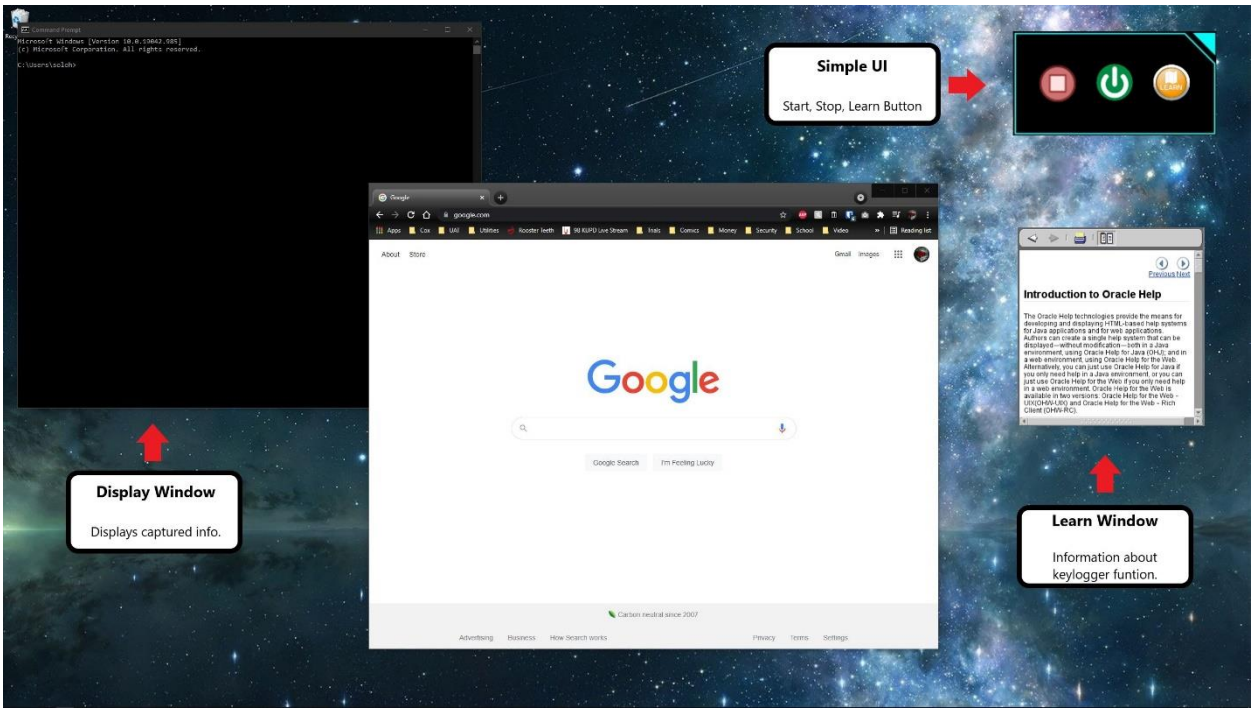
KEYS

Creator:

Levi Overstreet, Bachelor of Science in Network Security

Last Updated: 9/28/2023



Technical Field

This project sits within the Network Security technical field.

Background Information

I decided to pursue this project because it seemed like the most basic, entry level concept for security that covered areas that I saw as important. These areas are monitoring, malware, and response.

Prior Art (legal term)

For my project purpose, I couldn't really find anything that matched what it is I am trying to accomplish. There are plenty of commercial keylogger programs on the market but nothing that is directly built and marketed for training and research. Currently there are no programs that this project will be inspired by or built upon.

Sept. 9th – There are still no current offerings for what I propose. There has been an increase in software suites that are described as watchdog software but again, these do not function in the same way as I have outlined and are not used for the same purpose.

Sept. 28th – Still not able to find any current offerings of software that would be marketed as a leaning tool. All software suites in this area are marketed for their watchdog functionality.

Project Description

The goal of this keylogger project is to help educate people on the importance of security practices by displaying how a simple malware can be a dangerous thing, and to train those who are new to the security field what to look for as well as how to deal with malware like a keylogger program.

Innovation Claim

The way this project is making a keylogger program innovative is by having a viewable window opened when the program is running. This viewable window will show what is being captured, how it is logging it and to where it is "hiding" those logs. After each time the program ends, an after-action report will be produced summarizing what was seen in the viewable window.

Usage Scenario

A typical use of the program this project will produce will be in some form of learning environment. The keylogger program will be installed and while it is running it will have a window up that will display the location of where the program is installed, to demonstrate how a normal keylogger may be installed and hidden. This window will show the keystrokes it logs and to what programs or sites those keystrokes are connected. It will also display where it is saving the logs of what it has captured and how it is hiding those logs. This kind of visual insight can help inform managers the importance of security best practices as well as lay a foundation for training those coming into the security field where and what they might look for when dealing with malware, such as a keylogger.

Evaluation Criteria

The following questions will identify the successful completion of the project.

- Does the program install and operate as a keylogger program?
- Does the program provide a window to view what the program is doing?
- Is the install location of the keylogger displayed in the window?
- Are the keystrokes and associated program being captured displayed in the window?
- Is the location of the saved log files displayed in the window?
- Is the way the log files are hidden displayed in the window?

Objectives and Tasks Associated with the Project

Objective 1: Design the core program.

Will need to select which coding language would be best for this project.

Will need to study up on that coding language, as I do not know how to code.

Code the core program as designed into a workable Alpha state.

Objective 2: Testing.

Confirm information displays correctly.

Confirm log files save correctly.

Confirm UI functions as intended.

Description of Design Prototype

Upon program startup, the program will function as a normal keylogger with a small UI. There will be three buttons on the UI, a Start button, a Stop button, and a Learn button.

The start button will begin the keylogger functions as well as open the Display window. This window will display key information, such as the install location of the keylogger program, the location of saved log files, the file type the saved log files are being hidden as, and the captured keystrokes as well as the application/website to which it is associated.

The Stop button simply ends the keylogger functions and clicking on the button a second time will close the Display window. The Learn button will open a Help/Learn window that will have a searchable database of information pertaining to keylogger functions, uses, protection strategies, and hyperlinks to security resources about the above mentioned.

Evaluation Plan

The plan to evaluate this project will mainly follow testing parameters. Once there is a working program, I will install the keylogger and begin checking all listed features in the Evaluation Criteria to ensure that project is on track. This evaluation plan and the criteria may change over the course of this project. So, flexibility and remaining agile will be key.

Project Completion Assessment

Sept. 9th – Over this last week, I have been testing various coding languages to determine which would be best suited for this project. So far between building core functionality code, the evaluation is between using C# or Python. Both have merits for their use in this project. I think the choice will come down to which is easier for me to code.

Sept. 17th – This past week I decided on using Python for the coding language and started working on an outline for the code. I've come up with a semi-working iteration of the code. There are some functions that I have not yet been able to get to work.

Sept. 23rd – This past week was used for debugging and fixing broken code to get the prototype to a working state. It does currently work. Will be recording a prototype demo video to showcase its functionality as well as figuring out how to package the code into an executable file. I have also updated the SIP site to better display the project.

Sept. 28th – This week I recorded my demo video and updated my SIP site to display my code as well as highlight my demo video. This was to present it as outlined by the course requirements for this project.