
Ace
Cloud
Hosting
RANSOMWARE
- A BEGINNER'S GUIDE

Ransomware is a malicious software program that encrypts the victim's data and prevents access to it. The data is held at ransom so that the owner cannot access the files, applications, or databases. A ransom (usually cryptocurrency) is then demanded from the victim (owner of the data) to release the encryption key.

Ransomware attacks are common these days - China, India, and the USA being the most popular targets for hackers. It is generally categorized as a subset of malware (malicious software program) designed to enter a system or network and harm it.

Hackers use cryptocurrency to extort money because the blockchain network keeps their identity confidential.

BASICS OF RANSOMWARE

Ransomware is a malicious software program that encrypts the victim's data and prevents access to it. The data is held at ransom so that the owner cannot access the files, applications, or databases. A ransom (usually cryptocurrency) is then demanded from the victim (owner of the data) to release the encryption key.

Ransomware is designed and created to attack and spread quickly across networks or systems. This way, it paralyzes the entire organization, putting the business operations to a halt. Upon entering your system, the program encrypts the data and asks for a ransom to return it - hence the name.

The common motive of a ransomware attack is to extort money, usually in the form of cryptocurrency. The unique thing about ransomware attacks is that the victim is notified of the attack and is given instructions to retrieve the data.

As stated above, ransomware uses data encryption (asymmetric encryption) to restrict access to the data. A pair of keys is generated - a public key and a private key. The private key is used to 'free' the data and is made available only when the victim pays the ransom. If the owner does not get the private key, it is challenging to get access to the data.

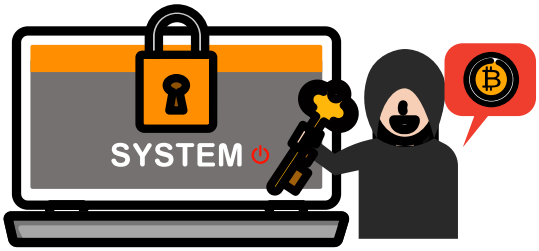
Ransomware is usually deployed through emails. It needs a target vector to establish its grip at the endpoint. After the grip is established, the malware stays in the infected system or network until its job is done. Upon successful deployment, ransomware searches for important files like word documents, spreadsheets, images, databases, and the like to encrypt them. The ransomware may also enter the system and try to exploit the entire organization.

TYPES OF RANSOMWARE

There are four main categories in which ransomware can be divided into:

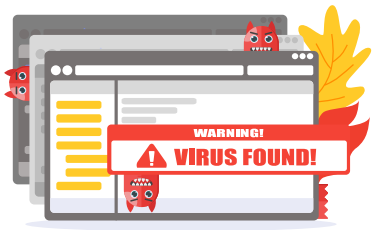
Crypto Ransomware

In this type of ransomware, the attackers encrypt the critical files and data so the users cannot access them without paying the ransom. WannaCry is a popular example of this type of ransomware - it affected more than 230,000 systems worldwide, and the money involved was around **$4 billion**. [1]



Locker Ransomware

In locker ransomware, the attackers lock the computers instead of locking the files. A ransom is demanded to unlock the systems. This way, the user cannot access any files, software, or data.



Scareware

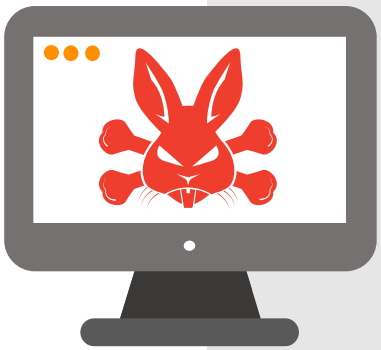
It is a fake software that displays a message. For instance, it may show that the device is infected with a virus and asks for money to resolve the issue. It may also display multiple popups.

Doxware (or Leakware)

Most of us store our data like pictures or videos on our devices. The attackers threaten to leak the data publicly and demand a ransom to keep it confidential. This is called Doxware.

EXAMPLES OF RANSOMWARE ATTACKS

Below is a list of popular ransomware attacks that caused mayhem globally.



Bad Rabbit

It is a dangerous ransomware and is delivered as an Adobe Flash Player update - flashes a message to the user that a new update is available. If the user is tricked, the malware gets installed. The main aim is to encrypt the entire hard disk.

Cerber

Cybercriminals offer Cerber as Ransomware-as-a-Service (RaaS). It is a silent malware and encrypts files by preventing Windows security features and antivirus from running. When the encryption is complete, it displays a ransom note on the desktop.

Locky

First released in 2016, Locky can encrypt up to 160 file types, primarily files used by engineers, testers, and designers. The popular deployment method is phishing - emails contain the malware that prompts the user to open a Word or Excel file.

WannaCry

WannaCry is one of the most prevalent ransomware attacks that exploit the Windows Server Message Block (SMB) protocol. It is also one of the most dangerous because it can self-propagate - it can infect other systems in a network.

GandCrab

GandCrab is one of the latest additions to the ransomware market (released in 2018). It encrypts the files and takes advantage of personal data and habits to demand a ransom from the user for not revealing such data.

CryptoLocker

CryptoLocker encrypted files of over 500,000 systems in 2017. [2] It spreads through unprotected downloads, emails, and other non-secure sites. New versions of Cryptolocker are so intelligent that they escape the antivirus as well.

MODES OF RANSOMWARE ATTACKS

There are multiple methods to inject malware into your system, like:

Email Attachments

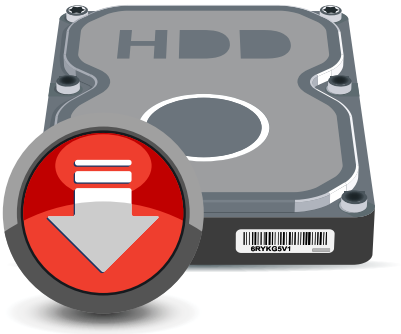
The most common way to inject ransomware into your system is by email attachments. The email consists of a link from a renowned organization. For instance, you can get an email from the university you studied at. This way, you trust the source and are not concerned about its authenticity.

Such emails contain **.exe** or **.scr** files, meaning that these files will execute a function upon downloading, and the user should not open them. In most cases, the users are not able to identify such files and end up opening them.

Botched URLs

Another form of phishing to inject ransomware into a system is through botched URLs. These URLs lure the user into clicking a link provided in the email.

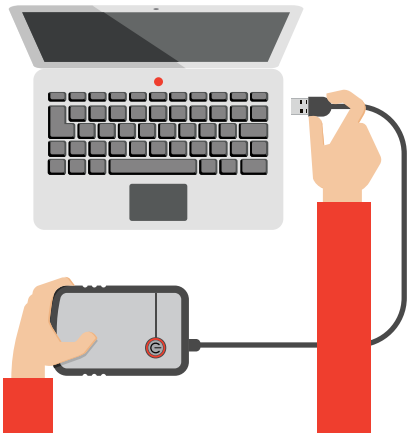
For instance, it's difficult to spot the difference between an 'I' in uppercase and an 'L' in lowercase. The URL can go like, **www.IRS.com**. It will look like the email is from the IRS, whereas it's a fake email containing a link to inject ransomware into your system.



Drive-by Downloads

Another type of malware injection is by drive-by downloads. These files get downloaded into your system without your knowledge through malicious websites. The Internet is full of thousands of such websites.

These websites have URLs similar to popular websites and infect your system when you open them. The malicious software then exploits the weaknesses in your system and infect the entire network.



External Storage Devices

There have been instances when attackers leave infected external storage devices in public places. So, if anyone plugs the device into a system, it infects the computer and encrypts all the important files.

If the system is connected to a network or a work laptop, the ransomware can spread across the network. It will then damage each device in the network and create an unwanted situation.

WHO IS TARGETED?

Companies that do not have a proper security mechanism in place and are likely to pay the ransom are targeted the most. Attackers target individuals and small businesses mostly because they feel at the least risk of getting attacked, do not have a cybersecurity system, and ignore the basic security measures such as installing the latest security updates.

Another popular reason to attack small businesses is that they do not have a proper BCDR (Business Continuity and Data Recovery) plan in place. Hence, if their data is affected, they have to pay the ransom or lose the data forever.

However, there have been instances where hackers have attacked renowned bodies. For instance, in 2013, the Police Department of Swansea, Massachusetts, paid a ransom of 2 Bitcoins to decrypt their data. [3]

HOW SERIOUS IS IT?

The FBI continuously monitors ransomware attacks in the country and has issued several warnings regarding the same. The situation is so bad that the FBI received 2,047 complaints about ransomware attacks in 2019, and the total money lost to cybercrime was estimated at around **$3.5 billion**. [4]

Ransomware attacks vary from a few hundred to thousands of dollars (depending upon the capacity of the organization). For instance, CryptoLocker (when it arrived in 2013) earned a profit of almost **$27 million** during the initial six months by infecting around half a million users. Ransomware hasn't looked back for a few years and is becoming widely popular among young hackers to extort easy money from individuals and businesses without revealing their identity. In fact, it has become a full-fledged industry (although illegal).

For those who do not wish to create their own ransomware, there's Ransomware-as-a-Service (RaaS). These hackers create and deploy ransomware on your behalf to extort money, or you can opt for open-source ransomware and modify it according to your needs.

WHAT SHOULD YOU DO IF YOU GET HIT BY A RANSOMWARE ATTACK?

If you have been hit by a ransomware attack, follow the steps given below to minimize the damage.

1. Stop all the business operations, isolate the infected device, and disconnect it from your organization's network. An infected device is a small inconvenience, but an infected network is a disaster for your business. It would help if you acted quickly; the sooner you act, the more likely it is to start your operations again.

2. Identifying the source (also known as Patient Zero) is an essential part of stopping the infection. If any device has opened more files than usual, you've got it. Otherwise, check your antivirus for any alert. For ransomware to enter any system, it requires user action, and most likely, there will be an alert.

3. Once you're done with it, try to find out the type of ransomware. You could take the help of your IT team for this or there are third-party websites that might help you with the same.

4. Report the matter to the authorities. They have access to some exclusive tools that can track the hackers. Also, ransomware is illegal, and like any other crime, it should be reported.

5. Check your backups for any damage. If you have an uninfected recent data backup, it is time to restore your system to as before and continue with your work. Please use your antivirus for scanning the system for malware files and erase its traces.

6. If your backup is also encrypted, or there isn't any, try to find a way to decrypt your data. There are several free decryption keys available online that might do the trick.

METHODS OF PREVENTION

The best way to minimize ransomware damage is by preventing an attack. Here's how you can do it.

Employee Training

Ransomware needs an action vector to enter any system and is usually sent through emails. If the person receiving such an email is aware of the danger and is vigilant, there are chances that ransomware will not enter your system. Conduct regular training sessions and teach your employees about the best practices.

Identify Loopholes

If you're a business owner, it is advised to conduct regular IT security checks, identify the loopholes, and improve them. If you can find loopholes, it's likely that a hacker will be able to do so.

Install the Latest Security Updates

Most people and businesses neglect the need to install the latest security updates. And that's how most systems get infected. Hackers pick the weak spots and deploy the ransomware to infect your system.

Data Backup

Ransomware attacks hold your data for a ransom. But, if you have created regular and multiple data backups, there's no need to pay a ransom.

Use Advanced Technologies

Usage of advanced technologies like cloud hosting to store your data on remote servers can be a game-changer in preventing your business from cyberattacks. Hosting providers have a team of IT professionals and cybersecurity experts that regularly monitor your data for any unusual behavior.

Implement Role-Based Access

Not every employee should have access to all the data. Deploy a role-based access system to restrict access to your data.

CONCLUSION

In this digital era, everything has moved on computer systems. It has its fair share of benefits and opens the doors for hackers and cybercriminals to gain unwanted access to the data.

If you get hit by a ransomware attack, it means significant losses for your business in more than one - financial loss, and your organization loses the clients' trust.

Hence, everybody should be aware of ransomware basics and contribute towards protecting businesses from getting hit by such attacks.

ABOUT
ACE CLOUD HOSTING

Ace Cloud Hosting (ACE) is an Intuit authorized Commercial Host and QuickBooks Solution Provider. Apart from QuickBooks hosting, the services offered include application hosting, private server hosting, managed server hosting, Desktop as a Service (DaaS), Virtual Desktop Infrastructure (VDI), and more. These offerings help clients to achieve their business goals in this fast-paced digital world by staying a step ahead of their competitors.

Ace Cloud Hosting is also the winner of multiple accolades like K2 2020 and 2019 Award for Customer Satisfaction, User Favorite Award by Accountex USA 2016 in application hosting category, and Great User Experience Award 2018 by FinancesOnline. ACE hosts your data on high-performance computing servers to ensure great performance with 99.999% uptime, round-the-clock support, 10-Day free trial, and 100-Day rolling backup.

REFERENCES

1. What impact did the WannaCry attack have? – **Kaspersky**
2. 10 ransomware examples – **Kaspersky**
3. FBI: $3.5B lost to cybercrime in 2019, led by business email compromise - **Health IT Security**
4. Is your data secure? 4 tips how to stay safe against ransomware - **Ace Cloud Hosting**
5. Top 10 FAQs you should know about ransomware - **Ace Cloud Hosting**

Ace Cloud Hosting

www.acecloudhosting.com