Detection of vulnerable activities using the network traffic and keylogging techniques

Bhavyajeet Singh Bhati

Department of Information Technologyt. name of organization
NMIMS MPSTME
Shirpur, Maharashtra, India

Krishna Chouhan

Department of Information Technologyt. name of organization
NMIMS MPSTME
Shirpur, Maharashtra, India

Mananjay Purohit

Department of Information Technologyt. name of organization
NMIMS MPSTME
Shirpur, Maharashtra, India

Shlesh Jain

Department of Information Technologyt. name of organization
NMIMS MPSTME
Shirpur, Maharashtra, India

***Abstract*— Every computer user deal with serious privacy and security challenges. Even though they are frequently employed, a range of security measures like as anti-virus, anti-spyware, updates, and patches cannot ensure total protection. Software keyloggers are a malware subtype with a rapidly growing presence. A type of rootkit software called a keylogger logs keyboard keystroke events and saves them in log files. Because of this, it can gather private information like usernames, PINs, and passwords and communicate it to a hostile attacker without the users' knowledge. Keyloggers pose a serious threat to both personal and professional activities, as well as e-commerce, online banking, email chatting, system databases, and other operations. Antivirus software is routinely used to identify and get rid of keyloggers. However, it cannot detect undetectable keyloggers. Online conversations, noting visited URLs, and another user behavior can also be logged. Additionally, certain keyloggers have the capacity to remotely connect to the attackers and transfer the log file directly to them. An overview of keylogger programmers, types, features, and technique is given in this paper.**

***Index Terms*— *Keylogger, hooking, malware rootkits based on signatures, anomaly based, OS, API*.**

I. INTRODUCTION:

The safety and security of data being transferred between users through a network is crucial in the modern world. Businesses invest a significant amount of money to protect their data, whether it be customer data, logistics data, or any other form. Algorithms for cryptography are used by businesses to protect sensitive data. The corporation suffers a significant cost as a result of a flaw in its security mechanism, and the individuals whose data was compromised also suffer personal loss. Creating data that is as secure as possible is a must right now.

Every computer user faces two major challenges: security and privacy. There are many different types of security measures, including antivirus and antispyware. These defenses fall short of offering total security. The malware category of keyloggers is one that is continually expanding. Keyloggers record user information that is entered using a keyboard. These may include the user's username, password, pin number, and other vital details that could pose a serious problem for the user.

A key logger is a piece of software that runs in the background and gathers and keeps track of data and human input. This malware can install itself on a computer and begin recoding inputs, which the attacker can utilise for harmful purposes. It is a type of spyware that monitors keyboard input.

The following are a few instances from real life that demonstrate the existence of keyloggers on computers. A company's boss employed software to track the actions of the workers to discover whether any of them were engaging in unethical behaviour and disrupting the harmony between work and life. Some keylogger examples show off their benefits, such when parents watch their kids' actions and encourage them to study. When a user enters information using a keyboard, the keylogger records it and generates

some patterns; these patterns are then sent to a device drive that is part of the operating system. Pressing and releasing the keys are separated by a predetermined amount of time.

Here, we'll concentrate on software keyloggers, which are further classified into two categories based on how the logs are sent. The interval for sending logs cannot be modified once it has been specified in either situation. This debate does not cover malware with changeable time intervals, such as botnets, Trojans, backdoors, and other keyloggers. Many of the keyloggers (both shareware and freeware) that we have tested are accessible online. 5 Software keyloggers fall into the following categories: To obtain the log files, an attacker would require physical access to the machine. 2. Remote keyloggers: These record user behaviour and transmit the log files to the attacker via email, FTP, network shares, botnets, P2P servers, etc.

II. Literature Survey:

A. Companion Research

The literature review for this study was conducted to ensure the best outcomes and to provide resources for future studies. The TCP protocol and the wireshark packet sniffer have been used by previous academics to examine packet analysis and network traffic monitoring in a number of researches works, such as [1]. The data were the TCP time sequence graph, TCP throughput graph, and TCP round trip time graph. based on network traffic analysis of data. Numerous recommendations for managing network traffic were offered by the researchers. In a manner similar to this, [3] proposed a novel strategy for system monitoring. Based on traffic behavior patterns and a history of related traffic, it can deliver precise information. While significant amounts of internet traffic data were tracked for study.

B. Network Monitoring

A network administrator may be able to take preemptive action using the information gathered by monitoring an operational network.

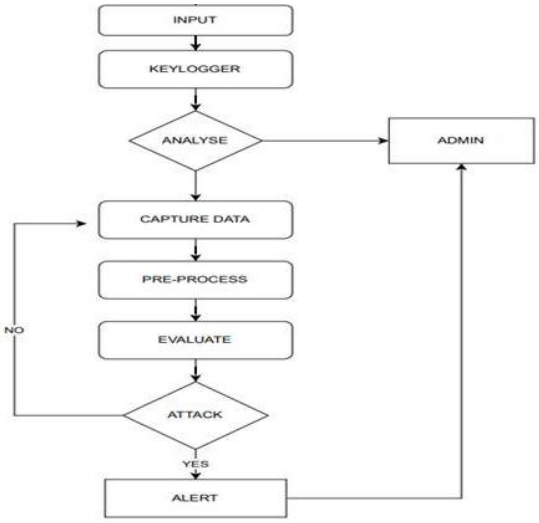
Manage the network and make usage data available to others. A network administrator can examine connection activity, error rates, and link status, among other things, to evaluate the usability and functionality of a network. A network administrator can keep track of the project's progress by gathering and studying this data over time. A failing component might also be spotted and replaced by the administrator before it entirely fails. Using SNMP, device data is routinely gathered [6].

Simple Network Management Protocol, managers can now have access to IP network nodes such as servers, workstations, routers, switches, and security devices (SNMP). It aids network managers in their attempts to keep an eye on and control network performance, track down and fix network issues, and prepare for network expansion. Administrators and agents can communicate using a message format provided by the SNMP application layer protocol. The three parts that make up the SNMP system are the SNMP manager, SNMP agents (managed node), and Management Information Base (MIB) [7].

C. Detection and prevention

Keyloggers have so far been investigated in this study from a black hat perspective, or how they are designed, implemented, and used. This section discusses one of the main goals of cybersecurity education, which is to teach students how to become "white hat hackers," or professionals who can identify security flaws and aid software developers in fixing them before malware can exploit the system. White hat hackers should therefore consider keylogger detection and prevention: While detection makes a specialty of locating a keylogger that has already infected a device so that it may be properly removed, prevention focuses on preventing keyloggers from accessing a device.

III. RESEARCH METHODOLOGY:



METHODOLOGY: KEYLOGGER SYSTEM:

Keylogger systems can be created using one of three basic techniques: Windows Keyboard Hook, Keyboard State Table, or Kernel-Based Keyboard Filter Driver [8]. To start, the operating system-based Windows Keyboard Hook technique gives hook-based keyloggers some capabilities for keyboard surveillance. When a key is pressed, the OS records the action and registers the character. Later, before reaching the original target that received the message, each message sent using this protocol is first approved by the application. This method is now used by the majority of keyloggers to record keystrokes.

Windows message hooks are available in two flavors: global hooks examine system-wide messages and local hooks examine message-specific to an application.

1) All keyboard messages can be read by the keyboard hook, which can then pass them on to the next hook function in a chain.
2) Can change the original message and send it to the next hook procedure.
3) By refusing to pass the message on to the next hook method, it has the power to halt the flow of the message.

The second technique makes use of a keyboard state table, which has a table containing the status of 256 virtual keys. Applications that employ a window interface therefore make use of this table. This table is often used by applications to determine the current status of the key, such as whether it is up or down. When the Ctrl or Shift keys are hit, a keylogger, for example, may use the GetKeyboardState API calls to reveal or disclose information about keystrokes by attaching its thread to the window's top-level thread message loop using the Attach-ThreadInput API. The Kernel-Based Keyboard Filter Driver approach installs them on a target system only after gaining administrator access, in contrast to other approaches. They are hard to detect and located at the kernel level. A keylogger can collect keystrokes and other data even before it reaches the operating system by utilising a keyboard filter driver that is installed prior to installing the system's keyboard device driver [9].

A. Keylogger Characteristics

The primary function of keyloggers is to record a user's keyboard activities, but they have advanced features that go far beyond that. They can, for example, monitor any computer programme that is running. Keyloggers record, sense, and send the following data [10]: Keyboard actions:

1) Monitoring the site
2) Chatting Watching
3) Program / Tracking Application
4) Recording Printing Activity
5) Clipboard recording and Monitoring
6) E-mail Reporting
7) Password Protection and Hot Key.

B. How keyloggers spread

Keyloggers are spread similarly to malicious software. With certain exceptions, software vendors define a keylogger as a piece of software intended to covertly record and monitor all keystrokes. For instance, a resentful spouse or partner can buy keylogger software and install it on the victim's machine to watch what she or he is doing. The methods listed below are primarily used to distribute keyloggers [11], [12]:

1) Opening emails and files with attachments triggers keylogger installation.
2) A keylogger may be installed when a file is opened from a P2P network's open-access directory.
3) A web page script that takes advantage of a browser vulnerability can put a keylogger on your computer. When a user accesses a compromised website, the keylogger programme is run automatically,
4) If a malicious programme is capable of downloading and installing further malware to the system, it may be able to install a keylogger on the target PC.

Proactive detection techniques:

Keylogger protection techniques are comparable to those used to identify other malware, especially rootkits. It is a good idea to use the following procedures [11] to thwart suspected keyloggers:

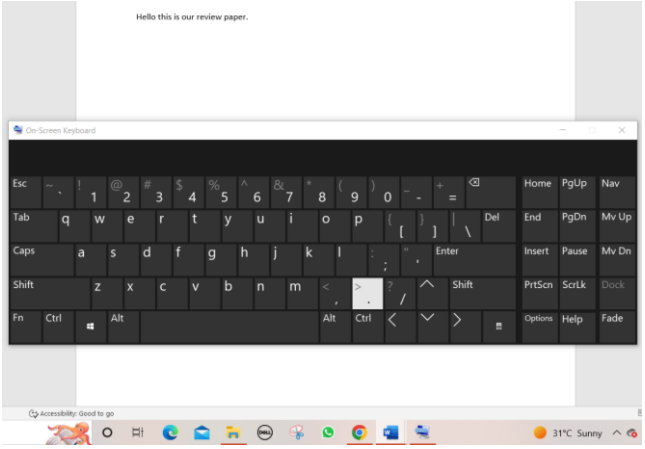
Keyloggers' primary objective is to retrieve sensitive information, hence two-step authentication or one-time passwords are essential.

Web filtering can be used to prevent access to shady websites. The keyboard is a keylogger's primary target. Therefore, substitute a virtual keyboard for a physical one.

Maintain and update your anti-malware program frequently. Monitor sensitive machines and turn them off when not in use by using keylogger detection software (such as SnoopFree Privacy Shield) [2].

Do not grant administrator access to an insider user. Install software policy controls on endpoints (such as WebSense CPM);
Stop unauthorized connections between endpoints and external websites. Using a virtual keyboard is the greatest strategy for providing a reliable detection technique against both keylogging hardware and software. An application included in the Windows

operating system's virtual keyboard displays an ethereal keyboard on the screen. The virtual screen keyboard's keys can be pressed with the mouse.



On-screen keyboards, on the other hand, are not a trustworthy detection strategy for thwarting keyloggers. Through an on-screen keyboard, a malicious application can quickly halt entered keystrokes and mouse clicks. It is recommended to use on-screen keyboards that have been properly designed to make sure that data communicated over the on-screen keyboard cannot be accessed. A function that lets users enter characters by briefly holding the mouse over a letter is also available on some virtual keyboards. So, the user doesn't even need to click the mouse button to input the password [4].

IV. RESULT AND DISCUSSION:

The conclusion is the security of the system is an important part of any organization to make the system more secure. The keylogger which is detected is analysed by the input keystrokes and the network traffic analysis. Analysers keeps the eye on the network activities and report to the admin/system administrator. Keyloggers are powerful tools that only compromise a user's personal information, such as their user name, password, pin number, and card bank, rather than the entire system. Many keyloggers are used illegally by their makers, despite the fact that certain keyloggers are used legally. This document covers the vast majority of keylogger types and concealing tactics used on rebellious users' machines. Additionally, we looked at keyloggers' situation today and their dissemination methods. In the end, we examined the detection methods already in use and provided some prevention strategies. Regulating keylogging technology within the company necessitates widespread awareness, regular monitoring, and multiple layers of protection, just like other risky code or threats. The key is to be conscious of the threat they pose, to understand how they are employed, and to have appropriate means of detecting them. The organization's incident response plan must consequently incorporate keylogger detection and mitigation.

REFERENCES:

[1] A. Bhandari, S. Gautam, T. K. Koirala, and M. R. Islam, "Packet Sniffing and Network Traffic Analysis Using TCP—A New Approach," in Advances in Electronics, Communication and Computing, ed: Springer, 2018, pp. 273-280.
[2] G. Canbek, “Analysis, design and implementation of keyloggers and anti-keyloggers,” Gazi University, Institute of Science And Technology, M.Sc. thesis (in Turkish), Sept. 2005, pp. 103.
[3] S. L. Rosa and E. A. Kadir, "Abnormal internet usage detection in LAN Islamic University of Riau Indonesia," in Proceedings of the International Conference on Intelligent Science and Technology, 2018, pp. 17-22.
[4] S. Shetty. 2006,” Introduction to Spyware Keyloggers”. http://www.securityfocus.com/print/infocus/1829.
[5] H. Pathak, A. Pawar and B. Patil, “A survey on keylogger-A malicious attack”, International Journal of Advanced Research in Computer Engineering and Technology, Vol. 4, Issue 4, Page 1465- 1469, Apr 2015
[6] T. Lammle, CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120: John Wiley & Sons, 2013.
[7] T. Lammle, CCNA Cisco Certified Network Associate Deluxe Study Guide: John Wiley & Sons, 2011.
[8] S. S. A. G. CANBEK. (2009) Keylogger Increasing Threats to Computer Security and Privacy. IEEE TECHNOLOGY AND SOCIETY MAGAZINE.
[9] D. Wampler, James H. Graham. “ANormality based method for detecting kernel rootkits”. ACM SIGOPS Operating Systems Review, 2008, 42(3).
[10] A. R. P. Kalpa Vishnani, and Radhesh Mohandas, "An In-Depth Analysis of the Epitome of Online Stealth: Keyloggers; and Their Countermeasures," Dept. of Computer Science & Engg, National Institute of Technology Karnataka, Surathkal, Srinivasnagar, Mangalore -575025, India, 2005.
[11] “How they work and how to detect them Part.”, http://www.securelist.com; accessed Sept. 2009.
[12] B. Whitty, “The ethics of key loggers,” Article on Technibble.com, June 2007 (accessed December 8, 2011), http://www.technibble.com/the-ethics-of-key-loggers/.