BOOT SECTOR

Explanation: These viruses infect the starting point of a computer's operating system, making them activate whenever the computer starts up.

The boot sector is a tiny, but crucial, section on a storage device like a hard drive, SSD, or USB flash drive. It's essentially the starting point for your computer when it boots up.

Example: Imagine a virus that hides in the very first part of your computer's memory, so every time you turn it on, the virus wakes up and starts spreading to other parts of your computer.

EXECUTABLE FILE VIRUS:

Explanation: These viruses attach themselves to programs you run on your computer.

An executable file, also referred to as an executable program or simply an executable, is a type of computer file that your device can directly run or execute.

Example: Think of a virus that attaches itself to your favorite game. When you run the game, the virus starts spreading and infecting other games you have on your computer.

DATA VIRUS:

Explanation: These viruses hide inside files like documents or pictures.

Example: Picture a virus hiding inside a harmless-looking email attachment. When you open the attachment, the virus starts spreading to other files on your computer.

ADWARE:

Explanation: Adware shows you ads without your permission.

Adware is a type of software that bombards you with advertisements, often in the form of pop-ups, banners, and even new browser windows. While some people consider it merely annoying, adware can pose a security risk. Here's a deeper dive into adware:

How it works:

Adware can be bundled with free programs you download from the internet. During installation, you might unknowingly accept adware along with the desired software.

You might also land on a malicious website that tricks you into clicking something that installs adware.

What it does:

Adware disrupts your browsing experience with excessive ads, slowing down your device and making it difficult to focus on what you want to see.

Some adware tracks your browsing habits and online activity, collecting data to target you with personalized ads. This data can be sold to third parties, raising privacy concerns.

In severe cases, adware might even redirect you to phishing websites or inject malware into your device. Phishing websites try to steal your personal information, and malware can harm your device or steal data.

Why it's dangerous:

Adware can be a gateway to more serious threats. The excessive ads might lead you to click on something malicious unknowingly.

Adware can slow down your device and drain its battery life.

By tracking your browsing habits, adware can compromise your privacy and expose you to targeted advertising that can feel intrusive.

Here are some examples of adware:

A free game that suddenly fills your screen with pop-up ads every time you launch it.

Example: You download a free game, but every time you play it, annoying ads keep popping up, even when you're not connected to the internet.

SPYWARE:

Explanation: Spyware secretly watches what you do on your computer.

Spyware is a type of malicious software designed to secretly monitor and collect information about your online activities, such as websites visited, keystrokes typed, usernames and passwords entered, and even personal or financial information. Unlike adware, which displays advertisements, spyware operates covertly without the user's knowledge or consent.

Spyware can be installed on your computer through various means, including downloading and installing infected software, clicking on malicious links or advertisements, or opening malicious email attachments. Once installed, spyware runs silently in the background, capturing sensitive information and sending it to remote servers controlled by cybercriminals.

Example: Imagine you're using your computer to log in to your online banking account to check your balance and make a transfer. Unbeknownst to you, spyware has been secretly

installed on your computer. As you enter your username and password, the spyware records this information.

RANSOMWARE:

Explanation: Ransomware locks up your files and demands money to unlock them.

Example: You click on a link in an email, and suddenly, all your important files are locked up, and a message appears asking for money to unlock them.

PHISHING:

Explanation: Phishing tricks you into giving away personal information.

Example: You get an email that looks like it's from your bank, asking for your password and account number. But when you enter them, it's actually a scammer trying to steal your information.

LOGIC BOMBS:

Explanation: Logic bombs are like time bombs in your computer that go off when certain conditions are met.

Example: Imagine setting a timer on your computer to delete all your files if you don't log in for a week.

RABBITS AND BACTERIA:

Explanation: These programs multiply really fast and use up all your computer's resources.

Example: Picture a program that keeps making copies of itself until your computer slows down and crashes because it's running out of memory.