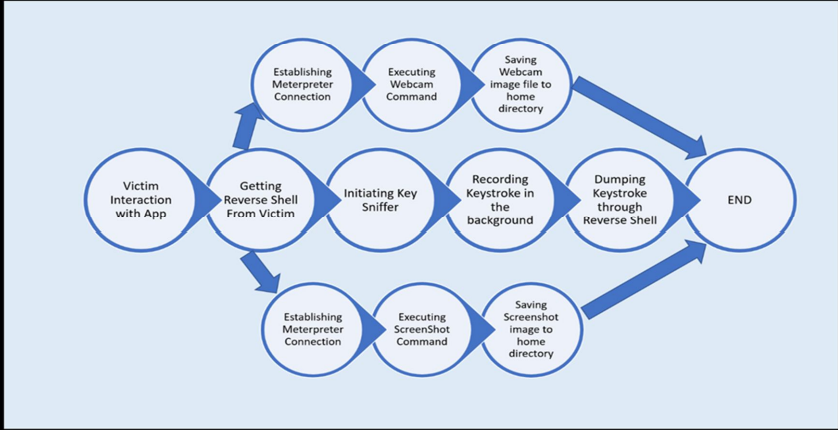
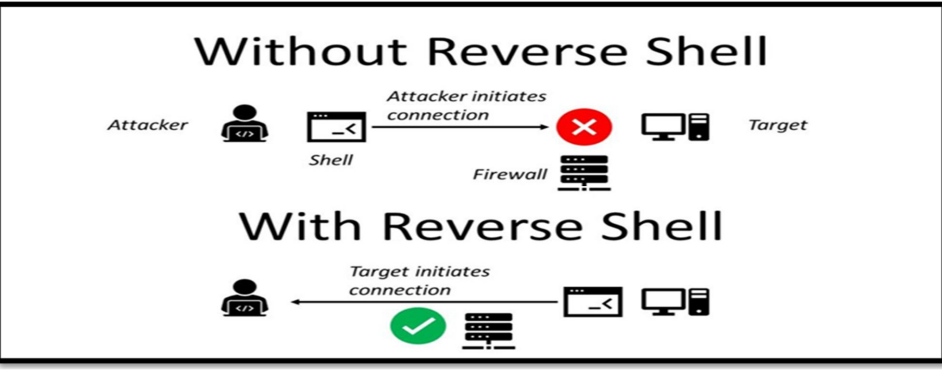


Fig. 5.1. Architecture of the Keylogger



Advantage of Keyloggers

* A key function of keyloggers in IT companies is the investigation of technical or network problems.
* It is utilised in security services to track suspects and gather evidence, aiding in the prevention of significant national threats.
* It is useful for someone who wishes to keep track of all the data on his computer in case someone else uses it.
* The ability for parents to monitor their children's online activities is incredibly useful.

Disadvantage of Keyloggers

* Keylogger usage closely relates to privacy concerns with regard to computers.
* Malicious users explicitly read out login information, such as names and passwords, and transfer it to unauthorised third parties when they perform Keylogger detection.
* Keyloggers are the perfect tools for today's covert operations or for accessing confidential company data. They can damage a company's reputation, finances, and business relationships; as a result, they may even cause a company to violate important laws, such the Data Protection Act.

# 6. CONCLUSION AND FUTURE SCOPE

With the advancement of technology and the widespread use of computers in both private and public settings, keylogger devices—both hardware and software—present a serious risk of cyber interception. Furthermore, because it is simple to get them there, buy them online, and do so for a fair price. The keylogger is a malicious programme that can read and gather information from the keyboard and is difficult to detect. As a result, this survey report provides an exhaustive reference to all you need to know about keylogger software. It's not always simple to tell if a keylogger is installed on your device. In terms of hardware keyloggers, the only method to spot them is by inspecting the keyboard internally and the wires connected to it. Once you've located the gadget, take it out manually.

Consequently, this is all the information concerning keyloggers that you need to be aware of.

* Attacks that log keystrokes get over all other safeguards. They give attackers useful account, identity, and intellectual property information and are simple to establish and manage. However, they are effective investigative tools.
* Keylogging technology management within your firm requires common sense and tiered defences, much like managing other dangers and technologies. Keylogger detection and containment should be a part of your incident response plan. The key is to be aware that they exist, understand how they are utilised, and put detection methods in place.
* This review article aims to provide insight into recent developments in keylogging attack risk mitigation. The author is aware that there may be some gaps in the literature review discussed in this article on the benefits of inventions related to keylogging assaults and hopes that there will be further developments in this field.

# 7. AUTHOR CONTRIBUTIONS

Myself SHIV SATYAM did all the parts

**8. CONFLICTS OF INTEREST**

The authors declare no conflict of interest.

# 9. ACKNOWLEDGEMENT

I would like to express my deep and sincere gratitude to my course instructor, Mr Matthew Caesar, Harinath Garudadri ,Ganz Chockalingam,at COURSERA and my University for giving me the golden opportunity to do this Summer/lnstitutional Training in the form of an online course along with a mini project that is the application of the knowledge that I learned from the online course and for providing invaluable guidance throughout the course on the topic of "Introduction to Cyber security & Cyber Attacks ”, and the guided project on the topic " design and simulate smart home networks in packet tracer.It was a great privilege and honor to work and study under Abhishek Jha sir’s (Guided Project Instructor) guidance. I am extremely grateful for what they have offered me. It helped me in doing a lot of research and I came to know and learned about a lot of things related to this topic.

Finally I would like to thank my parents and friends who helped me a lot in finalising this project in this limited time frame.

# 10. REFERENCES

[1] S. P. Goring, J. R. Rabaiotti and A. J. Jones, “Anti-keylogging measures for secure internet login: an example of the law of unintended consequences”, Computers & Security, Page 1-9, Feb 2007

[2] M. Mannan and P. C. van Oorschot, “Leveraging personal devices for stronger password authentication from untrusted computers”, Extended version of paper appeared in the proceedings of Financial Cryptography and Data security 2007, Version 6, Page 1-29, Oct 2008

[3] A. A. Nair and S. T. D., “An enhanced authentication mechanism against untrusted access and phishing attacks using USSD”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, Page 1188-1193, Aug 2013

[4] M. Trojahn and F. Ortmeier, “Biometric authentication through a virtual keyboard for smartphones”, International Journal of Computer Science & Information Technology, Vol. 4, No. 5, Page 1-12, Oct 2012

[5] D. Bhave, P. Bhavsar, S. Chavan and K. Gore, “Keyloggingresistant visual authentication protocol”, International Journal of Advanced Research in Computer and communication Engineering, Vol 5. Issue 2, Page 520-524, Feb 2016 [6] Keylogger protection-System security research, GData, Whitepaper, Page 1-8, Mar 2014

[7] S. Bharadwaj, R. Prathyusha and Rajeesh Kumar, “Attack resistant visually authenticated and secured system”, International Journal of Research and Engineering, Vol. 2, Issue 2, Page 16-19

[8] D. Nyang, A. Mohaisen and J. Kang, “Keylogging-resistant visual authentication protocols”, IEEE Transactions on Mobile Computing, Vol. 13, No. 11, Page 2566-2579, Nov 2014

**PLAGRISM REPORT**

