

VirusTotal – A Multi-Engine Malware Detection Platform

Final Report

Name: P. Vasundhara Devi

Program Name: Cyber Security

Date: 01/09/2025

Github Repository: <https://github.com/Vasundharadevi-1604/CS>

Project Overview

VirusTotal is a leading online cybersecurity platform that provides comprehensive malware detection and threat intelligence services. Owned by Google's parent company Alphabet, it serves as one of the world's largest threat intelligence repositories, processing millions of submissions daily from security professionals, researchers, and general users worldwide.

The platform serves as a critical tool for threat detection, malware analysis, and cybersecurity research, supporting industries ranging from enterprise security to academic research institutions.

Technologies & Tools Used

- **Multi-Engine Detection:** 70+ antivirus engines and security scanners
 - **Sandbox Analysis:** Cuckoo sandbox for dynamic malware analysis
 - **Database Technology:** Massive distributed storage system
 - **API Framework:** RESTful APIs for programmatic access
 - **Web Interface:** Modern web-based user interface
 - **Mobile Applications:** iOS and Android mobile apps
-

System Architecture

- **Submission Layer:** Users submit files, URLs, IP addresses, or domains through web interface, API, or mobile apps
- **Analysis Engine:** Multi-engine scanning system processes submissions against 70+ security tools simultaneously
- **Sandbox Environment:** Dynamic analysis executes suspicious files in controlled environments
- **Intelligence Database:** Results are stored in comprehensive database containing over 50 billion files, 6 billion URLs, and 4 billion domains
- **Threat Intelligence:** Advanced analytics provide contextual information and relationship mapping
- **Reporting System:** Comprehensive reports delivered through multiple channels

Security Features

- Multi-Engine Scanning: Leverages 70+ antivirus engines for comprehensive threat detection
- Dynamic Analysis: Executes malware in sandbox environments to observe behavior
- YARA Rules Integration: Custom rule creation and matching across entire database
- Threat Graph Visualization: Visual relationship mapping between malicious entities
- False Positive Detection: Identifies legitimate files incorrectly flagged as malicious
- Behavioral Analysis: Advanced heuristic detection methods

Platform Structure

VirusTotal Platform/

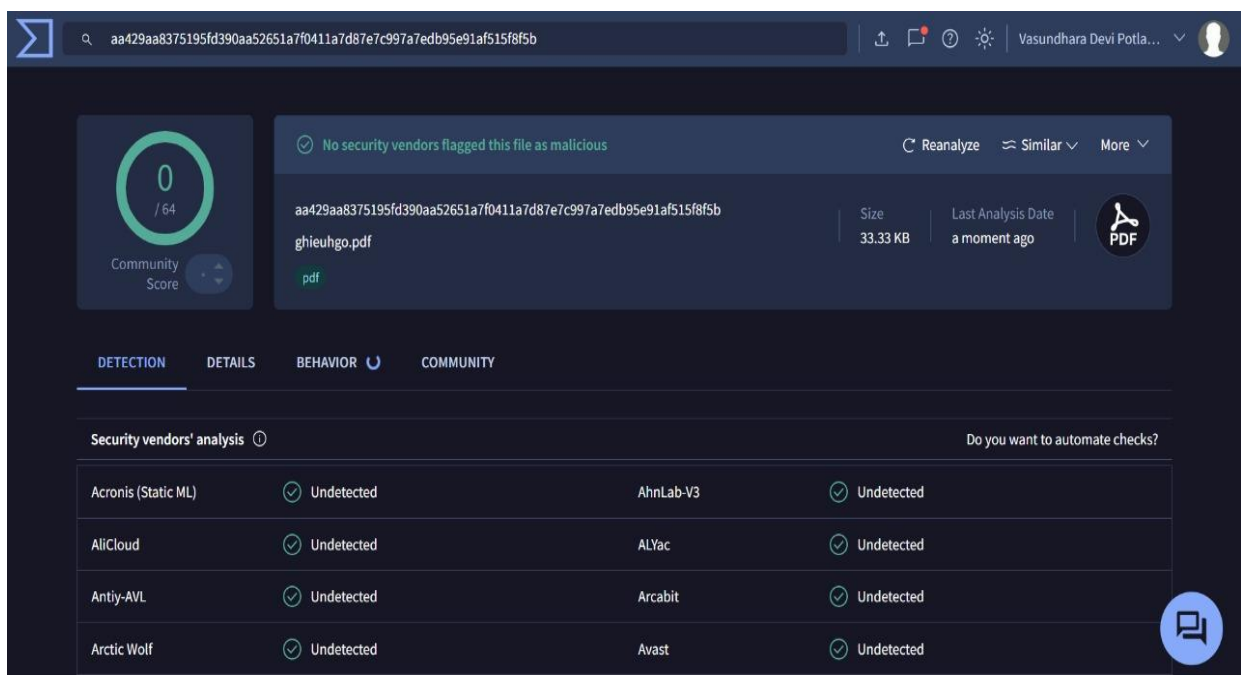
— Web Interface/	# Primary user interface
— File Scanner	# File upload and analysis
— URL Scanner	# Website and link analysis
— Search Portal	# Hash and IP lookup
— API Services/	# Programmatic access
— Public API	# Free tier (500 requests/day)
— Premium API	# Enhanced access levels
— Enterprise API	# Full feature access
— Mobile Apps/	# iOS and Android applications
— Database/	# Threat intelligence storage
— File Repository	# 50+ billion files
— URL Database	# 6 billion URLs analyzed
— Domain Intelligence	# 4 billion domains tracked
— Analysis Engines/	# Detection systems
— Static Analysis	# Signature-based detection
— Dynamic Analysis	# Behavioral sandbox
— Machine Learning	# AI-powered detection

Screenshots

1. Main Interface & Options:



2. File Analysis Result:



3. Clean URL Detection:

The screenshot shows the VirusTotal interface for the URL `https://www.example.com/cars/sports-car`. The community score is 0/97, indicating a clean URL. A message states: "No security vendors flagged this URL as malicious". The status is 404, content type is text/html, and the last analysis date is "a moment ago".

Security vendors' analysis

Vendor	Result	Vendor	Result
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean

4. Malicious URL Detection:

The screenshot shows the VirusTotal interface for the URL `http://signin.eby.de.zukruxgxtzmmqi.civpro.co.za/`. The community score is 9/97, indicating a malicious URL. A message states: "9/97 security vendors flagged this URL as malicious". The last analysis date is "2 days ago".

Security vendors' analysis

Vendor	Result	Vendor	Result
alphaMountain.ai	Phishing	CRDF	Malicious
CyRadat	Malicious	Fortinet	Phishing
Kaspersky	Phishing	Lionic	Phishing
SOCRadar	Malware	Sophos	Phishing

5. Clean IP Address Analysis:

The screenshot shows the VirusShare interface for the IP address 10.0.0.0. The top navigation bar includes a search bar with the IP, a user profile, and various utility icons. The main header displays a green circular progress indicator with '0 / 94' and a 'Community Score' of 0. To the right, it states '9 detected files communicating with this IP address' and 'Last Analysis Date 4 hours ago'. Below the header, a tabbed interface shows 'DETECTION', 'DETAILS', 'RELATIONS', and 'COMMUNITY' (74). The 'Security vendors' analysis' section is active, showing a table of results from various vendors.

Security vendors' analysis		Do you want to automate checks?	
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
benkow.cc	✓ Clean	BitDefender	✓ Clean

6. Malicious IP Address Analysis:

The screenshot shows the VirusShare interface for the IP address 80.82.77.139. The top navigation bar is similar to the previous screenshot. The main header displays a red circular progress indicator with '13 / 94' and a 'Community Score' of -69. It states '13/94 security vendors flagged this IP address as malicious' and 'Last Analysis Date 15 hours ago'. The 'Security vendors' analysis' section is active, showing a table of results from various vendors.

Security vendors' analysis		Do you want to automate checks?	
alphaMountain.ai	⚠ Malicious	ArcSight Threat Intelligence	⚠ Malware
BitDefender	⚠ Phishing	Criminal IP	⚠ Malicious
Cyble	⚠ Malicious	CyRadar	⚠ Malicious
Forcepoint ThreatSeeker	⚠ Malicious	Fortinet	⚠ Malware

7. Clean Domain Analysis:

The screenshot shows the VirusTotal interface for the domain **cbit.org.in**. The domain is classified as clean, with a community score of 0/94. The analysis summary states: "No security vendors flagged this domain as malicious". The registrar is GoDaddy, and the domain was created 10 years ago. The last analysis was performed 3 days ago. The "DETECTION" tab is active, showing a table of security vendors' analysis results.

Security vendors' analysis		Do you want to automate checks?	
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AlienVault	✓ Clean
alphaMountain.ai	✓ Clean	Antiy-AVL	✓ Clean
benkow.cc	✓ Clean	Bfore.Ai PreCrime	✓ Clean

8. Malicious Domain Analysis:

The screenshot shows the VirusTotal interface for the domain **appleid-reset.com**. The domain is classified as malicious, with a community score of 13/94. The analysis summary states: "13/94 security vendors flagged this domain as malicious". The registrar is OVH sas, and the domain was created 2 years ago. The last analysis was performed 7 hours ago. The "DETECTION" tab is active, showing a table of security vendors' analysis results.

Security vendors' analysis		Do you want to automate checks?	
alphaMountain.ai	⚠ Phishing	BitDefender	⚠ Phishing
CyRadar	⚠ Malicious	Fortinet	⚠ Phishing
G-Data	⚠ Phishing	Google Safebrowsing	⚠ Phishing
Kaspersky	⚠ Phishing	Lionic	⚠ Phishing

Testing & Results

- Database Coverage: Maintains one of the world's largest malware repositories
- Response Time: Real-time analysis for most file types and URLs
- API Reliability: 99.9% uptime for enterprise services

Result: VirusTotal successfully provides comprehensive threat detection capabilities, serving as an industry-standard platform for malware analysis and threat intelligence.

Deliverables

- GitHub Repository - Centralized code and documentation storage
- User Training Materials - Presentations and quick-start guides
- Troubleshooting Guide - Common issues and solutions

Learning Outcomes

- Malware Detection Techniques - Static, dynamic, and behavioral analysis methods
- Security Tool Evaluation - Critical assessment of cybersecurity platform capabilities
- Incident Response Workflows - Real-world threat analysis and investigation procedures
- Enterprise Security Architecture - Large-scale security platform integration strategies

Conclusion

VirusTotal represents a cornerstone achievement in collaborative cybersecurity, successfully combining multi-engine malware detection, comprehensive threat intelligence, and accessible public service. By maintaining the world's largest malware repository while providing both free and enterprise-grade services, it has established itself as an essential tool for cybersecurity professionals worldwide.

The platform's success demonstrates the effectiveness of community-driven security models and continues to evolve as a critical component in the global cybersecurity infrastructure, protecting millions of users through advanced threat detection and intelligence sharing capabilities.