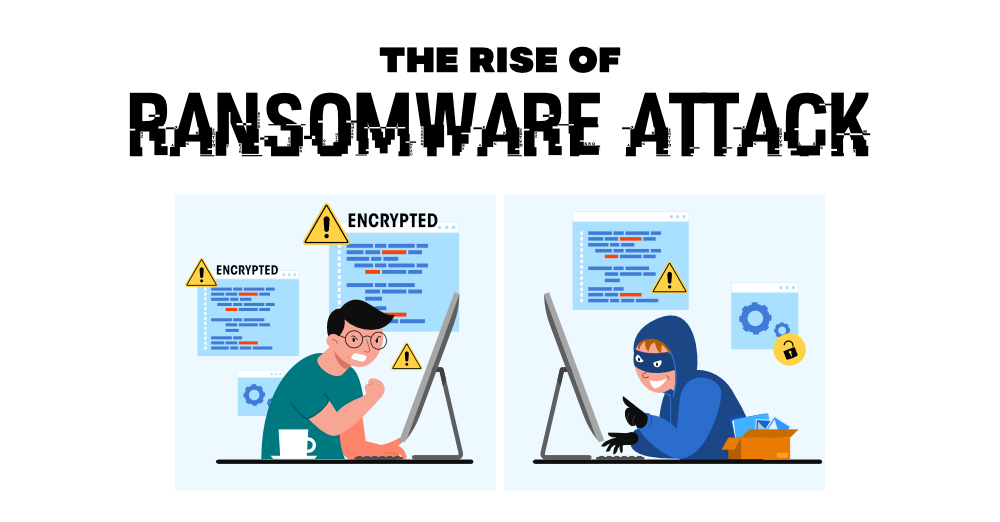
# Ransomware Attacks

COVID-19 has impacted the whole world in many ways forcing us to stay indoors, preventing social interactions, changing the way many businesses, educational institutions, companies work – but there is also another virus that’s made of 0’s and 1’s that has been spreading, infecting many computer systems causing issues and outages to many industries on a significant scale, and it is ***Ransomware.***



### What is Ransomware??

Ransomware is a type of malware that blocks access to systems and data unless a ransom is paid. It encrypts the victim’s files, drives making them inaccessible, and demands a ransom payment to decrypt them in Bitcoin and other cryptocurrencies making tracing and prosecuting the offenders difficult. In a properly implemented ransomware attack, recovering the files without the decryption key is very hard and time-consuming.

### How does Ransomware work?

Ransomware rarely infects systems directly, It is generally accompanied by other malware types like Trojans and Worms. After ransomware starts running it begins encrypting all the files, data on the drives preventing its access, and any other operations on the data. The process of file-encrypting ransomware, also called cryptoviral extortion, was invented by two researchers Young and Mordechai M. Yung at Columbia University. Cryptoviral extortion works by following a 3 round protocol carried out between the attacker and the victim:

1. First, the attacker generates a key pair & places the corresponding public key with the Trojan payload, and is released onto the open Internet waiting for a victim to download the infected file.
2. Then the Trojan starts executing on the victim device. It generates a random symmetric key and starts encrypting the victim’s data with it. It uses the public key in the payload to encrypt the symmetric key. This results in an asymmetric ciphertext that contains fewer characters along with the symmetric ciphertext of the victim’s data.
3. Then it zeroises the symmetric key, a practice of removing sensitive data like cryptographic keys, critical security parameters from a cryptographic program to prevent their recovery into the original plaintext data. Subsequently, it shows a message banner to the user that includes the asymmetric ciphertext & instructions on how to pay the ransom. The victim sends the asymmetric ciphertext and ransom (now mostly in cryptocurrencies) to the attacker.
4. When the attacker receives the ransom payment and ciphertext, they decrypt the asymmetric ciphertext sent by the victim with their (attacker’s) private key. Then the attacker sends back the symmetric key to the victim so that he can decrypt his encrypted data with the help of the symmetric key thereby completing a successful attack.

There has also been an increase in Ransomware as Service operators in recent days. Since its operation as a service is getting popular making more systems vulnerable even if the primary offender may not be that technically knowledgeable.

### Effects of Ransomware

* The primary function of Ransomware is to encrypt victim’s files making them unusable and the decryption key is given only when the ransom is paid
* The attacker might also steal sensitive information and threaten the Victim to publish the stolen data in the public.
* Depending on the system/company/service that suffered the attack they might not able to provide service to their users.
* When Ireland’s health services were hit by a ransomware attack, making most of the hospitals’ services down, and causing critical infrastructure failure.
* Education Institutions in the US/UK suffered ransomware causing the temporary shutdown affecting online learning for students.
* Attacking companies like SolarWinds and Kaseya make successful Supply-Chain Attacks increases the number of victims of the attack. In the case of Solar Winds which is not exactly a ransomware attack but its supply chain can cause a ransomware infection to its customers.
* Attack on US pipeline system has caused disruption of distribution of fuel causing the increase in prices and shortage of fuel.
* Paying ransom to the offenders motivating them to attack more targets, in some cases, the attackers returned to the same victim even after the ransom has been paid.
* Asking the ransom in Cryptocurrencies the attackers are protecting their identity and origin.
* There is no guarantee that the attackers will not disclose stolen data even after the ransom has been paid.
* Loss of Reputation will always be common to any cyberattack.

### Ransomware on the Rise

The increase in Ransomware attacks is been caused by dependency on the digital world due to the Pandemic. The sudden increase in Internet usage for almost everything like health, education, work, connecting to friends and family, and relying on services that are yet to be secure. Ransomware forces the victim to pay ransom sooner when compared to other cyberattacks because it restricts access to data. According to Reuters, more than 1500 organizations have fallen victim to Ransomware attacks. Disrupting services like Health services in Ireland and Pipeline systems in the US forces the companies to pay the ransom to restore the services sooner. Ransomware has been on the rise since the WannaCry worm in 2017 affecting Windows systems. Ransomware doesn’t attack directly so if any other malware has been made into your system you might expect a ransomware infection too.

The increase of Ransomware as Service operators, increase in Cloud services also helped in the growth of these attacks. The attack vector and the victims have tripled in 2020-21 when compared to 2015-16. The amount of ransom also increased from a few thousand dollars to tens of millions. The usage of cryptocurrencies also helped the offenders to receive the ransom in a simple and easy way

### Top Ransomware Groups

* **Maze (ChaCha) ransomware**– First spotted in 2019, Maze was one of the first to steal data before encryption. If the victim refused to pay the ransom, they used to threatened to publish the stolen files.
* **REvil (Sodin/Sodinokibi) ransomware**– Spotted in early 2019, REvil victims make up 11%. The malware affected almost 20 industries and quickly attracted the attention of experts for its technical abilities, such as the use of legitimate CPU functions to bypass security systems.
* **Netwalker (Mailto) ransomware**– Spotted in early 2020 and making more than 25 million USD, Netwalker earned a name for itself. It was offered to lease to scammers with its creators taking some share of profits.

### Top Ransomware Attacks (2020-21)

There are many companies that suffered Ransomware Attacks in 2020-21, here are the few notable attacks

* Attack on Ireland’s health services
* US Colonial Pipeline Attack
* Attack on Quanta, JBS FOODS
* Attack on Kaseya causing supply chain
* ACER, AXA Attack
* Attack on KIA MOTORS
* Cognizant Ransomware Attack
* Attack on University of California San Francisco
* Canon Ransomware Attack

### Protecting Yourself from Ransomware

Here are some tips to protect yourself and your company from ransomware attacks

1. **Backup your Data**– Ransomware encrypts your data, If you have a backup of your files you can easily restore the backup without paying the ransom. Data should be stored in a read-only format to prevent the spread of ransomware to drives containing recovery data.
2. **Apply patches regularly**– Keeping your system up-to-date provides some security with almost many types of cyberattacks. The patch for WannaCry has been available almost a month before the attack got some pace, yet it was successful for the offenders
3. **Anti Ransomware**– Most of the AntiVirus/Anti Malware solutions do provide ransomware protection to some extent, it’s always good to have an antivirus running.
4. **Awareness**– Ransomware doesn’t infect your system directly it will always come along with some other malware or Trojan. So be careful while downloading anything from the Internet, keep yourself away from malicious links, attachments.