

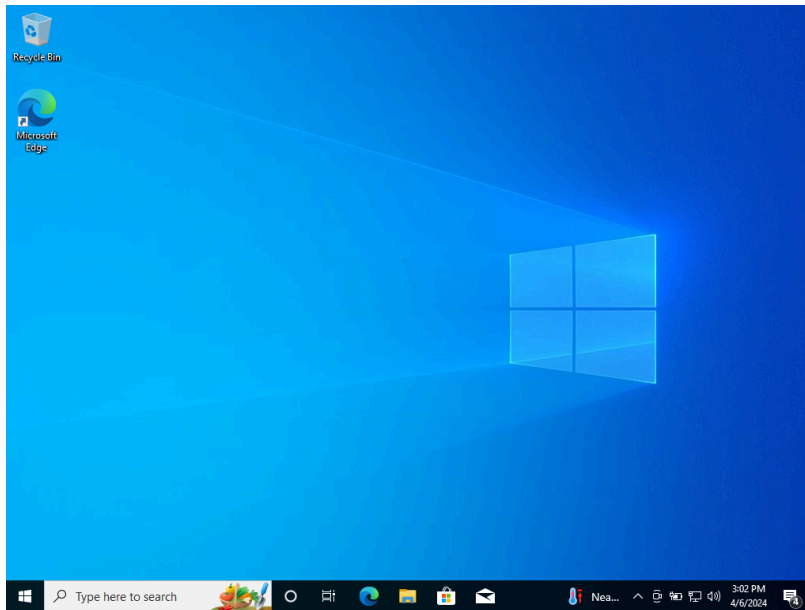
Employee Id : ST#IS#6248

## Task 5

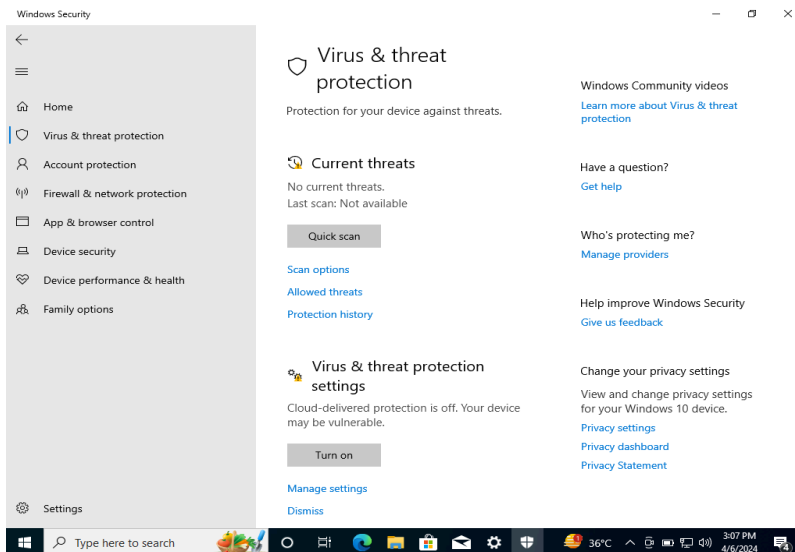
A. Create a Virus and Scan the file with the Virus Total tool. Make a report on it.

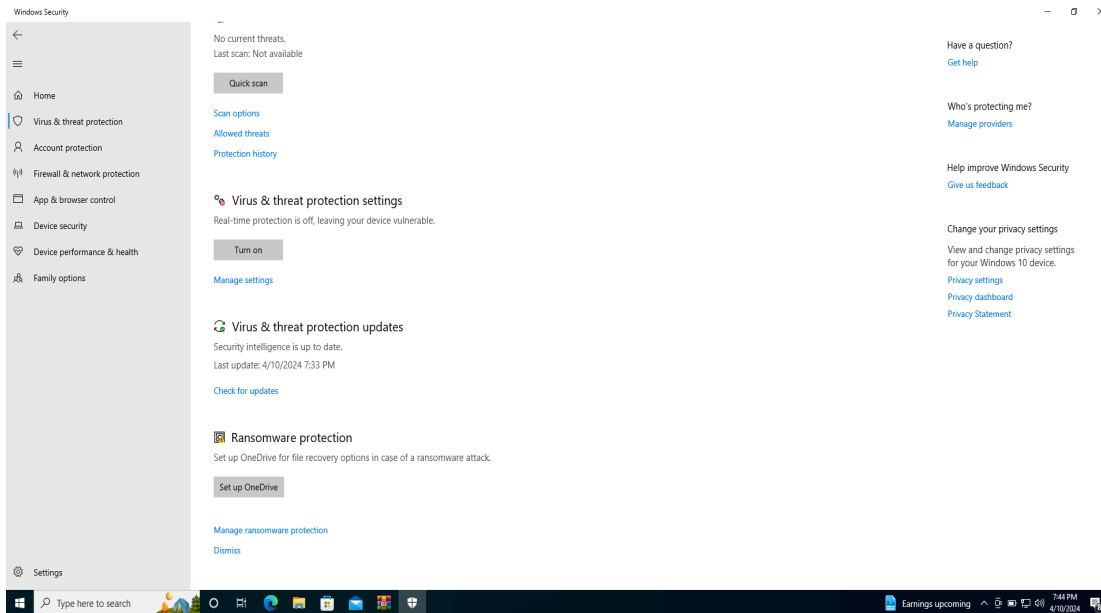
Tool Used : JPS Virus Maker and Virus Total Tool

Step 1 : Open the windows 10 OS in your virtual machine

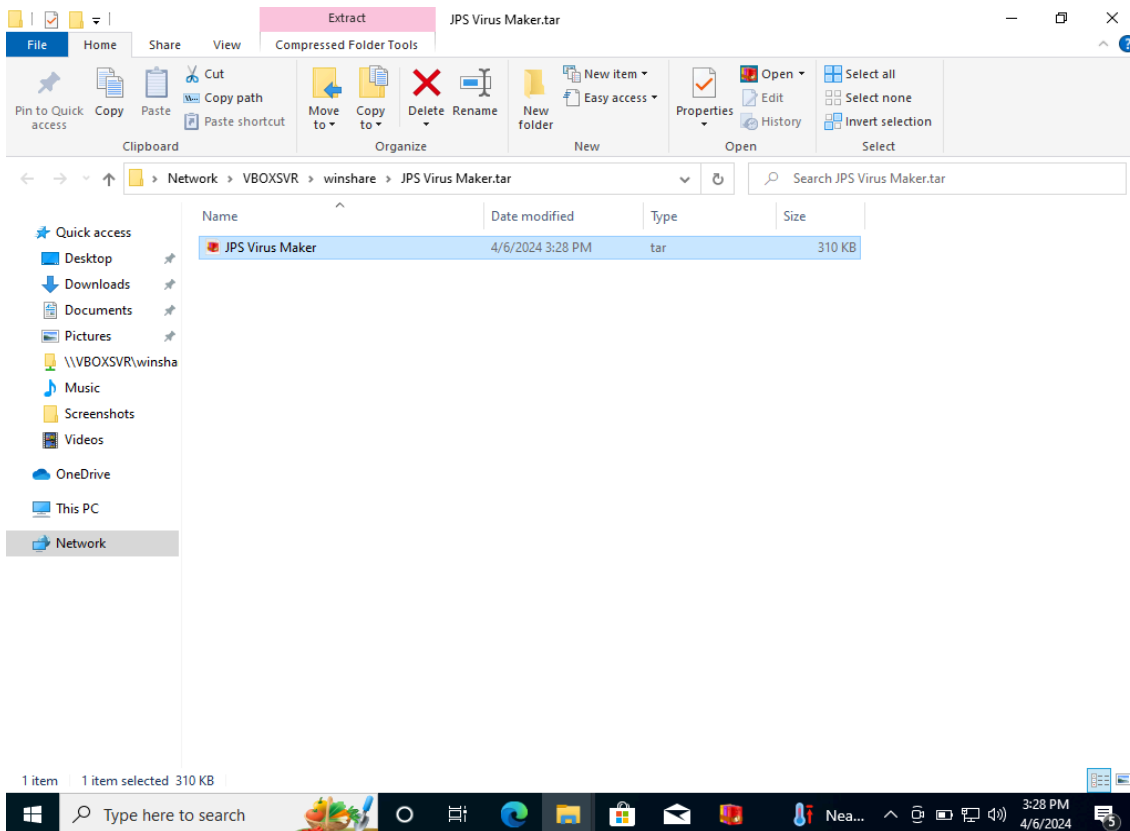


Step 2 : We need to turn off all the defenders, all firewalls and all the antivirus in the windows 10 system

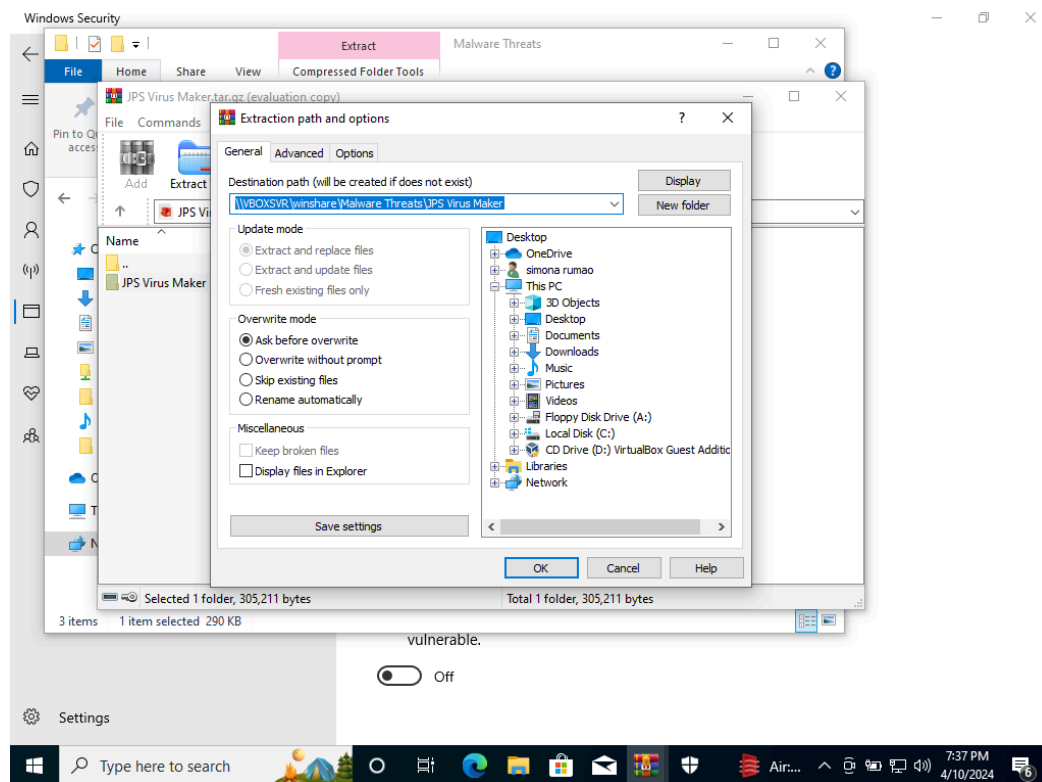




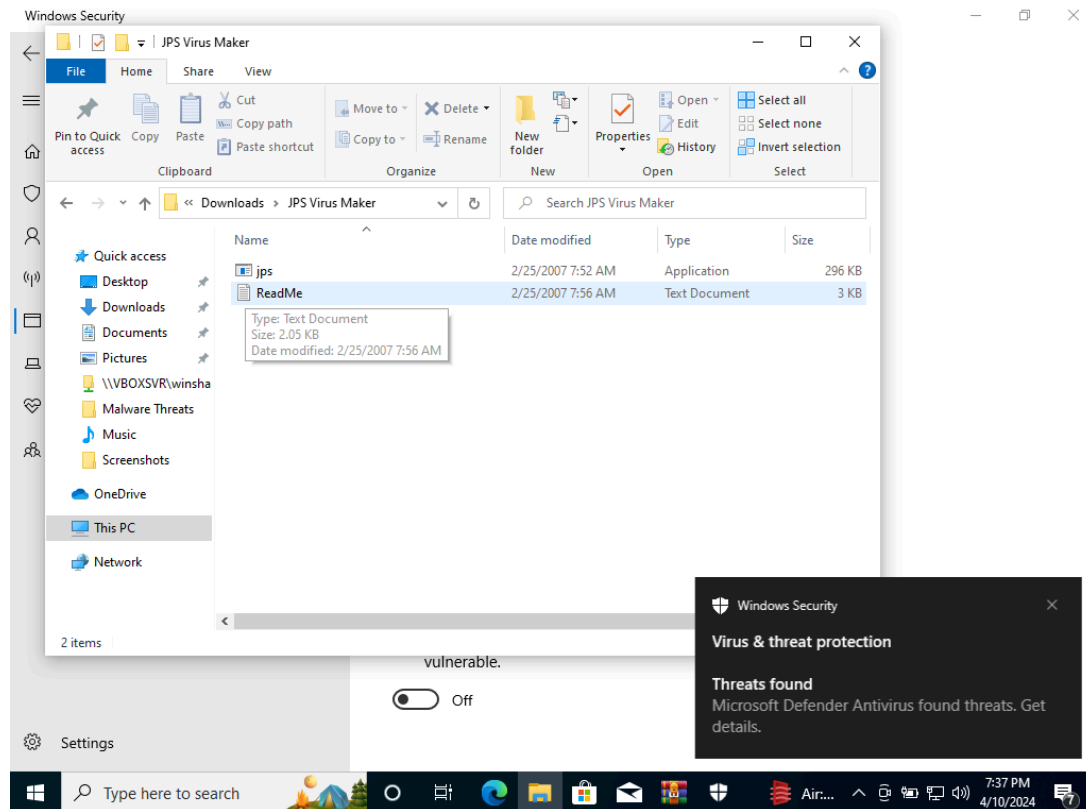
Step 3 : Then open the JPS Virus maker tool zip file in your system



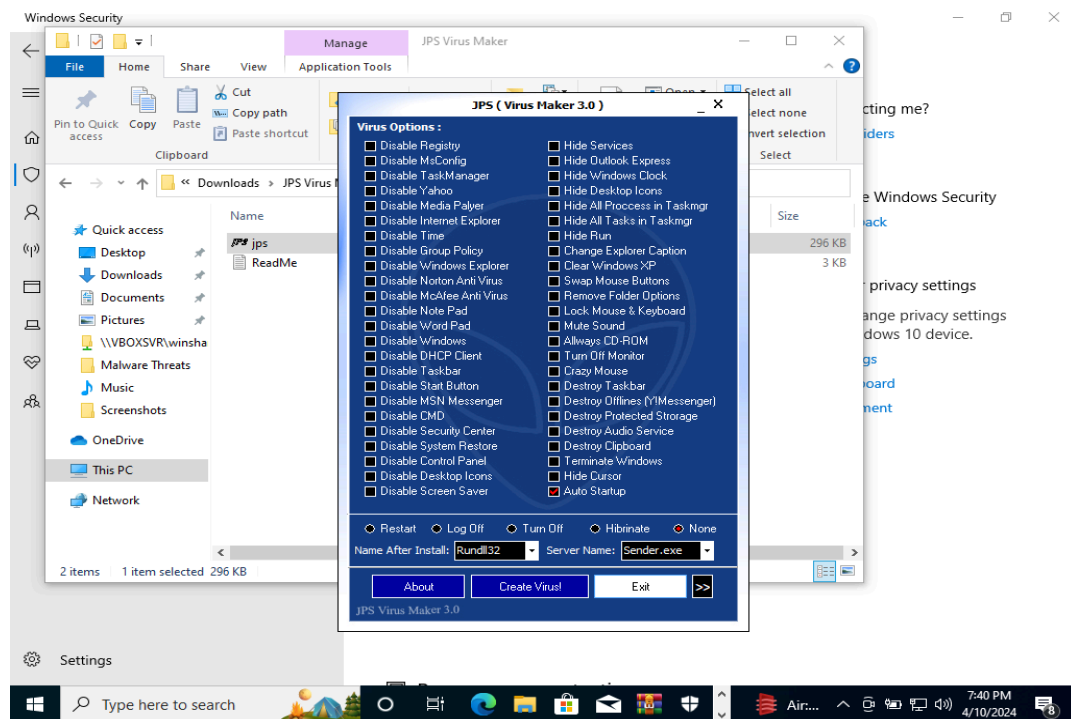
Step 4 : Then unzip the zip file in your system , if you don't turn off the firewalls then the firewall will delete the file itself



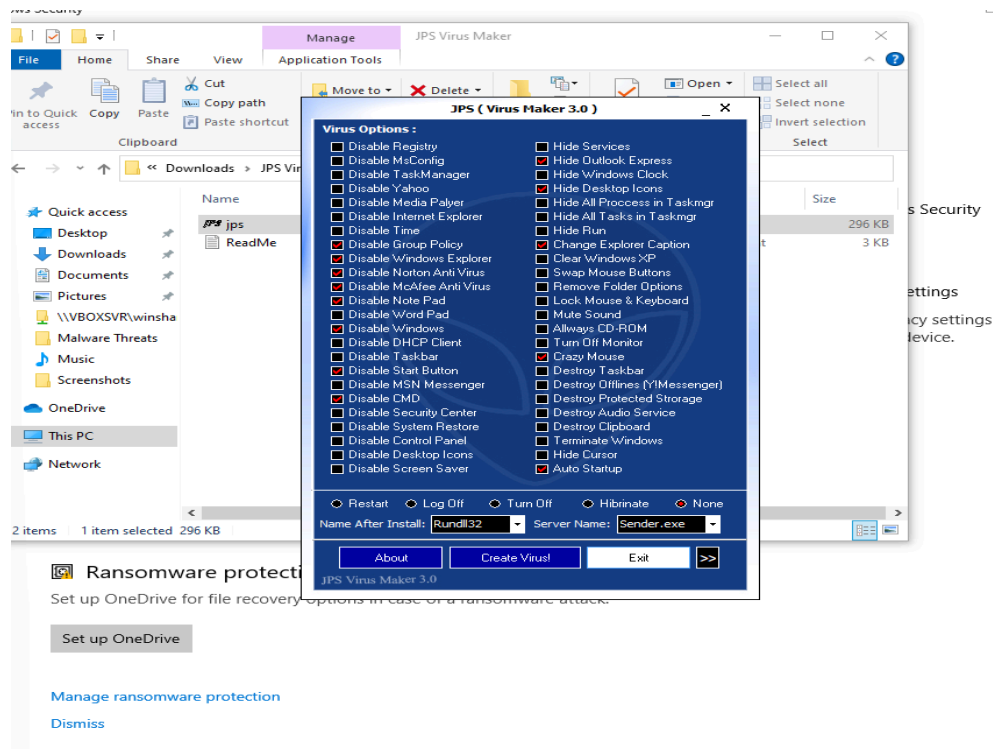
Step 5 : After unzipping we will get the application file that is exe file



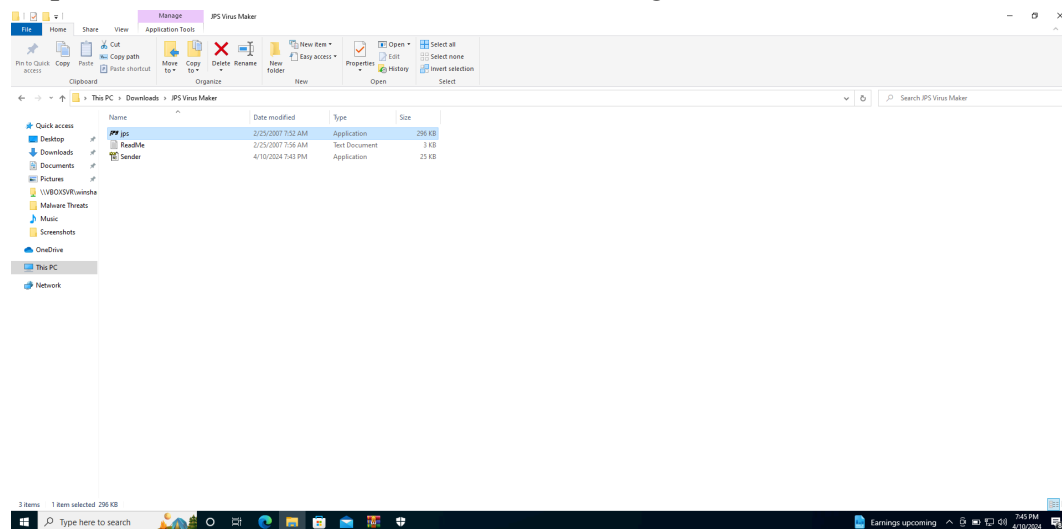
Step 6 : Open the application , we will get a some options to select the functionality of the virus



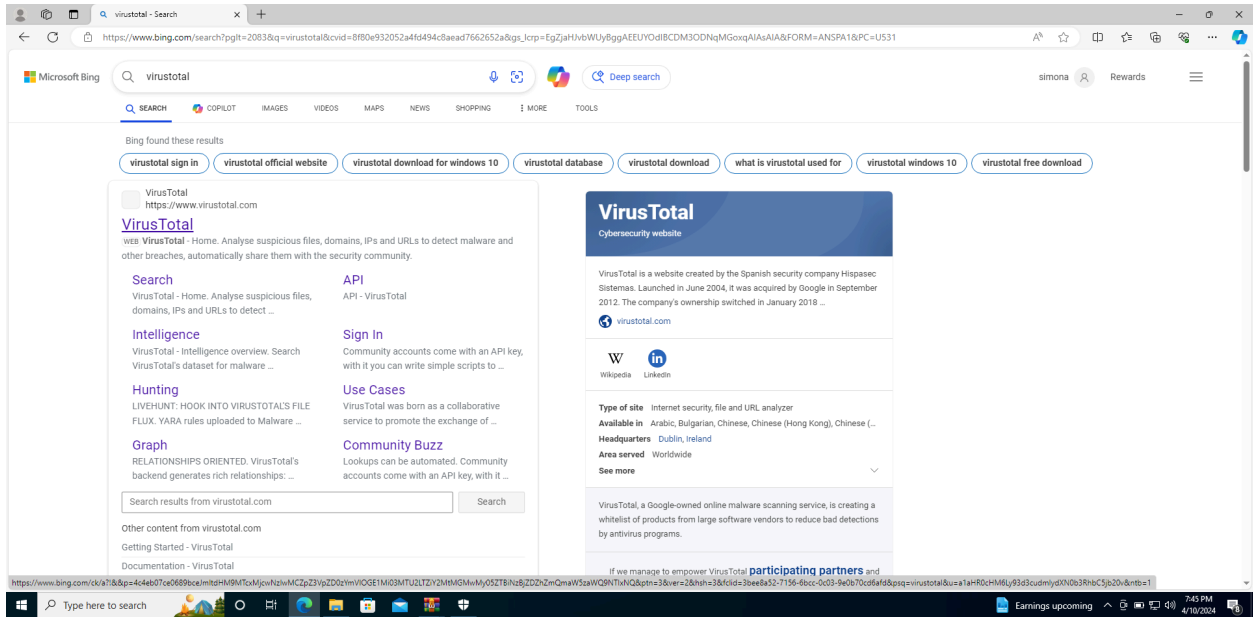
Step 7 : Tick the necessary options and click on the create Virus

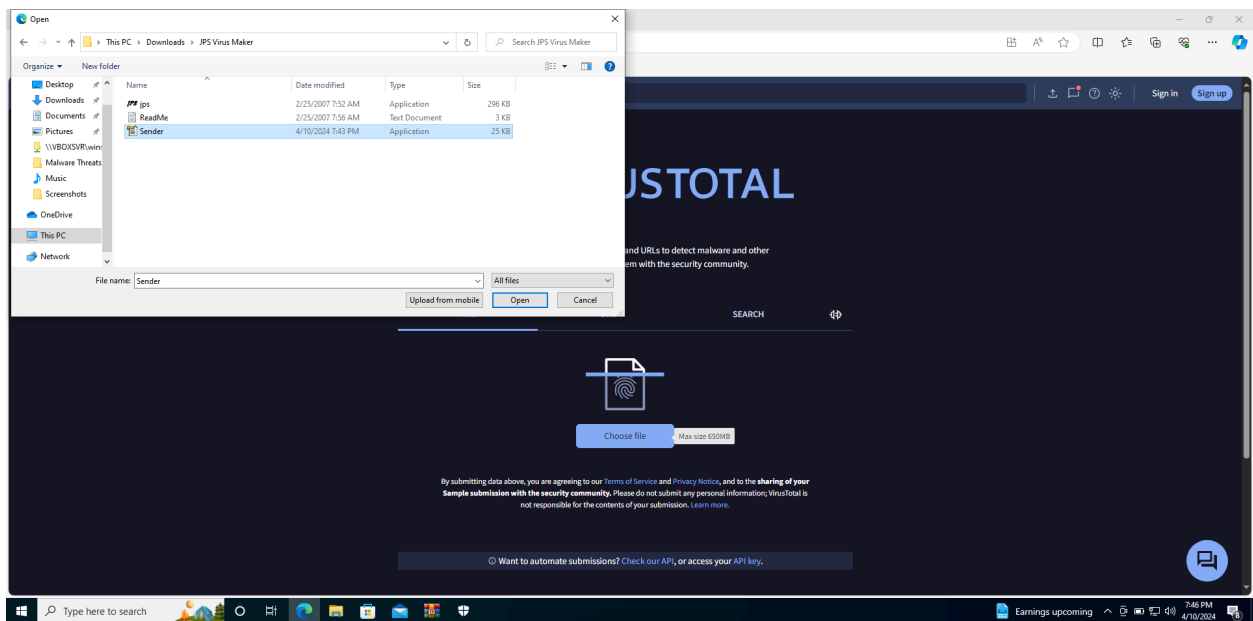
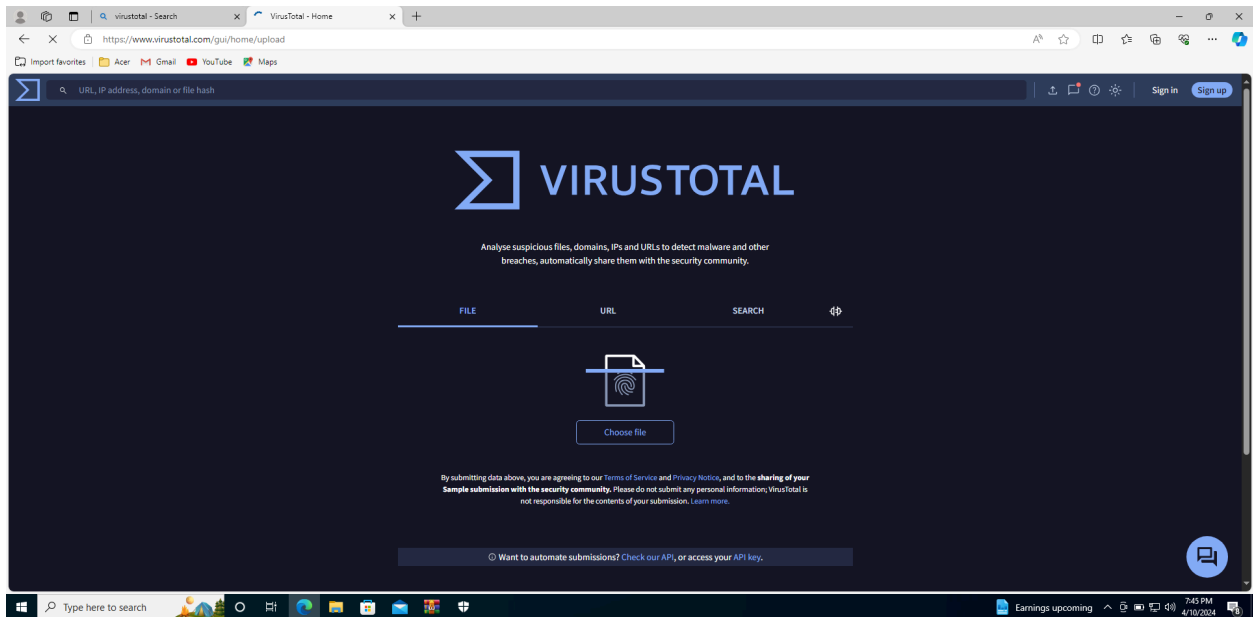


Step 8: Once we have created a virus, we will get a sender.exe file that is virus file



Step 8: Then open the virus total tool in your browser and upload the virus file sender.exe in the tool





## Step 9: Scan all the security vendors and identify all the malicious files all the vendors

The screenshot displays the VirusTotal analysis page for a file. The file's SHA256 hash is `bae7984733e4855b502592c860a20b0a610b392ec9b9cd655915f4ded0d05d9`. The file is identified as `Sender.exe`, with a size of 24.44 KB and a last modification date of 'a moment ago'. The file type is `EXE`.

The analysis shows a score of 63/71, indicating that 63 out of 71 security vendors have flagged the file as malicious. The file is categorized as a trojan, dropper, and spyware. The family labels are `fyyna`, `killav`, and `dlab`.

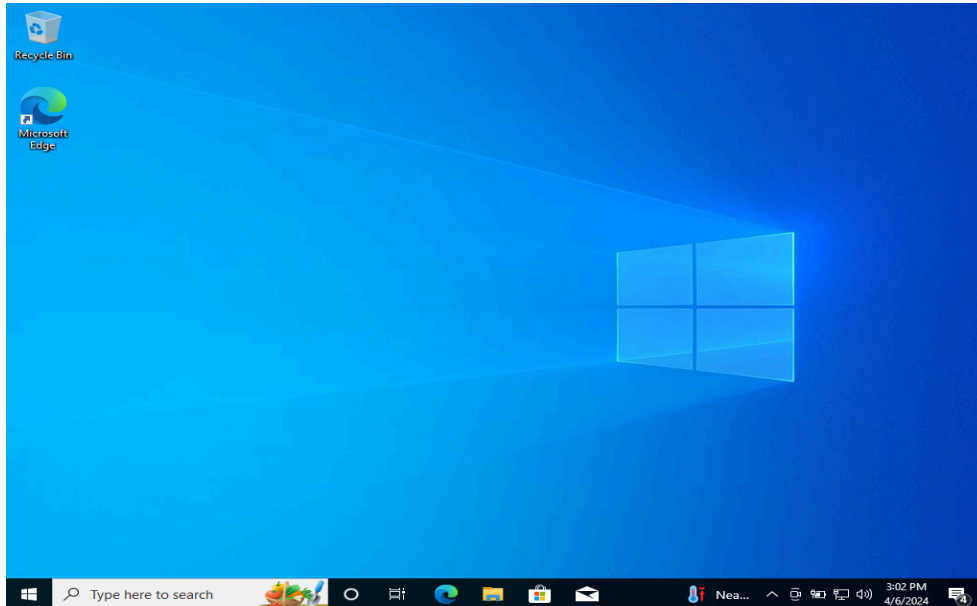
The 'Security vendors' analysis section shows a list of detections from various vendors. The table below summarizes the detections:

Vendor	Detection	Vendor	Detection
AhnLab-V3	Trojan.Win32.Xema.CS2178	ALYac	Backdoor.Delf.AVQ
Antiy-AVL	Trojan(Backdoor)/Win32.Delf	Arcabit	Backdoor.Delf.AVQ
Avast	Win32:Crypt-CWS [Trj]	AVG	Win32:Crypt-CWS [Trj]
Avira (no cloud)	TR/Hijacker.Gen	Baidu	Win32.Trojan.Delf.ac
BitDefender	Backdoor.Delf.AVQ	BitDefenderTheta	AI-Packer.2FF61CBF18
Bkav Pro	W32.AIDetect.Malware	ClamAV	Win.Trojan.Delf-9733756-0
CrowdStrike Falcon	Win/malicious.crodlhouse-890s (tr)	Cybereason	Upside
K7GW	Trojan (000a5de1)	Kaspersky	Trojan.Win32.Fyyna.dlab
Malwarebytes	Generic.Malware.ALDD5	MAX	Malware (ai Score=81)
MaxSecure	Trojan.Malware.9070886.susgen	McAfee	BackDoor-EKI
Microsoft	Trojan:Win32/Killav!pz	NANO-Antivirus	Trojan.Win32.Daws.dzdlrg
Panda	Trj/Genetic.gen	QuickHeal	Trojan.Killav.S20040
Rising	Harm.Delf.Ilf (CLASSIC)	Sangfor Engine Zero	Suspicious.Win32.Save.a
SecureAge	Malicious	SentinelOne (Static ML)	Static AI - Malicious PE
Skyhigh (SWG)	Behaves Like Win32.Dropper.mc	Sophos	Troj/Cimga-H
SUPERAntiSpyware	Trojan.Agent/Gen-Killav	Symantec	SMG.Heur!gen
TEHTRIS	Generic.Malware	Tencent	Trojan.Win32.Fyyna.hb
Tragmine	Malicious.high.ml.score	Trellix (FireEye)	Generic.mg.af3d3d9972befac
TrendMicro	TROJ_MALQ1FA	TrendMicro-HouseCall	TROJ_MALQ1FA
Varist	W32/Backdoor.FPQJ-0021	VBA32	SScope.Trojan.Prosti.2
VIPRE	Backdoor.Delf.AVQ	VirT	Backdoor.Win32.Delf.AVQ
ViRobot	Backdoor.Win32.Delf.25028	WithSecure	Trojan.TR/Hijacker.Gen
Xcitium	Backdoor.Win32.Delf.NGG@pwh	Yandex	Backdoor.Delf3JuULWwSow4B

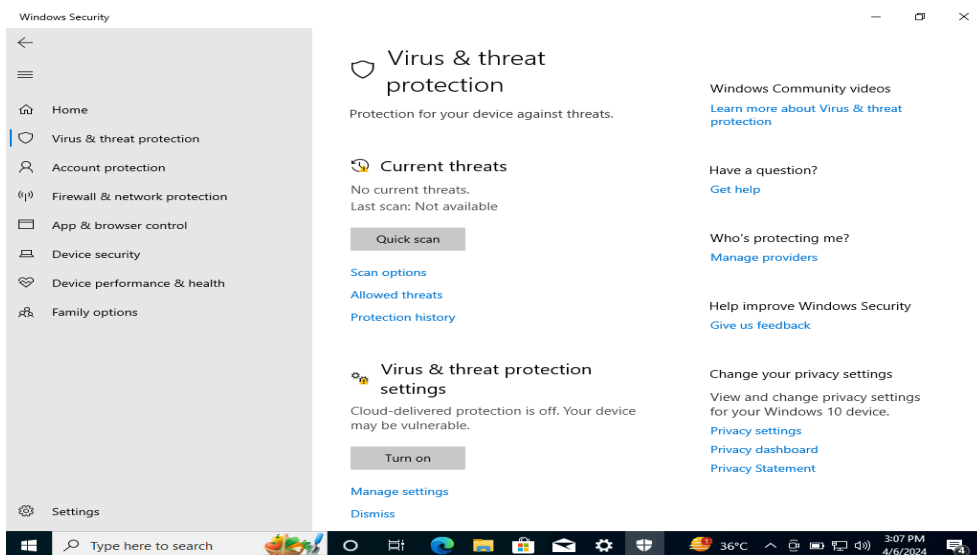


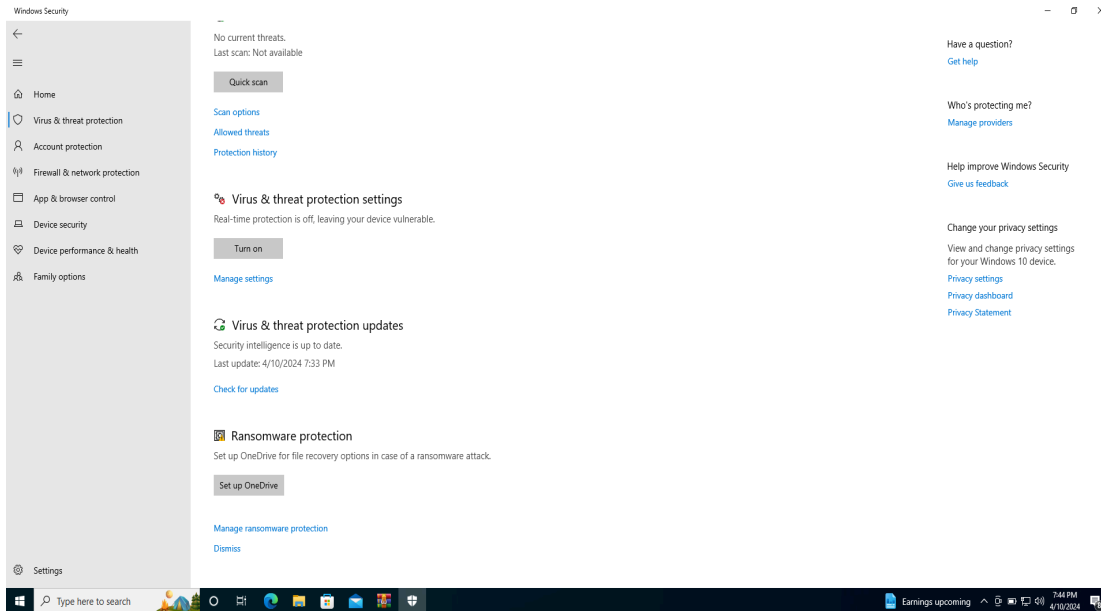
B. Create a trojan file using the NJRAT tool Scan the file with Virus Total and Report the details of security vendors who found it is a malicious file.

Step 1 : Open the windows 10 OS in your virtual machine

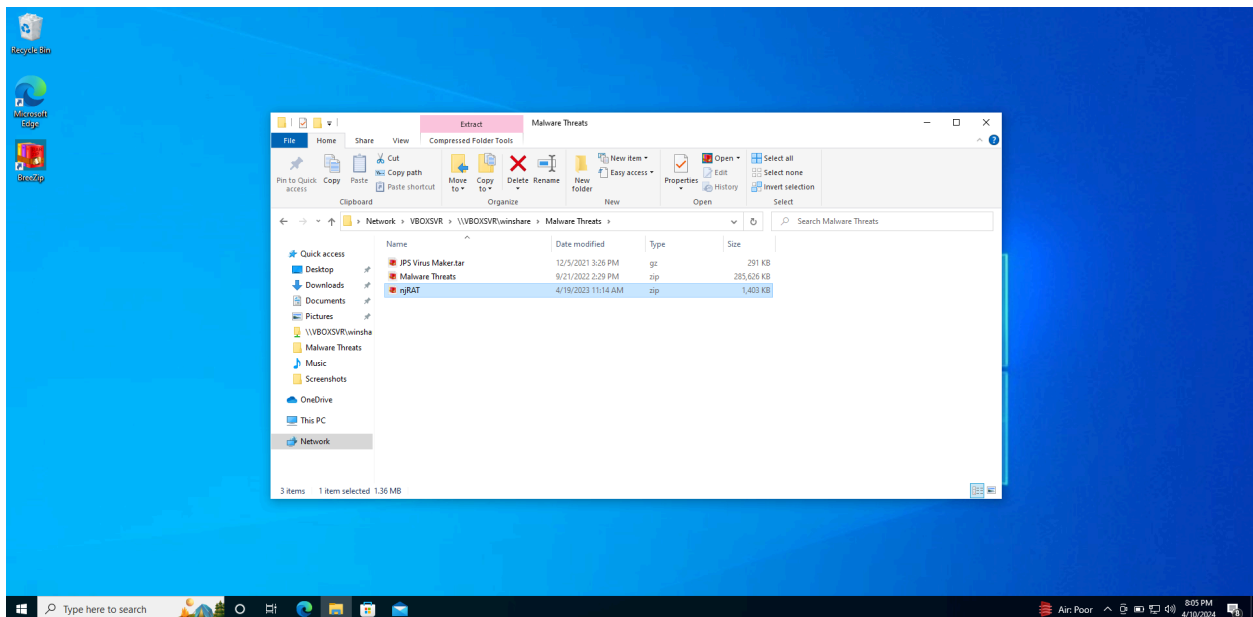


Step 2 : We need to turn off all the defenders, all firewalls and all the antivirus in the windows 10 system



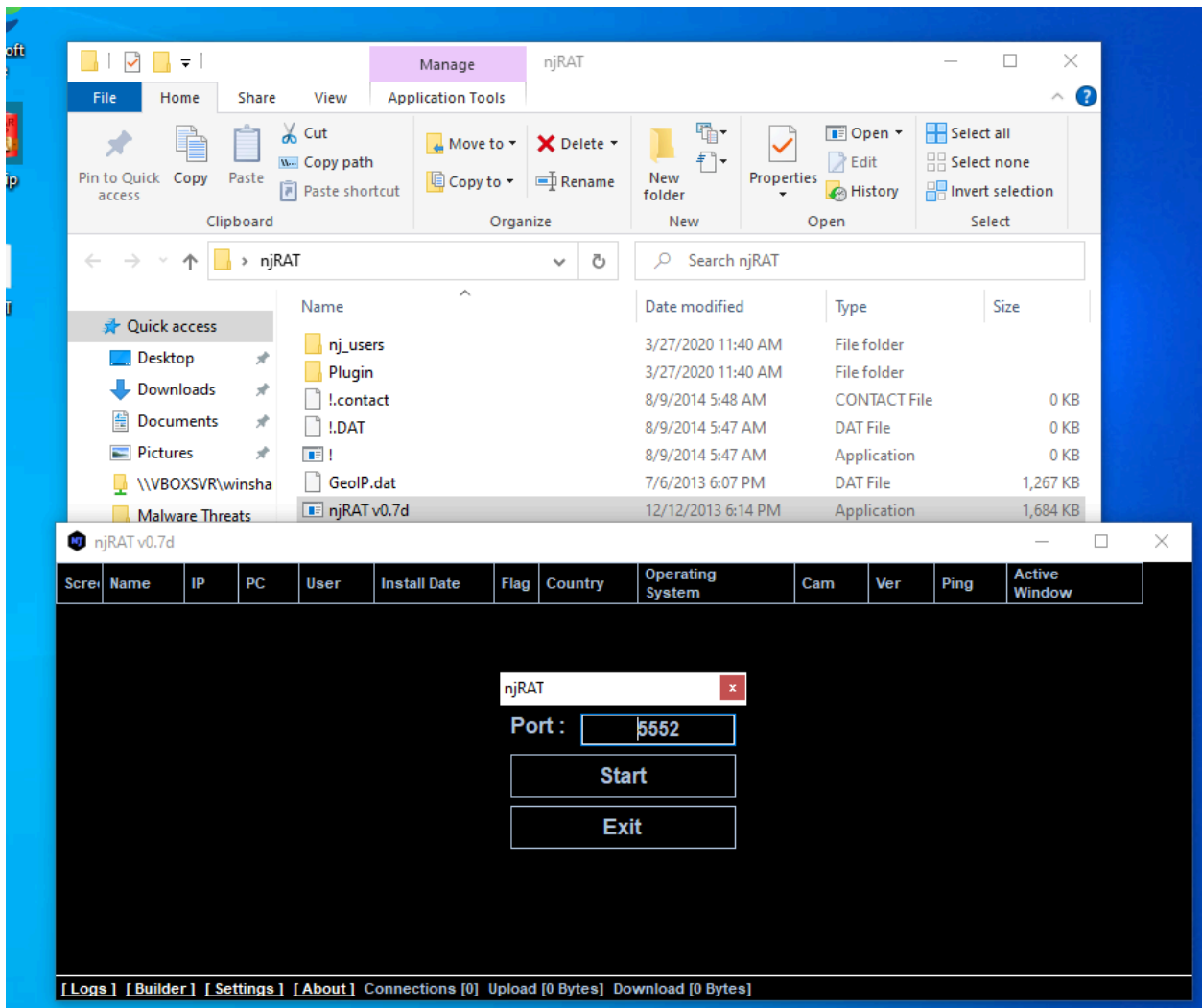
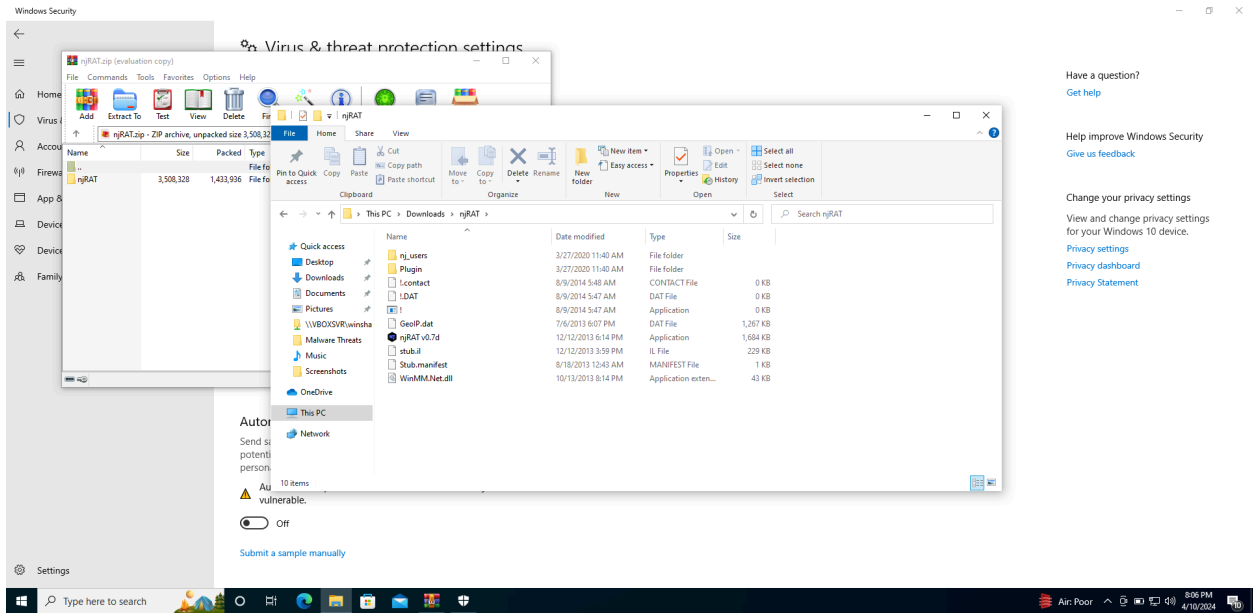


Step 3 : Then open the NJRAT tool zip file in your system

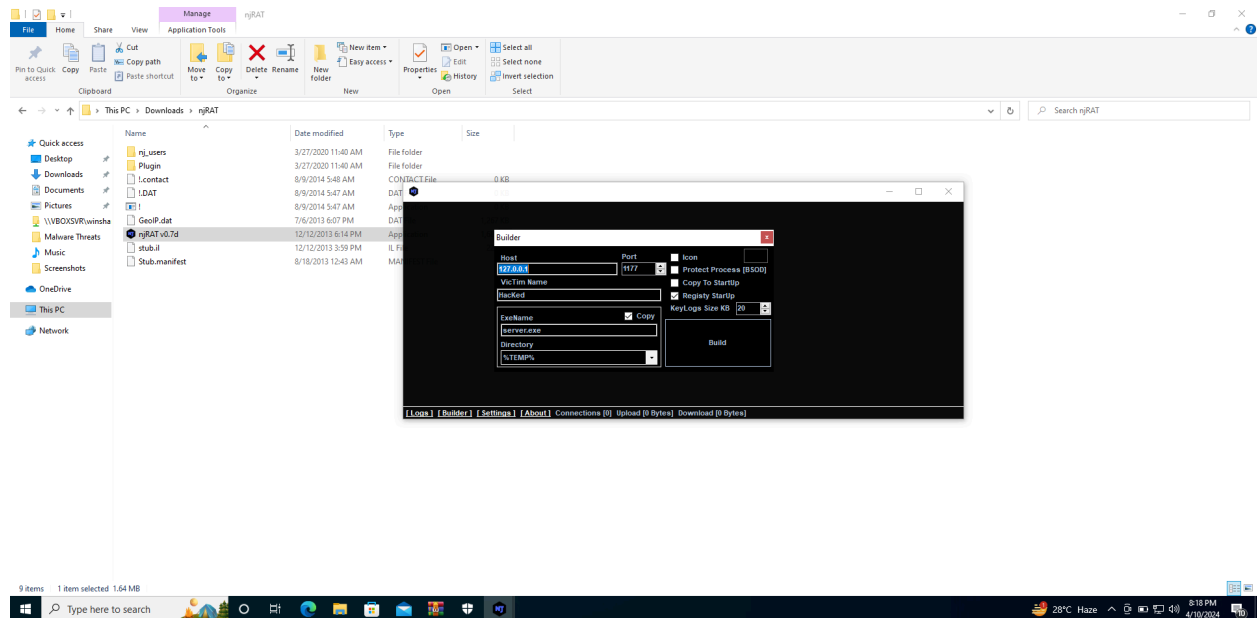


Step 4 : Then unzip the zip file in your system , if you don't turn off the firewalls then the firewall will delete the file itself

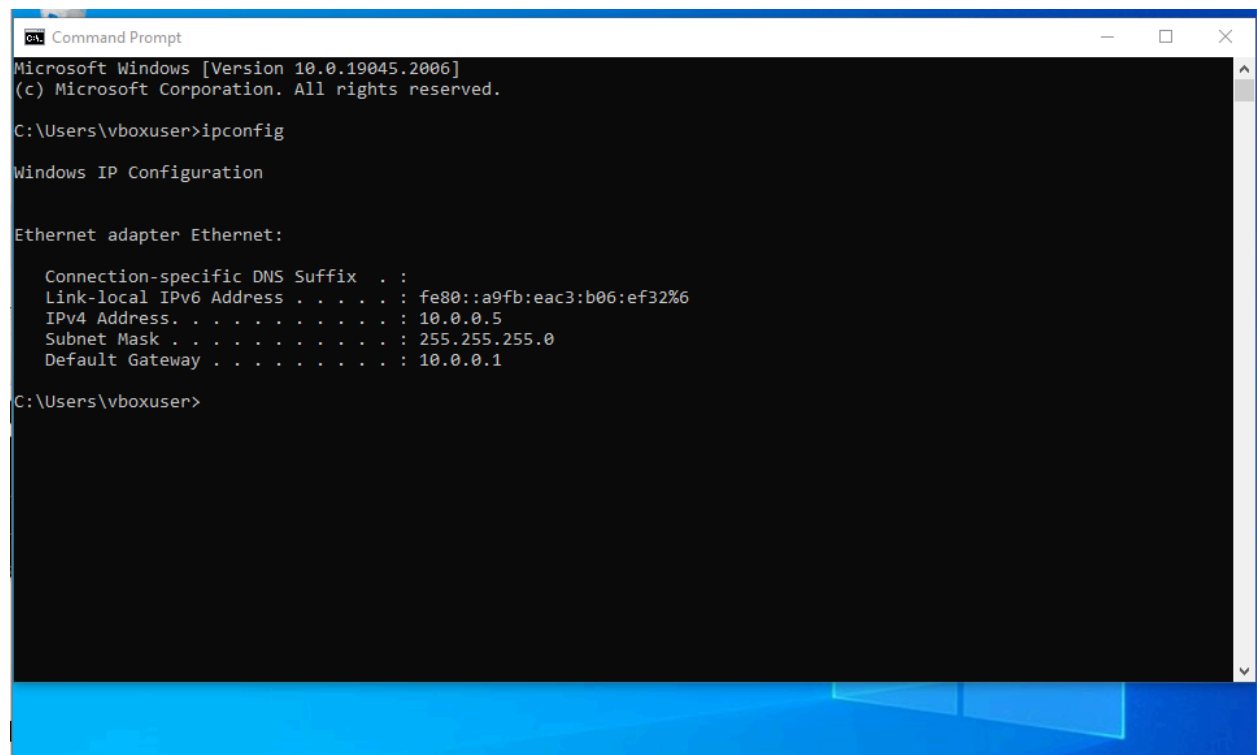
Step 5 : After unzipping we will get the application file that is exe file



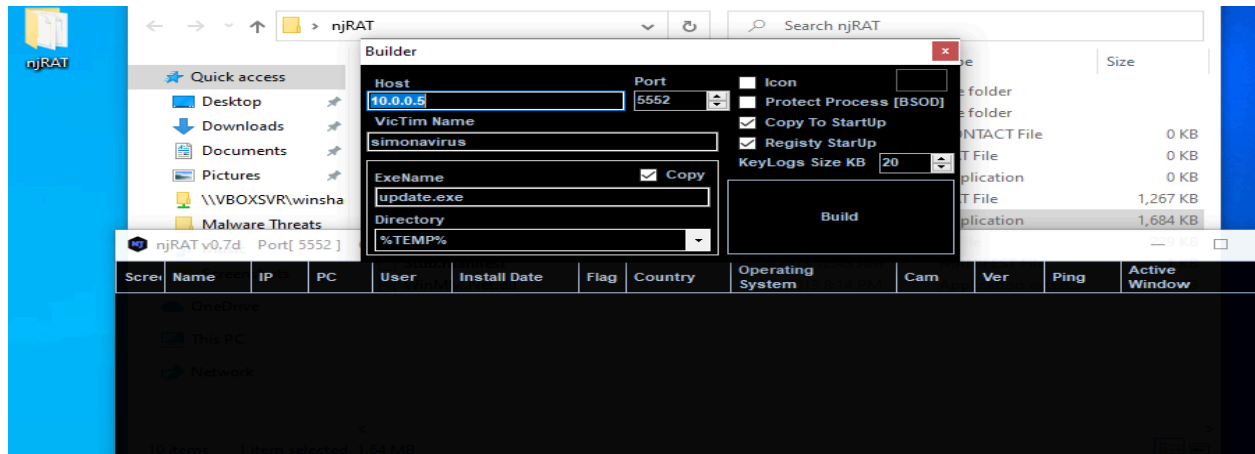
Step 6: Click on the builder at your left hand side bottom section



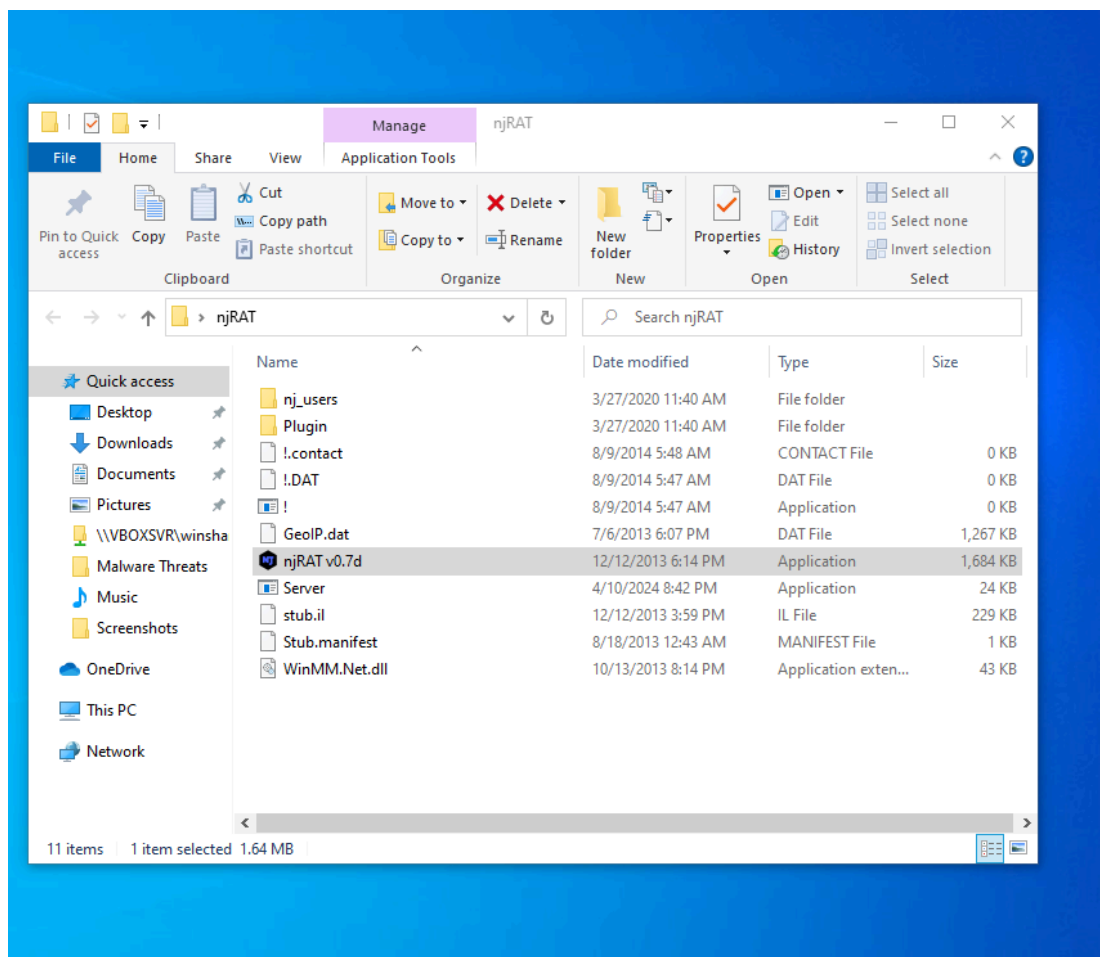
Step 7 : Then enter the Host IP address, here we will mention the windows 10 Ip address



Step 6 : Open the application , we will get a some options to select the functionality of the Trojan, we will tick the options and create a virus



Step 7: Once we have created a Trojan, we will get a sender.exe file that is virus file



Step 8: Then open the virus total tool in your browser and upload the virus file in the tool

Microsoft Bing search results for "virustotal". The page shows a list of search results, including "VirusTotal" and "VirusTotal - Home". The "VirusTotal" result is highlighted, showing a description of the service and a link to the website. The "VirusTotal - Home" result is also visible, showing a description of the service and a link to the website.

Bing found these results

[virustotal sign in](#) [virustotal official website](#) [virustotal download for windows 10](#) [virustotal database](#) [virustotal download](#) [what is virustotal used for](#) [virustotal windows 10](#) [virustotal free download](#)

**VirusTotal**  
Cybersecurity website

VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004, it was acquired by Google in September 2012. The company's ownership switched in January 2018 ...

[virustotal.com](#)

**Wikipedia** **LinkedIn**

**Type of site** Internet security, file and URL analyzer  
**Available in** Arabic, Bulgarian, Chinese, Chinese (Hong Kong), Chinese (...)  
**Headquarters** Dublin, Ireland  
**Area served** Worldwide  
**See more**

VirusTotal, a Google-owned online malware scanning service, is creating a whitelist of products from large software vendors to reduce bad detections by antivirus programs.

If we manage to empower VirusTotal **participating partners** and


VirusTotal - Home

URL, IP address, domain or file hash

**VIRUSTOTAL**

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

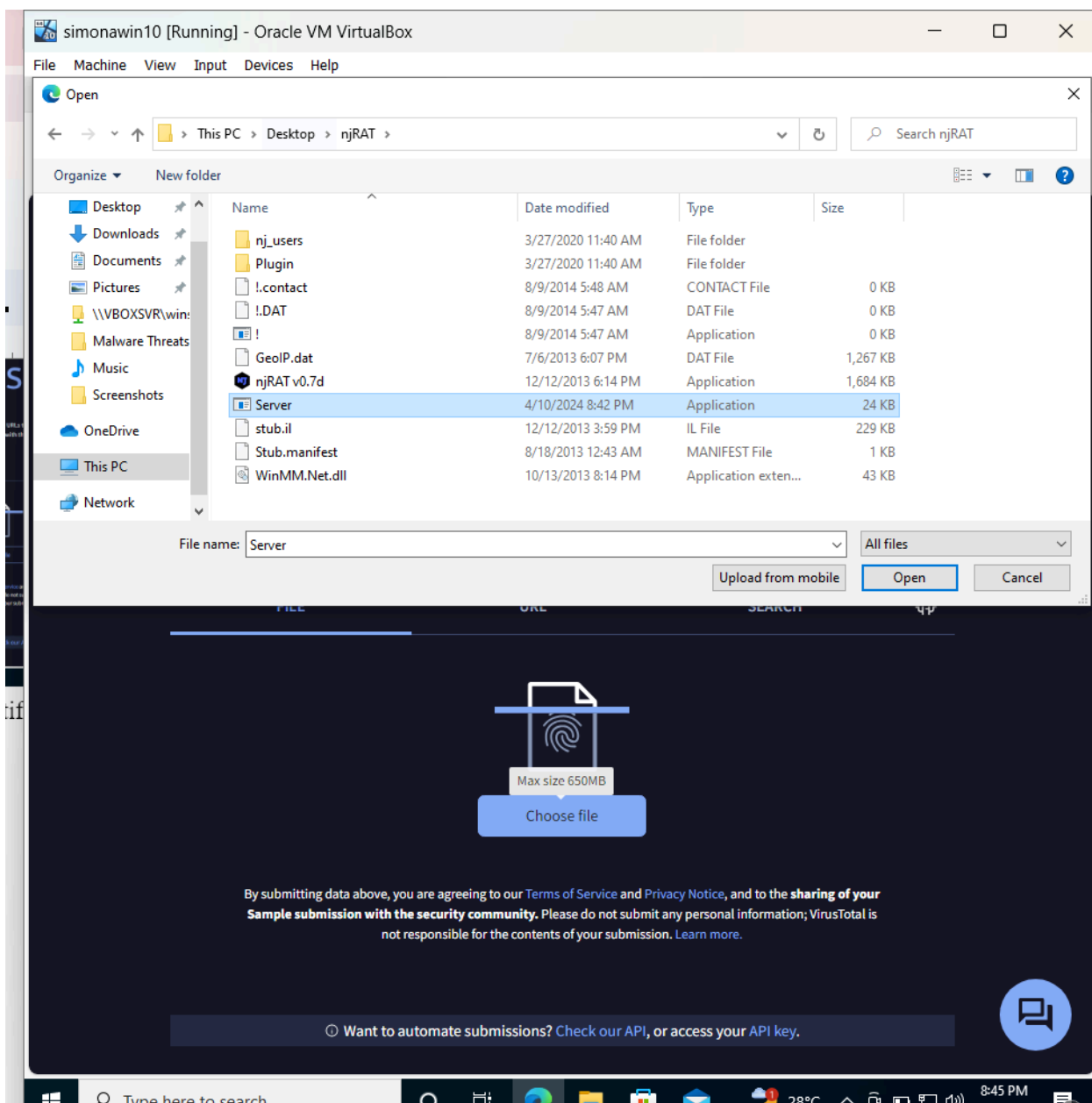
**FILE** **URL** **SEARCH**



[Choose file](#)

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the [sharing of your sample submission with the security community](#). Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

[Want to automate submissions? Check our API, or access your API key.](#)



Step 9: Scan all the security vendors and identify all the malicious files all the vendors

57

Community Score

57/69 security vendors and no sandboxes flagged this file as malicious

Reanalyze

Similar

More

e5fc5082e502edf165c0013899d670642a572233674181815196df1ee7a8fb9c

Server.exe

Size23.50 KB

Last Modification Datea moment ago

EXE

peexeassembly

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat labeltrojan.msl/bladabindi

Threat categoriestrojan dropper

Family labelsmilbladabindidifa

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Win-Trojan/Zbot.24064
ALYac	Generic.MSIL.Bladabindi.1D331915	Antiy-AVL	Trojan[Backdoor]/MSIL.Bladabindi.as
Arcabit	Generic.MSIL.Bladabindi.1D331915	Avast	MSILAgent-DRD [Trj]
AVG	MSIL.Agent-DRD [Trj]	Avira (no cloud)	TR/Dropper.Gen7
Baidu	MSIL.Backdoor.Bladabindi.a	BitDefender	Generic.MSIL.Bladabindi.1D331915
BitDefenderTheta	Gen:NN.Zemslf.36802.bmW@ammaXf	Bkav Pro	W32.FamVT.binANhb.Worm
ClamAV	Win.Packed.Generic-9789615-0	CrowdStrike Falcon	Win/malicious.configs.1009.00

e5fc5082e502edf165c0013899d670642a572233674181815196df1ee7a8fb9c

SecureAge

Malicious

SentinelOne (Static ML)

Static AI - Malicious PE

Skyhigh (SWG)

BehavesLike.Win32.BackdoorNJ.Rat.mm

Sophos

Troj/DoNot-P

Symantec

Backdoor.Ratenjay

Tencent

Trojan.Msl.Bladabindi.za

Trapmine

Malicious.moderate.ml.score

Trellix (FireEye)

Generic.mg.5e0eb813b20158c

TrendMicro

BKDR.BLADAB1.SMC

TrendMicro-HouseCall

BKDR.BLADAB1.SMI

Varist

W32/MSIL\_Bladabindi.AU.genIEldorado

VBA32

Trojan.MSIL.Bladabindi.Heur

VIPRE

Generic.MSIL\_Bladabindi.1D331915

ViriT

Backdoor.Win32.Generic.AWM

ViRobot

Backdoor.Win32.Bladabindi.Gen.A

WithSecure

Trojan.TR/Dropper.Gen7

Xcitium

Backdoor.MSIL.Bladabindi.A@566ygc

Zillya

Trojan.Disfa.Win32.27264

ZoneAlarm by Check Point

Trojan.MSIL.Disfa.bqg

Alibaba

Undetected

CMC

Undetected

Cymet

Undetected

Gridinsoft (no cloud)

Undetected

Kingsoft

Undetected

Lionic

Undetected

Palo Alto Networks

Undetected

SUPERAntiSpyware

Undetected

TACHYON

Undetected

TEHTRIS

Undetected

Yandex

Undetected

Zoner

Undetected

Avast-Mobile

Unable to process file type

Type here to search

28°C Mostly clear

8:46 PM