Types of Malware and Their Characteristics

---

1. **Virus**
    - **Method of Spread**: Viruses attach to legitimate programs, executable files, or documents. They propagate when these infected files are shared, such as through email attachments, downloads, or infected external storage devices.
    - **Effect on Systems**: Viruses can damage or erase files, slow down system performance, or cause crashes. Some viruses may carry additional harmful payloads that further corrupt data or interfere with system functions.
    - **Example**: The ILOVEYOU Virus (2000) spread via an email attachment titled "ILOVEYOU," overwriting files, self-replicating, and sending copies to contacts, resulting in damages estimated at $10 billion.
2. **Worm**
    - **Method of Spread**: Worms spread autonomously, often taking advantage of vulnerabilities in network services or operating systems. They don't need a host file, allowing them to self-replicate and spread rapidly across networks.
    - **Effect on Systems**: Worms use up network bandwidth, slow down network performance, and can carry harmful payloads like ransomware or spyware.
    - **Example**: WannaCry (2017) was a ransomware worm that exploited a vulnerability in Windows, infecting over 230,000 computers worldwide, encrypting files, and demanding ransom, affecting many global industries.
3. **Trojan Horse**
    - **Method of Spread**: Trojans disguise themselves as legitimate files or software. They usually spread via email attachments, downloads, or malicious website links.
    - **Effect on Systems**: Trojans can create backdoors for hackers, granting them remote access to infected systems. They might steal sensitive data, install more malware, or act as entry points for other attacks.
    - **Example**: Zeus Trojan is a banking Trojan that compromised millions of computers, stealing banking credentials and other private data through phishing emails and malicious sites.
4. **Ransomware**
    - **Method of Spread**: Ransomware typically spreads via phishing emails, infected websites, or harmful attachments. Upon activation, it locks the user out of their system or encrypts their files.

- **Effect on Systems**: Ransomware encrypts the data and demands payment to restore access. It can disrupt business operations and lead to financial loss, especially if no backups are available.
- **Example**: CryptoLocker (2013) was spread through email attachments, encrypting user files and demanding ransom payments in cryptocurrency, marking one of the earliest large-scale ransomware attacks.

5. **Spyware**
    - **Method of Spread**: Spyware often comes bundled with legitimate software or is unknowingly downloaded from malicious websites. It can also spread through Trojans.
    - **Effect on Systems**: Spyware tracks user activity, collects sensitive information like login credentials or browsing history, and may slow down system performance.
    - **Example**: FinSpy is a surveillance spyware used by certain governments that intercepts communications and keystrokes from infected devices, typically spread via phishing links or malicious websites.
