VELLORE INSTITUTE OF TECHNOLOGY – VELLORE

WINTER SEMESTER 2022-23

NETWORK INFORMATION SECURITY

Prof. Dr. NAVANEETHAN C

Title

Advance Key Logger Using Python

REVIEW - 1	
NAME	NITHISH G
REG NO.	22MCA0370
COURSE	NETWORK INFORMATION SECURITY
COURSE ID	ITA6007
FACULTY	Prof. Dr. NAVANEETHAN C
SLOT	D1/TD1
DATE	06-04-2023

Abstract

A keylogger is a type of software that records every keystroke made on a computer or mobile device. It is designed to run in the background without the user's knowledge, and it can capture all kinds of keystrokes, including passwords, credit card numbers, and other sensitive information. The purpose of a keylogger can vary depending on who is using it. Some individuals may use it to monitor their own computer usage, while others may use it for malicious purposes such as stealing login credentials or other sensitive data.

Despite its controversial nature, keyloggers can be useful tools in certain situations, such as monitoring the activity of employees in the workplace or tracking the online activities of children. However, it is important to use them responsibly and within the boundaries of the law.

In this project, we aim to develop a keylogger that not only captures keystrokes but also captures other information such as screenshots, application logs, and system logs. This additional information can provide more context and help in the analysis of the data collected by the keylogger. We also aim to implement security measures to prevent unauthorized access to the data collected by the keylogger.

Existing System

- The existing systems for keylogging are often designed for malicious purposes, and may be distributed as malware to unsuspecting users. These keyloggers are often undetectable by traditional antivirus software and can be used to steal sensitive information such as login credentials and credit card numbers. They are typically designed to be stealthy and may not provide any additional functionality beyond capturing keystrokes.

Proposed System

- In contrast, our proposed system for key logging aims to provide a more comprehensive and secure solution. The system will capture not only

keystrokes, but also other information such as screenshots, application logs, and system logs. This additional information can provide context and help in the analysis of the data collected.

- The proposed system will have several advantages over existing systems. Firstly, it will be more comprehensive, capturing more information than just keystrokes. This will provide a more complete picture of the user's activity and help in the analysis of the data collected. Additionally, the security measures implemented in the proposed system will help to protect the data collected from unauthorized access, ensuring that it can be used responsibly and within the boundaries of the law.

Features of Advance key logger

Feature	Description
Keystroke logging	Records every keystroke typed by a user, including passwords, usernames, and other sensitive information.
Clipboard logging	Records clipboard activity, capturing everything that a user copies and pastes.
Application logging	Logs application activity, including the programs a user opens and the files they access.
System logging	Logs system activity, including events and errors.
Screenshot capturing	Takes periodic screenshots of a user's screen, providing a visual record of their activity.
Remote access	Can transmit the captured data to a remote server or other destination, allowing an attacker to monitor a user's activity from afar.
Persistence	Designed to remain undetected and continue running even after the system is rebooted.
Encryption	Uses encryption to securely transmit the captured data to its destination to protect it from being intercepted.
Analysis	Includes analysis features that can help identify patterns and anomalies in a user's activity, which can be useful for security or forensic purposes.

Modules/Components

Module/Component	Description
Key logger	Captures keystrokes and other relevant data, such as clipboard data and system and application logs.
Persistence	Ensures that the keylogger is persistent and can survive system restarts and other events that might otherwise terminate it.
Networking	Sends the captured data to a remote server or other destination over the network.
User interface	Displays and interacts with the captured data, such as in a GUI or command-line interface.
Encryption	Encrypts the captured data to protect it from unauthorized access or interception.
Analysis	Analyzes the captured data and identifies any sensitive information that may have been captured.
Reporting	Generates reports of the findings from the analysis, including any vulnerabilities or security issues that were identified.
Refinement	Refines the keylogger to improve its functionality and security, based on the findings from the analysis and reporting.

---------- Thank You ----------