Digital Egypt Pioneers

Types of Malware and Their Characteristics

Ammar Yasser Mohamed
Course Code: ONL3_ISS2_S2
26 August 2025

1 Introduction

Malware (malicious software) refers to programs specifically designed to disrupt, damage, or gain unauthorized access to systems. Different types of malware have unique behaviors, spreading mechanisms, and impacts on victims. This assignment explains five major types of malware with real-world examples.

2 Viruses

Characteristics: Viruses attach themselves to executable files or documents and activate when the host file runs. They often corrupt files or disrupt system functionality.

Spread: Email attachments, infected downloads, and removable media.

Impact: File corruption, slowdown of systems, and data loss.

Real-life Example: The *ILOVEYOU virus* (2000) spread via email attachments disguised as love letters, infecting millions of computers worldwide and causing billions in damages.

3 Worms

Characteristics: Worms are self-replicating malware that spread without user intervention, often exploiting network vulnerabilities.

Spread: Network connections, insecure services, and infected websites.

Impact: Network congestion, system crashes, and widespread infections.

Real-life Example: The *SQL Slammer worm* (2003) spread within minutes across the internet, disabling ATM services and airlines due to massive network congestion.

4 Trojans

Characteristics: Trojans disguise themselves as legitimate software but secretly execute malicious activities. They do not replicate like viruses or worms.

Spread: Fake downloads, malicious email links, and pirated software.

Impact: Remote access for attackers, credential theft, and backdoors into systems.

Real-life Example: The *Zeus Trojan* targeted banking credentials through keylogging and man-in-the-browser attacks, stealing millions of dollars globally.

5 Ransomware

Characteristics: Ransomware encrypts victim data and demands payment (usually in cryptocurrency) for decryption keys.

Spread: Phishing emails, malicious websites, and exploit kits.

Impact: Data encryption, financial loss, and operational disruption.

Real-life Example: The *WannaCry ransomware attack* (2017) infected over 200,000 systems in 150 countries, crippling hospitals, businesses, and government institutions.

6 Spyware

Characteristics: Spyware secretly monitors user activity, collecting sensitive information such as browsing habits, keystrokes, or credentials.

Spread: Bundled with freeware, malicious links, and drive-by downloads.

Impact: Identity theft, privacy invasion, and unauthorized financial transactions.

Real-life Example: The *CoolWebSearch spyware* hijacked browsers, redirected traffic, and collected user data, affecting millions of users in the early 2000s.

7 Comparison Table

Malware Type	**How it Spreads**	**Impact on Systems**	**Real-life Example**
Virus	Email attachments, infected downloads, removable media	Corrupts files, slows systems, causes data loss	ILOVEYOU Virus (2000)
Worm	Network vulnerabilities, insecure services, infected websites	Network congestion, system crashes, rapid propagation	SQL Slammer Worm (2003)
Trojan	Fake software, malicious email links, pirated downloads	Remote access for attackers, data theft, backdoors	Zeus Trojan (2007+)
Ransomware	Phishing emails, malicious websites, exploit kits	Encrypts data, demands ransom, disrupts operations	WannaCry (2017)
Spyware	Bundled software, drive-by downloads, malicious links	Monitors activity, steals data, invades privacy	CoolWebSearch Spyware (2000s)