

What is VirusTotal ?

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 to Chronicle, a subsidiary of Google. VirusTotal is a free service that uses more than 50 antivirus engines on the VirusTotal web service to analyze suspicious files and URLs. Using VirusTotal facilitates the quick detection of viruses, worms, Trojans, and all kinds of malware.



How it works:-

VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal.

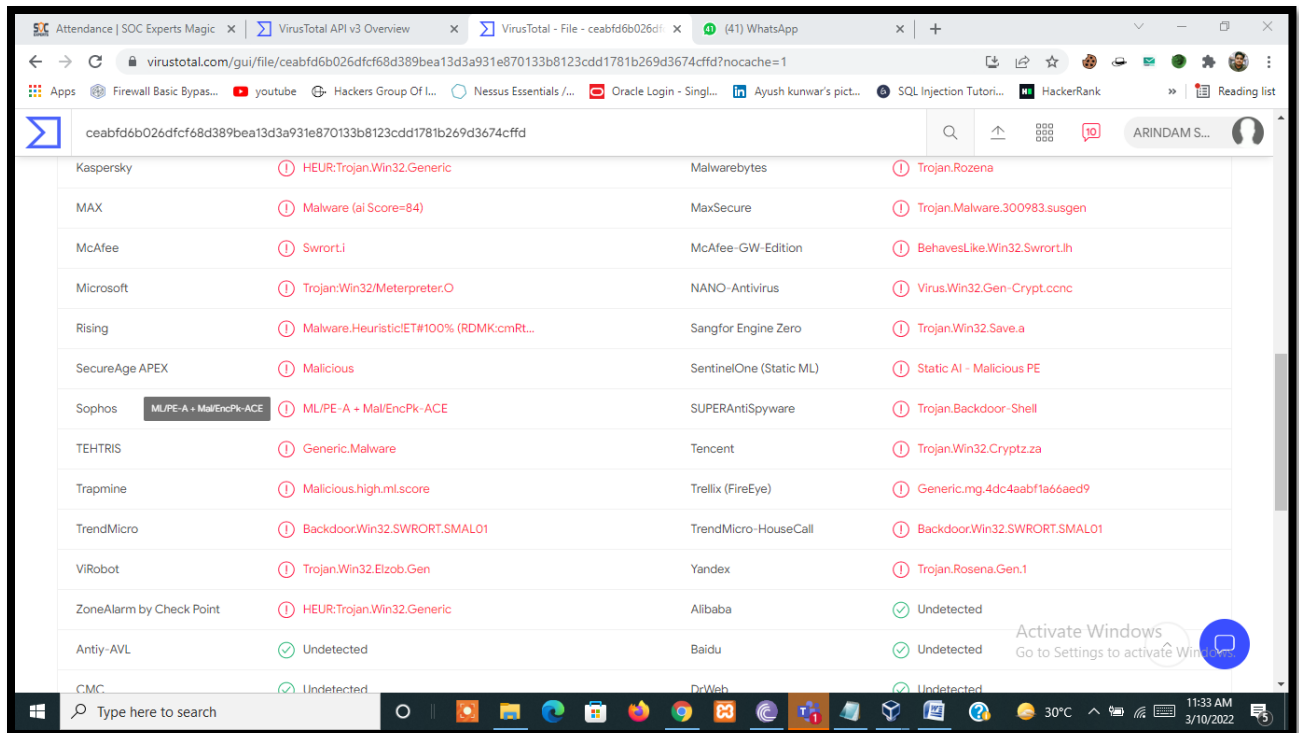
VirusTotal offers a number of file submission methods, including the primary public web interface, desktop uploaders, browser extensions and a programmatic API. The web interface has the highest scanning priority among the publicly available submission methods. Submissions may be scripted in any programming language using the HTTP-based public API. As with files, URLs can be submitted via several different means including the VirusTotal webpage, browser extensions and the

API. Upon submitting a file or URL basic results are shared with the submitter, and also between the examining partners, who use results to improve their own systems. As a result, by submitting files, URLs, domains, etc. to VirusTotal you are contributing to raise the global IT security level. This core analysis is also the basis for several other features, including the VirusTotal Community: a network that allows users to comment on files and URLs and share notes with each other. VirusTotal can be useful in detecting malicious content and also in identifying false positives -- normal and harmless items detected as malicious by one or more scanners.

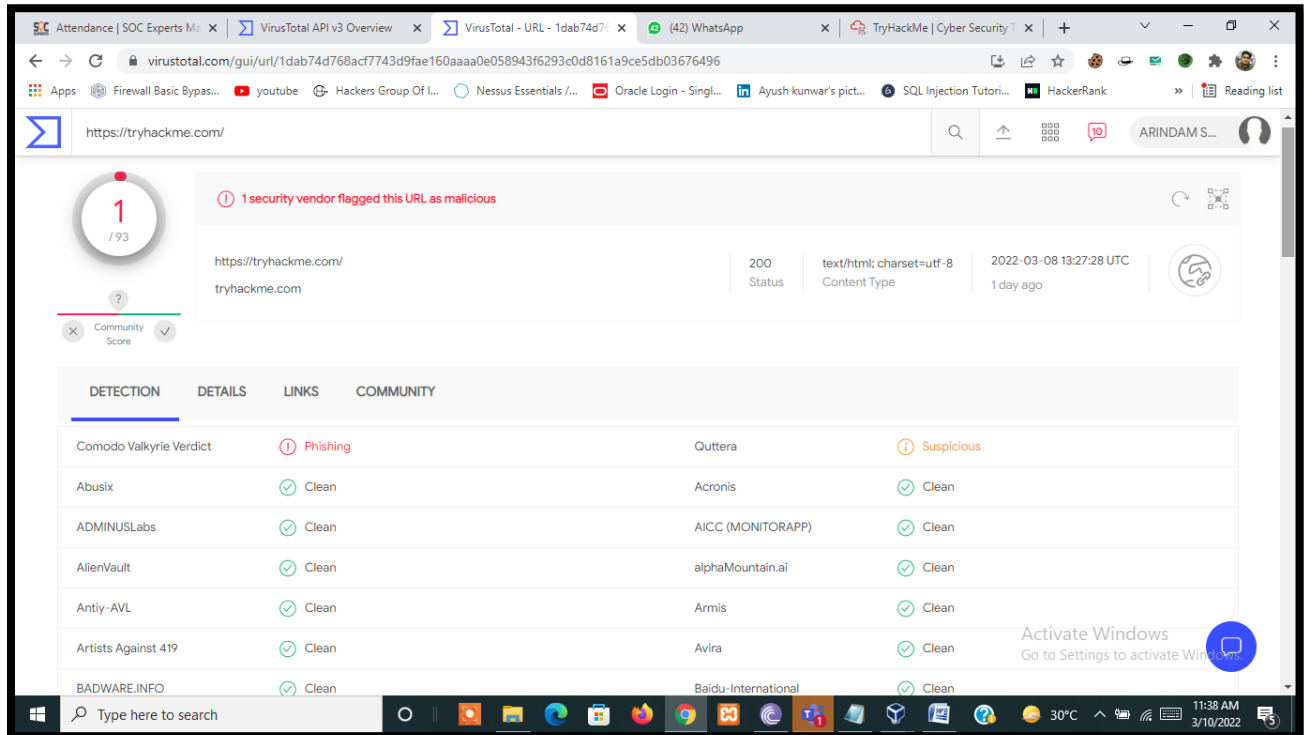
FILE Analysis:- Here I have tested a malicious EXE file named virus.exe which I have made by using Metasploit framework.

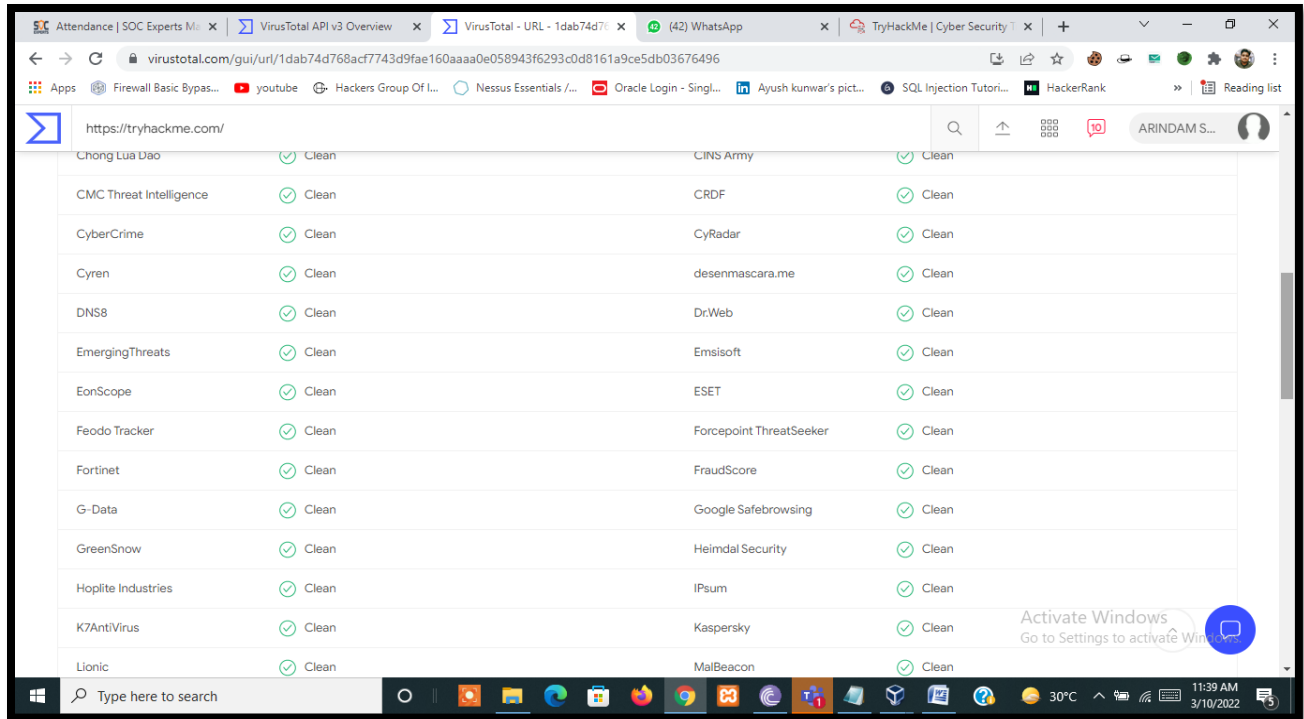
The screenshot shows the VirusTotal web interface for a file analysis. The file is identified as 'ab.exe' with a size of 72.07 KB, submitted on 2022-03-10 at 05:57:59 UTC. The file is flagged as malicious by 51 security vendors. The analysis shows several detections, including Trojan.CryptZ.Gen, Trojan.Win32.Shell.R1283, Win32.Meterpreter-C [Trj], Trojan.Swroot.A, and Trojan.CryptZ.Gen. The file is also flagged as suspicious by Acronis (Static ML).

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis (Static ML)	⚠ Suspicious	Ad-Aware	⚠ Trojan.CryptZ.Gen
AhnLab-V3	⚠ Trojan/Win32.Shell.R1283	ALYac	⚠ Trojan.CryptZ.Gen
Arcabit	⚠ Trojan.CryptZ.Gen	Avast	⚠ Win32.Meterpreter-C [Trj]
AVG	⚠ Win32.Meterpreter-C [Trj]	Avira (no cloud)	⚠ TR/Patched.Gen2
BitDefender	⚠ Trojan.CryptZ.Gen	BitDefenderTheta	⚠ Gen:NN.ZexaF.34264.eq1@eGDXRbf
CAT-QuickHeal	⚠ Trojan.Swroot.A	ClamAV	⚠ Win.Trojan.Swroot-5710536-0

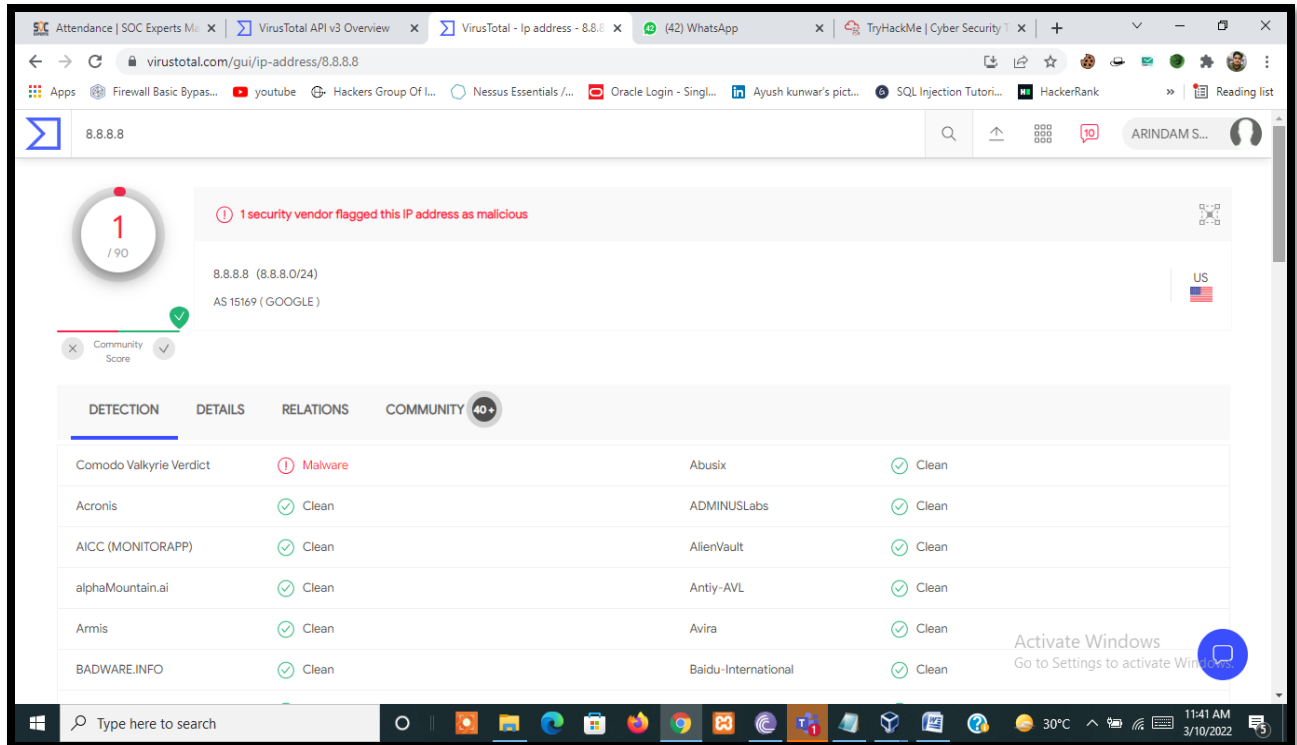


URL Analysis:- Here I have scanned tryhackme 's website.





SEARCH Option:- Here I have searched using IP address 8.8.8.8 which is belong to Google.



8.8.8.8

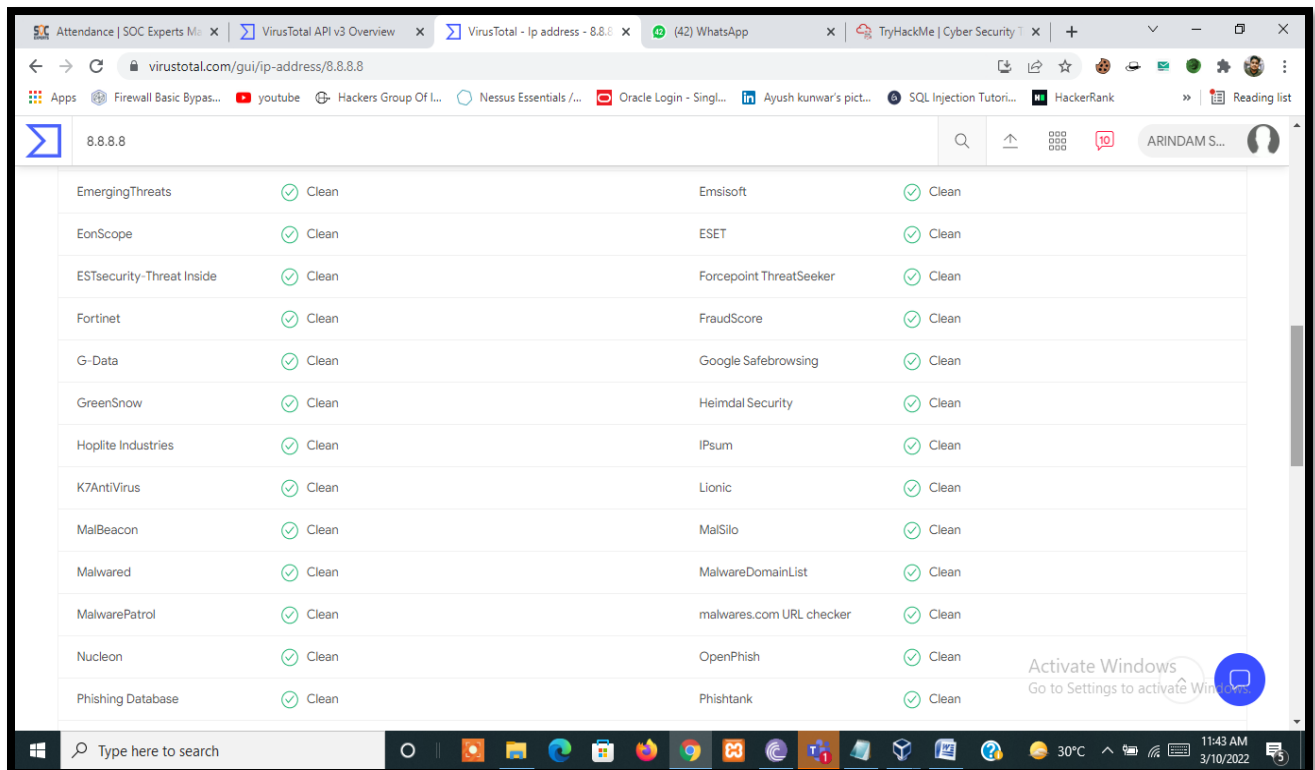
1 security vendor flagged this IP address as malicious

8.8.8.8 (8.8.8.0/24)
AS 15169 (GOOGLE)

Community Score

DETECTION	DETAILS	RELATIONS	COMMUNITY
Comodo Valkyrie Verdict	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Armis	Clean	Avira	Clean
BADWARE.INFO	Clean	Baidu-International	Clean

Activate Windows
Go to Settings to activate Windows



8.8.8.8

EmergingThreats	Clean	Emsisoft	Clean
EonScope	Clean	ESET	Clean
ESTsecurity-Threat Inside	Clean	Forcepoint ThreatSeeker	Clean
Fortinet	Clean	FraudScore	Clean
G-Data	Clean	Google Safebrowsing	Clean
GreenSnow	Clean	Heimdal Security	Clean
Hoplite Industries	Clean	IPsum	Clean
K7AntiVirus	Clean	Lionic	Clean
MalBeacon	Clean	MalSilo	Clean
MalwareD	Clean	MalwareDomainList	Clean
MalwarePatrol	Clean	malwares.com URL checker	Clean
Nucleon	Clean	OpenPhish	Clean
Phishing Database	Clean	Phishtank	Clean

Activate Windows
Go to Settings to activate Windows