International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

SYSTEM SURVEILLANCE USING KEYLOGGER

Dr. Vilas Joshi[1]

Divya Prakash[2], Kishlay Kumar[3], Shubham[4], Shubham[5]

Computer Engineering Department, ISBM College of Engineering Nande, Pune-412115,

India Savitribai Phule Pune University

Abstract: The System Surveillance using Keylogger project is a monitoring tool that captures keystrokes and screenshots on a computer system using Python. The objective of this project is to provide a means for parents, employers, and administrators to monitor computer activity for the purposes of safety, productivity, and security. There are a large number of products available to organizations that allow them to monitor the computer activities of their employees, including their email, internet usage, and actions on their personal computers. However, it is important to understand the scope and limitations of such monitoring. Companies can view a range of user activities, but there may be certain computer activities that are not visible to workplace monitoring depending on the monitoring software and policies in place.This paper describes the design and implementation of the System Surveillance using Keylogger project, including the architecture, functionality, and user interface.

I. INTRODUCTION

In numerous IT foundation organizations now-a-days, information security and information recuperation are the foremost vital variables which are essentially sent in Computer Forensics. Computer forensics comprises the craftsmanship of analyzing computerized media to protect, recoup and dissect the information in a successful manner.

There are numerous cases where information recuperation is required. Keylogging is one of the foremost well known spying computer programs in computer history, so by using keylogger applications clients can recover information within the time of catastrophe and harming of working records due to loss of power etc. Keyloggers are particularly successful in observing progressing wrongdoings. This is often an observation application utilized to track the clients which log keystrokes, employ log records to recover data, and capture a record of all written keys. The collected data is spared on the framework as a covered up record or messaged to the admin or the measurable analyst.

Keyloggers are a sort of malware (we are illustrating for moral purposes as different educators are utilizing the same for framework observing) that persistently track client commitment from the comfort within the endeavor to recuperate personal and private information. Key lumberjacks can e-mail or ftp the report containing keystrokes logged, back to the spying person. These keyloggers work watchfully out of location to capture the client activity on the support, so each one of the keystrokes are put absent in a well-shrouded document.

We are making the program keylogger, there are numerous sorts of keyloggers but we are focussed on the program.

II. PROBLEM DEFINITION

Keyloggers are mainly designed only for a specific functionality of logging and do not cause damage by infecting the systems the way viruses do. Instead, Keylogging programs Monitor the keystrokes of the victim in order to covertly grab all information by capturing the activities performed on a computer.

Keyloggers capture the strokes made by keys and save such information in concealed log files, which is then forwarded to the admin. In the process, Keyloggers end up leaving behind a small footprint in terms of memory and processor utilization. Most of them cannot be seen in the ‘Task Manager’ nor can be noticed among processes. It is often challenging to distinguish between the log files and the OS files, even after listing the entire directory.

Many keyloggers primarily focus on storing keystrokes, but with the implementation of capturing screenshot and mouse click can further increase the area of surveillance of the system.

III. LITERATURE SURVEY

Author: Robbi Rahim, Heri Nurdiyanto, Ansari Saleh A, Dahlan Abdullah, Dedy Hartama and Darmawan Napitupulu.

The development of technology is very fast, especially in the field of Internet technology that at any time experiencing significant changes, The development also supported by the ability of human resources, Keylogger is a tool that most developed because this application is very rarely recognized a malicious program by antivirus, keylogger will record all activities related to keystrokes, the recording process is accomplished by using string matching method. The application of string matching method in the process of recording the keyboard is to help the admin in knowing what the user accessed on the computer.

Author: Preeti Tuli, Priyanka Sahu

The goal of this paper is to give an idea about some of the benefits that anyone can get from the complete monitoring of the system network. Keylogging programs, commonly known as keyloggers, are a type of malware that maliciously tracks user input from the keyboard in an attempt to retrieve personal and private information. Keystroke logging, also known as key logging, is the capture of typed characters/number [2]. The data captured can include document content, passwords, user ID's, and other potentially sensitive bits of information. The program logs all keystrokes (aka Keystroke Logging) along with the name of the application in which the keystrokes were entered. It also notes the window captions and all URLs visited with a web browser. This allows you to review all the text written by your employer/user, whether it was created with a text editor, email client or an on-line text control on a web page. You can view all the pages visited by your employ/user and the passwords for all their on-line accounts. For easier monitoring, you can also turn on automatic screenshot capture.

Author: Stig Arild Ysterud

One goal of this research is to investigate keyloggers and ways to monitor detecting methods that are used in attacks through the usage of honeypots.
First of all the difference of this subject title "Honeynets and Honeypots" is explained: Honeynet is a computer network specifically to be attacked. The hosts that comprise a honeynet and serve as attack targets are called Honeypots. A honeypot is a trap set to detect, deflect or in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.

IV. ASSUMPTIONS AND DEPENDENCIES

Assumptions: The following Assumption was taken into consideration:

- The user has a reliable internet connection to upload the keystroke and screenshot data to the cloud.
- The cloud storage service is secure and can protect the data from unauthorized access.
- The user has created an account on the cloud storage service and has provided the necessary login credentials to the keylogger and screenshot modules.

Dependencies:

The dependencies are as follows:

- The keylogger and screenshot modules rely on the Python programming language and specific libraries such as pynput. These dependencies must be installed on the computer for the modules to function properly.
- The keylogger and screenshot modules must have access to system resources, such as the keyboard and screen, to capture keystrokes and screenshots.
- The keylogger and screenshot modules must be able to write data to the local file system to store captured keystrokes and screenshots.

V. SYSTEM ARCHITECTURE

The System Surveillance using Keylogger project consists of two main modules: the Keylogger

module and the Screenshot module. The system architecture is designed to capture keystrokes and screenshots of the computer in real-time and store them locally or remotely to an online cloud storage service.

The Keylogger module captures all keystrokes made on the computer, including those made in password fields. It uses the pynput library in Python to monitor the keyboard and save the captured keystrokes to a log file. The log file can be saved locally or remotely to an online cloud storage service.

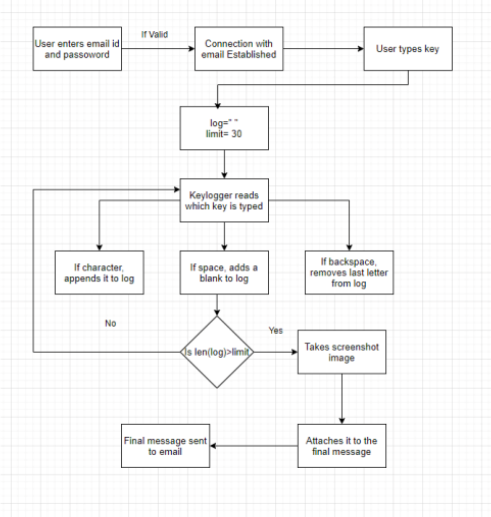
The Screenshot module captures images of the computer screen at predefined intervals. It uses the pynscreenshot library in Python to take screenshots of the entire screen or just a specific window. The screenshots are saved as image files that can also be saved locally or remotely to an online cloud storage service.

The Keylogger and Screenshot modules are designed to run in the background without any user interaction. The system can be configured to start automatically when the computer boots up and run continuously in the background. The modules can be configured to store captured keystrokes and screenshots locally or remotely to an online cloud storage service.

VI. SYSTEM DESIGN

Requirements gathering: The first step in the system design process is to gather requirements for the System Surveillance using Keylogger project. This involves identifying the key features and functionality that the system should have, such as capturing keystrokes and screenshots, storing the captured data locally or remotely using FTP, and sending email notifications using SMTP.

Architecture design: Once the requirements are identified, the system architecture is designed. The architecture consists of three main modules: the Keylogger module, the Screenshot module, and the FTP module. The Keylogger module captures all keystrokes made on the computer and saves them to a log file. The Screenshot module captures images of the computer screen at predefined intervals using PyScreenshot library and saves them as image files. The FTP module is responsible for uploading the captured keystrokes and screenshots to an online cloud storage service using FTP.



Module design: The Keylogger, Screenshot, FTP modules are designed to work independently. The Keylogger module uses the keyboard library to capture keystrokes. The Screenshot module uses the PyScreenshot library to capture screenshots. The FTP module uses the ftplib library to upload the captured data to the cloud storage service

Integration design: Once the Keylogger, Screenshot, and FTP modules are designed, they are integrated to work together as a system. The modules can be configured to start automatically when the computer boots up and runs continuously in the background. The SMTP module can be used to send email notifications with the captured data to a specified email address.

.

VIII. SOFTWARE AND HARDWARE REQUIREMENTS

Language used : Python (version 3.9 and above

Software Requirements : Pycharm

Hardware Requirements :

- RAM: 512MB (minimum requirement)
- Hard Disk: 1GB working space (minimum requirement)
- Processor: Any Processor
- Operating System: Any operating system

IX. OTHER SPECIFICATION

A. *Advantages*

1. Monitoring and recording all keystrokes made on a computer can provide insight into user behavior, help with troubleshooting, and identify security issues.
2. Capturing screenshots at regular intervals can provide visual context to the captured keystrokes and help in identifying unauthorized access and other security threats.
3. Remote access to the captured data via FTP enables easy access to the data and analysis from any location.
4. Email notifications provide real-time alerts and help with incident response in case of any unauthorized access or suspicious activity.

B. *Limitations*

1. This system may be seen as invasive and can violate user privacy if not used in a responsible and ethical manner.
2. The system may consume a considerable amount of computer resources, which can affect system performance.
3. The captured data may include sensitive information, so proper security measures should be taken to protect it from unauthorized access.
4. It is possible that antivirus software may flag this system as malware or a threat, leading to unintended consequences such as deletion or quarantine of the system files. Therefore, it is important to ensure that the system is not used for malicious purposes and is only installed on computers with appropriate consent and authorization.

X. CONCLUSION

A key logger is a type of software that is designed to record every keystroke made by a user on their computer's keyboard, often without their knowledge. This software is also referred to as a keyboard capturer. While they may seem intrusive, key loggers can be valuable tools in certain settings. For example, employers can use them to monitor employee computer activity and ensure that work is being completed efficiently, without any unnecessary delays or distractions.

XI. ACKNOWLEDGMENT

We would like to take this opportunity to thank all the people who were part of this seminar in numerous ways, people who gave unending support right from the initial stage.

In particular we wish to thank Dr. Vilas as internal project guide who gave their co-operation timely and precious guidance without which this project would not have been a success. We thank them for reviewing the entire project with painstaking efforts and more of his, unbanning ability to spot the mistakes.

We would like to thank our H.O.D Prof. B. B. Gite for his continuous encouragement, support and guidance at each and every stage of the project.

And last but not the least we would like to thank all my friends who were Associated with me and helped me in preparing my project. The project named “System Surveillance Using Keylogger” would not have been possible without the extensive support of people who were directly or indirectly involved in its successful execution.

XII. REFERENCES

- S. Moses, J. Mercado, A. Larson and D. Rowe, "Touch interface and keylogging malware," 2015 11th International Conference on Innovations in Information Technology (IIT), Dubai, 2015, pp. 86-91.doi: 10.1109/INNOVATIONS.2015.7381520
- Solairaj, S. C. Prabanand, J. Mathalairaj, C. Prathap and L. S. Vignesh, "Keyloggers software detection techniques," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016, pp. 1-6, doi:10.1109/ISCO.2016.7726880
- Advanced Keylogger- A Stealthy Malware for Computer Monitoring, Asian Journal of Convergence in Technology ISSN NO: 2350-1146 I.F-5.11 Volume VII and Issue I, Aarushi Dwivedi, Krishna Chandra Tripathi, M.L. Sharma.
- University of Oslo- Keylogging of user interaction in physical and virtual environments and its implications for honeypot analysis Stig Arild Ysterud stigay@ifi.uio.no Network and System Administration 20th May 2014
- M. Dadkhah, A. Ciobotaru, et. al, “An Introduction to Undetectable Keyloggers with Experimental Testing”, International Journal of Computer Networks and Communications Security - September 2014
- Enhancement Keylogger Application for Parental Control and Monitor Children's Activities, Mohamad Yusof Darus, Muhammad Azizi Mohd Ariffin, Journal of Positive School Psychology http://journalppw.com 2022, Vol. 6, No. 3, 8482–8492