

Task 5: Malware Types & Behavior Analysis (Basic)

Step 1: Understand Malware Types (Theory)

Briefly study and note definitions:

- **Virus** – Attaches to files, spreads when file runs
 - **Worm** – Self-replicates over networks
 - **Trojan** – Disguised as legitimate software
 - **Ransomware** – Encrypts files and demands ransom
 - **Spyware** – Steals user data
 - **Adware** – Shows unwanted ads
-

Step 2: Choose a Known Malware Sample (Safe Method)

Use **known malware hashes** (safe & allowed).

Example hashes (you can use any one):

I use the ip address

Step 3: Analyze Using VirusTotal

1. Open <https://www.virustotal.com>
2. Go to **Search** tab
3. Paste the **ip address**

https://www.virustotal.com/gui/ip-address/2409:40c1:4a:637e:6116:1fcc:457ce07d/detection

2409:40c1:4a:637e:6116:1fcc:457ce07d

0 / 92
Community Score

No security vendor flagged this IP address as malicious

2409:40c1:4a:637e:6116:1fcc:457ce07d (2409:40c0::/31)
AS 55836 (Reliance Jio Infocomm Limited)

IN

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

0xSI_f33d	? Unrated	Abusix	? Unrated
Acronis	? Unrated	ADMINUSLabs	? Unrated
AILabs (MONITORAPP)	? Unrated	AlienVault	? Unrated
alphaMountain.ai	? Unrated	AlphaSOC	? Unrated
Antiy-AVL	? Unrated	ArcSight Threat Intelligence	? Unrated
AutoShun	? Unrated	Axur	? Unrated
benkow.cc	? Unrated	Bfore.Ai PreCrime	? Unrated

Do you want to automate checks?

https://www.virustotal.com/gui/ip-address/2409:40c1:4a:637e:6116:1fcc:457ce07d/details

2409:40c1:4a:637e:6116:1fcc:457ce07d

0 / 92
Community Score

No security vendor flagged this IP address as malicious

2409:40c1:4a:637e:6116:1fcc:457ce07d (2409:40c0::/31)
AS 55836 (Reliance Jio Infocomm Limited)

IN

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic Properties

Network	2409:40c0::/31
Autonomous System Number	55836
Autonomous System Label	Reliance Jio Infocomm Limited
Regional Internet Registry	APNIC
Country	IN
Continent	AS

Google results

No Results

Search for "2409:40c1:4a:637e:6116:1fcc..." on Google

Sort by: Relevance

ENHANCED BY Google

Step 4: Analyze Detection Report

From VirusTotal, note:

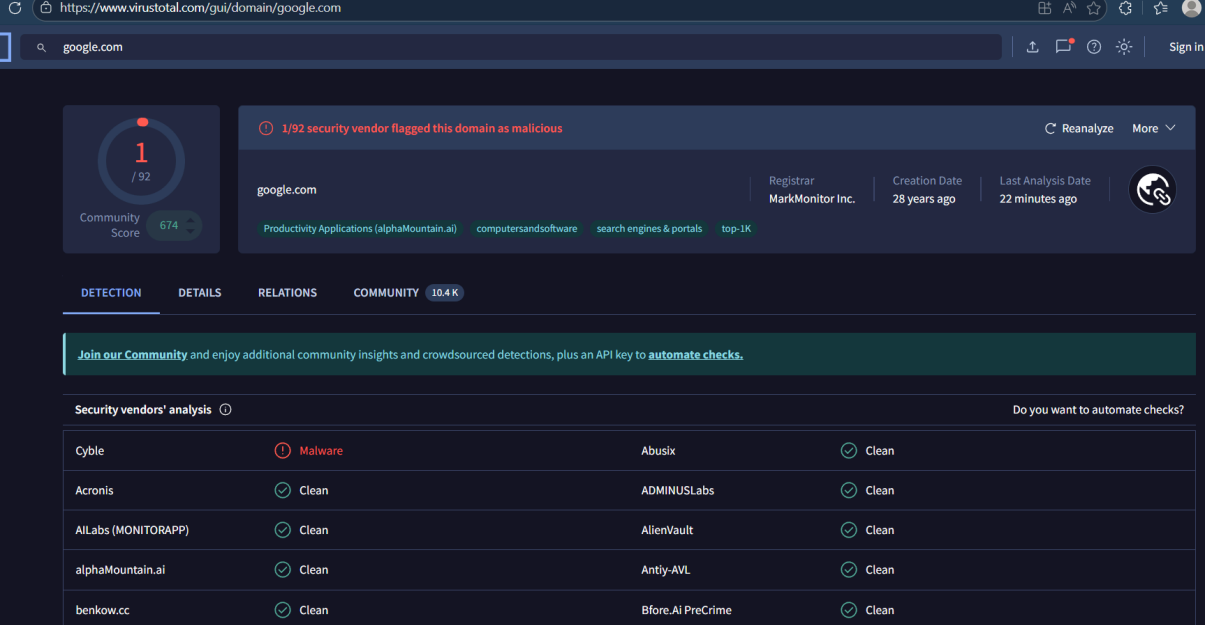
- **Detection ratio** (e.g., 0/92)
- **Malware type** (Trojan, Ransomware, etc.)
- **Threat labels**
- **First seen / Last seen**

Example: 0/92 in the ss

Step 5: Observe Behavior Indicators

From **Behavior / Relations** tabs, identify:

- Suspicious registry changes
- File creation or deletion
- Network connections (C2 servers)
- Process injection
- Persistence mechanisms



The screenshot shows the VirusTotal domain analysis interface for google.com. The top section displays a Community Score of 674 (1/92) and a warning that 1/92 security vendors flagged the domain as malicious. Below this, the domain is categorized as 'Productivity Applications (alphaMountain.ai)', 'computersandsoftware', 'search engines & portals', and 'top-1K'. The 'DETECTION' tab is active, showing a table of security vendors' analysis results.

Security vendors' analysis		Do you want to automate checks?	
Cyble	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AlIabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
benkow.cc	Clean	Bfore.Ai PreCrime	Clean

Step 6: Malware Lifecycle (Short Explanation)

Include this flow in your report:

Infection → Execution → Persistence → Command & Control → Damage

Step 7: Malware Spread Methods

Mention common methods:

- Email attachments
- Fake software downloads
- USB drives
- Exploit kits
- Malicious websites

Step 8: Prevention Methods

Write simple controls:

- Antivirus software
- Firewall
- Software updates
- Email filtering
- User awareness
- Avoid unknown downloads