

# 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**

Community Score 0 / 92

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.

Community Score 0 / 92

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

Sort by: Relevance

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

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**

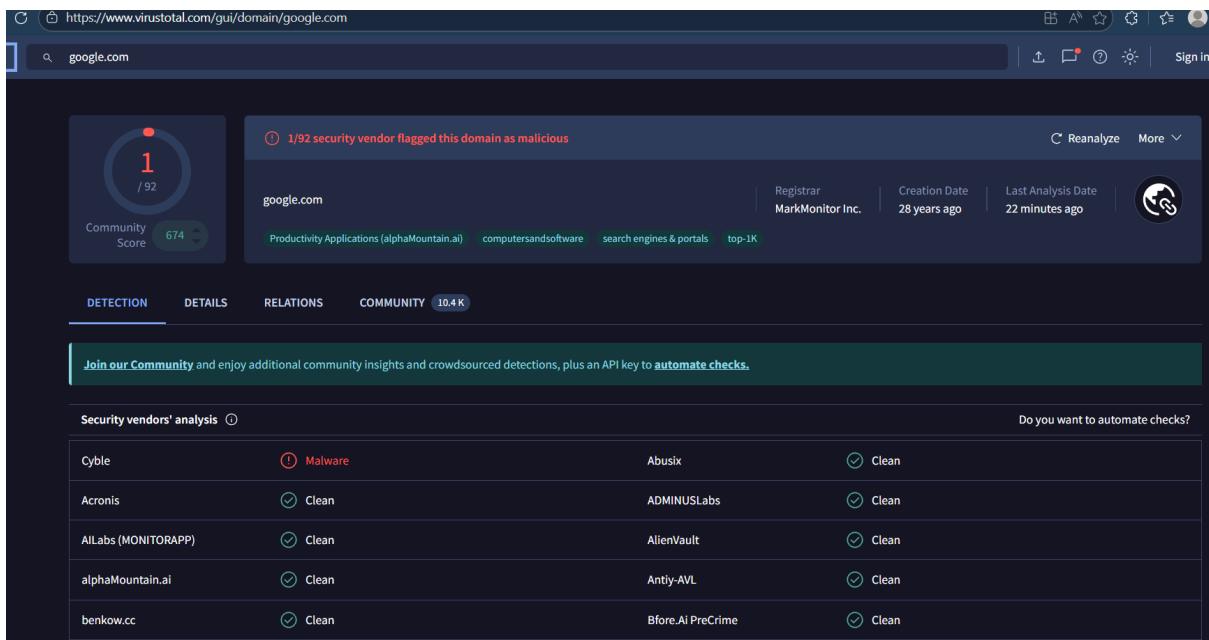
Example: 0/92 in the ss

---

## 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



Security vendors' analysis		Do you want to automate checks?	
Cyble	⌚ Malware	Abusix	ⓘ Clean
Acronis	ⓘ Clean	ADMINUSLabs	ⓘ Clean
Allabs (MONITORAPP)	ⓘ Clean	AlienVault	ⓘ Clean
alphaMountain.ai	ⓘ Clean	Anty-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