

What Is Ransomware?

Ransomware is a type of malware that holds your data or systems hostage. A cyber criminal can use ransomware to lock a device, network, or server and withhold data access until the victim pays a ransom. Payment is typically in Bitcoin so law enforcement can't trace it.



TRAFFIC DISTRIBUTION SYSTEM

In this ransomware scenario, website traffic is redirected to a website that hosts an exploit kit. The redirection often happens via pop-ups or malicious advertisements. The kit is used to expose computer weaknesses before installing the ransomware.

LOCKERS

Locker ransomware is malware that locks users out of their systems and allows cyber criminals to take over control of the infiltrated devices until a ransom is paid. The users only see an instruction page with payment methods.

SELF-PROPAGATION

This type of ransomware spreads throughout an affected system and attacks any additional computers or devices connected to a shared network.

CRYPTO

This type of ransomware encrypts files on the computer and sometimes files on connected drives. If it goes undetected for a long time, encrypted files may overwrite legitimate files even in backups.

Examples of Ransomware and How They Work

05

04

06

01

02

03

PHISHING

The most common way to spread ransomware files is through phishing emails. Cyber criminals leverage social engineering techniques to convince unsuspecting victims to download and/or open an attachment containing malware.

EXTORTION

In this type of attack, cyber criminals may demand payment before encrypting files or damaging systems. They may claim that they have infiltrated your systems and unless a ransom is paid, they will destroy your data.

Who Could Be a Ransomware Target?

Any type of business, government, organization, or individual could be a ransomware target. Cyber criminals look to victimize anyone willing to pay a ransom to regain access to their device, network, or server, as well as the data it holds. Because of this, it's vital that all your employees can successfully detect and avoid this type of cyber threat.

