**Name – Mukul Jindal**

**Group – 3CS10**

**Roll No – 102116063**

1. Worm

A worm virus refers to a malicious program that replicates itself, automatically spreading through a network. In this definition of computer worms, the worm virus exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.

Worms consume large volumes of memory, as well as bandwidth. This results in servers, individual systems, and networks getting overloaded and malfunctioning. A worm is different from a virus, however, because a worm can operate on its own while a virus needs a host computer.

1. Virus

A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See malicious code.

1. Trojans

A Trojan Horse (Trojan) is a type of malware that disguises itself as legitimate code or software. Once inside the network, attackers are able to carry out any action that a legitimate user could perform, such as exporting files, modifying data, deleting files or otherwise altering the contents of the device. Trojans may be packaged in downloads for games, tools, apps or even software patches. Many Trojan attacks also leverage social engineering tactics, as well as spoofing and phishing, to prompt the desired action in the user.

1. Spyware

Spyware is malicious software that enters a user’s computer, gathers data from the device and user, and sends it to third parties without their consent. A commonly accepted spyware definition is a strand of malware designed to access and damage a device without the user’s consent.

Spyware collects personal and sensitive information that it sends to advertisers, data collection firms, or malicious actors for a profit. Attackers use it to track, steal, and sell user data, such as internet usage, credit card, and bank account details, or steal user credentials to spoof their identities.

Spyware is one of the most commonly used cyberattack methods that can be difficult for users and businesses to identify and can-do serious harm to networks. It also leaves businesses vulnerable to data breaches and data misuse, often affects device and network performance, and slows down user activity.

1. Botnets

A botnet (short for “robot network”) is a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.” Each individual machine under the control of the bot-herder is known as a bot. From one central point, the attacking party can command every computer on its botnet to simultaneously carry out a coordinated criminal action. The scale of a botnet (many comprised of millions of bots) enables the attacker to perform large-scale actions that were previously impossible with malware. Since botnets remain under control of a remote attacker, infected machines can receive updates and change their behaviour on the fly. As a result, bot-herders are often able to rent access to segments of their botnet on the black market for significant financial gain.