**Common Threats & Attack Vectors**

Cyber threats and attack vectors are methods or pathways that malicious actors use to compromise systems, steal data, or disrupt operations. Below are some of the most common threats and attack vectors in cybersecurity:

**A. Common Cyber Threats**

**1. Malware**

Malicious software designed to harm systems, including:

* **Viruses** – Self-replicating programs that infect files.
* **Worms** – Spread across networks without user interaction.
* **Trojans** – Disguised as legitimate software to trick users.
* **Ransomware** – Encrypts data and demands payment for decryption.
* **Spyware** – Secretly monitors user activity.

**2. Phishing & Social Engineering**

Deceptive attempts to steal sensitive information via:

* **Email Phishing** – Fraudulent emails impersonating trusted entities.
* **Spear Phishing** – Targeted attacks on specific individuals.
* **Whaling** – Phishing aimed at high-profile targets (e.g., executives).
* **Vishing (Voice Phishing)** – Scams conducted via phone calls.
* **Smishing (SMS Phishing)** – Fraudulent text messages.

**3. Denial-of-Service (DoS/DDoS) Attacks**

Overwhelm systems with traffic to disrupt services:

* **DoS** – Single-source attack.
* **DDoS** – Multiple sources (botnets) amplify the attack.

**4. Man-in-the-Middle (MitM) Attacks**

Attackers intercept and alter communications between two parties (e.g., via unsecured Wi-Fi).

**5. Insider Threats**

Employees or contractors misuse access to leak data or sabotage systems (intentionally or accidentally).

**6. Zero-Day Exploits**

Attacks targeting unknown vulnerabilities before developers can patch them.

**7. Advanced Persistent Threats (APTs)**

Long-term, stealthy attacks by well-funded groups (e.g., nation-state hackers).

**B. Common Attack Vectors**

**1. Email Attachments & Links** – Malware delivery via phishing emails.

**2. Weak Passwords & Credential Theft** – Brute force, credential stuffing, or keylogging attacks.

**3. Unpatched Software** – Exploiting known vulnerabilities in outdated systems.

**4. Misconfigured Security Settings** – Open ports, default passwords, or excessive permissions.

**5. Third-Party Vendors & Supply Chain Attacks** – Compromising less-secure partners to reach primary targets.

**6. USB & Removable Media** – Malware spread via infected external devices.

**7. Cloud Misconfigurations** – Exposed storage buckets or weak API security.

**8. IoT & Mobile Devices** – Poorly secured smart devices acting as entry points.

**C. Mitigation Strategies**

* **Regular Patching** – Keep systems and software updated.
* **Employee Training** – Awareness programs to combat phishing.
* **Multi-Factor Authentication (MFA)** – Adds an extra layer of security.
* **Network Segmentation** – Limits lateral movement in case of a breach.
* **Endpoint Protection** – Antivirus, EDR (Endpoint Detection & Response).
* **Encryption** – Protects data in transit and at rest.
* **Incident Response Plan** – Preparedness for quick threat containment.

Understanding these threats and attack vectors helps organizations strengthen their cybersecurity posture and reduce risk.