MINI PROJECT REPORT

ON

VIRUS DETECTOR USING PYTHON

FOR

NAAN MUDHALVAN: CYBER SECURITY

Submitted by

S.BARTH KUMAR(815120121008)

D.BOOPATHI(815120121011)

P.DHIVAHAR(815120121015)

Under the guidance of

Mr.R.KUTTIMANI M.E.,

DEPARTMENT OF BIO MEDICAL ENGINEERING

DHANALAKSHMI SRINIVASAN INSTITUTE OF TECHNOLOGY

SAMAYAPURAM,TRICHY.621112

- INTRODUCTION:.
  This Virus Detection System is an application which shows the way of approaching a generic antivirus software product. Unlike. Some antivirus products which bind themselves to specific signatures of some particular viruses, this simulation provides a generic approach by which we are able to detect more than a single virus with a common virus code in the database.

System Specification:

1. Hardware Requirements:

• PROCESSOR

: Intel Pentium

ll or above

• PROCESSOR speed above

: 1.76 GHZ or

• RAM above

: 32 MB or

• HDD

: 40 MB

2. Software Requirements:

PLATFORM

XP

FRONT END

BACK END ACCESS

: WINDOWS

: C. C#.NET : MS

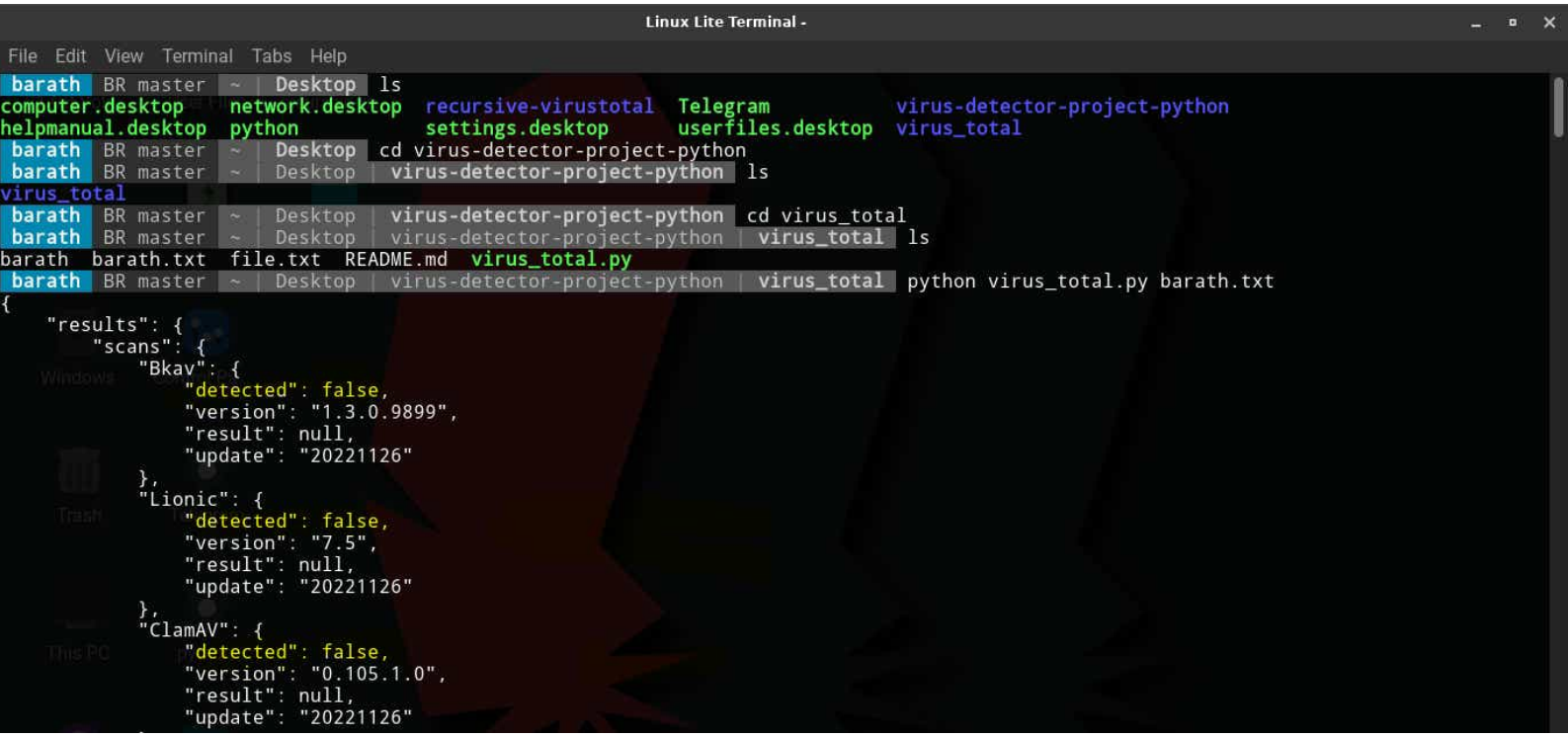
Scope of Definition:

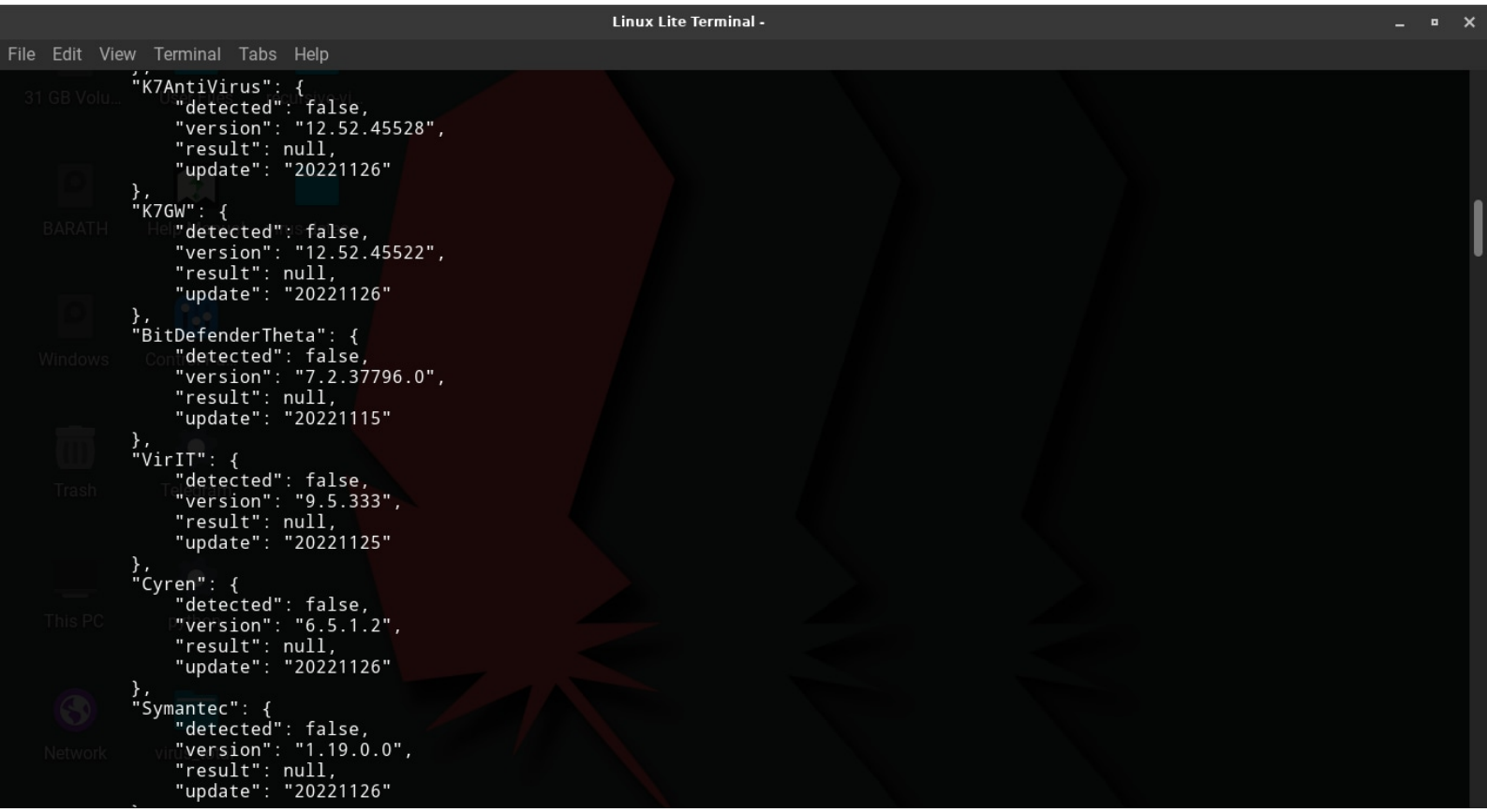
The damage caused by computer viruses is more serious than ever in today's society,

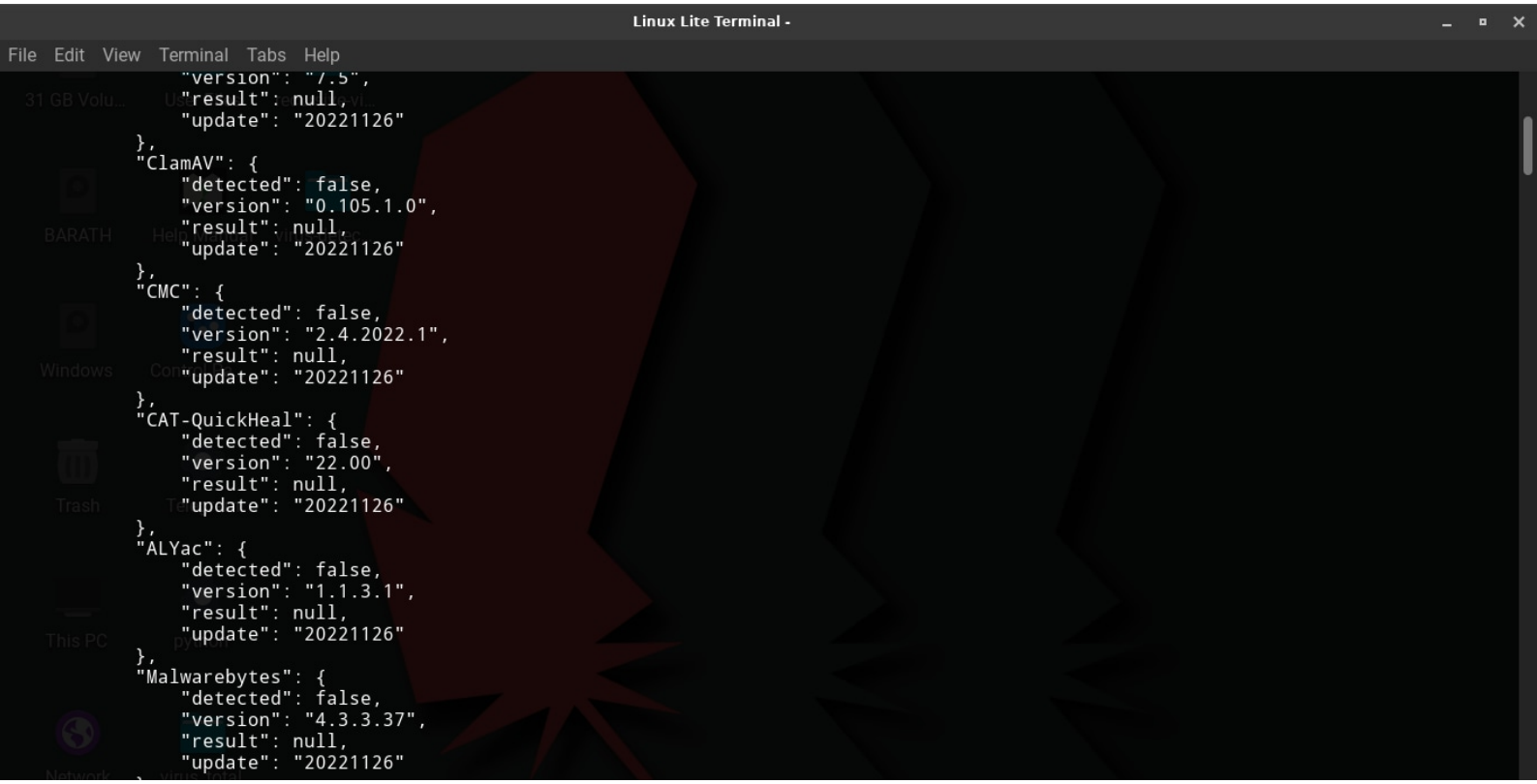
where personal communication, corporate business, and social infrastructures heavily depend on computer networks.

- CODING FOR VIRUS DETECTER
  #!/usr/bin/python
-
- import sys
-
- import hashlib
-
- import json from virus_total_apis import PublicApi as public_api
-
- =#Calculate the total number of arguments
-
- n = len(sys.argv)
-
- # Read files
-
- def file_input(file_name):
-
- file = open(file_name,”rb”) output = file.read()
-
- return output

- If(n == 1 or n>2):
-
- print(“Hinvalid Syntax”) print(“Syntax:/virus_total.py <file_name>”)
-
- else:
-
- api_key=“498718070c62793afc526c51dbe520 0830f890be87078d0a13e2af48d2
-
- content = file_input(sys.argv[1])
-
- md5_sum = hashlib.md50)
-
- md5_sum.update(content)
-
- digest = md5_sum.hexdigest()
-
- vt = public_api(api_key)
-
- response = vt.get_file_report(digest) print(json.dumps (response,sort_keys=False,indent-4))


Linux Lite Terminal -
File Edit View Terminal Tabs Help
barath BR master ~ | Desktop ls
computer.desktop network.desktop recursive-virustotal Telegram virus-detector-project-python
helpmanual.desktop python settings.desktop userfiles.desktop virus_total
barath BR master ~ | Desktop cd virus-detector-project-python
barath BR master ~ | Desktop | virus-detector-project-python ls
virus_total
barath BR master ~ | Desktop | virus-detector-project-python cd virus_total
barath BR master ~ | Desktop | virus-detector-project-python | virus_total ls
barath barath.txt file.txt README.md virus_total.py
barath BR master ~ | Desktop | virus-detector-project-python | virus_total python virus_total.py barath.txt
{
"results": {
"scans": {
"Bkav": {
"detected": false,
"version": "1.3.0.9899",
"result": null,
"update": "20221126"
},
"Lionic": {
"detected": false,
"version": "7.5",
"result": null,
"update": "20221126"
},
"ClamAV": {
"detected": false,
"version": "0.105.1.0",
"result": null,
"update": "20221126"


Linux Lite Terminal -
File Edit View Terminal Tabs Help
"K7AntiVirus": {
"detected": false,
"version": "12.52.45528",
"result": null,
"update": "20221126"
},
"K7GW": {
"detected": false,
"version": "12.52.45522",
"result": null,
"update": "20221126"
},
"BitDefenderTheta": {
"detected": false,
"version": "7.2.37796.0",
"result": null,
"update": "20221115"
},
"VirIT": {
"detected": false,
"version": "9.5.333",
"result": null,
"update": "20221125"
},
"Cyren": {
"detected": false,
"version": "6.5.1.2",
"result": null,
"update": "20221126"
},
"Symantec": {
"detected": false,
"version": "1.19.0.0",
"result": null,
"update": "20221126"


Linux Lite Terminal -
File Edit View Terminal Tabs Help
"version": "7.5",
"result": null,
"update": "20221126"
},
"ClamAV": {
"detected": false,
"version": "0.105.1.0",
"result": null,
"update": "20221126"
},
"CMC": {
"detected": false,
"version": "2.4.2022.1",
"result": null,
"update": "20221126"
},
"CAT-QuickHeal": {
"detected": false,
"version": "22.00",
"result": null,
"update": "20221126"
},
"ALYac": {
"detected": false,
"version": "1.1.3.1",
"result": null,
"update": "20221126"
},
"Malwarebytes": {
"detected": false,
"version": "4.3.3.37",
"result": null,
"update": "20221126"

Linux Lite Terminal -

File Edit View Terminal Tabs Help


```
            "Fortinet": {
                "detected": false,
                "version": "6.4.258.0",
                "result": null,
                "update": "20221126"
            },
            "AVG": {
                "detected": false,
                "version": "22.11.7701.0",
                "result": null,
                "update": "20221126"
            },
            "Panda": {
                "detected": false,
                "version": "4.6.4.2",
                "result": null,
                "update": "20221126"
            }
        },
        "scan_id": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855-1669474646",
        "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
        "resource": "d41d8cd98f00b204e9800998ecf8427e",
        "response_code": 1,
        "scan_date": "2022-11-26 14:57:26",
        "permalink": "https://www.virustotal.com/gui/file/e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855/detection/f
-e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855-1669474646",
        "verbose_msg": "Scan finished, information embedded",
        "total": 60,
        "positives": 0,
        "sha256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
        "md5": "d41d8cd98f00b204e9800998ecf8427e"
    },
    "response_code": 200
}
```

• Modules Overview:

Four modules have been used in this project whose detailed description can be found in the project report itself. They are listed below:

• Home Page: The home page is beginning module of Virus Detection System. From here. Through the options provided. User's can navigate to other modules of the antivirus system.

Database Update: This module is for making the antivirus software more efficient, effective and accurate. It is further divided into two categories: the first is for adding new code to the database and the second is for deleting the existing code from the system database.

• Scanning Module: This module is the part where scanning of the infected file. Folder or system is done. Here, user is provided with option to scan the file they want and the selected file. Folder or system is passed the dis-assembler module below. Scanning module into three sub-categories: scanning a single file. Scanning a specific folder and scanning the entire system.

• Disassembler Module: This is the core part of this virus detection system project software. This module takes the selected files from the scanning module and translated them to assembly level code. Then, the code thus generated for each file scanned will be passed to the next module present in the system.

- Features:

- The software is applicable in managing the bugs that Occur during development of software and to track the older issues.

- It facilitates searching facility to bug history and solution.

- The system is fully secured; authentication method is adopted to manage security.

- It stores the older bug reports so that they can be easily solved when they reappear.

- The application helps the project manager in evaluating the works of employees.

- The proposed software is capable of auto update when latest version is available.

- Conclusion:

This Virus Detection System (in ASP. NET) does not focus on aspects like real-time monitors, file system drivers, graphical user interfaces, plug- ins, etc. It simply includes main elements of a generic antivirus software product. The full project report of this antivirus system project can downloaded from the download link in the post.


VIRUS
DETECTED

THANK YOU