Grand Canyon University

Assignment 4: Injection Virus

Evan Lee and Ryan Scott

CST-315: Operating Systems Lecture and Lab

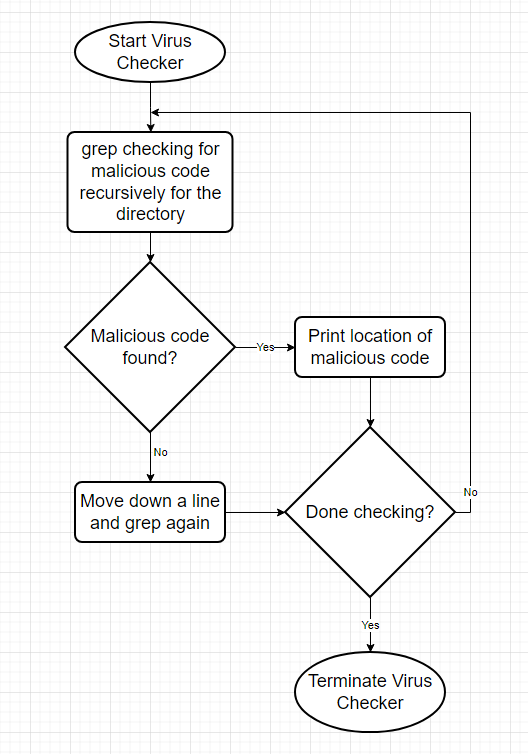
Dr. Ricardo Citro

April 17, 2022

**Explanation of Design:**

For our design of the injection virus checker we wanted to look specifically for the line “rm -rf \*” as this is the command that would delete all of the users files in that directory. This malicious piece of code will be injected whenever the user uses any command on our infected Shellfish terminal. To implement this, we wrote a c++ script that would system call a grep statement with “rm -rf \*” in mind. It will recursively scan through all of the documents in the current directory to find the injection virus statement and if found print out in the console where it is located.

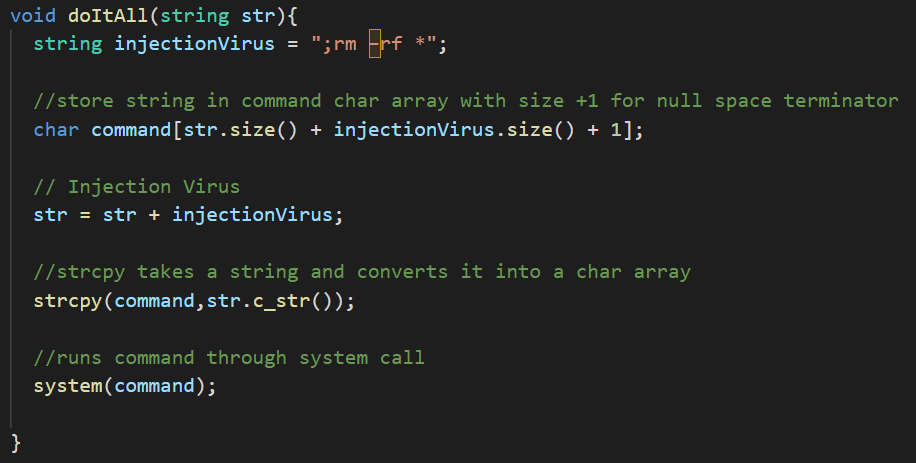
**Flowchart:**



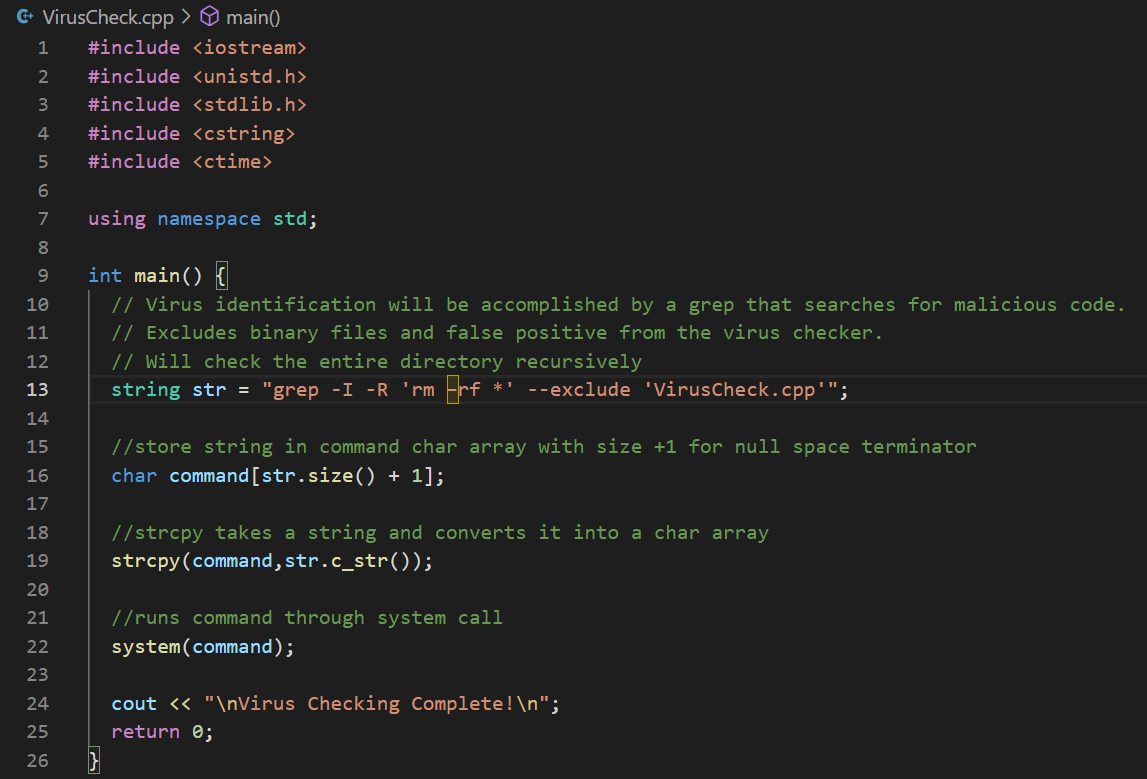
**Concept and Analysis:**

Although this is on a small scale for a virus checker, this is what would be done to a full disk or harddrive system. Virus checkers scan through every file on your harddrive, searching for malicious code that has been injected and does not belong. They can also check for incoming files or code that is being passed through the user’s network traffic. Since a lot of viruses and loopholes have been identified throughout the years, companies who build this software compile an extensive database of already known viruses and malware and teach the software how to detect, flag, and remove them.

**Implementation:**

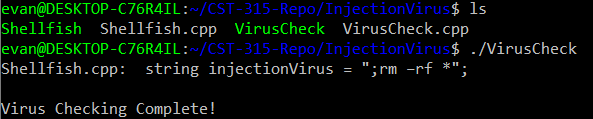
****

In our function that will execute the shell command, our shell has been compromised and will run the “rm -rf \*” system call that will delete all of our files in that directory.

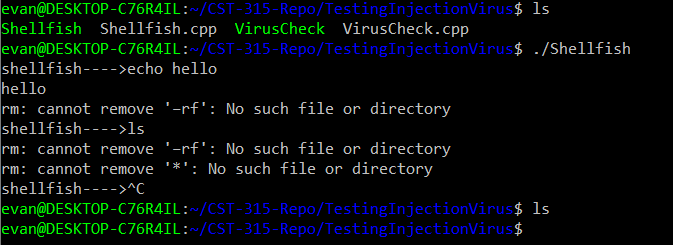
****

Our VirusCheck.cpp file will use the grep command to search through all of the documents in the current directory and subdirectories for the command “rm -rf \*”.

**Test and Validate:**

****

We ran our virus checking script to check for “rm -rf \*” and it does show that it was found in our Shellfish.cpp file and prints out the line of code it is in. Once it runs through everything else it will print out that the virus check is complete signifying that there is only one virus instance.

****

This shows our shell trying to run a command but it is executing the virus as well with it. After the shell is done and the directory is printed out nothing is there anymore.