Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

Real Time Working of Keylogger Malware Analysis

Manan Kalpesh Shah [1], Devashree Kataria [2], S. Bharath Raj [3], Priya G [*]
Department of CSE, VIT Vellore

Abstract **- In the world with increasing technology the safety should also increase. The effect of malware is getting worse, studies say. There are two kinds of malware analysis listed here. Static Malware Analysis is one, and Dynamic Malware Analysis is another. It is likely that about one out of many large companies systematically monitors the computer, internet, or email use of its user's employees. Today, over a hundred different products are available that will allow companies to see what their customers do on their "personal" computers, in their emails, and on the internet at work. This paper, of course, aims to propose a real time working keylogger. Both keystrokes along with the screenshot of the application in which the keystrokes were entered are logged by the keylogging software and sent via an email. Using this we capture all information in text form. Security is the at most importance in the current generation and thus key logging and its other functions motivated us to take up the topic.**

Keywords—Malware, Detection, Hackers, Keylogger, Keystroke, Emails

I.INTRODUCTION

Idealistic hackers attacked computers in the early days because they could, or to show off to one another. Cracking machines, however, has become an industry today. Despite recent improvements in computer hardware and software security, in both frequency and sophistication, attacks on computer systems have increased. Unfortunately, there are major limitations in current strategies to identify malware and evaluate unknown code samples. Today, the Internet is becoming an integral part of many people's everyday lives. Many resources are available on the Internet and are also rising day by day. These programmes are being made use of by more and more people. Examples of commercial services offered on the Internet are online banking or advertisement. There are people on the Internet with malevolent intent, just as in the real world, by taking advantage of legitimate users whenever money is involved. Malware such as malicious-intention apps helps these individuals achieve their objectives. Antivirus software is designed to block or delete malicious software and its files from your device by detecting, preventing, and taking action.[1] Your machine will also search for behaviours that may indicate the existence of new, unidentified malware. We concentrate on a specific form of malware, keyloggers. Keyloggers have become an increasingly serious issue because most antiviral remedies make them essentially undetectable.

II.WHAT IS MALWARE?

Malware is malicious software or a programme to manipulate the device and gain private information from the user. Computer viruses, worms, Trojans, ransomware, scareware, spyware, cryptocurrency miners, adware, and other programmes are provided with malware of various names to hack computer systems for harmful purposes [2]. The purpose of such malware can vary in terms of the purpose of its creation and the collection of personal data from its decision-making systems. Malware stands for malicious software, crafted without the informed consent of the user, to damage a computer device. Malware is typically classified into the following categories:

1. Virus: It is a programme that links to other programmes to infect the programme and perform certain unwanted functions
2. Trojan: Trojan makes self-copies and steals data from them. It is a standalone malicious software that aims to fully automatically corrupt other computers without assistance from outside powers, such as other programmes.
3. Worms: A worm is a self-replicated computer malware programme that uses computer and network resources without permission from the authenticated user. Network bandwidth is consumed within the network. On the target computer, this is a security shortcoming.
4. Spyware: It is installed without the consent of a user in order to disclose the user 's actions to the attacker.
5. Rootkit: Rootkit is a malware programme that generates a loophole for the hacker to use in the device, modifies log files and removes data files.[3]

III. MALWARE ANALYSIS

The process of determining the purpose and characteristics of a given malware sample, such as a virus, worm, or Trojan horse, is malware analysis. This process is a required step in order to be able to establish successful malicious code detection techniques [3]. Basically, the methods used to analyse malware can be divided into two categories: static and dynamic (live). The static analysis tools aim to analyse a binary without the binary actually being performed. The behaviour of a binary after it has been executed can be analysed through live analysis software. The following sections explain Static and Dynamic Analysis in depth. A nearly intractable problem is automated malware detection. It is simply not possible for one programme to evaluate another programme 's exact actions. [4]

Static analysis - Static analysis is called testing software without running it. It is possible to apply static analysis techniques to various representations of a programme. The binary representation of a programme can also be used by static analysis software. Some data gets lost while compiling a programme's source code into a binary executable. This lack of data further complicates the task of code analysis. Often manually, the task of inspecting a given binary without

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

executing it is carried out. For example, some useful details, such as data structures and functions used, can be extracted if the source code is available. Once the source code has been compiled into a binary executable, this data gets lost and thus impedes further study. For static malware analysis, there are distinct techniques used. Any of the explanations below are.[5]

- File fingerprinting: In addition to inspecting obvious external binary features, this involves file-level operations such as computing the binary's cryptographic hash (e.g., md5) to differentiate it from others and check that it has not been changed.
- File format: Additional useful information can be obtained by exploiting the metadata of a specified file format. In order to specify the file form, this requires the magic number on UNIX systems. For example, a lot of information can be extracted from a Windows binary that is usually in PE (portable executable) format, such as compilation time, imported and exported functions, as well as strings, menus, and icons.
- AV scanning: If the examined binary is a well-known malware, one or more AV scanners are highly likely to detect it. Using one or more AV scanners takes time, but often it becomes a requirement.
- Detection of packers: Malware is now often distributed in an obfuscated form, such as encrypted or compressed. Using a packer, this is done, although it is possible to use arbitrary algorithms for adjustment. [6]

Limitation of Static Analysis - The source code of malware samples is usually not readily accessible. That reduces to those that retrieve the information from the binary representation of the malware the relevant static analysis techniques for malware analysis. Consider, for instance, that most malware targets host in the IA32 instruction set running instructions.[7] If the binary employs self-modifying code techniques, the disassembly of such programmes may result in ambiguous results.

Dynamic Analysis **-** In order to evaluate the malicious activity, which is called dynamic malware analysis, a given malware sample can be executed within a managed environment and track its behaviour. Dynamic malware analysis evades the constraints of static analysis (unpacking problem) because Dynamic Malware Analysis is performed during runtime and malware unpacks itself. The real action of a programme is therefore easy to see. [10]

The key downside, however, is the so-called dormant code: that is, dynamic analysis typically tracks only one execution path, unlike static analysis, and thus suffers from insufficient code coverage. In addition, if the research environment is not adequately isolated or limited, there is a possibility of compromising third-party systems. In addition, samples of malware can modify their actions or stop executing at all once they detect that they are being executed in a managed analysis environment. [10]

IV.KEYLOGGER

Keyloggers are commonly referred to as tracking software, software for controlling user operation, controlling keystroke systems, keystroke recorders, keystroke loggers, keyboard sniffers, and snoop ware. While keyloggers' primary objective is to track the keyboard behaviour of a user, they now have capabilities that extend beyond that feature. On a computer, they can monitor almost everything that runs.[12] Some keyloggers, known as "screen scrapers," allow a target machine to be visually tracked by taking periodic snapshots of the screen. You can then use the captured images to obtain useful information about the user. Advanced keyloggers can monitor operations such as cutting, copying, and pasting, Internet use, file operations, and printing. Keyloggers are often used to track the activities of users and to capture data such as personally identifiable or otherwise private or sensitive data. Keyloggers, including viruses and worms, are distinct from other forms of spyware or malware. They share system resources with legitimate programmes, remain invisibly resident on the system for as long as required, and are carefully and clearly programmed to perform their tasks without drawing users ' attention. Examples of corporate spyware based on keystroke logging have also reported substantial growth, despite organisations having anti-virus software, anti-spyware, and firewalls.[13] The Websense Web@ Work Survey 2006 reported that the growth in keylogger instances had increased. There are several various computer-based operations being tracked by keyloggers. Users' keystrokes or other operating system activities are saved and/or transmitted through keyloggers on local or remotely accessible discs. In most cases, keyloggers send the keystroke logs to the attackers by email.[13][14]

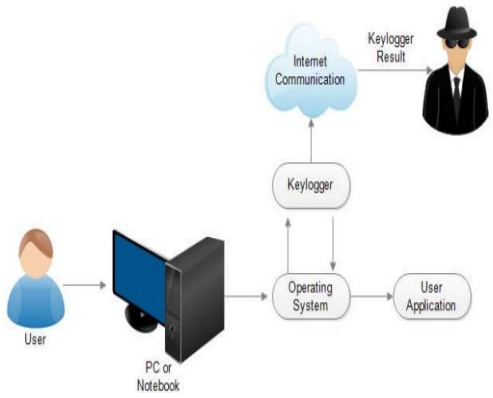

Figure 1 – Keylogger Outline

V.TYPES

It is possible to divide keyloggers primarily into two categories: hardware and software:

Keyloggers for Hardware - Small electronic devices used to record the data between a keyboard interface and an I / O port are hardware keyloggers. After being installed on a computer system, they store the keystrokes in their built-in memory. Some models are mounted within the computer case, within the keyboard port, or directly within the keyboard itself, while others are plugged into the end of the keyboard cord. This hardware does not use the resources of any computer. [14]. Anti-viral tools or scanners cannot identify it because it operates on the hardware platform. It also does not use the hard

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

disc of the computer to store the records of the keystrokes. The recorded keystrokes can be stored in their own memory, which normally exceeds 2 MB, in encrypted form. To relay keystrokes using the improved encoding scheme, an acoustic keylogger, a sort of hardware keylogger, was implemented. This is accomplished by examining the repetition frequency, the timing of different keyboard strokes, and other background details of related acoustic keystroke signatures. This keylogger is potentially more noticeable than a conventional keylogger because it absorbs the processing resources of a computer during data transmission, and because it causes faint, structured sounds to be generated by the internal computer.[16]

Keyloggers for Software - In the target operating system, software keyloggers monitor systems that collect keystroke data, store them on disc or in remote locations and send them to the intruder who installed the keylogger. On the Internet market, commercial software keyloggers are readily available while the parasitic ones are created or used by hackers. There are several real-life incidents that have involved keyloggers. Operating system-specific and Windows operating systems are tracking methods for device keyloggers.[17] The operating system's keyboard driver converts a keystroke into a Windows message called WM KEYDOWN when a user presses a key in the WOS. In the machine message queue, this message is moved. In turn, the WOS will place this message in the message queue of the application thread related to the active window on the computer. The thread polling this queue sends the message to the active window's window procedure. The Keyboard State Table method, the Windows Keyboard Hook method, the Kernel-Based Keyboard Filter Driver method and Innovative methods are four main methods for designing keylogger systems. Computer keyloggers have a variety of features:

- Any user-type keystroke;
- Mouse (clicks and movements) actions;
- Opened or centred windows title;
- Periodic or event-triggered screenshots of screens;
- Running applications and statistics of usage;
- Operations of the file system (create, rename, change, access and delete);
- Internet use (pages visited and duration of visit per page);
- Sent, received, and even unsent emails [16]

VI.KEYLOGGERS IN ACTION

For several purposes, keyloggers may be used to satisfy various requirements of different users, including government, military, and law enforcement organizations' offices, information security experts, employees, administrators, parents, teachers, and couples. The majority of keyloggers are used for confidential information collection and identity theft, and these uses are illegal. But valid applications, such as intrusion detection, police computer forensics, parental control, monitoring and surveillance in the workplace, and disaster recovery, are also available.[18]

In our paper we are going to be showing the implementation of keylogger and the way it will be a serious threat to computers. Keystroke logging is additionally called key-logging or keyboard capturing. This can be the act of recording the keystrokes on a keyboard. It's typically done covertly so as to confirm that the user i.e. person using the keyboard is in the dark about his or her actions being monitored. Data can then be retrieved by the person operating the logging program.

Figure 2: Keylogger

VII.PROPOSED METHODODLOGY

When the code is executed, the user is asked to sign in using his email credentials. If the entered data is wrong an error will pop up not allowing the program to send the data. If the details are entered right the program starts to record the data the user types. We have added conditions for example a limit to be sent. So, if the word limit exceeds the given amount the data will automatically be sent to the email id as provided by the user. The keyboard input is recorded and based on what is pressed, different conditions are called.

- For a normal letter, it gets added to the string
- If a backspace, the last letter gets deleted
- If space key is pressed, a white space is added between the words.

After reaching the word limit it then takes a screenshot using the pyscreenshot. grab () function. It then saves the image and attaches it the final message which is first encoded into a string using the MIMEText. The final message is then sent to the user.

Functional Requirements

- SMTP server
- Email library
- Internet connection

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

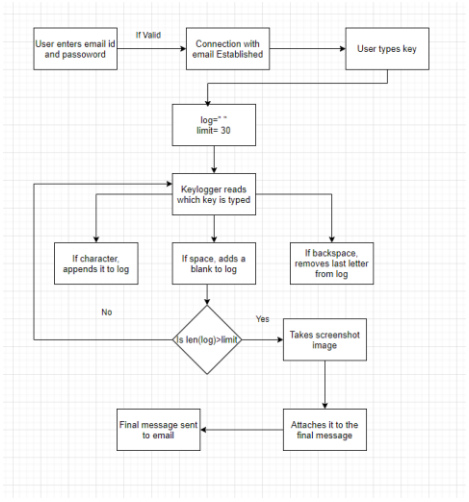

Figure 3 : Methodology used

VIII.RESULTS

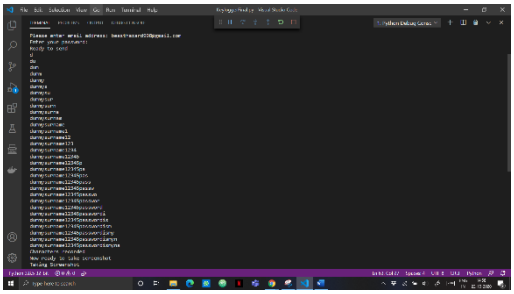

Figure 4 – Executing the code

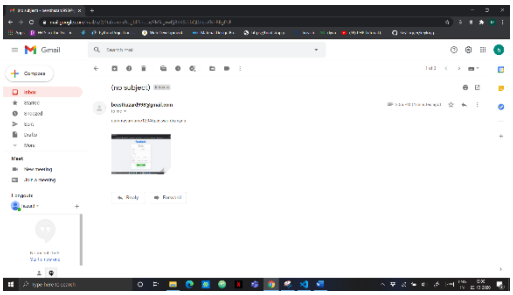

Figure 5 – Email sent by the keylogger

As you can see when the user starts typing his or her details on the Facebook signup page, each key stroke pressed by him is recorded. After reaching the word limit it then sends out an email with the keystroke and email attached. This can be dangerous as the password typed by the user is clearly visible to the intruder.

IX.SOFTWARE SECURITY MEASURES

To protect personal or institutional information properties, measures to detect keyloggers are necessary.[19] Users of computers should know how to identify the presence of mounted keyloggers on their computers. Some of the general metrics are:

- Firewall, antispyware, anti-keylogger, and anti-virus software warnings.
- Some keys do not work properly.
- It takes time after a key is pressed for a character to appear on the screen.
- Mouse clicks don't always work.
- Double clicks and drag-drop operations work oddly.

Even after restarting a system, if any of these signs occur, it is probable that a keylogger remains in the operating system. Users should always keep keylogger threats in mind when entering sensitive information through a keyboard. Even if virtual keyboards are present in applications such as online banking or online shopping to enter personal data, virtual keyboards do not fully protect the personal information of users. It should not be overlooked that certain sophisticated keyloggers are able to take screenshots to show sensitive details based on mouse clicks. Any additional steps that can be taken are as follows:

- Always be mindful of any operation on the machine
- Using other methods for prevention, such as firewalls, anti-virus, anti-spyware and anti-spam software.
- Never let your machine leave others alone.
- Always be mindful of keylogger signals and tracking systems for operation.
- Use keyboards on the phone.
- Maintain up-to - date security updates.
- Only download programmes from reputable websites.
- Read all security alerts, licencing agreements, and pop-ups for privacy declarations.[19]

For detecting and removing spyware, malware, and viruses, use one or more anti-spyware software.

X.CONCLUSION

We have discovered the fundamentals of malware, malware detection, and malware analysis approaches. We've also heard about static malware analysis limitations. Dynamic malware analysis is the best way to test malware samples, following the controversy between static and malware analysis. We have gone through the different methods for malware detection in this.

Keyloggers are important tools with several tasks that can be performed. Although some keylogger implementations are legitimate, many (maybe most) keyloggers are illegally used. Normal machine-to - machine interface safety mechanisms do not secure computer systems from attacks by keyloggers. In order to combat keylogger intrusions, human-to - machine interfaces must be considered. It is expected that the risks of keyloggers will emerge more and more. Users should be conscious and follow protective measures of this high risk of using computers. Unfortunately, although there are papers, materials, and websites about keyloggers, there is not enough data, especially about emerging threats. Using a full security solution that covers a broad spectrum of threats is the most productive way to reduce security risks. In certain cases, the judicious use of keyloggers by employers and computer owners may enhance security, privacy, and productivity.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

XI.REFERENCES

[1] https://www.researchgate.net/publication/ 267777154_Malware_Analysis
[2] https://www.uc.edu/content/dam/uc/infosec/do cs/policies/Information_Security_Incident_Management_and_Respo nse_Policy_9.1.8.pdf
[3] https://www.ijcsmc.com/docs/papers/May2015/ V4I5201599a46.pdf
[4] http://www.academia.edu/Documents/in/MalwareDetection
[5] https://www.researchgate.net/publication/303869 808_Information_security
[6] https://pdfs.semanticscholar.org/b832/6dec72b01db80c6fb3844920e d61794268c2.pdf
[7] https://pdfs.semanticscholar.org/6f98/eaabc025ad13a49cdf917665db 4313107bbc.pdf?_ga=2.24736638.57537598.1596081439-1260235423.1596081439
[8] Bayer, U., Moser, A., Kruegel, C. and Kirda, E. (2006) Dynamic Analysis of Malicious Code. Journal in Computer Virology, 2, 67-77. http://dx.doi.org/10.1007/s11416-006-0012-2
[9] Moser, A., Kruegel, C.and Kirda, E. (2007) Limits of Static Analysis for Malware Detection. 23rd Annual Computer Security Applications Conference, Miami Beach, 421-430.
[10] Dynamic Analysis of Malware, http://0xbadcab1e.lu/papers/analyse.pdf
[11] 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.
[12] J. Wurtzel, "Bugging your keyboard," BBC News, Science/Nature; http://news.bbc.co.uk/1/hi/sci/tech/1638795.stm, accessed Sept. 2006.
[13] Anti-Spyware Coalition, "Spyware definitions and supporting documents," ASC, working rep., June 29, 2006; http://www.antispywarecoalition.org/documents/documents/ ASCDefinitionsWorkingReport20060622. pdf; accessed Sept. 2007.
[14] W. Fabian, "Beyond cryptography: Threats before and after," in Proc. Int. Carnahan Conf.
[15] S. Sagiroglu and G. Canbek, "Keyloggers," IEEE Technology and Society Magazine, vol. 28, no. 3, pp. 10 –17, fall 2009.
[16] Stout, Kent,"Central Logging with a Twist of COTS in a Solaris Environment.", SANS Institute, March 2002, URL: http://www.sans.org/rr/papers/52/540.pdf
[17] ThinkGeek.com, "Spykeylogger,"2010(accessedMay 8, 2010), http://www.thinkgeek.com/gadgets/security/c49f/.
[18] https://iopscience.iop.org/article/10.1088/1742-6596/954/1/012008/meta
[19] Information about keylogger Available at http://coolhackingtricks. blogspot.in/20 11 III Iwhat-is-keylogger.html
[20] Mohammad, W., Robin, S., Avita, K., Goudar, R.H., Singh, D.P., Bhakuni, P., Tyagi, A.: A Framework for Detection and Prevention of Novel Keylogger Spyware Attacks. In: Proceedings of 7th International Conference on Intelligent Systems and Control (2013)
[21] Li, S., Roland, S.: A Novel Anti-Phishing Framework Based on Honeypots. IEEE eCrime Researchers Summit (2009)