iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.51006

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Keylogger Deployment and Detection

Sankalp Thorat[1], Riyesh Rahate[2], Das Paramjeet Singh[3], Ganesh Shinde[4]
[1, 2, 3, 4]*Student, Computer Engineering, MGMCET*

Abstract: ***T Keylogger is software used to record keystrokes of a user. It is a very important tool of surveillance as it records the activity of a user. Keyloggers can be used for constructive as well as destructive and malicious purposes. In this project we intend to make a keylogger which can be used as a means of control and surveillance by employers and parents. We also intend to create a program which can be used to detect keyloggers embedded in our system without our permission. Passwords are the need of the hour and so is its protection. Keystrokes monitoring by using keylogger is an advanced way to steal passwords and valuable data and more sophisticated methods of doing this are cropping up. Keyloggers provide a middle ground for surveillance as it is neither too invasive, nor too lax. In this project we make a case for a better use of keyloggers and enlightening people about the various uses and dangers of keyloggers. Keylogger detection is an important part of cybersecurity, given how easy it is to code a keylogger and easy to deploy, keylogger detectors should be of high importance and must be included in all malware detection software. In this project we explore the different types of keyloggers, their effectiveness, and their shortcomings and base our opinion on these facts.***
Keywords: Control, Surveillance, Keyloggers, Cybersecurity, Record

I. INTRODUCTION

The term ‘keylogger’ itself is not malicious; it’s just software for logging keystrokes. However, a keylogger isn’t always software; it can also be a device. The creators of such software offer many cases in which it would be appropriate to use keyloggers, including: 1)Parental control: many children are given unrestricted access to the internet at a young age but their minds are still quite impressionable and parents would still want to monitor their browsing, thus not completely blocking the internet access of their children; 2) Company security: many employees use their work computers for personal use as well, companies need to monitor this as there can be sensitive data on the device which can be accessed by a hacker who might’ve entered dues to an employee’s carelessness while using the system for their personal use; 3)People in a relationship can use a keylogger to track the actions of their significant others on the Internet if they suspect them of cheating. Keyloggers are of two types—hardware and software. Keylogging devices are rarer than software. There are a lot of legitimate programs which are designed to allow administrators to track what employees do throughout the day, or to allow users to track the activity of third parties on their computers. Legitimate software can be used by a bad actor to deliberately steal confidential user information such as passwords. There are hardware devices can be plugged between keyboard port and the CPU and some can be attached to the PC hardware inside itself, they intercept all the signals as you one types out that but that will need physical access to the computer.

II. LITERATURE REVIEW

The main problem of a keylogger is it is very difficult to categorize it by its pattern. There are so many different key loggers in this world and each one has its own pattern. There are Kernel based keyloggers which obtain root access to hide itself in the operating system and intercept keystrokes that pass through the kernel. These kinds of keyloggers are very powerful because they reside at the kernel level which makes them very difficult to detect. The next one is Memory-based computer keylogger which modifies sets of codes to bypass normal authentication, a memory-based keylogger is also difficult to detect, as it operates directly from computer memory. It records keys as they pass through the path of the operating system to reach their destination. A computer keylogger software infection will eventually result in data breaches. With your personal information in the wrong hands, unauthorized actions will follow.

A. Disadvantages of Keyloggers

1) Unsophisticated keyloggers are easily detected using antimalware software
2) Experts can detect a keylogger easily
3) Keyloggers overload the system and this is easily caught by even the most casual of users

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Many anti-viruses include keylogger detection mechanism in their software, but there is a lot of overlap between the databases of signatures of these keyloggers, this will cause more harm than good because attackers always tend to be a step ahead. A user-space keylogger hides itself as a background process and then starts logging keystrokes, thus mutating almost every day, that's why signature matching does not work anymore.

Mugdha Kolte in "Unprivileged proposed detection of user-space keyloggers" process analysis based approach to detect such malicious program. By sending string to all the other running programs and monitor their allocated memory size changing pattern, detection of keylogger is possible. The major drawback of this approach is that it is tedious- it takes a lot of time to constantly monitor.

The user has to run that program for a full system scan to detect the malware, but the problem arises within two scanning gap period. The victim is still unprotected within that time. Ortolani proposed a new technique for detection of keyloggers through input/output monitoring: by implementing a controlled way of sending strokes into the system and constantly monitoring the behavioral changes made by input/output provided a better solution, but Windows do not provide this kind of permission to the user level. It needed privileged API permission to get proper information. And then entering the string through an unprivileged API command, a pattern has been generated from the output. That helps to find out suspicious activity.

III.METHODOLOGY

A. Proposed System-

Our proposed system includes-

1) Building a user-friendly interface which will allow the user to choose between deploying a keylogger and detecting a keylogger in the system of their choice.
2) Our frontend involves the interface and our backend involves a Python program which will log all the keystrokes and make decisions based on keylogger deployment algorithm.
3) If the user wishes to detect a keylogger, the backend program will use the keylogger detection algorithm.

B. Algorithm

1) Deployment

a) The program will wait for all the system processes to initialize.
b) The keylogger daemon is initialized and the process will be gauged in scale of time.
c) A log file is created for the current session to log all the keystrokes and maintain a record.
d) If no event occurs, keylogger continues listening to the strokes.
e) If an event occurs, the keylogger classifies the type of keystroke that has occurred- special key which are commands or normal text input.
f) If a special key that gives a command has been entered then it is compared with a value in a dictionary and recorded in the log file.
g) If a normal text i.e. anything in the range of ASCII characters has been inputted, the ASCII code is converted to its respective character and this is exported to the log file.
h) The inputs along with their timestamps are recorded in the log file.

2) Detection

a) The program checks if there has been any delay in normal registering of keystrokes.
b) If there is no delay then exit. If there is a delay then go to step 3.
c) Import the list of all the startup processes and monitor them for memory usage.
d) Simulate pseudo-random keywords and observe the resource usage within the processes.
e) If any processes have irrelevant memory usage, they are removed for e.g. system processes, user processes are kept and monitored.
f) Input pre-determined strings and obtain memory values.
g) If the same increment patterns are observed go to step 8, else go to step 5.
h) The process is flagged as a keylogger and exit.

C. Block Diagram

1) Deployment

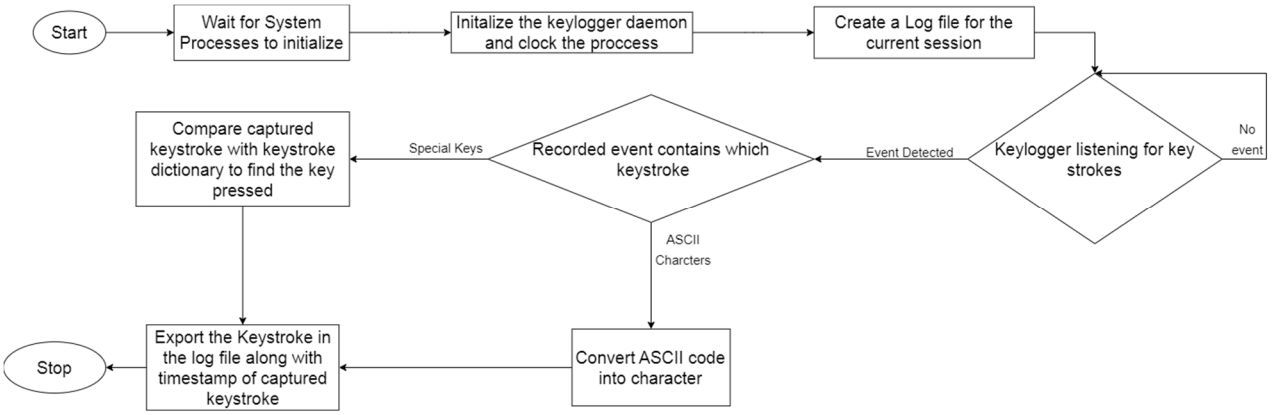


Fig. 1 Keylogger Deployment

2) Detection

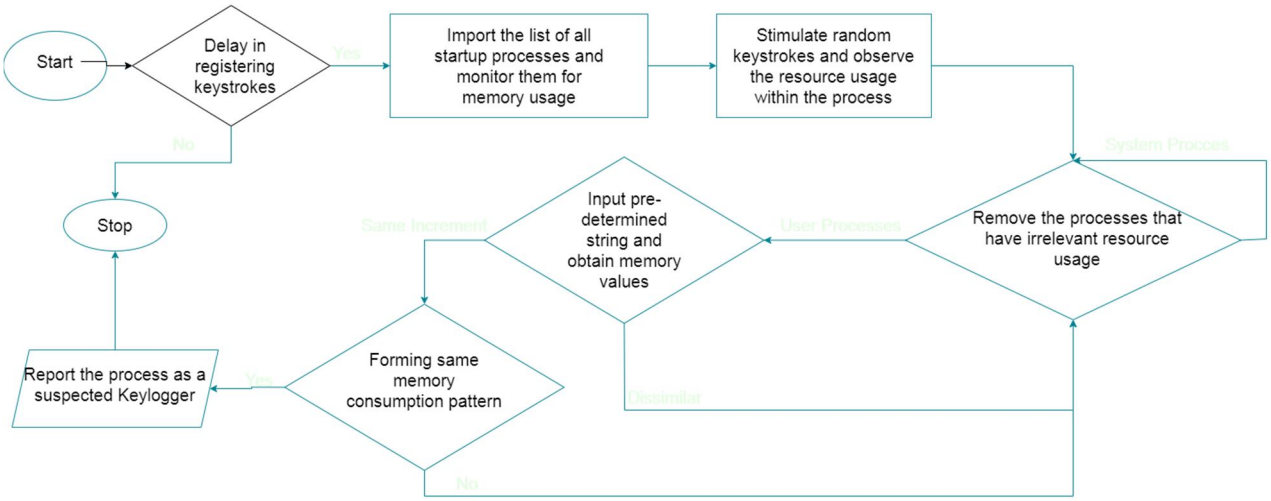


Fig. 1 Keylogger Detection

IV. FUTURE SCOPE

1) Privilege escalation mitigations (Running keylogger in non-admin mode to avoid privilege exploitation)
2) Using UTF-8 Unicode characters instead of ASCII (UTF-8 will provide a higher scope for character detection)
3) Optimizing heuristic operation of keylogger (Optimizing RAM usage so that the keylogger uses low RAM and becomes difficult to get noticed

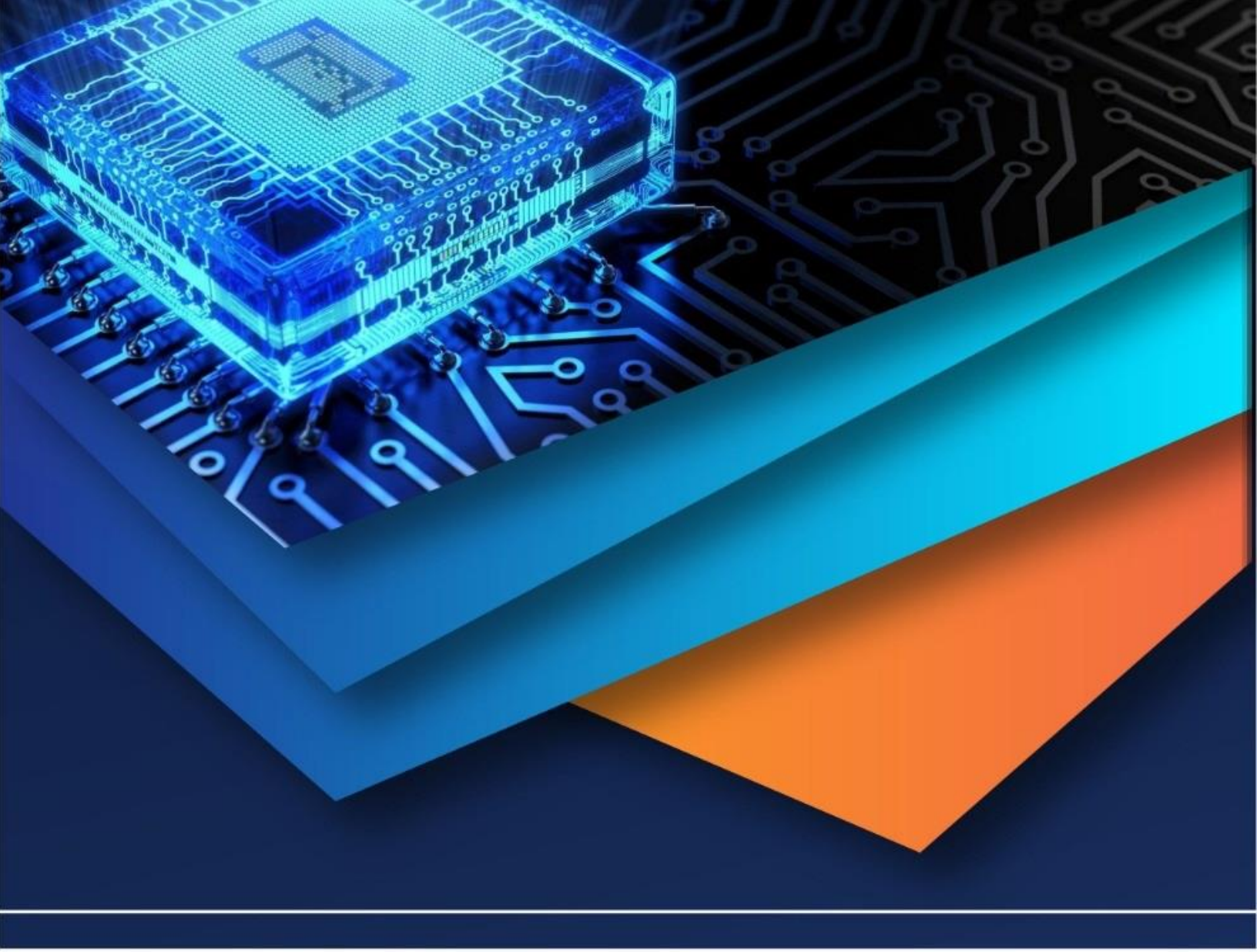
V. CONCLUSION

We have thus designed a system to deploy and detect a keylogger. This system is not perfect by any stretch and we aim to better it as time goes on. We aim to make this system more user-friendly and interactive. There are multiple ways of capturing keystrokes since all a keylogger needs is to sit between processes and record it and there are multiple ways to detect a keylogger, there is no single, perfect way of detection.

We need to be with the times and ahead of a malicious user. And also for searching in RAM will be easier if we use any searching mechanism or string matching program. The goal was to create a method for keylogger detection and make it easier for non-technical person. This proposed method does not need any special technical knowledge. Any regular person will be able to handle it.

REFERENCES

[1] Md. Bayzid Ahmed, Mohiuddin Shoikot, Jafrul Hossain, Anisur Rahman. Keylogger Detection using memory forensic and network monitoring. Research October 2019.
[2] Chien-Wei Hung, Fu-Hau Hsu*, Shih-Jen Chen, Chang-Kuo Tso, Yan-Ling Hwang, Po-Ching Lin, and Li-Pin Hsu, A QTE-based Solution to Keylogger Attacks, The Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2012), Rome, Italy, August 19 -24, 201
[3] Rao, Ahsan. (2017). Detection of unprivileged keylogger.
[4] Creutzburg, Reiner. (2017). The strange world of keyloggers -an overview, Part I. Electronic Imaging. 2017. 139-148. 10.2352/ISSN.2470-1173.2017.6.MOBMU-313.
[5] Unprivileged detection of user space keyloggers" by Mugdha Kolte from MITCOE International Journal of Innovation Research in Science, Engineering and Technology
[6] Stefano Ortolani, Cristiano Guiffrida, Bruna Crispo: Bait Your Hook: A Novel Detection Technique for key loggers; S. Jha, R. Sommer, and C. Kreibich (Eds.): RAID 2010, LNCS 6307, pp. 198–217, 2010. c_Springer-Verlag Berlin Heidelberg 2010
[7] Mahak Arora, Kamal Kumar Sharma, Sharad Chauhan: Cyber Crime Combatting Using Keylog Detector Tool; Mahak Arora et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3, Issue 2, June 2016, pp. 1-
[8] R Sreeram Sreenivas, Dr R Anitha; Detecting keyloggers based on traffic analysis with periodic behavior; PSG College of Technology, Coimbatore, India
[9] Keylogger Detection and Containment by Stefani Ortolani(PHD Thesis) from Vrije Universiteit Amsterdam.
[10] Graeme Massina(2018, February 26), Computer Forensics: Memory Forensic, Retrieved from https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/memory-forensics/
[11] Eliézer Pereira(2017, June 1), RAM Memory Forensic Analysis, Retrieved from https://www.cybrary.it/0p3n/ram-memory-forensic-analysis/
[12] Limon, Gabriela. (2010). Forensic physical memory analysis: an overview of tools and techniques.[12]Vidas, Timothy. (2006). TheAcquisition and Analysis of Random Access Memory. J. Digital Forensic Practice. 1. 315-323. 10.1080/15567280701418171.[13]Case, Andrew and Golden G. Richard. "Memory forensics: The path forward."Digital Investigation20 (2017): 23-3
[13] https://www.linkedin.com/pulse/6-confirmed-signs-key-logger-infections-prevention-computer-arun-kl
[14] https://icssindia.in/blogs/what-is-keylogger/
[15] https://enterprise.comodo.com/computer-keylogger-software.php
[16] https://www.geeksforgeeks.org/hardware-keylogger/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY