What Is Ransomware?

Ransomware is a type of malware and cybercrime that holds data for ransom. Access to data on computer networks, mobile devices, and servers is locked until the victim pays a ransom.

Common targets of ransomware include companies, individuals, organizations such as educational institutions, governments and hospitals. The two main types of ransomware are crypto ransomware and locker ransomware.

Ransomware can take on multiple forms. One of the most common methods of ransomware attack is with a phishing scam. A carefully worded email is sent urging the recipient to open an attachment or download a file. This action installs vector ransomware that takes over the computer and can infiltrate the entire computer network, locking everyone on the network out of their computers.

The goal of ransomware is to convince the victim to pay a ransom to unlock their data. Typically, the criminals behind ransomware demand the payment in Bitcoin – cryptocurrency that cannot be traced. Once the payment is secured, the victim receives an unlock code or decryption file that releases the data on the computer network, mobile device or servers.

Ransomware is a type of social engineering that criminals use to infect computers, infiltrate company networks and steal data.

What Are the Main Types of Ransomware?

Crypto Ransomware

Crypto ransomware prevents access to personal files and data. Crypto ransomware is smart enough to find valuable data on the computer or mobile device, encrypting it and locking out the victim.

Crypto ransomware looks for flaws and weaknesses in computers and devices – seeking out data that has not been backed up. This data can be anything of importance including financial data, large work projects, phone numbers, photos, tax and videos,

This type of malware is very savvy, encrypting all valuable data before revealing itself to the victim. This data is held ransom until the victim agrees to pay.

Crypto ransomware typically does not lock the entire computer or mobile device. Victims can usually still access any areas that are not encrypted and trapped by the ransomware.

Typically, the email is worded with a sense of urgency and with the need for the recipient to protect themselves from crime. The email is designed to appear to come from a legitimate source, for example customer service for Apple, a bank, Microsoft, PayPal or other known company.

Crypto ransomware is also referred to as data locker.

Locker Ransomware

Locker ransomware locks and shuts down the entire computer or mobile device. Victims are asked to pay a ransom to release the computer or mobile device.

Typically, the locked system allows the victim only limited access – forcing the victim to only interact with the ransomware criminal. Sections of the keyboard might be locked, or the mouse is frozen, effectively only allowing the victim to respond to the ransomware demands.

Locker ransomware usually does not infiltrate the entire computer network or attack the files on the computer. This makes it easier to find the malware and remove it without paying the ransom.

Because locker ransomware can be removed from the computer, criminals often use social engineering tactics to convince the victim to pay. For example, the ransomware pretends to be a tax authority or law enforcement agency that threatens to issue fines and other penalties for supposed illegal online activities. This causes the victim to panic and pay whatever price is demanded.

Locker ransomware is also referred to as computer locker.

What Are Common Ransomware Techniques?

File Encryption

Crypto ransomware uses either symmetric or asymmetric file encryption. Symmetric encryption uses the same key to encrypt and decrypt the data. Asymmetric encryption uses a public key to encrypt the data and private key to decrypt the data.

Symmetric encryption is a much faster method of encrypting data and files however, if the key is discovered by the victim, it is much easier to decrypt the data. With asymmetric encryption the criminal does not need to worry about protecting the public key since it cannot be used to decrypt the data.

Savvy crypto ransomware uses a combination of symmetric and asymmetric file encryption. Common types of file encryption include downloaded public key, embedded public key and embedded symmetric key.

Screen Locking

Locker ransomware uses screen locking to lock the victim out of their computer or mobile device. This means the victim cannot access anything on the computer or mobile device, including the operating system or other network services.

Often a ransom message is displayed on the screen in a continuous loop. The screen may include a countdown timer or an increasing ransom demand.

Common types of screen locking include Android locker ransomware, browser locking and Windows locker ransomware

How Does Ransomware Work?

Downloaders

When a downloader infiltrates a computer, it then downloads more ransomware malware that further infects the computer or mobile device. Typically this type of ransomware allows cybercriminals to control the computer or device.

Malvertisement

Fake criminal advertisements are displayed on real websites that direct the victim to a website hosting an exploit kit.

Phishing

Phishing or spam email uses social engineering techniques to convince victims to download or open attachments.

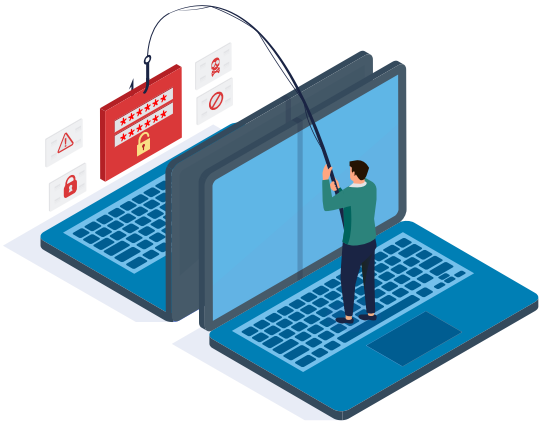
Self-Propagation

The ransomware spreads on the affected system, attacking any computers or devices on a shared network.

Traffic Distribution System

Website traffic is redirected using the Traffic Distribution System to a website that hosts an exploit kit. The exploit kit is used to expose computer weaknesses, and the ransomware is installed with drive-by-download malware.

Who Is A Ransomware Target?



Any business, government, organization or person is a target for ransomware. Cybercriminals are looking for anyone who is willing to pay a ransom to regain access to their computer networks, data, mobile devices or servers.

Cybercriminals do not care who they attack with their ransomware. Because of this, it's critically important that your employees and organization are cyber secure.

The ease-of-use of ransomware for cybercriminals highlights why it is so important that everyone in your organization is aware of the threats and risks of ransomware.

Ransomware simulation allows you to identify which employees are prone to ransomware and to educate your team on how easy it is for social engineering attacks to happen.