El *ransomware* es un tipo de software malicioso (o malware) que se encarga de encriptar los archivos de un sistema, permitiendo así al ciberdelincuente que lo ha implementado demandar un rescate (en inglés, ransom) por la devolución o recuperación de los archivos. Este rescate normalmente se pide en forma de criptomonedas, debido a la dificultad o imposibilidad de saber la verdadera identidad del destinatario de estas. Esto quiere decir también que los ataques de *ransomware* han visto un incremento desde la creación de las criptomonedas, y su subsecuente expansión a través de los mercados globales.

La consecuencia del encriptado de los archivos con un *ransomware* puede variar: Como mínimo, se sufre la pérdida del acceso a los datos. Como consecuencia final, se pierde la operatividad completa del sistema, ya que estos datos, según el tipo de *ransomware*, pueden ser cifrados, extraídos, borrados, exfiltrados (liberados al público) o incluso el sistema mismo puede quedar inhabilitado.

Existen distintos tipos de *ransomware*:

* Hoax: En inglés, significa estafa. Recibe este nombre porque solo simula el cifrado de los archivos, sin hacerlo realmente. Es en realidad un tipo de ingeniería social destinada a engañar al usuario para que pague.
* Scareware: Del inglés scare (asustar), utiliza como señuelo normalmente un anuncio molesto que nos dice que nuestro sistema está infectado o se encuentra en peligro, y que la única solución es la de instalar el programa que se nos ofrece para solucionarlo (que en realidad es el auténtico *ransomware*).
* Bloqueadores de pantalla: Como su nombre lo indica, bloquean la pantalla entera, volviendo efectivamente inutilizable el sistema, lo que no solo niega el acceso a archivos sino a otras funcionalidades o programas del ordenador o dispositivo. A veces, según el tipo, puede que solo la pantalla esté bloqueada, y los archivos no estén cifrados o perdidos. Otras veces, el bloqueo y cifrado de archivos es total. En este tipo de bloqueadores, el mensaje que veremos en pantalla nos instruirá sobre cómo desbloquear los archivos (normalmente con un pago). En algunas ocasiones incluso puede el *ransomware* ir un paso más allá y utilizar un mensaje engañoso, como un mensaje que parezca provenir de una fuente oficial (como la policía), y que indique que ha sido esta autoridad quien ha bloqueado el ordenador, dando “legitimidad” así al cobro de una multa y al desbloqueo de los archivos.
* *Ransomware* de cifrado: Cifra la información para exigir un rescate. Solo los ciberdelincuentes saben Cuál ha sido el algoritmo de cifrado y cuál es la manera de revertirlo. En algunos casos, los archivos directamente son eliminados, en vez de encriptados.
* Doxware: Emplea una técnica de presión sobre el usuario al amenazarle con hacer públicos los datos extraídos, lo cual puede dañar tanto la reputación del usuario como su negocio.

Uno de los ataques de *ransomware* más recientes y famosos es WannaCry. En mayo de 2017, este gusano (un tipo de malware que se autoreplica) atacó a computadoras que en ese momento utilizaran un sistema operativo Windows no actualizado, y encriptó sus datos, exigiendo un pago en Bitcoin por su recuperación. Irónicamente, este ataque fue posible gracias a que una vulnerabilidad encontrada por la agencia de seguridad nacional de Estados Unidos (NSA) se filtró y fue aprovechada por actores maliciosos. Se estima que el ataque afectó unas 300000 computadoras, y su daño monetario se estima en los miles de millones. Una segunda versión del mismo *ransomware* atacó a una compañía de semiconductores taiwanesa en agosto del siguiente año.