

Documentation

Generic Virus Scanner

- Ashwin Ramesh

Brief

A simple generic virus scanner, that matches signatures located in a text document with files in a particular directory.

Code Pseudocode

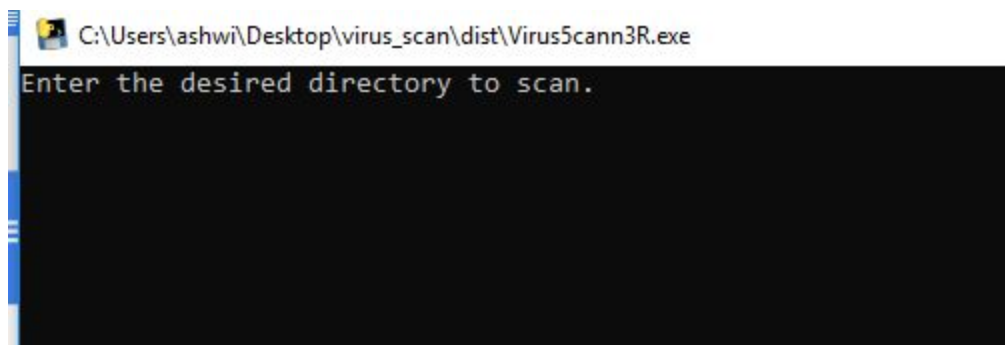
```
main()
{
    enter directory -> input
    enter signature path -> input
    boyerMatchAlgo(files_in_dir, signature file)
    if match -> Virus detected
    else -> no virus detected
}
```

Code Analysis

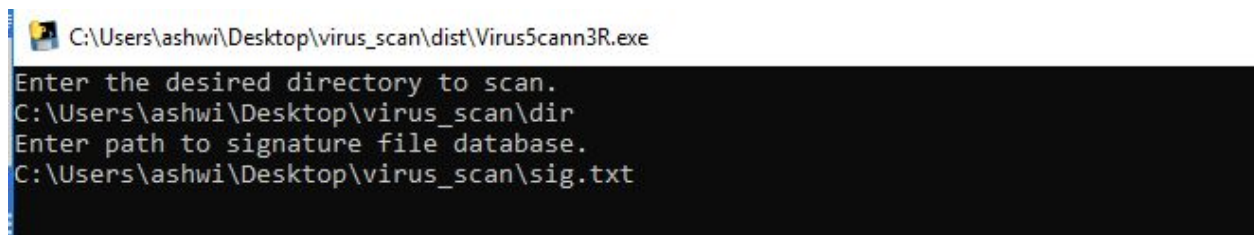
The main function takes in 2 inputs the full directory path for scanning for viruses and the path for the signatures files which is a file with signatures meant for matching with the files in the directory. Each signature must be on a new line in the signature file. To simulate infected files, I generated the files in the directory using notepad and changed the files extension to .exe and .jpg. Theoretically the code should be capable of reading actual large files because it opens each file in the binary mode and does a string search there. Also I implemented the Boyer-Moore search algorithm for faster string matches. I used python2.7 to run the python scripts and used pyinstaller.exe to generate the windows executable files.

Execution

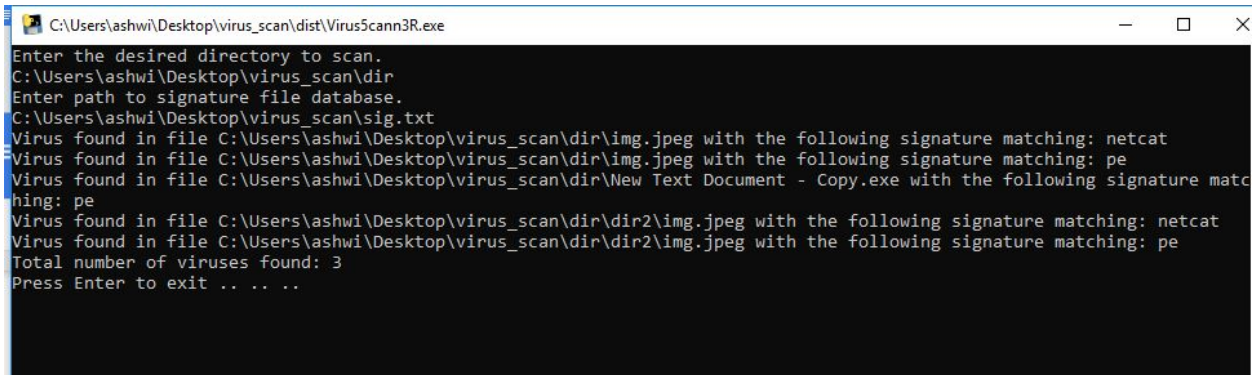
Sample directory and signature files have been provided for convenience. The Signature files must contain any number of signatures each signature must be on a new line. Open Viru5cann3R.exe for 64bit machines and Viru5cann3R_32.exe for a 32bit machine.



Enter the directory to scan and the location of the signature file.



The scanner then proceeds to perform signature matches and displays which signature matched successfully and the number of infected files.



```
C:\Users\ashwi\Desktop\virus_scan\dist\Virus5cann3R.exe
Enter the desired directory to scan.
C:\Users\ashwi\Desktop\virus_scan\dir
Enter path to signature file database.
C:\Users\ashwi\Desktop\virus_scan\sig.txt
Virus found in file C:\Users\ashwi\Desktop\virus_scan\dir\img.jpeg with the following signature matching: netcat
Virus found in file C:\Users\ashwi\Desktop\virus_scan\dir\img.jpeg with the following signature matching: pe
Virus found in file C:\Users\ashwi\Desktop\virus_scan\dir\New Text Document - Copy.exe with the following signature matching: pe
Virus found in file C:\Users\ashwi\Desktop\virus_scan\dir\dir2\img.jpeg with the following signature matching: netcat
Virus found in file C:\Users\ashwi\Desktop\virus_scan\dir\dir2\img.jpeg with the following signature matching: pe
Total number of viruses found: 3
Press Enter to exit .. .. .
```

Testing

I did not test on actual viruses, but however created my own malicious looking files.

While running the executable on another machine, I realised that I was using a 64bit compiler which will not work in 32bit machines, and so I converted the compiler build to 32bit and ran pyinstaller.exe again to generate a new 32bit exe file.

Disclaimer

This is a generic and simple virus scanner, designed for educational purposes. This program is not to be tested in any way against a real world, complex virus, especially those that use packers to obfuscate their binary signature.