**What are Threat and its types?**

Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

**Threat** can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

**Software attacks** mean attack by Viruses, Worms, and Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

**Malware** is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

1. Infection Methods
2. Malware Actions

Malware on the **basis of Infection** Method are following:

1. **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms –** Worms are also self-replicating in nature but they don’t hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.
3. **Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the ‘Trojan Horse’ tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.

Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, and Remote Access Trojans etc. 

1. **Bots –**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

Malware on the **basis of Actions:** 

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer’s desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware –** It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection.

One of the most common examples of spyware is KEYLOGGER. The basic job of key logger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.

1. **Ransomware –** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
2. **Scareware –** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
3. **Rootkits –** are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
4. **Zombies –** They work similar to Spyware. Infection mechanism is same but they don’t spy and steal information rather they wait for the command from hackers.