---

1. Different Types of Malware

Malware (malicious software) is designed to harm, exploit, or gain unauthorized access to systems.

Virus

- Attaches itself to legitimate files or programs.
- Requires user action (like opening a file) to spread.
- Can corrupt or delete data.
- Example behavior: infecting `.exe` files.

Worm

- Self-replicates without user interaction.
- Spreads across networks automatically.
- Consumes system and network resources.
- Example: spreading via network vulnerabilities.

Trojan

- Disguises itself as legitimate software.
- Does not self-replicate.
- Creates backdoors for attackers.
- Example: fake software cracks or games.

Ransomware

- Encrypts files and demands payment for decryption.
- Often spreads via phishing emails.
- Causes major financial and operational damage.
- Example: WannaCry, LockBit.

---

2. Uploading Malware Hashes to VirusTotal

Instead of uploading actual malware files (which is dangerous), analysts usually upload **file hashes** (MD5, SHA-1, or SHA-256).

Why hashes?

- Safe and legal
- Identifies known malware
- Avoids spreading malicious files

How it's done

1. Get the file hash.
2. Go to VirusTotal.
3. Paste the hash into the search bar.
4. View the analysis report.

---

3. Analyzing Detection Reports

VirusTotal shows how many antivirus engines detect the file as malicious.

Key things to look for

- **Detection ratio** (e.g., 45/70 engines flagged)
- **Malware family name**
- **Threat labels** (Trojan, Ransomware, Backdoor)
- **First seen date**

What it tells us

- High detection = likely malicious
- Multiple names = different vendors classify differently
- Low detection = possibly new or obfuscated malware

---

4. Behavior Indicators

Behavior indicators show **what the malware does**, not just what it is.

Common indicators

- Modifies registry keys
- Creates new processes
- Contacts suspicious IP addresses
- Downloads additional payloads
- Disables antivirus services

Why behavior matters

- Detects zero-day malware
- Helps identify intent
- Used in behavioral detection systems

---

5. Malware Lifecycle

Most malware follows a similar lifecycle:

1. **Delivery** – Phishing email, USB, website download
2. **Execution** – User opens file or exploit runs
3. **Installation** – Malware embeds itself in system
4. **Command & Control (C2)** – Communicates with attacker
5. **Action on Objective** – Steal data, encrypt files, spy

Understanding this helps in **early detection and response**.

---

6. How Malware Spreads

Malware spreads through multiple channels:

- Phishing emails
- Malicious websites
- Infected USB drives
- Software cracks and pirated tools
- Network vulnerabilities
- Drive-by downloads

Attackers often rely on **human mistakes**, not just technical flaws.

---

7. Prevention Methods

Preventing malware is easier than removing it.

Best practices

- Keep systems updated
- Use reputable antivirus software
- Avoid unknown links and attachments
- Disable macros in documents
- Use strong passwords
- Educate users on phishing attacks
- Enable firewalls and intrusion detection systems

---

8. Summary of Findings

- Malware comes in different forms, each with unique behavior.
- VirusTotal is a valuable tool for identifying known malware using hashes.
- Detection reports help confirm malicious intent.
- Behavioral indicators reveal what malware actually does.
- Malware follows a predictable lifecycle.
- Most infections happen due to unsafe user actions.
- Strong security hygiene significantly reduces risk.
