Ransomware

Es un software de extorsión o rescate, que puede bloquear el acceso a un sistema o a sus archivos y posteriormente exigir un rescate por su liberación.

¿Cómo funciona?

La infección por ransomware se produce de la siguiente manera.
En primer lugar, el malware obtiene acceso al dispositivo. Dependiendo del tipo de ransomware, cifrará todo el sistema operativo o archivos concretos. A continuación, el programa exigirá un rescate a la víctima en cuestión. Como el malware está diseñado para permanecer **sin ser detectado durante el mayor tiempo posible**, es difícil detectar una infección.

¿Cómo se da?

Las formas más comunes son: visitar sitios web maliciosos o comprometidos, descargar archivos adjuntos maliciosos, software o descargas infectadas o Vulnerabilidades de software.

Tipos

El tipo también supone una gran diferente cuando se trata de identificar y hacer frente a los efectos del ransomware, entre los tipos están:
Ransomware de bloqueo: bloquea las funciones básicas del ordenador, impidiendo el acceso al sistema operativo o a funciones esenciales, pero no cifra los archivos del usuario.
Ransomware de cifrado: mucho más común y dañino, cifra los archivos de la víctima, haciéndolos inaccesibles sin la clave de descifrado. Es el tipo de ransomware más extendido y el que causa mayores pérdidas.

Ejemplos

WannaCry

Es un ransomware de cifrado, los cibercriminales lo usan con el fin de extorsionar a un usuario para que pague. Este ataca cifrando archivos valiosos para que no se puedan acceder a ellos o bien bloqueando el acceso al ordenador para que no se puedan usar.

CryptoLocker

Los ciberdelincuentes usaban CryptoLocker para obtener acceso a un sistema y cifrar los archivos. Usaban técnicas de ingeniería social con el fin de engañar a los empleados para que lo descargaran en sus equipos, lo cual después infectaba la red. Una vez descargado mostraba un mensaje de rescate en el que ofrecían descifrar los datos si se realizaba el paso.