Ransomware & its flavors, tips & tools to fight back

By - Yuvank Soni

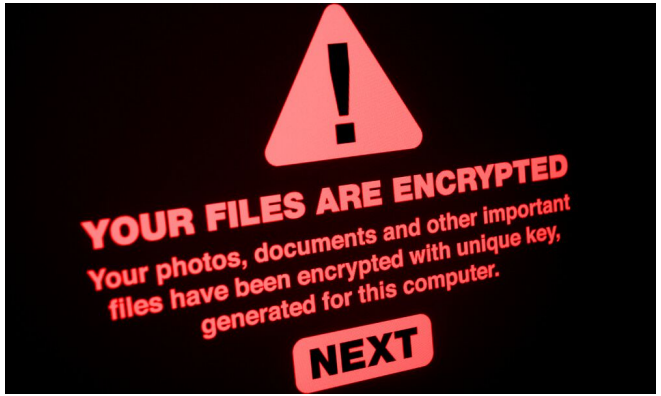
Today's Agenda

1. What is Ransomware?
2. What was the 1st Ransomware Attack?
3. What was the biggest Ransomware Attack till date?
4. What was the Exploit?
5. Which companies were attacked?
6. How much was the total loss because of attack?
7. Recent big ransomware attack?(Colonial Pipeline Hack)
8. Attacker's mindset
9. Types of ransomware attacks?
10. Types of ransomware?
11. How the attacks happen?
12. How to be secured from Ransomware?
13. How can you be safe if you are under attack?

What is Ransomware?

Ransomware is a type of malicious software that gains access to files or systems and blocks user access to those files or systems. Then, all files, or even entire devices, are held hostage using encryption until the victim pays a ransom in exchange for a decryption key. The key allows the user to access the files or systems encrypted by the program.

Ransom + Malware = Ransomware



What was the 1st Ransomware Attack?

It’s been said that Ransomware was introduced as an AIDS Trojan in 1989 when Harvard-educated biologist Joseph L. Popp sent 20,000 compromised diskettes named “AIDS Information – Introductory Diskettes” to attendees of the internal AIDS conference organized by the World Health Organization. The Trojan worked by encrypting the file names on the customer's’ computer and hiding directories. The victims were asked to pay $189 to PC Cyborg Corp. at a mailbox in Panama.

What was the biggest Ransomware Attack?

The biggest Ransomware attack till date is **WannaCry**. The **WannaCry ransomware attack** was a worldwide cyberattack in **May 2017** by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through EternalBlue.

What was the Exploit?

EternalBlue was an exploit developed by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers at least a year prior to the attack. Although the EternalBlue exploit was officially named MS17-010 by Microsoft it affects only Windows operating systems, anything that uses the SMBv1 (Server Message Block version 1) file-sharing protocol is technically at risk of being targeted for ransomware and other cyberattacks.

Which companies were attacked by WannaCry?

More than 3,00,000 computers were attacked in over 150 countries; the worst hit was Britain's National Health Service, affecting 36 hospitals across the country.

Globally, companies that were affected include Nissan Motors, FedEx, China National Petroleum, Renault SA, Deutsche Bahn, Hitachi, Sberbank of Russia, Yancheng police department in China, and the Russian Interior Ministry.

Given the number of computers that run on the older version of the Windows operating system, India was the third worst-hit country.

How much was the total loss because of WannaCry?

As the ransomware spread beyond Europe, computer systems in 150 countries were crippled. The WannaCry ransomware attack had a substantial financial impact worldwide. It is estimated this cybercrime caused **$4 billion** in losses across the globe.

The attackers demanded $300 worth of bitcoins and then later increased the ransom demand to $600 worth of bitcoins. If victims did not pay the ransom within three days, victims of the WannaCry ransomware attack were told that their files would be permanently deleted.

Recent big Ransomware Attack?

1. Colonial Pipeline -

   American oil pipeline system Colonial Pipeline Company suffered a major ransomware attack in May this year.

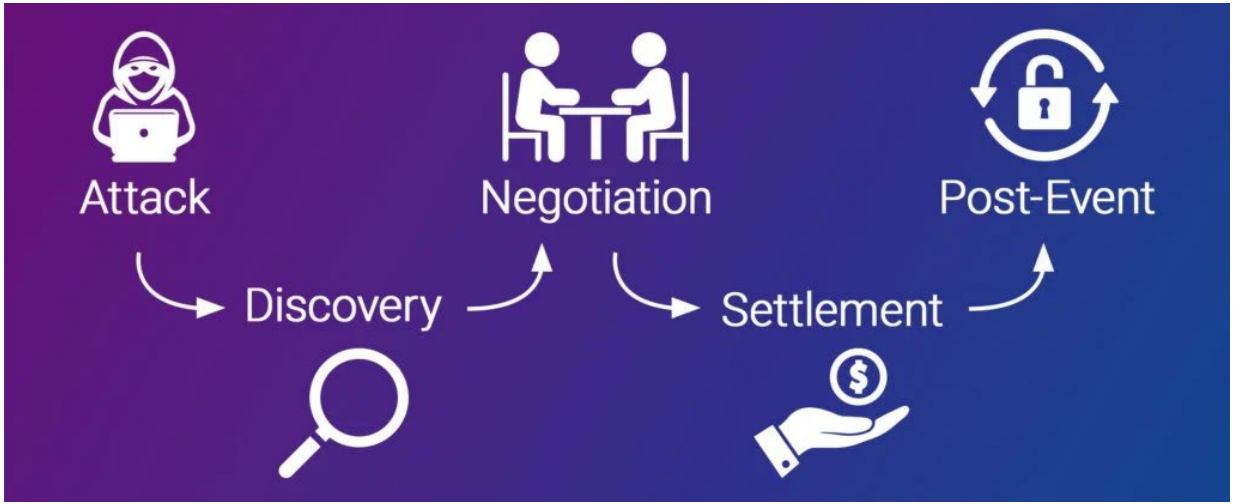
   Despite affecting just its IT systems, Colonial Pipeline Company shut down its entire pipeline operations to prevent further harm. With the FBI’s help, the company paid $4.4 million in bitcoin, as demanded by the hackers.

Mindset of Attacker on Ransomware Attack

Human error,

Loopholes,

Social Engineering, etc.



Types of Ransomware Attacks?

Targeted

Example - Colonial Pipeline Hack

Opportunistic

Example - Wannacry

Types of Ransomware?

Crypto ransomware

Crypto ransomware encrypts valuable files on a computer so that they become unusable. Cyber Criminals that leverage crypto-ransomware attacks generate income by holding the files to ransom and demanding that victims pay a ransom to recover their files.

Locker ransomware

Unlike crypto-ransomware, Locker ransomware does not encrypt files. Instead goes one step further, and it locks the victim out of their device. In these types of attacks, cybercriminals will demand a ransom to unlock the device.

How the attacks happens?

Because of you!

Yes, people themselves are responsible for the attacks, the attacker can easily trick anyone by using social engineering and some other tactics and make an easy trap for people to fall in.

Everytime you see an unknown link, an attachment from an unknown or malicious mail, Ask yourself twice, do you really need to click on that?

How to be secured from Ransomware?

1. Update your software and operating system regularly
2. Do not click on suspicious links
3. Never open untrusted email attachments
4. Do not download from untrusted websites
5. Avoid unknown USBs
6. Use a VPN when using public Wi-Fi
7. Install internet security software
8. Update your internet security software
9. Backup your data

How can you be safe if you are under attack?

1. If you are a company you will have a cyber security team working day and night to protect the data of the company and its clients.
2. But if you are just a fellow citizen you will not have the fancy arrangements, so if you are undergoing an ransomware attack you just need to identify the type of malware and go to **nomoreransom.org**, download the decryptor and run that.
3. Never pay the ransom, it will encourage the attackers for more attacks.

Thank you!
Let's Connect?

- LinkedIn: linkedin.com/in/yuvanksoni
- Twitter: twitter.com/yuvanksoni
- Instagram: instagram.com/yuvanksoni

OR

- Google "Yuvank Soni"

Any Questions?