Faculty of Engineering
Cairo University

Cyber Security Project Report

Keyractor

Name	Code
Ahmed Osama Zahran	9210026
Yousef Mohamed Haggag	9211436
Abdelrahman Abdelfattah	9210587
Mohamed Adel	9211006

Under Supervision of:
Eng: Ayman Reda

Keylogger and Password Extractor

Introduction

The Keylogger and Password Extractor is a project designed to monitor and record keystrokes on a target system. Additionally, it uses pattern matching technique as regex to extract potential passwords from the logged keystrokes.

Features

a. Keylogging: The project captures keystrokes made by the user on the target system and logs them into a log file.
b. Password Extraction: The project includes a pattern matching technique that analyzes the logged keystrokes to identify potential passwords, emails and usernames using regex.
c. Anti-Malware: A scanner to scan for malicious patterns of a keylogger and warn the client of suspected malware before shutting their process down.

Assumptions

- We assume that the suspect fell for the trick of running the keylogging program, which we tried to make easier to believe by naming the folder and file photoshop.exe and making it have the same icon.
- The exe isn't recognized by the windows defender as a malware but still exe has no author because we couldn't fraud a hashing certificate for the application, while we did try some stuff to avoid it, it still does warn the user about it so we assume that the victim clicks "run it anyway".

Input

A bunch of random keystrokes on the keyboard that would preferably be the user opening their browser, typing part of a website's name hitting enter and then logging in, but could be any other random input.

Output

- An RSA encrypted file “log.rsa” with the suspect’s keystrokes logged to it “this is then sent by email to the attacker”.
- A log.txt file that has the keystrokes, generated from the log.rsa through the extractor.
- An out.txt file that has all the potential passwords, emails and usernames from the log.txt file.

System Requirements

- Python: Version 3.6 or higher
- Additional Python packages: pynput, pyperclip, pywin32

Usage

a. Running the Keylogger:

- The keylogger is packaged as an exe with the name photoshop, hoping to trick the suspect to open it.
- Once the suspect opens it, it will act as if it crashed, but it will run in the background and will show in the task manager as “adobe photoshop 2021” to be the least concerning.

b. Monitoring Keystrokes:

The keylogger will start monitoring and logging keystrokes as soon as the program is executed. The logged keystrokes will be saved in an RSA encrypted file named "log.rsa" in the project directory, and thus even if the suspect was to find it, they wouldn’t understand its content.

c. Sending the log file to the attacker:

Using the python built in library “smtplib”, we send background emails to the attacker with the RSA encrypted log file as an attachment.

d. Extracting information:

Once the attacker receives the email, they download the attached file and run the extractor program which does the following:

- Decrypts the log file that was received into log.txt.
- Use regex to find all passwords, emails and potential usernames in the log file.
- The information identified by the algorithm will be sent to an out.txt file.

Security and Legal Considerations

- Ethical Usage: It is crucial to use this project responsibly and legally. We ensured that we had the proper authorization to monitor keystrokes and only use it on systems we own or have explicit permission to access.
- Privacy and Data Protection: Respecting privacy rights and handling any collected data in compliance with applicable laws and regulations.
- Antivirus Considerations: we bypassed windows defender at least, so considering harmful consequences of our app we made an Anti-Malware.

Conclusion

The Keylogger and Password Extractor project provides a powerful tool for monitoring and extracting potential passwords from logged keystrokes. By following this documentation, you can install, configure, and utilize the project effectively while maintaining ethical and legal standards. Remember to always use this tool responsibly and respect privacy rights.