| | | | |
|---|---|---|---|
| **Course Name:** | **Information and Cyber Security Laboratory** | **Semester:** | **VII** |
| **Date of Performance:** | **13 / 08 / 25** | **Batch No:** | **B - 1** |
| **Faculty Name:** | **Prof. Makrand Kulkarni** | **Roll No:** | **16014022050** |
| **Faculty Sign & Date:** | | **Grade/Marks:** | **__ / 25** |

# Experiment No: 4

**Title:** Malware Analysis using Viras Total

**Aim and Objective of the Experiment:**

1. Submit a sample file to VirusTotal.
2. Analyze result.
3. Identify behavior (e.g., registry changes, persistence).
4. Suggest defenses.

**COs to be achieved:**

CO2: Discuss software flaws, malware and detection techniques.

**Books/Journals/Websites referred:**

https://docs.virustotal.com/
https://youtu.be/EmYO_YLnOTg?si=wB16-T1RqrZkd8yE

**Tools required:**

Virus Total

**Theory:**

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.
Originally launched in June 2004 by Hispasec Sistemas (a Spanish security company), VirusTotal was acquired by Google in 2012. Since January 2018, it's been operated under Chronicle, a Google subsidiary focused on security intelligence.

Few features:

- **Free and unbiased:** VirusTotal is free to end users for non-commercial use.
- **Many contributors:** VirusTotal's aggregated data is the output of many different antivirus engines, website scanners, file and URL analysis tools, and user contributions.
- **Raising the global IT security level through sharing:** Scanning reports produced by VirusTotal are shared with the public VirusTotal community. Users can contribute comments and vote on whether particular content is harmful. In this way, users help to deepen the community's collective understanding of potentially harmful content and identify false positives.
- **Real-time updates:** Malware signatures are updated frequently by VirusTotal as they are distributed by antivirus companies, this ensures that our service uses the latest signature sets.
- **Detailed results:** VirusTotal not only tells you whether a given antivirus solution detected a submitted file as malicious, but also displays each engine's detection label (e.g., I-Worm.Allaple.gen).

**Stepwise Implementation details:**

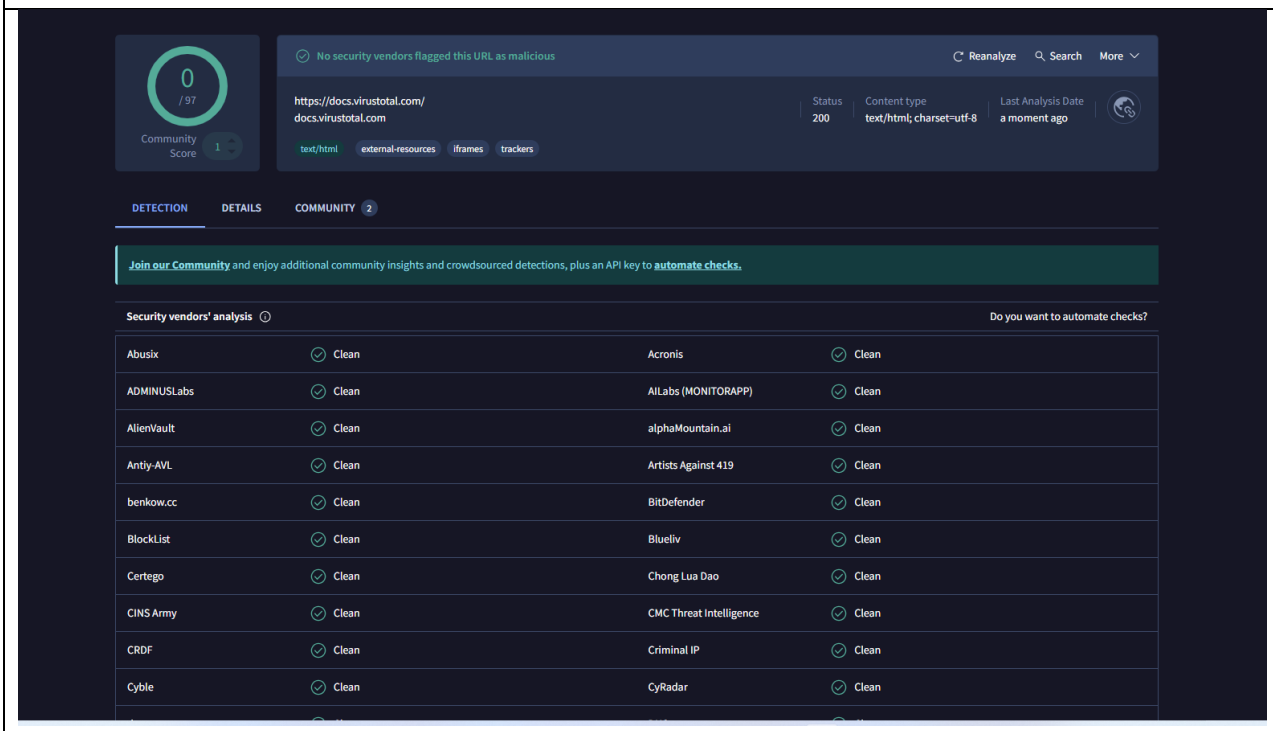
**STEP 1:** Submit a sample file (size less than 650 MB) to VirusTotal.

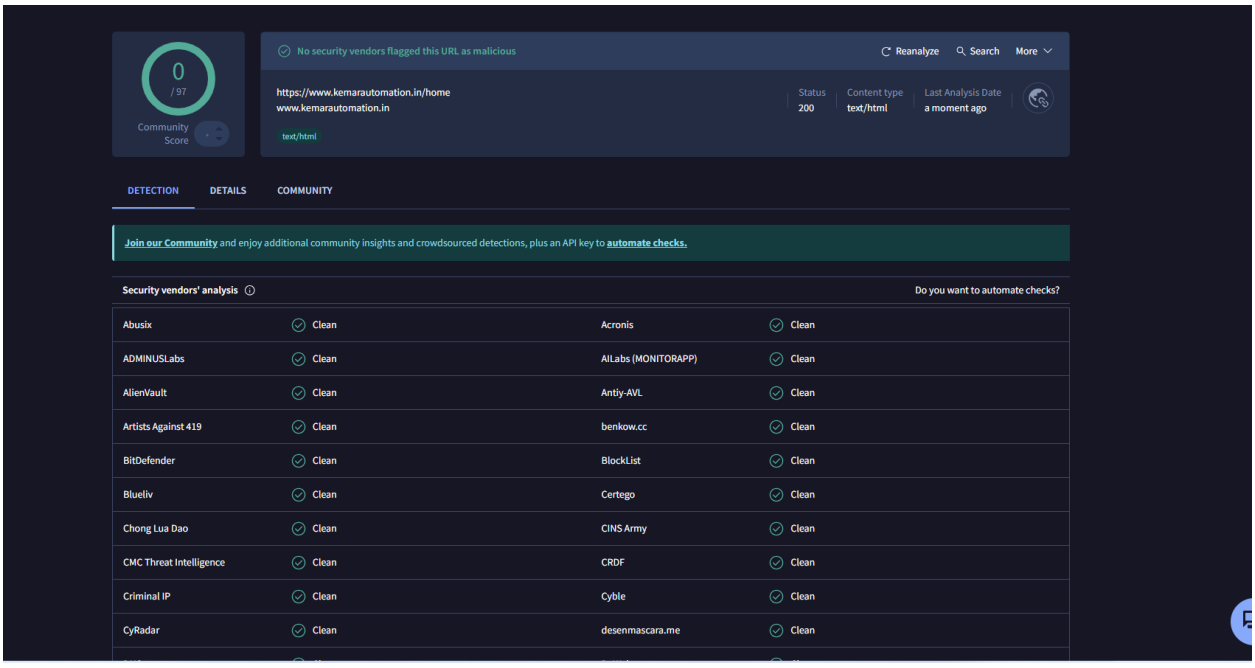
**STEP 2:** Analyze result.

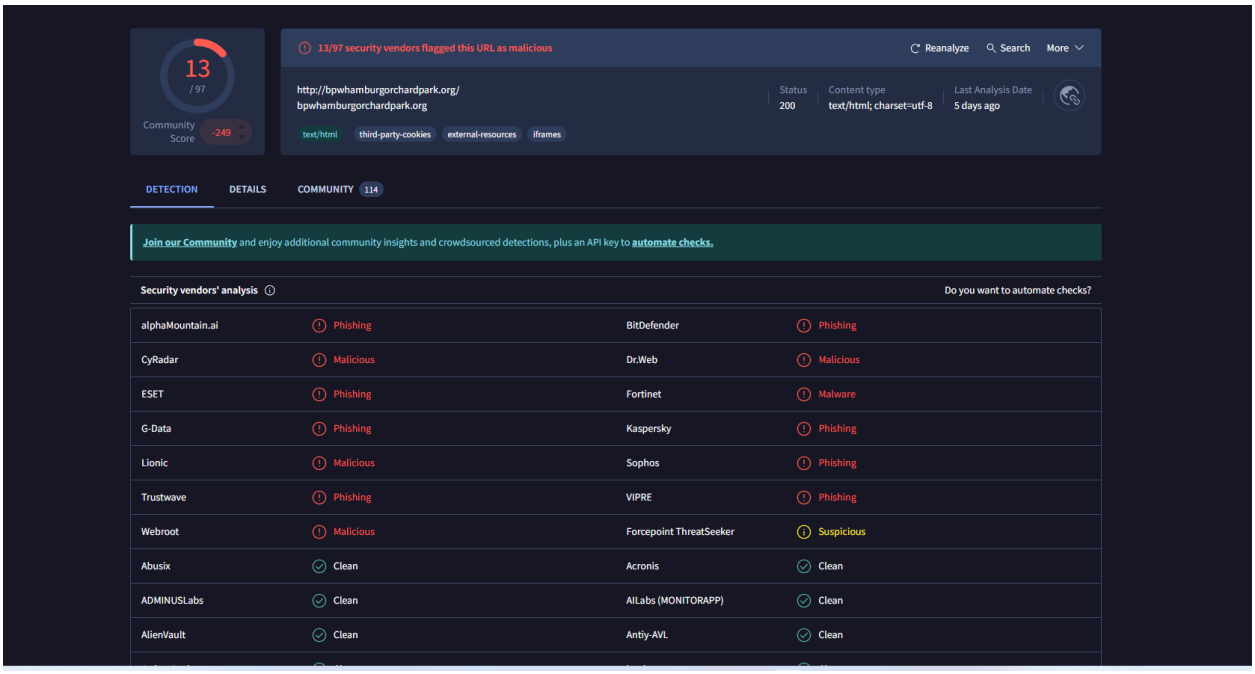
**STEP 3:** Identify behavior (e.g., registry changes, persistence).

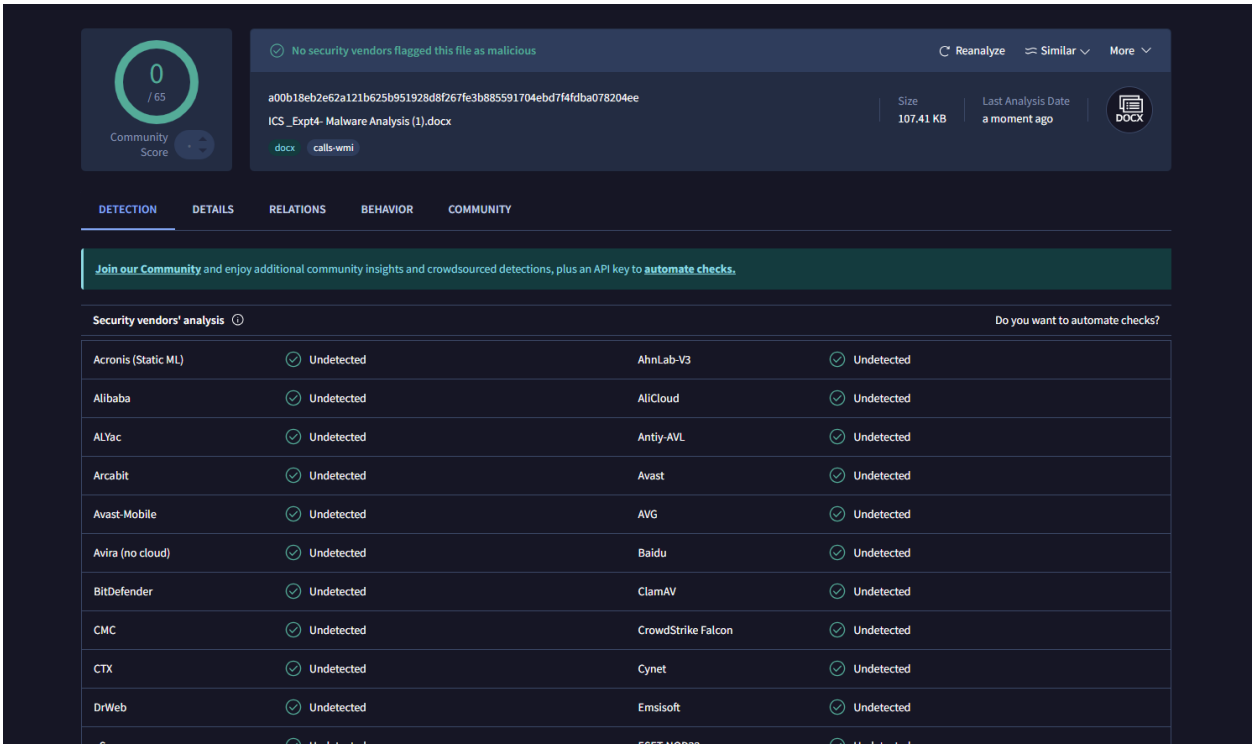
**STEP 4:** Suggest defenses.

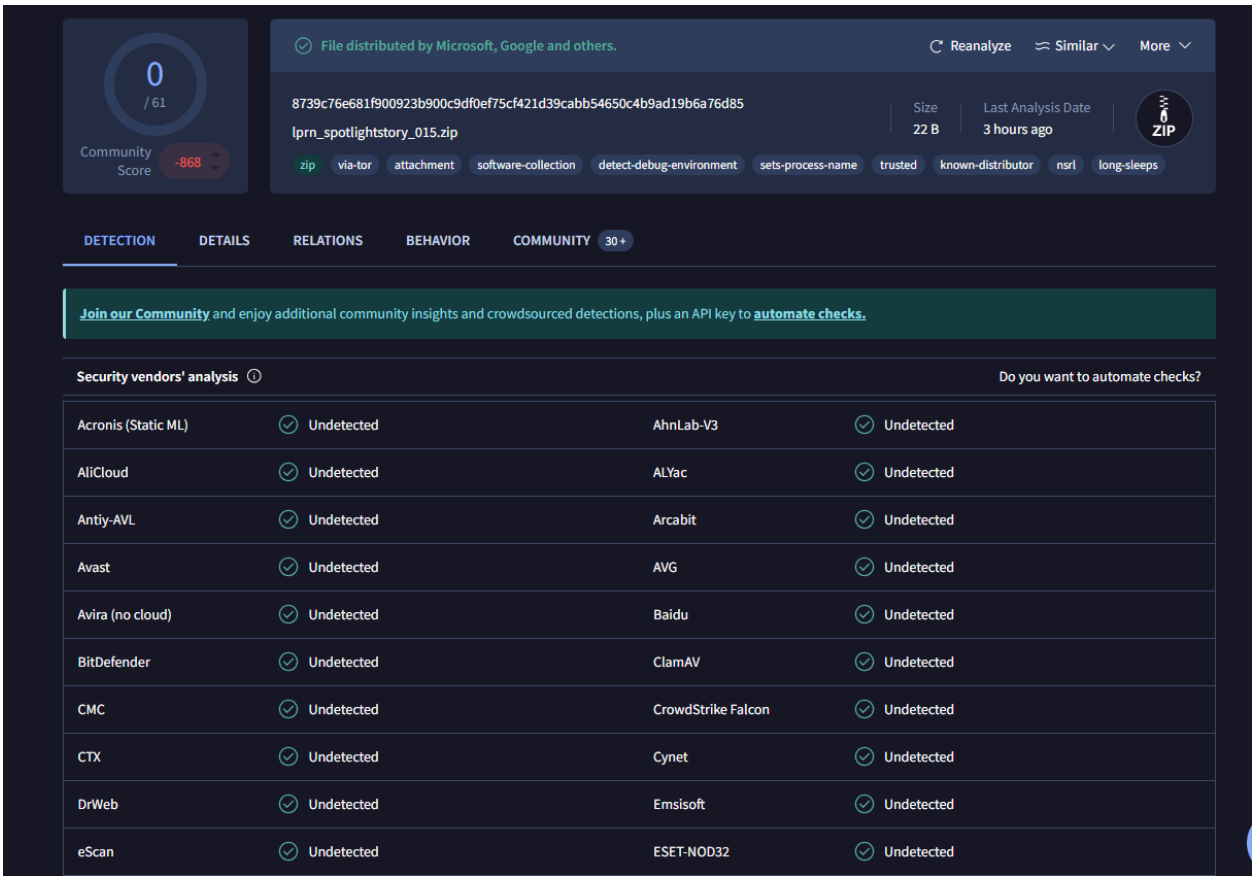
## Screenshots:




13
/ 97
Community Score
-249
13/97 security vendors flagged this URL as malicious
Reanalyze
Search
More
http://bpwhamburgorchardpark.org/
bpwhamburgorchardpark.org
Status
200
Content type
text/html; charset=utf-8
Last Analysis Date
5 days ago
text/html
third-party-cookies
external-resources
iframes
DETECTION
DETAILS
COMMUNITY 114
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
alphaMountain.ai Phishing
BitDefender Phishing
CyRadar Malicious
Dr.Web Malicious
ESET Phishing
Fortinet Malware
G-Data Phishing
Kaspersky Phishing
Lionic Malicious
Sophos Phishing
Trustwave Phishing
VIPRE Phishing
Webroot Malicious
Forcepoint ThreatSeeker Suspicious
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (MONITORAPP) Clean
AlienVault Clean
Antiy-AVL Clean


0
/ 65
Community Score
No security vendors flagged this file as malicious
Reanalyze
Similar
More
a00b18eb2e62a121b625b951928d8f267fe3b885591704ebd7f4fdba078204ee
ICS_Expt4- Malware Analysis (1).docx
docx
calls-wmi
Size
107.41 KB
Last Analysis Date
a moment ago
DOCX
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML) Undetected
AhnLab-V3 Undetected
Alibaba Undetected
AliCloud Undetected
ALYac Undetected
Antiy-AVL Undetected
Arcabit Undetected
Avast Undetected
Avast-Mobile Undetected
AVG Undetected
Avira (no cloud) Undetected
Baidu Undetected
BitDefender Undetected
ClamAV Undetected
CMC Undetected
CrowdStrike Falcon Undetected
CTX Undetected
Cynet Undetected
DrWeb Undetected
Emsisoft Undetected




## Post Lab Subjective/Objective type Questions:

1. **Explain limitations of Virus Total.**

   VirusTotal is a popular online service that scans files, URLs, and IPs using multiple antivirus (AV) engines and security tools. While it's widely used, it has some important limitations:

   - False Negatives:
     Not all malware is detected. If the malware is new (zero-day) or highly obfuscated, many AV engines may fail to flag it.
   - False Positives:
     Sometimes, legitimate files may be incorrectly flagged as malicious, leading to confusion.
   - No Behavior Analysis:
     VirusTotal mostly relies on static scanning. It doesn't deeply analyze how a file behaves during execution in real time (like sandboxing solutions do).

- Limited Context:
  It tells you if something is flagged but doesn't always explain why or provide details about attack vectors, persistence mechanisms, or payloads.
- Not Always Up-to-Date:
  AV engines inside VirusTotal may not always be synced to the latest signatures, so there can be a detection lag.
- Not a Complete Security Solution:
  VirusTotal should be used as a supporting tool for malware analysis, not as a replacement for endpoint protection, intrusion detection systems, or forensic tools.

**2. Explain Malware and its common types.**

Malware (short for *malicious software*) is any software intentionally designed to damage, disrupt, steal, or gain unauthorized access to computer systems, networks, or data.

- Virus
  Attaches itself to legitimate programs or files.
  Spreads when the infected program/file is shared or executed.
  Can delete files, corrupt data, or slow down systems.

- Worm
  Self-replicates and spreads across networks without user action.
  Often used to overload systems or spread other malware.

- Trojan Horse (Trojan)
  Disguises itself as a legitimate program (e.g., fake software, cracked apps).
  Creates backdoors for attackers to steal data or control systems.

- Ransomware
  Encrypts user data and demands ransom for decryption.
  Example: WannaCry, Locky.
  Causes financial loss and downtime.

- Spyware
  Secretly monitors user activity (keystrokes, browsing history, credentials).
  Often used for identity theft and espionage.

| **Conclusion:** |
| --- |
| The experiment showed that VirusTotal helps in detecting potential malware but has limitations in behavior analysis. Complementing it with behavioral monitoring and layered defenses ensures stronger protection against threats. |

**Signature of faculty in-charge with Date:**