1. Virus

- **Spread Mechanism**:
    - Viruses attach themselves to legitimate executable files, programs, or documents. They spread when an infected file is shared, such as through email attachments, file downloads, or infected removable media.
- **Impact on Systems**:
    - Can corrupt or delete files, slow down system performance, or cause crashes. In some cases, viruses may deliver payloads that further damage data or disrupt system functionality.
- **Example**:
    - **ILOVEYOU Virus (2000)**: Spread via an email attachment with the subject "ILOVEYOU," this virus overwrote files, replicated itself, and sent copies to the user's email contacts, causing damage estimated at $10 billion.

2. Worm

- **Spread Mechanism**:
    - Worms spread independently, often exploiting vulnerabilities in network services or operating systems. They do not require a host file, which allows them to self-replicate and spread across networks more efficiently.
- **Impact on Systems**:
    - Worms consume bandwidth, slow down network performance, and can deliver malicious payloads. Some worms also contain ransomware or spyware components.
- **Example**:
    - **WannaCry (2017)**: A ransomware worm that exploited a vulnerability in Windows systems, infecting over 230,000 computers worldwide. It encrypted files and demanded ransom, impacting industries and institutions globally.

3. Trojan Horse

- **Spread Mechanism**:
    - Trojans disguise themselves as legitimate software or files. They often spread through email attachments, software downloads, or malicious links on websites.

- **Impact on Systems**:
    - Trojans can open backdoors for hackers, allowing remote control over infected systems. They may also steal data, install additional malware, or serve as entry points for other attacks.
- **Example**:
    - **Zeus Trojan**: A banking Trojan that infected millions of computers, stealing banking credentials and other sensitive information. It spread via phishing emails and malicious websites.

4. Ransomware

- **Spread Mechanism**:
    - Ransomware is usually delivered through phishing emails, infected websites, or malicious attachments. Once executed, it locks the user out of their system or encrypts their files.
- **Impact on Systems**:
    - Ransomware encrypts data and demands a ransom payment to restore access. It disrupts operations and can lead to significant financial losses if systems or data backups are unavailable.
- **Example**:
    - **CryptoLocker (2013)**: Spread through email attachments, CryptoLocker encrypted user files and demanded ransom payments in cryptocurrency. It was one of the first ransomware campaigns to have a significant impact on users worldwide.

5. Spyware

- **Spread Mechanism**:
    - Spyware often comes bundled with legitimate software or is downloaded unknowingly from malicious websites. It can also spread through Trojans.
- **Impact on Systems**:
    - Spyware monitors user activity, gathers sensitive information (such as login credentials, browsing history), and may cause degraded system performance.
- **Example**:
    - **FinSpy**: A spyware tool used for surveillance by certain governments, capable of intercepting communications, keystrokes, and data from

infected devices. It is often distributed through malicious links or phishing attacks.