Logic bomb

It is a malicious code that is secretly inserted into a computer network, operating system or software application. It remains inert until a specific condition occurs, when this condition is met, the logic bomb is activated and devastates the system by damaging data, deleting files or wiping hard drives. They are small fragments of code contained in other programs. Although they can be malicious, in principle they are not, although it is a very fine line.

Characteristics

- It remains inert for a certain time: Like common timer bombs, logic bombs are not intended to be activated directly.
- Its payload is unknown until the moment it is activated: The payload is the malware component that performs the malicious activity.
- The activity is a certain condition: The detonator of the logic bomb is the condition that must be met.

Examples

Siberian oil pipeline sabotage

In 1982, the first attack of this type is considered to have happened. The CIA was allegedly informed that a KGB agent had stolen from a Canadian company the plans for an advanced control system, along with its software, for use on an oil pipeline in Siberia. The CIA had apparently programmed a logic bomb into the system to sabotage its enemy.

UBS attack by Roger Duronio

In 2006 at the investment banking firm UBS. The attack was led by Roger Duronio, a systems administrator at UBS Group AG. Duronio was apparently dissatisfied with his bonus pay, so he decided to “get even” with it by means of a time-bomb malware attack. His goal was to wipe out the firm’s servers so traders could not trade. When the bomb was activated it disabled 2,000 servers in 400 offices.