Malicious Software (Malware) Types

# Backdoor / Trapdoor

**What is it?:** A backdoor is a method of bypassing normal authentication or encryption in a computer system, allowing unauthorized access to the system.

**How to protect yourself:** Use firewalls, keep software updated, and monitor network traffic for unusual activity.

**Example:** The Back Orifice tool is an example of a backdoor used for remote access.

# Trojan Horse

**What is it?:** A Trojan horse is a type of malware that disguises itself as legitimate software but carries a malicious payload.

**How to protect yourself:** Avoid downloading software from untrusted sources and use antivirus software.

**Example:** The Zeus Trojan used to steal banking information.

# Viruses

**What is it?:** A virus is a type of malware that attaches itself to legitimate programs and spreads when those programs are run.

**How to protect yourself:** Use antivirus software and avoid opening unknown email attachments.

**Example:** The ILOVEYOU virus which spread through email in 2000.

# Worms

**What is it?:** Worms are standalone malware programs that replicate themselves to spread to other computers over a network.

**How to protect yourself:** Keep systems updated and use a firewall.

**Example:** The WannaCry worm that targeted Windows systems in 2017.

# Zombie

**What is it?:** A zombie is a computer infected with malware that allows it to be controlled remotely, often as part of a botnet.

**How to protect yourself:** Use up-to-date antivirus software and monitor for unusual network activity.

**Example:** Computers in the Mirai botnet used for DDoS attacks.

# Ransomware

**What is it?:** Ransomware encrypts the victim’s data and demands payment to restore access.

**How to protect yourself:** Backup data regularly and avoid suspicious links or downloads.

**Example:** CryptoLocker, which encrypted files and demanded Bitcoin payment.

# DoS Attack

**What is it?:** A Denial of Service (DoS) attack aims to make a machine or network resource unavailable by overwhelming it with traffic.

**How to protect yourself:** Use network security tools like intrusion detection systems and rate limiting.

**Example:** Ping of Death.

# DDoS Attack

**What is it?:** A Distributed Denial of Service (DDoS) attack uses multiple systems to flood a target with traffic.

**How to protect yourself:** Use content delivery networks (CDNs) and DDoS mitigation services.

**Example:** GitHub DDoS attack in 2018.

# Spam

**What is it?:** Spam involves sending unsolicited messages, often advertisements, in bulk.

**How to protect yourself:** Use spam filters and avoid subscribing to untrusted mailing lists.

**Example:** Email spam promoting fake lottery winnings.

# Spyware

**What is it?:** Spyware secretly gathers user information without their knowledge.

**How to protect yourself:** Use anti-spyware tools and be cautious with software installations.

**Example:** CoolWebSearch which tracked browsing habits.

# Tracking Cookies

**What is it?:** Tracking cookies are small files stored in a user’s browser to track their online activity.

**How to protect yourself:** Clear cookies regularly and use privacy-focused browsers or extensions.

**Example:** Third-party advertising cookies tracking user behavior across sites.