International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 7 ǁ July 2023 ǁ PP. 144-149

Cyber Security-Ransomware

Rutuja Salvi
Student, MCA
Finolex Academy of Management and Technology
Ratnagiri, Maharashtra

Mrunali Patil
Student, MCA
Finolex Academy of Management and Technology
Ratnagiri, Maharashtra

Abstract: This research paper examines the current state of ransomware attacks, including the tactics and methods used by attackers, the impact on victims, and the challenges in defending against these attacks. The paper begins by providing an overview of the history and evolution of ransomware, including the early days of "police trojans" to the sophisticated, targeted attacks of today. It then delves into the various techniques used by attackers to spread ransomware, such as phishing emails, exploit kits, and malicious attachments. The paper also examines the financial impact of ransomware on victims, including the cost of paying ransoms and the disruption to normal business operations.

The research then examines the current state of ransomware defence, including the use of endpoint protection and backup solutions, incident response planning, and efforts to disrupt ransomware distribution networks.

Lastly, the paper concludes by providing recommendations for organizations and individuals on how to protect themselves from ransomware attacks, such as regularly updating software, implementing strict security protocols, and backing up important data. It also suggests future research directions for the field.

Overall, this paper aims to provide a comprehensive understanding of the current state of ransomware attacks and the challenges in defending against them. It is intended for security professionals, researchers, and decision-makers in organizations who are looking to better understand the threat of ransomware and develop effective strategies for protection

Date of Submission: 05-07-2023 Date of acceptance: 16-07-2023

I. INTRODUCTION:

Definition of ransomware: Ransomware is a type of malicious software that encrypts a victim's files. The attackers then demand a ransom from the victim to revive access to the files hence the name "ransomware."

Overview of the current state of ransomware attacks: Ransomware attacks have been on the rise in recent years, targeting individuals, businesses, and government agencies. These attacks can have severe consequences, including financial losses, disruption of services, and damage to reputation. Ransomware attacks are often highly sophisticated and well-funded, making them difficult to defend against. In 2021, ransomware attacks caused over $11 billion in damages globally, according to estimates from cybersecurity firms. The healthcare, education, and government sectors have been attacks. The COVID-19 pandemic has also led to an increase in ransomware attacks, as attackers have exploited the increased reliance on remote work and online services.

The impact of cybercrime ransomware on individuals, businesses, and government agencies: Ransomware attacks can have significant impacts on individuals, businesses, and government agencies. For individuals, ransomware attacks can result in the loss of personal files and financial hardship. For businesses, ransomware attacks can lead to lost revenue, damage to reputation, and regulatory penalties. Government agencies may also suffer financial losses and disruption of essential services as a result of ransomware attacks.

In addition to the direct financial costs of ransomware attacks, there are also indirect costs, such as the time and resources required to respond to and recover from the attack. Ransomware attacks can also have psychological impacts on victims, causing stress and anxiety.

The impact of ransomware attacks can be particularly severe for small businesses and individuals, who may not have the resources or expertise to effectively defend against these attacks. Government agencies may also be particularly vulnerable to ransomware attacks, as they often hold sensitive information and provide essential services to the public.

Overall, ransomware attacks can have serious consequences for individuals, businesses, and government agencies, and it is important for all parties to take steps to protect against these attacks.

HOW RANSOMWARE WORKS:

The technical details of ransomware attacks: Ransomware attacks often involve the use of phishing emails or exploiting software vulnerabilities to gain access to a victim's computer. Once the attackers have access, they can install ransomware on the victim's system, which then encrypts the victim's files and demands a ransom to restore access.

The technical details of ransomware attacks can vary, depending on the specific type of ransomware and the methods used by the attackers. In general, however, ransomware attacks follow a similar pattern:

Initial access: The attackers gain initial access to the victim's computer through a variety of means, such as phishing emails, software vulnerabilities, or social engineering techniques.

Ransomware installation: Once the attackers have gained access to the victim's computer, they install the ransomware on the system. This may be done through a variety of means, such as downloading and executing a file, or exploiting a software vulnerability.

File encryption: The ransomware then encrypts the victim's files, making them inaccessible to the victim.

Ransom demand: The attackers then demand a ransom from the victim in exchange for the decryption key, which is required to restore access to the encrypted files. The ransom may be paid in a variety of forms, such as cryptocurrencies or prepaid debit cards.

File decryption: If the victim pays the ransom, the attackers may provide the decryption key, allowing the victim to decrypt the encrypted files. However, there is no guarantee that the attackers will actually provide the decryption key, even if the victim pays the ransom.

However, the general pattern described above is common to many ransomware attacks.

The encryption process used by ransomware is often very sophisticated and difficult to break. In some cases, the attackers may also use additional tactics, such as deleting the victim's backup files or installing additional malware, to increase the pressure on the victim to pay the ransom.

Once the victim pays the ransom, the attackers may or may not provide the necessary decryption key to restore access to the victim's files. Even if the attackers do provide the decryption key, there is no guarantee that the victim will be able to fully restore their system or that all of the malware has been removed.

Overall, ransomware attacks are highly disruptive and can have severe consequences for victims. It is important for individuals and organizations to take steps to protect against these attacks, including keeping software and operating systems up to date, using antivirus software, and being cautious about opening emails and links from unknown sources

METHODS USED FOR DISTRIBUTING RANSOMWARE:

The methods used to distribute ransomware: There are several methods that attackers may use to distribute ransomware, including:

Spam emails: Attackers may send spam emails that contain a link or attachment that, when clicked, installs ransomware on the victim's computer. These emails may be disguised as legitimate messages, such as invoices, job offers, or notifications from delivery services.

Software vulnerabilities: Attackers may exploit software vulnerabilities to install ransomware on a victim's computer. This may be done through drive-by downloads, in which the victim's computer becomes infected simply by visiting a compromised website, or through the use of malicious software updates or apps.

Social engineering: Attackers may use social engineering techniques to trick victims into installing ransomware themselves. For example, they may send a message pretending to be from a trusted source, such as a government agency or a bank, asking the victim to download a file or install a software update.

Drive-By Downloads: A drive-by attack, sometimes called a drive-by download, is a malware attack that grip vulnerabilities in various web browsers, plugins, or apps, to launch the attack. It does not need any human action to initiate, meaning an employee solely needs to unknowingly browse an infected website. Once the attack is begun, the hacker can hijack the device, spy on the user’s activity or steal data and personal information.

Other methods: In addition to spam emails and exploiting software vulnerabilities, attackers may also use other methods to distribute ransomware, such as installing it on physical media (e.g.USB drives) and leaving them in places where they are likely to be found and used, or by using social media or other online platforms to spread the malware.

TECHNIQUES UTLIZE BY ATTACKERS TO HIDE THEIR IDENTITY:

Using anonymous communication channels, such as the Tor network, to hide the attacker's IP address and location.

Using cryptocurrency as a payment method to make it more difficult to trace the transaction back to the attacker.

Using multiple layers of encryption to make it harder for law enforcement or security professionals to decrypt the ransom demand and trace it back to the attacker.

Using disposable or throwaway email addresses and other types of online identities to further obscure the attacker's identity.

Using compromised servers or other types of infrastructure as a "hop" to further conceal the attacker's true location.

Anonymous payment methods: One common technique used by attackers to conceal their identity is to use anonymous payment methods, such as cryptocurrency, to receive the ransom payment. Cryptocurrencies, such as Bitcoin, can be difficult to trace, making it harder for law enforcement to identify the attackers.

Complex networks of intermediaries: Attackers may also use complex networks of intermediaries to further conceal their identity. These intermediaries may be individuals or organizations that are unaware of the true nature of the transaction and are used to transfer the ransom payment from the victim to the attackers.

TOR or other anonymity networks: Attackers may also use anonymity networks, such as TOR, to conceal their identity and location. These networks can make it difficult for law enforcement to trace the source of the attack.

It's worth noting that despite these efforts to conceal their identity, many ransomware attackers have still been successfully identified and prosecuted. This is often due to mistakes or oversights on the part of the attacker, or the use of advanced forensic techniques by law enforcement or security professionals.

CASE STUDIES OF RANSOMWARE ATTACKS

There have been numerous high-profile ransomware attacks in recent years that have caused significant disruption and financial losses. Here are a few examples:

A. **The WannaCry attack in May 2017:** This attack affected more than 200,000 computers in 150 countries, including the UK's National Health Service. It encrypted the files on infected computers and demanded a ransom payment in Bitcoin in order to decrypt them.

B. **The Petya/Not Petya attack in June 2017:** This attack affected thousands of organizations around the world, including major companies such as Maersk and Merck. It was spread through a malicious software update for a Ukrainian accounting program.

C. **The Locker Goga attack in January 2019:** This attack affected the Norwegian aluminum company Norsk Hydro, leading to a loss of $71 million. It also affected other companies in the manufacturing and engineering sectors.

D. **The Ryuk attack in August 2019:** This attack targeted the City of New Orleans, leading to a total cost of $7.5 million. It also affected other municipalities and school districts across the US.

E. **The Maze attack in May 2020:** This attack targeted the Travelex currency exchange company, leading to a loss of $2.3 million and the temporary shutdown of the company's online services. It also affected other companies in the finance, healthcare, and manufacturing sectors.

The consequences of these attacks (e.g., financial losses, disruption of services)

Loss of access to important data: Ransomware attacks often involve encrypting the files on an infected computer or network, making them inaccessible to the victim. This can result in the loss of important documents, records, or other data.

Loss of access to critical data: Ransomware attacks often involve encrypting the victim's files, making them inaccessible until the ransom is paid. This can disrupt business operations and cause financial losses

Loss of revenue: If an organization is unable to access its data or systems, it may be unable to conduct business as usual, leading to a loss of revenue.

Financial losses: Ransomware attacks often demand payment in exchange for decrypting the victim's data, and failing to pay the ransom can result in the permanent loss of important files. In addition, the cost of responding to a ransomware attack, including paying for technical support, can be significant.

Disruption of operations: Ransomware attacks can disrupt business operations and lead to lost productivity. This can be particularly damaging for organizations that rely on access to certain data or systems to function properly.

Damage to reputation: A ransomware attack can damage an organization's reputation if it is perceived as being vulnerable to cyber threats. This can lead to a loss of customer trust and a reduce in business.

Legal consequences: In some cases, ransomware attacks may violate laws or regulations, such as data protection laws. This can result in legal consequences for the victim organization.

Best practices for individuals and organizations to protect themselves against ransomware

Keep software and systems up to date: Ensuring that all software and systems are up to date with the latest patches and security updates can help to reduce the risk of a ransomware attack.

Use strong, unique passwords: Using strong, unique passwords for all accounts can help to prevent unauthorized access to systems and data.

Use two-factor authentication: Enabling two-factor authentication adds an extra layer of security by requiring a second form of authentication in addition to a password.

Enable firewalls and antivirus software: Firewalls and antivirus software can help to block incoming threats and prevent malware from infecting systems.

Back up data regularly: Regularly backing up important data to an external location (e.g., a cloud service or physical storage device) can help to ensure that important files can be restored in the thing of a ransomware attack.

Educate employees: Training employees on cybersecurity best practices, including how to identify and report potential threats, can help to reduce the risk of a successful ransomware attack.

Be cautious when clicking on links or downloading attachments: Exercise caution when clicking on links or downloading attachments, especially if you receive them from unfamiliar sources. This can help prevent accidental downloads of malware.

Have a response plan in place: Having a plan in place for responding to a ransomware attack can help minimize the impact of an attack and allow you to quickly get your systems back up and running

Consider ransomware insurance: Some insurance policies may cover the cost of responding to a ransomware attack, including paying the ransom and restoring affected systems.

The role of law enforcement in investigating and prosecuting ransomware attacks

Law enforcement agencies play a critical role in investigating and prosecuting ransomware attacks. When a ransomware attack occurs, law enforcement agencies may be involved in a number of activities, including:

Gathering and analyzing evidence: Law enforcement agencies will work to gather and analyze evidence related to the attack, such as log files, network traffic data, and ransom demands. This evidence can be used to identify the perpetrators and build a case against them.

Tracking down the perpetrators: Law enforcement agencies may use a variety of techniques to track down the perpetrators of a ransomware attack, including analyzing IP addresses, tracing cryptocurrency transactions, and working with international partners.

Making arrests: If law enforcement agencies are able to identify the perpetrators of a ransomware attack, they may make arrests and bring criminal charges against them.

Providing support to victims: Law enforcement agencies may also provide support to victims of ransomware attacks, including helping them to recover their data and working with them to prevent future attacks.

Overall, law enforcement agencies play a crucial role in investigating and prosecuting ransomware attacks, and their efforts can help to deter future attacks and protect the public from this type of cybercrime.

DEFENDING AGAINST RANSOMWARE ATTACKS:

Keep software and systems up to date: Ensuring that all software and systems are up to date with the latest patches and security updates can help to reduce the risk of a ransomware attack.

Use strong, unique passwords: Using strong, unique passwords for all accounts can help to prevent unauthorized access to systems and data.

Use two-factor authentication: Enabling two-factor authentication adds an extra layer of security by requiring a second form of authentication in addition to a password.

Enable firewalls and antivirus software: Firewalls and antivirus software can help to block incoming threats and prevent malware from infecting systems.

Back up data regularly: Regularly backing up important data to an external location (e.g., a cloud service or physical storage device) can help to ensure that important files can be retrieved in the things of a ransomware attack.

Educate employees: Training employees on cybersecurity best practices, including how to identify and report potential threats, can help to reduce the risk of a successful ransomware attack.

Be cautious when clicking on links or downloading attachments: Exercise caution when clicking on links or downloading attachments, especially if you receive them from unfamiliar sources. This can help prevent accidental downloads of malware.

Have a response plan in place: Having a plan in place for responding to a ransomware attack can help minimize the impact of an attack and allow you to quickly get your systems back up and running

Consider ransomware insurance: Some insurance policies may cover the cost of responding to a ransomware attack, including paying the ransom and restoring affected systems.

Law enforcement agencies play a critical role in investigating and prosecuting ransomware attacks. When a ransomware attack occurs, law enforcement agencies may be involved in a number of activities, including:

Gathering and analyzing evidence: Law enforcement agencies will work to gather and analyze evidence related to the attack, such as log files, network traffic data, and ransom demands. This evidence can be used to identify the perpetrators and build a case against them.

Tracking down the perpetrators: Law enforcement agencies may use a variety of techniques to track down the perpetrators of a ransomware attack, including analyzing IP addresses, tracing cryptocurrency transactions, and working with international partners.

Making arrests: If law enforcement agencies are able to identify the perpetrators of a ransomware attack, they may make arrests and bring criminal charges against them.

Providing support to victims: Law enforcement agencies may also provide support to victims of ransomware attacks, including helping them to recover their data and working with them to prevent future attacks.

Overall, law enforcement agencies play a crucial role in investigating and prosecuting ransomware attacks, and their efforts can help to deter future attacks and protect the public from this type of cybercrime.

II. CONCLUSION:

Ransomware attacks continue to be a significant threat to individuals and organizations. These attacks involve encrypting the files on a victim's computer or network and demanding a ransom payment in exchange for decrypting them. Ransomware attacks can have serious consequences, including the loss of important data, financial losses, disruption of operations, damage to reputation, and legal consequences.

To protect against ransomware attacks, it is important for individuals and organizations to follow best practices, such as keeping software and security protocols up to date, regularly backing up data, being cautious when opening emails and attachments, using a pop-up blocker, enabling two-factor authentication, and educating employees about the risks of ransomware. Law enforcement agencies also play a crucial role in investigating and prosecuting ransomware attacks.

Despite the ongoing threat of ransomware attacks, it is possible to mitigate the risks and protect against these types of cyber threats by following best practices and staying vigilant.

Ransomware is a type of malignant software that encrypts a victim's files. The victim is then asked to pay a ransom to the attackers in order to restore access to the files, hence the name "ransomware." It is important to take preventative measures to protect against ransomware attacks because they can have serious consequences for individuals and organizations. Ransomware attacks can result in the loss of important data and disruption of critical systems, leading to financial losses and reputational damage.

There are several steps that you can take to protect yourself and your organization against ransomware attacks:

Keep your operating system and software up to date: Make sure that you are running the latest version of your operating system and all of the software that you use. This is important because new versions of software often include security updates that can help to protect against new threats.

Use antivirus software: Antivirus software can help to protect your computer against malware by scanning your system for malicious software and quarantining or removing it.

Back up your data: It is important to regularly back up your data in case you do fall victim to a ransomware attack. This way, you will have a copy of your data that you can restore from in case your original files are encrypted.

Be cautious when opening emails and clicking links: Ransomware is often spread through email attachments or links to malicious websites. Be cautious when opening emails and clicking links, especially if you do not know the sender.

Enable two-factor authentication: Two-factor authentication (2FA) adds an extra level of security to your online accounts. When you enable 2FA, you will need to enter a code that is sent to your phone or email in addition to your password in order to log in. This makes it tough for attackers to gain access to your accounts.

REFERENCES:

[1]. “Ransomware: An Overview of the Landscape and Mitigation Strategies" SANS Institute (https://www.sans.org/readingroom/whitepapers/incident/ransomware-overview-landscape-mitigation-strategies-37200)

[2]. “Ransomware: Past, Present, and Future” McAfee (https://www.mcafee.com/enterprise/en-us/assets/reports/rpt-ransomware-past-present-future.pdf)

[3]. "Ransomware: One Year Later" Symantec (https://www.symantec.com/content/dam/symantec/docs/reports/ransomware-one-year-later-report-en.pdf)

[4]. "Ransomware: The State of the Threat” The Trend Micro (https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ransomware-the-state-of-the-threat)

[5]. “Ransomware: An Emerging Threat" Centre for an Internet Security (https://www.cisecurity.org/white-papers/ransomware-an-emerging-threat/)

[6]. "Ransomware: Past, Present and Future" by Check Point Research (https://research.checkpoint.com/ransomware-past-present-future/)

[7]. "Ransomware: The Growing Menace" by Norton (https://us.norton.com/internetsecurity-emerging-threats-ransomware-the-growing-menace.html)

[8]. "Ransomware: How to Protect Your Business" by Kaspersky Security (https://www.kaspersky.com/business-blog/cybersecurity/ransomware-how-to-protect-your-business/)

APPENDICES:

Appendix I: Additional Statistics on Ransomware Attacks

According to a report by Cybersecurity Ventures, ransomware attacks are expected to cost businesses over $11.5 billion in 2019, up from $325 million in 2015.

A survey by Malwarebytes found that ransomware attacks affected 38% of small and medium-sized businesses in 2018.

The same survey found that the average ransom demand increased from $294 in 2016 to $1,077 in 2018.

A report by the FBI's Internet Crime Complaint Center (IC3) found that the average ransom paid by victims of ransomware attacks was $1,077 in 2017, up from $294 in 2016.

Appendix II: Case Studies of Ransomware Attacks

Case Study A: The WannaCry Attack

In May 2017, a ransomware attack known as WannaCry infected more than 200,000 computers in 150 countries. The attack exploited a vulnerability in older versions of the Windows operating system and encrypted the victims' files, demanding a ransom of $300 in bitcoin to decrypt them. The attack had a significant impact on the healthcare sector, with hospitals in the UK and Spain being forced to cancel surgeries and turn away patients. The attack was eventually stopped by a researcher who discovered a "kill switch" in the malware's code, but not before it had caused an estimated $4 billion in damages.

Case Study B: The Bad Rabbit Attack

In October 2017, a ransomware attack known as Bad Rabbit infected computers in Russia, Ukraine, and other countries in Eastern Europe. The attack was disguised as an update to Adobe Flash and encrypted the victims' files, demanding a ransom of 0.05 bitcoin (approximately $285 at the time of the attack). The attack affected a number of high-profile organizations, including the Ukrainian Ministry of Infrastructure, the Kiev Metro, and the Russian news agency Interfax. The total number of victims and the number of damages caused by the attack are not known.

Appendix III: Technical Details on Ransomware Encryption

Ransomware attacks typically use one of two types of encryptions: symmetric or asymmetric.

A Symmetric encryption utilizes the same key for both encryption and decryption. This means that the attacker can decrypt the victim's files once the ransom has been paid. Examples of symmetric encryption algorithms commonly used in ransomware include AES and Blowfish.

An Asymmetric encryption uses two pair of keys: a public key for encryption and a private key for decryption. The attacker generates a public-private key pair and gives the victim the public key to encrypt the files. The private key is kept by the attacker and is used to decrypt the files once the ransom has been paid. Examples of asymmetric encryption algorithms commonly used in ransomware include RSA and Elliptic Curve Cryptography (ECC).