Bomba lógica

Es un código malicioso que se inserta secretamente en una red informática, sistema operativo o una aplicación de software. Permanece inerte hasta que se produce una condición especifica, cuando esta condición se cumple, la bomba lógica se activa y devasta el sistema dañando datos, borrando archivos o limpiando discos duros. Son pequeños fragmentos de código contenidos en otros programas. Aunque pueden ser maliciosos, en principio no lo son, aunque es una línea muy fina.

Características

- Permanece inerte durante un tiempo determinado: Como las bombas comunes con temporizador, las bombas lógicas no están pensadas para que se activen directamente.
- Su carga útil se desconoce hasta el momento en que se activa: La carga útil es el componente de malware que realiza la actividad maliciosa.
- La actividad es una condición determinada: El detonador de la bomba lógica es la condición que debe cumplirse.

Ejemplos

Sabotaje del oleoducto Siberiano

En 1982, se considera que paso el primer ataque de este tipo. La CIA fue supuestamente informada de que un agente de la KGB había robado a una empresa canadiense los planos de un avanzado sistema de control, junto con su software, para su uso en un oleoducto en Siberia. Al parecer, la CIA había programado una bomba lógica en el sistema para sabotear a su enemigo.

UBS attack by Roger Duronio

En 2006 en la empresa UBS, dedicada a la banca de inversión. El ataque fue dirigido por Roger Duronio, un administrador de sistemas de UBS Group AG. Parece que Duronio no estaba satisfecho con su paga de incentivos, por lo que decidió “vengarse” mediante un ataque de malware con bomba de tiempo. Su objetivo era borrar los servidores de la empresa para que los tradders no pudieran operar. Cuando la bomba de activo desactivo 2000 servidores en 400 oficinas.