Types of Malwares and Their Characteristics

Overview

This report explains the unique characteristics and behaviors of five common types of malware. For each type, we explore:

- **How it spreads** (e.g., email attachments, infected websites, removable media)
- **The impact on infected systems** (e.g., data corruption, data theft, system hijacking)
- **Real-life examples or case studies** demonstrating each malware type in action

---

1. Viruses

- **Spread**: Viruses attach to legitimate files or programs, requiring human interaction to activate and spread. Transmission methods include email attachments, downloads from untrusted sources, and infected removable media like USB drives.
- **Impact**: Viruses corrupt or delete files, slow down systems, and may render systems inoperable, leading to data loss or crashes.
- **Example**: The **ILOVEYOU virus** (2000) spread as an email attachment titled "ILOVEYOU," causing widespread data loss by overwriting files.

---

2. Worms

- **Spread**: Worms autonomously self-replicate, exploiting vulnerabilities in network services to propagate across networks without a host file.
- **Impact**: Worms overload networks, causing slowdowns or crashes and may carry other malicious software.
- **Example**: **Conficker** (2008) exploited Windows vulnerabilities to create a botnet of infected computers, posing significant risks globally.

---

3. Trojans

- **Spread**: Disguised as legitimate software, Trojans are often distributed via email links, downloads from compromised sites, or bundled with authentic software.

- **Impact**: Trojans provide unauthorized access to systems, leading to data theft, remote control of systems, and may act as gateways for ransomware or spyware.
- **Example**: **Emotet** (2014) began as a banking Trojan and evolved to deploy multiple types of malware, targeting industries worldwide.

---

4. Ransomware

- **Spread**: Often spread through phishing emails, malicious attachments, or compromised websites.
- **Impact**: Ransomware encrypts files or locks systems, demanding payment for data restoration. It can result in financial loss and operational disruptions.
- **Example**: **WannaCry** (2017) used an NSA-developed exploit, affecting healthcare, finance, and other sectors globally.

---

5. Spyware

- **Spread**: Installed through deceptive downloads, infected websites, or bundled with legitimate software.
- **Impact**: Spyware monitors user activities, collecting sensitive data, which can lead to identity theft and financial losses.
- **Example**: **FinSpy** (FinFisher) is used in targeted attacks to gather sensitive data from devices.