# 💣 Lecture 16 – Types of Malware and Cyber Attacks

---

## 🧠 What is Malware?

**Malware** (short for *Malicious Software*) refers to any software intentionally created to **damage, disrupt, or gain unauthorized access** to computers, networks, or systems.

It can **steal information, delete files, lock systems, spy on users, or spread across networks.**

---

## ⚙️ 1. Virus Attack

### 🔹 Definition:

A **computer virus** is a type of malware that **spreads through user interaction**, such as opening infected files or applications.

### 🔹 How it works:

- A virus **attaches itself** to legitimate programs or files.
- It activates **only when the infected file is executed** by the user.
- Once activated, it can **replicate** and infect other files.

### 🔹 Key Points:

- Needs **user interaction** to spread.
- Can **slow down systems**, **delete data**, or **corrupt files**.
- Prevented using **antivirus software** and **safe browsing practices**.

**Example:**
A malicious .exe file disguised as a game installer infects the system when opened.

---

## 🪱 2. Worm Attack

🔹 **Definition:**

A **worm** is a **self-replicating** malware that spreads **without user interaction** — through networks, USBs, or email attachments.

🔹 **Characteristics:**

- Does not need any human action to spread.
- Consumes **bandwidth and system resources**.
- Often **hard to remove** once it infects the network.
- Can spread automatically to all folders you click.

🔹 **Prevention:**

- Use **Command Prompt (CMD)** to detect/remove suspicious scripts.
- Keep **OS and antivirus updated**.
- Close **unnecessary open ports**.

🔹 **Example:**

The **ILOVEYOU Worm** spread through email attachments and infected millions of computers in 2000.

---

## 🔐 3. Ransomware Attack

🔹 **Definition:**

**Ransomware** is malware that **encrypts (locks)** your files and demands a **ransom (money)** to unlock them.

🔹 **How it works:**

1. Attacker infects your system.
2. Files get **encrypted** (you can’t open them).
3. A message appears demanding **payment in Bitcoin** to decrypt the data.

🔹 **Why Bitcoin?**

- **Anonymous** and **untraceable**, making it perfect for cybercriminals.

🔹 **Examples:**

- **WannaCry (2017)** and **Petya** ransomware attacks.

🔹 **Prevention:**

- Don’t open unknown attachments.
- Backup your data regularly.
- Use **ransomware protection** in antivirus tools.

---

🤖 **4. Bot Attack**

🔹 **Definition:**

A **bot** is a small program designed to **automate tasks**.
When used maliciously, bots can perform **network attacks** or **spread malware**.

🔹 **How it works:**

- Once installed, bots connect to a **command-and-control (C&C)** server.
- The attacker can then use thousands of bots (botnet) to:
    - Send spam emails
    - Launch DDoS attacks
    - Spread malware

🔹 **Example:**

- The **Mirai Botnet (2016)** — used IoT devices to launch massive DDoS attacks.

---

## 🧩 5. Trojan Attack

🔹 **Definition:**

A **Trojan Horse** is malware disguised as a **legitimate software or file**.

🔹 **How it works:**

- Appears to be safe (e.g., “Free Game” or “System Cleaner”).
- Once executed, it allows attackers to:
    - Install **other malware** (like worms or ransomware)
    - Steal data or control your system

🔹 **Key Point:**

Trojan is **not self-replicating**, but can **carry** other malware inside.

**Example:**
A fake “junior software” installation file containing a Trojan script.

---

## 🦹 6. Spyware

🔹 **Definition:**

**Spyware** secretly monitors user activities and sends data to a third party without permission.

🔹 **Purpose:**

- Steal **personal data**, **passwords**, **financial info**, or **browsing habits**.

🔹 **Example:**

- **Pegasus** – a spyware made by **Israel’s NSO Group**, capable of stealing phone data, recording calls, and tracking users.

🔹 **Prevention:**

- Avoid suspicious links and untrusted apps.
- Use **anti-spyware software**.
- Keep system permissions limited.

---

## ⌨️ 7. Keylogger

🔹 **Definition:**

**Keyloggers** are programs that **record keystrokes** made by a user to capture sensitive data (like passwords).

🔹 **How it works:**

- Installed as software or browser extensions.
- Records every key pressed and sends logs to attackers.

🔹 **Real Examples:**

- **Segurazo Antivirus** was accused of collecting user data.
- **DriverPack.io** sometimes installs extra unwanted programs.

🔹 **Prevention:**

- Avoid unnecessary extensions.
- Use **on-screen keyboards** for banking.
- Enable **multi-factor authentication**.

---

## 🩹 8. Wiper Malware

🔹 **Definition:**

A **Wiper** is malware designed to **delete data permanently** and **erase system logs** to cover its tracks.

🔹 **Purpose:**

- Cause **irreversible damage**.
- Often used in **cyber warfare** or **revenge attacks**.

**Example:**
The **Shamoon** wiper attack deleted data on 30,000 Saudi Aramco computers.

---

## 🪙 9. Cryptojacking

🔹 **Definition:**

**Cryptojacking** is when an attacker secretly uses your computer's resources to **mine cryptocurrency** (like Bitcoin).

🔹 **How it works:**

- A malicious script runs in your background.
- Your CPU/GPU works hard — slowing your system.
- The hacker earns cryptocurrency using your device.

🔹 **Prevention:**

- Block malicious browser scripts.
- Use antivirus that detects **mining malware**.

---

## 📧 10. Phishing

🔹 **Definition:**

A **social engineering attack** using **fake communication** (emails, SMS, or calls) to steal personal information.

🔹 **Example:**

An email says:

"Your Instagram password is compromised, click here to reset."

Once you click and enter details, the attacker captures your credentials.

🔹 **Prevention:**

- Check sender email and URLs.
- Don't share OTPs or passwords.
- Use spam filters and awareness training.

---

## 🎭 11. Spoofing

🔹 **Definition:**

**Spoofing** means **pretending to be someone else** to trick a user into revealing sensitive information.

🔹 **Types:**

- **SMS Spoofing** – Fake messages (like from your bank or telecom).
- **Email Spoofing** – Fake sender address to look real.
- **Caller ID Spoofing** – Fake phone number display.

🔹 **Purpose:**

To collect personal data, banking info, or passwords.

---

## 🔑 12. Password Attack

🔹 **Definition:**

An attempt to **guess or crack** a user's password using automated tools or common patterns.

🔹 **Common Weak Password Sources:**

- Birth dates
- Favorite colors, foods, hobbies
- Pet or partner names
- Famous players, gods, or cities

🔹 **Attack Techniques:**

- **Brute Force Attack:** Trying every possible password.
- **Dictionary Attack:** Using a list of common words (password dictionary).
- **Social Engineering:** Guessing passwords using personal info from social media.

🔹 **Prevention:**

- Use **strong passwords** (mix of letters, numbers, symbols).

- Enable **2FA**.
- Avoid personal or guessable words.

---

### 🌐 13. DDoS Attack (Distributed Denial of Service)

🔹 **Definition:**

A **network attack** where multiple bots send huge amounts of traffic to a target server to make it unavailable.

🔹 **How it works:**

- Attackers use thousands of infected systems (botnet).
- Floods server with fake requests.
- Legitimate users can't access the service.

🔹 **Example:**

DDoS attacks on gaming servers or banking websites.

🔹 **Prevention:**

- Use **firewalls** and **rate limiting**.
- Employ **DDoS protection services** like Cloudflare.

---

### 💉 14. Code Injection Attack

🔹 **Definition:**

Attackers inject **malicious code or queries** into an application to **manipulate or access data** in a database.

🔹 **Example:**

**SQL Injection** – attacker sends malicious SQL query to:

- Access data
- Modify or delete records
- Bypass authentication

SELECT * FROM users WHERE username='' OR '1'='1' --;

- 🔹 **Prevention:**
  - Use **input validation** and **prepared statements**.
  - Sanitize all form inputs.

---

### 🌎 15. Cross-Site Scripting (XSS)

- 🔹 **Definition:**

An attack where hackers inject **malicious JavaScript or HTML** code into a webpage's **input fields** to execute in another user's browser.

- 🔹 **Example:**

Inserting <script>alert('Hacked')</script> in a website comment box.

- 🔹 **Result:**
  - Steals cookies
  - Redirects users
  - Executes unauthorized actions
- 🔹 **Prevention:**
  - Validate and **sanitize user input**.
  - Use **Content Security Policy (CSP)**.

---

### ⏰ 16. Logic Bomb

- 🔹 **Definition:**

A **Logic Bomb** is a malicious script that activates when a specific condition or time is met.

- 🔹 **Example:**
  - An employee sets a script to delete files **after 30 days of resignation**.
  - Attack triggers when a specific file or date condition is true.

🔹 **Prevention:**

- Use **audit trails** and **code reviews**.
- Restrict administrative privileges.

---

🧩 **Summary Table**

| Attack Type | Spreads By | Main Effect |
|---|---|---|
| Virus | User interaction | File corruption |
| Worm | Network (no user input) | Self-replicates |
| Ransomware | Infected downloads | File encryption & ransom |
| Bot | Botnet control | Automated attack tasks |
| Trojan | Fake software | Installs hidden malware |
| Spyware | Background process | Steals information |
| Keylogger | Software/Hardware | Records keystrokes |
| Wiper | Script/Remote | Deletes all data |
| Cryptojacking | Hidden mining | Uses CPU for crypto |
| Phishing | Email/SMS | Steals credentials |
| Spoofing | Fake communication | Identity theft |
| Password Attack | Guessing/brute force | Account breach |
| DDoS | Network flooding | Server downtime |
| Code Injection | SQL query | Data manipulation |
| XSS | HTML input | Client-side attack |
| Logic Bomb | Timed trigger | Conditional system damage |