Ransomware

Ransomware is a ransomware or extortion software, which can block access to a system or its files and then demand a ransom for their release.

How does it work?

Ransomware infection occurs in the following way.
First, the malware gains access to the device. Depending on the type of ransomware, it will encrypt the entire operating system or specific files. The program will then demand a ransom from the victim in question. Since malware is designed to remain undetected for as long as possible, it is difficult to detect an infection.

How does it occur?

The most common ways are: visiting malicious or compromised websites, downloading malicious attachments, infected software or downloads, or software vulnerabilities.

Types

The type also makes a big difference when it comes to identifying and dealing with the effects of ransomware, types include:
Lockdown ransomware: blocks basic computer functions, preventing access to the operating system or essential functions, but does not encrypt the user's files.
Encryption ransomware: Much more common and damaging, it encrypts the victim's files, making them inaccessible without the decryption key. It is the most widespread type of ransomware and the one that causes the greatest losses.

Examples

WannaCry

This is an encryption ransomware, used by cybercriminals to extort a user into paying. It attacks by encrypting valuable files so that they cannot be accessed or blocking access to the computer so that it cannot be used. It is believed to have infected around 230,000 computers worldwide, causing an estimated $4 billion in losses.