NETWORK SECURITY

ASSIGNMENT - 1

TOPIC : RANSOMWARE

SUBMITTED BY

Rishab Banthia
18BCN7076

SUBMITTED TO

Prof. Sibi Chakkaravarthy
Dept. of Computer Science

INTRODUCTION

Malware is a code or software which is intentionally designed to cause damage to the client, server, computer or any other computer network. There are a wide variety of malware and some of them are :

- Worms
- Ransomware
- Trojan Horse
- Spyware
- Adware , etc.

Ransomware is an attack where it encrypts the files and systems of the victim and prevents its access to their owner. The data can only be decrypted or retrieved by the help of the decryption key which is owned by the attacker which means that the key has to be purchased or the demands of the attacker have to be fulfilled so that they can again access their data.

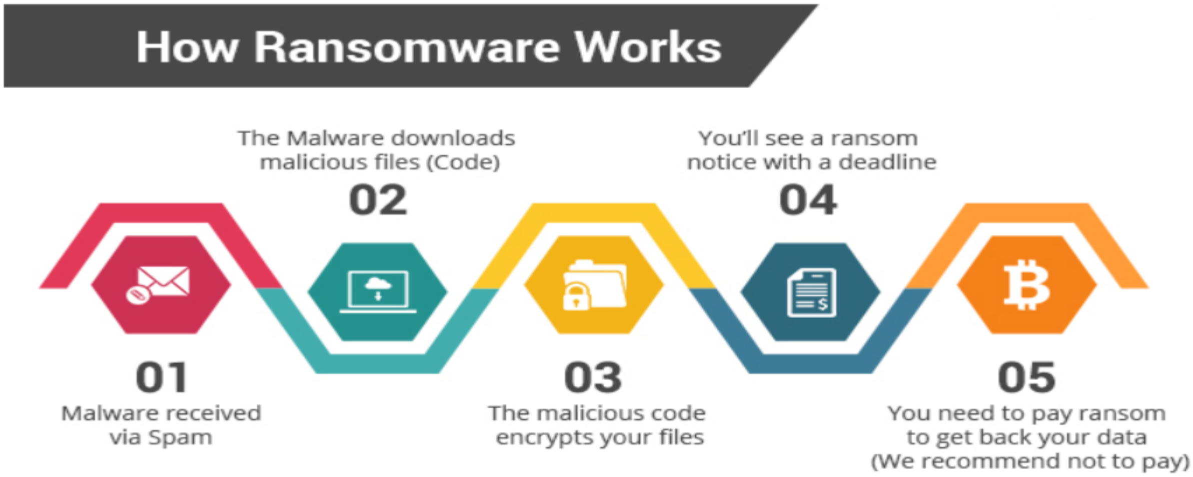
Phishing attacks are the most common way that the attacker uses to attack the victim.There other ways like via spam, social engineering efforts, drive-by downloading,etc.

Ransomware is of two types : encryptors and lockers. Encryptors are the means by which all the files of the system are encrypted on a PC or network but still the PC or network is accessible. Lockers are the means by which it locks the entire operating system there by making the whole system inaccessible.

HOW DOES RANSOMWARE WORK AND IT'S PROCESS

Firstly, the malicious code or software is installed in the system which can be done in many ways like phishing mails, via spam, downloading a software from an untrusted site, clicking on malvertising ads which release the malware or by a USB drive, etc which then encrypts the data on your computer or the network or the file making it inaccessible to the owner to access and this may lead to information leak or destroying your data, if the demands are not fulfilled by the victim.

Secondly, it is not necessary that the attacker requires user interaction to attack the victim, if there is any vulnerability present in the software installed the same can happen.

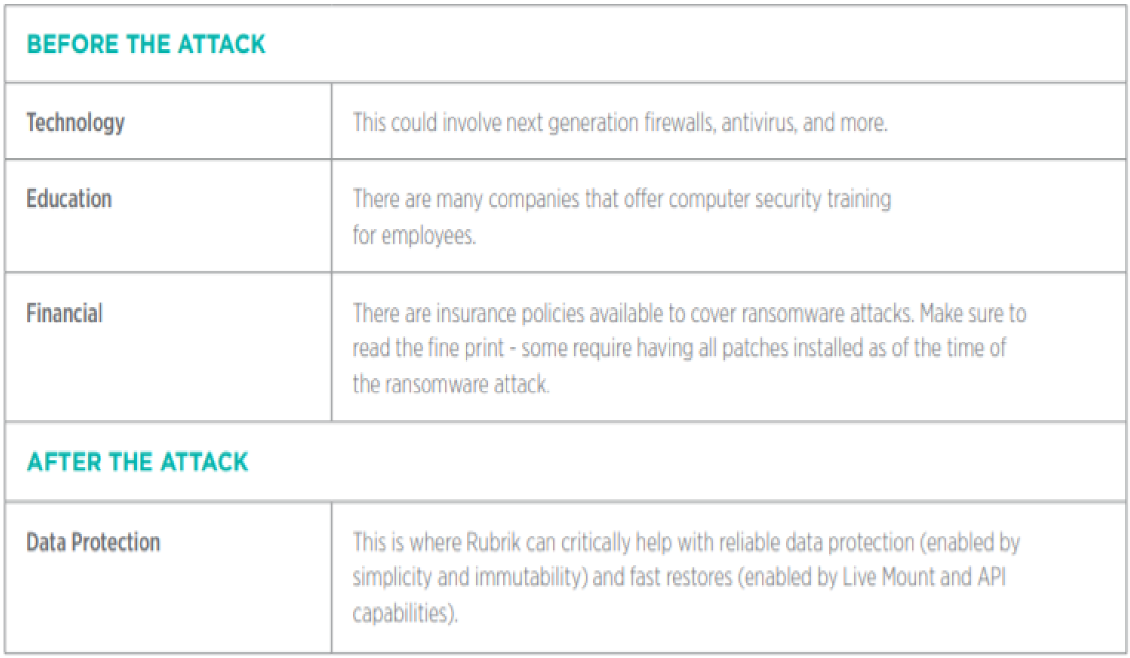

How Ransomware Works
The Malware downloads malicious files (Code)
02
You'll see a ransom notice with a deadline
04
01
Malware received via Spam
03
The malicious code encrypts your files
05
You need to pay ransom to get back your data (We recommend not to pay)

FACTS AND STATISTICS

- In the Internet Crime Report 2020, it stated that they received 2474 complaints which were identified as ransomware attacks with minimum losses of $29.1 million in the USA.
- India ranked second with an almost 39% increase in ransomware attacks in 2020 after the USA.
- It is said that by the end of 2021 every 11 seconds there will be a ransomware attack on the businesses.
- According to the Cyber Threat Defense report 2020, 62% of the organizations have been victimized by the ransomware in which 58% of the firms opted to pay the ransom and there was 13% increase in the attacks over the year before.
- It is instructed to all that the ransom should not be paid and be informed to the required authorities to resolve the issue but mostly everyone pays and mostly the issue is resolved because the firm cannot take risk to leak their data and decrease their value in the market.
- 48% of victims who get attacked lack the incident response (IR) plan.
- Only 58% of people have a formal security policy and rules in action.
- Ransomware attacks in India have risen to 11% in 2021.
- Phishing attacks have increased a lot during the pandemic i.e. 667% according to the forbes.

PREVENTIVE MEASURES

- Have a Backup of your data on a regular time interval so that even if attacked you can have your backup and format your system and be safe.
- Having a security mechanism or protocol applied in your emails and web gateways.
- Keep your software up to date.
- Have an Incident Response plan.
- Train your employees for these types of attacks.
- Response Plan
  1. Isolate the Infection
  2. Identify the Infection
  3. Report
  4. Determine your options
  5. Restore and refresh
  6. Plan to prevent recurrence
- Ways the virus can enter your system or network
  1. Human Attack Vectors are Phishing and Social Media.
  2. Machine Attack Vectors are Drive-by, System Vulnerabilities, Malversting, Network Propagation,
- According to the below table, you can also follow these things



BEFORE THE ATTACK	
Technology	This could involve next generation firewalls, antivirus, and more.
Education	There are many companies that offer computer security training for employees.
Financial	There are insurance policies available to cover ransomware attacks. Make sure to read the fine print - some require having all patches installed as of the time of the ransomware attack.
AFTER THE ATTACK	
Data Protection	This is where Rubrik can critically help with reliable data protection (enabled by simplicity and immutability) and fast restores (enabled by Live Mount and API capabilities).

CASE STUDIES

- **Ransomware At A Restaurant (RAAS)**
  The owner of the cafe Hard Times in Bethesda,MD on March 19th,2016 was having problems with their Point of Sale(PoS) system and recognized that the PoS was compromised. When they contacted the FBI they were told to pay the ransom as asked or rebuild their system. The ransom asked was $10,000 in bitcoin. And the restaurant was closed for seven days as they were not able to reopen due to this issue. So, it is not important that it might happen to only large companies, it can happen to anyone. Everyone should be prepared and ready.

- **Not Just Hospitals Attacked**
  Barts Health Trust, which runs hospitals across the Uk was hit by a massive ransomware attack in May of 2017. The attack began in the middle of the night and the systems were completely frozen and all the files were encrypted. The attacker demanded a very large amount of bitcoin in order to have their files back. All the data related to hospital stuff was encrypted like the surgery timings, patients medical history, patient appointments and their contact information, internal phone lines not working. All the surgeries were postponed and only urgent operations were operated.

  Later,they payed around 108,000 in euros in bitcoin to this #WannaCry ransomware attack.

- **A Ransomware Attack Prevented**
  A leading supplier of timber products in South Queensland, Australia Langs Building Supplies was recently hit by a ransomware attack. The company had their data backed up and were able to resolve this issue without even paying a single penny.

  This attack entered into the system via an email link that was sent to an employee and then one of their production files was showing a cryptolocker and there were 15000 files in it showing encrypted messages which needed a passcode to open it. But as their data management solution was API-driven they wrote down a script which retrieved their data from the last snapshot of the server in VM and where back up in one hour and it seemed that nothing happened.

ROLE OF CRYPTOCURRENCY

With the increase in the ransomware attacks, it has also become very important that the ransom payments be untraceable to the attacker. Cryptocurrencies like bitcoin, ethereum, monero,etc which use distributed ledgers, such as blockchain, to track transactions and the use of cryptocurrency by the criminals adds to the challenge of identifying them.

Criminals demand that their victims send the ransom payments via bitcoin but as the attacker receives the ransom in the designated digital wallet which stores the public and private keys, the criminals try to obfuscate these funds as quickly as possible to avoid detection and tracking. For obfuscating their funds, the method they follow is “chain hopping” which involves exchanging funds in one cryptocurrency for another using any of a variety of cryptocurrency exchanges. The funds become very difficult to trace once they have been exchanged and to further shield themselves they follow the money-mule service providers to set up accounts with the false or stolen credentials.There are other privacy coins such as Monero that are designed for privacy and are untraceable but these coins are not much in use because of their absence in liquidity in the market as compared to bitcoin.

Cryptocurrencies are difficult to trace but now blockchain analysis can help interpret public blockchain ledgers and, with the proper tools, government agencies, cryptocurrency businesses, and financial institutions can understand which real-world entities transact with each other. Blockchain analytic companies are able to show that a given transaction took place between two different cryptocurrency exchanges, for example a transaction between the individual and the organization. With the blockchain analytic tools and the KYC details, it becomes possible for the law enforcement authorities to gain transparency in blockchain activity which is not possible in the traditional financial system.

Some recommendations that could help reduce or disrupt these payment systems are :

- Payment systems like these should be disrupted so that these types of attacks can be less profitable.
- The infrastructure used to facilitate these payments should be disrupted or should be made to follow the rules related to these attacks.
- Ransomware actors should be criminally prosecuted so that they do not facilitate these attacks later.

FUTURE OF RANSOMWARE ATTACKS

In recent years, ransomware attacks have boosted so much that it has become a multi-billion dollar industry and will keep growing. Due to the pandemic many organizations have shifted to Software as a service(SaaS) platform. Many companies can’t imagine their businesses without the use of cloud services like G Suite, Salesforce, Dropbox, Microsoft Office 365, etc. So many organizations are turning to SaaS and it is just a matter of time that ransomware attacks happen.

Now might be the perfect time for the cybercriminals to expand their areas of attack and one of them will be cloud based attacks. Before the cloud based ransomware attacks were less but now due to the situation the cloud based attacks have increased.

There few reasons that there will be a great surge in the number of ransom attacks in future :-

- Cloud based ransomware attacks will give the cybercriminals a larger platform and a huge number of users at one place.
- Ransomware attackers looking for new areas of attack or new markets.
- Implementing a new generation of ransomware attacks.
- Maximizing profits with these attacks.
- Less awareness of cloud based attacks.

Here is a scenario where ransomware attacks targeting the SaaS data is :-

- The user might get an email from the cloud service provider which would need the user to click on it and update their app but this would serve as a phishing attack.
- Next, the user will install the malicious app or an extension for the web browser like in google and would request a bunch of permissions to access their data which would seem normal to the victim who thinks it is a regular update.
- And at last after all the permissions are granted, the app will start encrypting their data on the cloud and the victim will have no clue that they have been attacked.
- This would lead to encryption of their data and would also cost them a load of their savings.

There are still few ways where you can keep yourself updated and safe from these attacks in the future , which is not far.

- Monitor your SaaS environment 24 by 7 by using third-party providers who use ML/AI for analyzing, detecting and solving these attacks.
- Beware and protect yourself from phishing.
- Most importantly back up your data.

- If you own a company, train and monitor your employees.

The future of these ransomware attacks can be also called ransomware 2.0 because this will revolutionize these ransomware attacks.

CONCLUSION

It is sure and confirms that ransomware attacks are not going anywhere. This makes it very important to the businesses and everyone who is at risk to get attacked that they adopt the data management strategy of multi-layered security, easy automation and quick recovery. If an enterprise is prepared for these types of attacks then this is the solution or the least that one can do for preventing ransomware and many other dangerous attacks.

REFERENCES

- https://comodosslstore.com/blog/what-is-ransomware-5-straightforward-steps-to-protect-against-it.html
- https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/brief-spark-ransomware-remediation-prevention.pdf
- https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
- https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- https://ciso.economictimes.indiatimes.com/news/india-becomes-the-second-most-targeted-country-for-ransomware-after-surge-in-attacks-over-the-last-three-months/78526081
- http://www.cybercelldelhi.in/ransomware.html
- https://www.forbes.com/sites/forbesbusinesscouncil/2020/06/05/the-future-of-ransomware-2-0-attacks/?sh=435fef8c4dc9