What is Malware

Malware, short for "malicious software," refers to any type of software that is designed to harm or exploit a computer system, network, or mobile device.

Types of malware

1.Virus: Replicate themselves and spread to other systems.

2.worms: Self-replicating malware that spreads without user interaction.

3.Torjans: Disguise themselves as legitimate software to gain access to a system.

4.spyware: Secretly monitors and collects user data.

5.Adware Displays unwanted advertisements.

6.Ransomware: Encrypts files and demands payment for decryption.

Effects of malware

1. Data theft : Malware can steal sensitive information.
2. System crashes : Malware can cause system instability and crashes.
3. Identity theft: Malware can be used to steal personal identities.
4. Financial loss :Malware can lead to financial losses through ransomware or stolen financial information.

History of malware

Early Years (1960s-1970s)

1. *First malware*: The first malware, called "Creeper," was discovered in 1971. It was an experimental self-replicating program that infected Apple II computers.
2. *Early viruses*: The first virus, called "Elk Cloner," was discovered in 1982. It infected Apple II computers and was created by a 15-year-old high school student.

Key Player in Malware Discovery

1. *Fred Cohen*: Known as the "father of computer viruses," Cohen wrote the first paper on computer viruses in 1984.

WannaCry Ransomware Attack (2017)

On May 12, 2017, a global cyberattack was launched using the WannaCry ransomware. The malware exploited a vulnerability in the Windows operating system, specifically in the SMBv1 protocol. The attack affected over 200,000 computers in over 150 countries.

- ## How it Spread

The malware spread rapidly through:

1. Email phishing: Malicious emails with infected attachments or links.

2. Infected software downloads: Downloading software from untrusted sources.

3. Infected websites: Visiting websites that hosted the malware.

4. Network vulnerabilities: Exploiting weaknesses in network security.

- ## Impact

The WannaCry attack had significant consequences:

1. Data encryption: The malware encrypted files on infected computers, making them inaccessible.

2. Ransom demands: Hackers demanded ransom payments in Bitcoin to restore access to encrypted files.

3. Global disruptions: The attack disrupted critical infrastructure, including hospitals, transportation systems, and businesses.

4. Financial losses: Estimated losses exceeded $4 billion.

- **Response and Mitigation**

1. Microsoft released patches: Microsoft issued emergency patches for Windows operating systems.

2. Antivirus software updates: Antivirus software vendors released updates to detect and remove the malware.

3. Backup and recovery: Organizations with backups were able to restore their systems.

4. International cooperation: Global law enforcement agencies collaborated to investigate and prosecute the perpetrators.

- **The WannaCry attack highlighted the importance of:**

1. Regular software updates: Keeping software up-to-date to patch vulnerabilities.

2. Robust backup systems: Maintaining backups to ensure business continuity.

3. Cybersecurity awareness: Educating users about phishing and other social engineering tactics.

4. Global cooperation: Collaborating internationally to combat cyber threats.