Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as Ukash and Bitcoin are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the "WannaCry worm", traveled automatically between computers without user interaction.
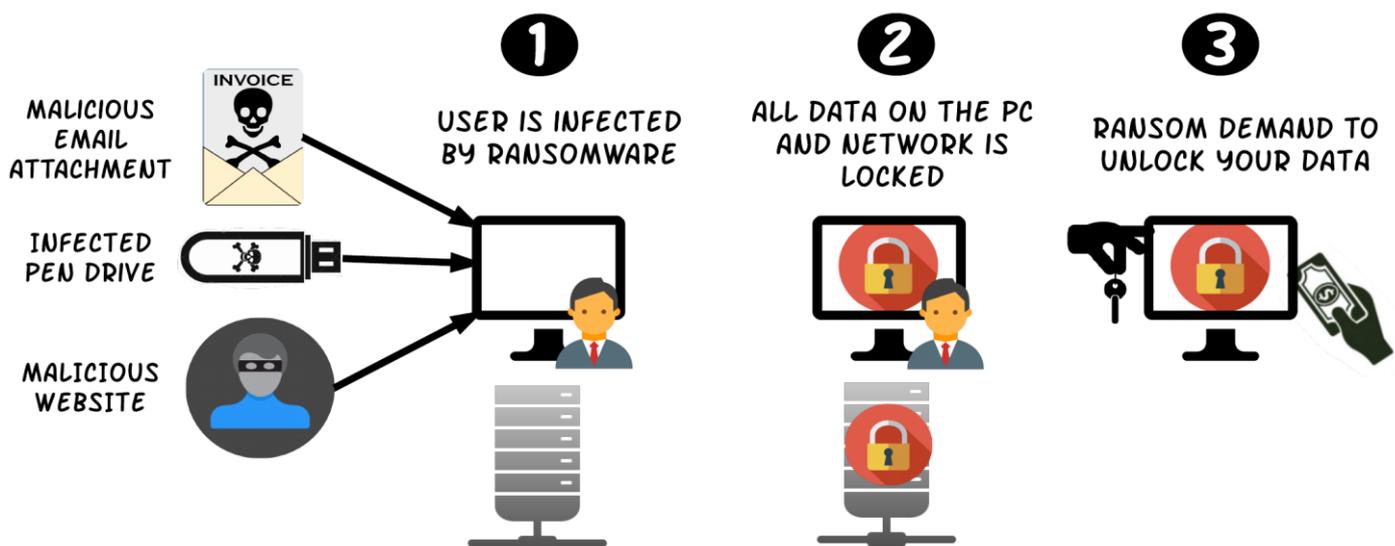
Ransomware attacks are typically carried out using a Trojan, entering a system through, for example, a downloaded file or a vulnerability in a network service. The program then runs a payload, which locks the system in some fashion, or claims to lock the system but does not (e.g., a scareware program). Payloads may display a fake warning purportedly by an entity such as a law enforcement agency, falsely claiming that the system has been used for illegal activities, contains content such as pornography and "pirated" media.

Encrypting ransomware reappeared in September 2013 with a Trojan known as CryptoLocker.

In May 2017, the WannaCry ransomware attack spread through the Internet, using an exploit vector named EternalBlue, which was leaked from the U.S. National Security Agency.

The ransomware attack, unprecedented in scale, infected more than 230,000 computers in over 150 countries, using 20 different languages to demand money from users using Bitcoin cryptocurrency.

HOW RANSOMWARE WORKS?

MALICIOUS EMAIL ATTACHMENT

INFECTED PEN DRIVE

MALICIOUS WEBSITE

❶ USER IS INFECTED BY RANSOMWARE

❷ ALL DATA ON THE PC AND NETWORK IS LOCKED

❸ RANSOM DEMAND TO UNLOCK YOUR DATA