MALICIOUS PROGRAMS

NAME:ARANI BANERJEE
YEAR: 4TH YEAR
SEMESTER: 8TH SEM
ROLL.NO: 16800116089
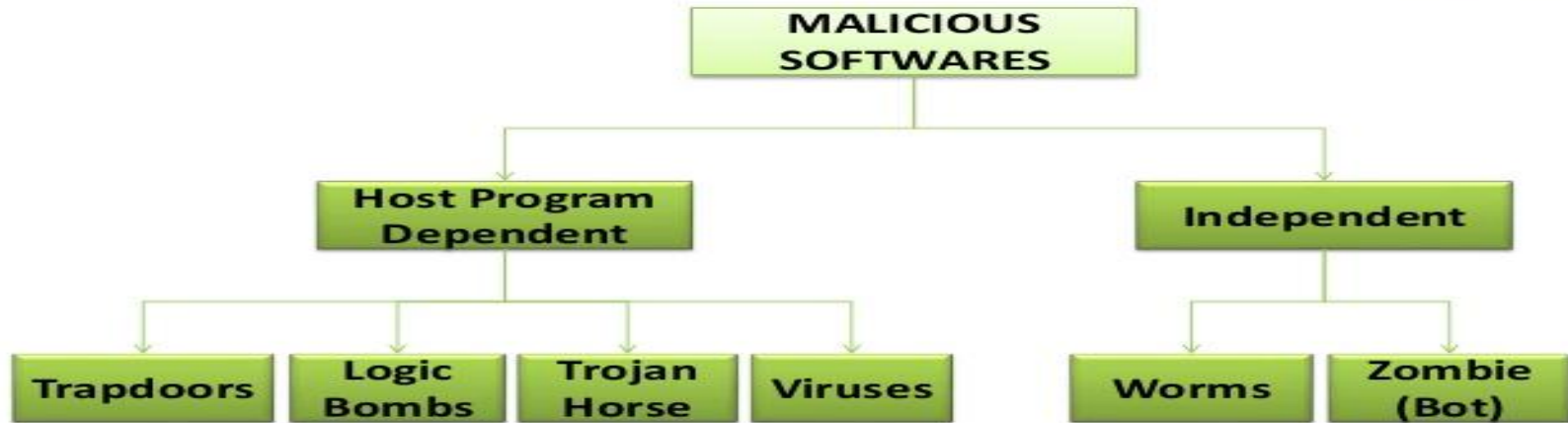**REG.NO**: 161680110008

What is Malicious Software ?

The words "**Malicious Software**" coin the word "*Malware*" and the meaning remains the same. Malicious Software refers to any **malicious program** that causes harm to a computer system or network. Malicious Malware Software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware or rootkits.

Their mission is often targeted at accomplishing unlawful tasks such as robbing protected data, deleting confidential documents or add software without the user consent.

Common example of malware includes-**viruses**,**worms**, **trojan horses** and **spyware.**

TYPES OF MALICIOUS PROGRAMME

Categories of Malicious Software

MALICIOUS SOFTWARES

- **Host Program Dependent**
  - Trapdoors
  - Logic Bombs
  - Trojan Horse
  - Viruses
- **Independent**
  - Worms
  - Zombie (Bot)

<u>Terminology of malicious programme</u>

<u>Computer Virus</u>

A computer virus is a malicious software which self-replicates and attaches itself to other files/programs. It is capable of executing secretly when the host program/file is activated. The different types of Computer virus are Memory-Resident Virus, Program File Virus, Boot Sector Virus, Stealth Virus, Macro Virus, and Email Virus.

<u>Worms</u>

A worm is a malicious software which similar to that of a computer virus is a self-replicating program, however, in the case of worms, it automatically executes itself. Worms spread over a network and are capable of launching a cumbersome and destructive attack within a short period.

Terminology of malicious programme

Trojan Horses

Unlike a *computer virus* or a worm – the trojan horse is a non-replicating program that appears legitimate. After gaining the trust, it secretly performs malicious and illicit activities when executed. Hackers make use of trojan horses to steal a user's password information, destroy data or programs on the hard disk. It is hard to detect!

Spyware/Adware

Spyware secretly records information about a user and forwards it to third parties. The information gathered may cover files accessed on the computer, a user's online activities or even user's keystrokes.

Adware as the name interprets displays advertising banners while a program is running. Adware can also work like spyware, it is deployed to gather confidential information. Basically, to spy on and gather information from a victim's computer.

Methods of protection against malicious software

Malicious Software is definitely a security threat for corporate users and individuals, thereby detecting and fighting malware remains on top of the agenda for many firms. Since the time BYOD culture started to flourish, Endpoint Security and Endpoint Protection have become the topics of discussion in many IT conference rooms. Many corporates today try to implement the best Endpoint Security or Endpoint Protection software to steer clear of the dangers.

Remember, if it is an individual system, it is essential to have an antivirus installed and if you already have one in place see to that it is updated at regular intervals. This approach will help you to remain safe during new breakouts. Comodo's Free Antivirus, Endpoint Security, Endpoint Protection Solutions are your best option for detecting and fighting malicious software. For more details visit our official page!