Mariam Mostafa Amin Mostafa

Types of Malware and Their Characteristics:

1. Virus

Spread Mechanism:
The majority of the viruses today spread through infected email attachments, shared files, or malicious downloads. Once a virus is executed, it attaches itself to clean files or programs and infects when these files are transferred or accessed.

Impact on Systems:
They can destroy files, slower performance of the system, eliminate data, or even render systems unable to work. Some viruses are designed to steal data or grant attackers remote access.

Real-Life Example:
ILOVEYOU Virus (2000): This email-transmitted virus had the subject line "ILOVEYOU." An attached file opened and simply overwritten files, stole data, and spread to all of the user's email contacts, hence infecting millions of systems worldwide and billions in damages.

2. Worm

Spread Mechanism:
Worms spread themselves automatically over the network without exploiting some vulnerability in a software or network protocol. Unlike viruses, worms don't require user interaction to bring infection, and their replication occurs very rapidly.

Impact on Systems:
Unlike viruses, worms consume system resources and slow down networks. They can even destroy or modify files. Some worms come with payloads, such as ransomware or backdoors, that create additional security risks.

Real-Life Example:
WannaCry (2017): This ransomware worm leveraged a Windows vulnerability named EternalBlue to compromise thousands of systems worldwide. It encrypted files and asked for ransoms. WannaCry hit hospitals, banks, and businesses-developing the concept of how destructive a self-replicating worm could be.

3. Trojan

Spread Mechanism:
Trojans normally appear as very useful software or files. They usually spread via phishing emails, fake downloads, or compromised websites. Unlike viruses and worms, Trojans do not self-replicate.

Impact on Systems:
It opens the backdoors for the attacker to control and access the infected system remotely. It may steal data, even keystroke logging of the victim's action, monitoring activity, etc, and deploying further malware.

Real-Life Example:
Emotet (2014): While Emotet started as a banking Trojan, it later evolved to become a malware loader responsible for installing ransomware and other types of malware. It is spread primarily via phishing emails and has caused huge financial and reputational damage to organizations the world over.

4. Ransomware

Spread Mechanism:
Most of the ransomware spreads through phishing emails, infected websites, or via exploit kits that take advantage of system vulnerabilities. Some types of ransomware have a worm fashion spread, thus spreading on their own across the network.

Impact on Systems:
The ransomware encrypts user files or locks a user out of their system and demands a ransom, typically to be paid in cryptocurrency. Most often, even after receiving the payment, files are not returned upon request.

Real-Life Example:
CryptoLocker (2013): First ransomware to gain headlines around the world, CryptoLocker encrypted user files and demanded payment in return for the decryption keys. It spread through infected email attachments and is estimated to have affected over 250,000 systems.

5. Spyware

Spread Mechanism:
Most of the spyware operates via downloads of bundled software, visiting malicious websites, or as attachments to phishing emails. Others are installed by exploiting vulnerabilities left behind by other malware.

Impact on Systems:
Spyware works in the background to monitor the activities of a user; it steals sensitive information like login ID passwords, personal data, history of browsing, and even financial details. These could be very dangerous for users' privacy and may lead to identity theft easily.

Real-Life Example:
DarkHotel, 2007-Present: It was an advanced spyware that targeted business executives while they traveled to specific hotel chains. The keystrokes were logged and the data stolen. Using exploited Wi-Fi and malicious hotel software updates, attackers installed spyware in executive devices.

6. Adware

Spread Mechanism:
Adware can be propagated through various free software downloads or through the installation of applications from malicious websites. Sometimes, it may come in the form of compromised ads, malvertising, whose click-through might lead users to download adware.

Impact on Systems:
Adware pops up different kinds of undesirable advertisements, which actually hinder smooth browsing and can hang systems. Though not as deadly as other malware, some adware steals user information without any consent and can pave the way for other highly attacking malware.

Real-Life Example:
Fireball (2017): Fireball was an adware campaign that affected more than 250 million computers worldwide, hijacking web browsers to pop up or display ads and collect user data. Primarily designed for ad revenue generation, Fireball had the capability to unleash more severe attacks.

7. Rootkit

Spread Mechanism:
Many rootkits spread via spam emails, malicious downloads, or by taking advantage of various system vulnerabilities. Some rootkits require administrative privileges and thus trick users to let the malware into the system.

Impact on Systems:
Rootkits provide an intruder unauthorized access and control at a low level over a system, hiding malicious processes from security applications. Various malware can be installed using rootkits, data can be stolen using them, and remote system access can be provided.

Real-Life Example:
Sony BMG Rootkit (2005): Sony began including a rootkit in some of its compact disks to fend off pirates. Unfortunately, this rootkit introduced security vulnerabilities in the systems for other types of malware to operate under the radar, and it raised an immense public outcry.

8. Botnet

Spread Mechanism:
The botnets are created through malware that normally spreads via phishing, malicious downloads, or through vulnerabilities. A device, when infected, joins several other compromised devices under the control of an attacker.

Impact on Systems:
They allow the attacker to use the network of infected devices for malicious activities, including the launching of DDoS attacks, sending spam messages, or performing brute-force attacks, which grossly affects the availability of a network and causes immense loss of data and money.

Real-Life Example:
Mirai Botnet, 2016: Mirai targeted IoT devices with weak security to create a huge botnet that launched record-breaking DDoS attacks, including against Dyn-a company which provided internet infrastructure. This had crippled several popular websites, including Twitter, Netflix, and Reddit.

9. Keylogger

Spread Mechanism:
Keyloggers are distributed via phishing emails, malicious program downloads, and physical installation on the target device. They can also be deployed by other malware, such as Trojans.

Impact on Systems:
Keyloggers record all of the information exchanged on the keyboard of a computer, which could include sensitive information from password entries, credit card numbers, or even personal messages. Normally used for espionage or identity theft.

Real-Life Example:
Olympic Destroyer (2018): A malware strike that targeted the Pyeongchang Winter Olympics contained a keylogging function to exfiltrate login credentials. The espionage-driven attack caused disruptions to the Olympic IT infrastructure and, until today, has shown the risks of keyloggers.