I. Definition some kind of security threats and attacks:

1. Adware:

* Adware: often called advertising-supported software by its developers, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process. Some advertisements also act as spyware, collecting and reporting data about the user, to be sold or used for targeted advertising or user profiling.
* The software may implement advertisements in a variety of ways, including a static box display, a banner display, full screen, a video, pop-up ad or in some other form.



1. Hacker:

* A hacker: is a person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means. The term also may refer to anyone who uses their abilities to gain unauthorized access to systems or networks in order to commit crimes.
* A hacker may, for example, steal information to hurt people via identity theft or bring down a system and, often, hold it hostage in order to collect a ransom.



1. Browser hijacker:

* Browser hijacking is a form of unwanted software that modifies a web browser's settings without a user's permission, to inject unwanted advertising into the user's browser. A browser hijacker may replace the existing home page, error page, or search engine with its own. These are generally used to force hits to a particular website, increasing its advertising revenue.



1. Malware attack:

* Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. By contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug. A wide variety of malware types exist, including computer viruses, worms, Trojan horses, …
* Malware is created with an objective in mind. While it could be said that the objective is limited only to the imagination of its creator, this will focus on some of the most common objectives observed in malware.



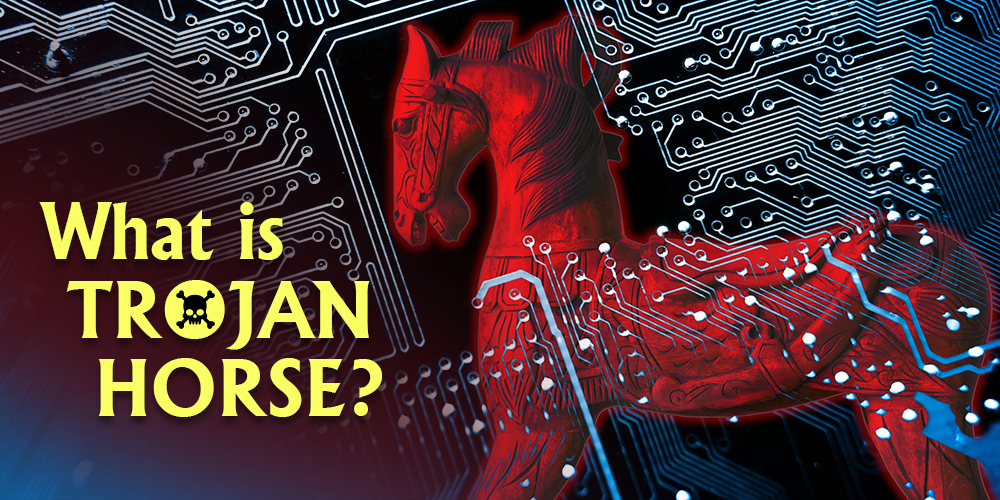
1. Spyware:

* Spyware is software with malicious behavior that aims to gather information about a person or organization and send it to another entity in a way that harms the user.
* For example, by violating their privacy or endangering their device's security. This behavior may be present in malware as well as in legitimate software. Websites may engage in spyware behaviors like web tracking. Hardware devices may also be affected.
* Spyware is frequently associated with advertising and involves many of the same issues. Because these behaviors are so common, and can have non-harmful uses, providing a precise definition of spyware is a difficult task.



1. Trojan:

* In computing, a Trojan horse is any malware that misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.



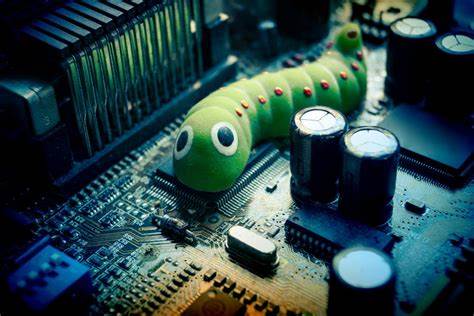
1. Virus:

* A computer virus is a malicious software program loaded onto a user’s computer without the user’s knowledge and performs malicious actions. Description: The term 'computer virus' was first formally defined by Fred Cohen in 1983. Computer viruses never occur naturally.
* A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus, a metaphor derived from biological viruses.
* In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code.



1. Worm:

* A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.
* It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue.



II. Write a letter report to the IT supervisor on the most serious incident. You will need to give recommendations on how to deal with the incident from the IT supervisor.