Arya's Ranframe: A Comprehensive Framework for Ransomware Defense

Anjum Zameer Bhat[1] and Arya Virmani[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

Ransomware is one of the most popular attacks that threaten victims by encrypting their personal confidential data. This article aims to provide a comprehensive examination of Ransomware attacks and their consequences for individuals, systems, and IT infrastructure. It also investigates the many forms of attack's that are utilized as a prerequisite for Ransomware attacks. Investigating the processes utilized to prevent ransomware attacks from occurring before they enter the local area network. Discovery of ways for reducing the impact of ransomware attacks at a level of difficulty for the attacker. Based on the findings, a few recommendations and conclusions are given. The study's approach comprises acquiring information through surveys and interviews from various users, victims, and working professionals who are the study's primary stakeholders. It also covers research based on many research papers and articles that conduct ransomware research. The study examines ransomware attacks and their consequences holistically. It also identifies the types of attacks that result in access gaining for ransomware attacks and discusses the most powerful and destructive ransomware attacks in the past, which had a significant impact on victims and various organizations in IT infrastructure. At the end of the investigation and analysis, recommendations and conclusions are provided in order to avoid or minimize and reduce the impact of ransomware assaults, making it impossible for the attacker to execute an attack.

Introduction

Cyber security refers to the protection of internet-connected equipment and services from malicious or damaging attacks by hackers, fraudsters, and cybercriminals. It is a branch of information security that deals with tactics for protecting devices and services against bad actors such as hackers, spammers, and fraudsters. Today's experts are more concerned with devising the best plan to protect all assets from computers and cell phones to networks and databases against cyber attacks (Kelley,2022). The security of every company begins with three principles: confidentiality, integrity, and availability. Confidentiality: Access to secret data and functions should be restricted to authorized persons only. Integrity: Only authorized people and devices may change, add, or remove sensitive data and actions. Availability: Systems, services, and information must be available on-demand in compliance with service-level-based requirements (Kelley,2022).

Ransomware is a specific kind of malicious software that encrypts the user's or victim's data and demands a ransom in exchange for the decrypting key. It may also access and encrypt the organization's essential and secret data, preventing people from accessing programs, databases, and so on. These assaults, which mostly target major networks, databases, and file servers, cause hundreds of millions of dollars in damage each year. CryptoWall3 alone caused $320 million in damage in 2015, while CryptoLocker was one of the most notorious ransomware assaults. These attacks are profitable, causing hundreds of millions of dollars in damage each year. In the year 2013, the ransomware CryptoLocker infected about 250,000 PCs and paid the makers $3 million (Simoiu, Bonneau, Gates, & Goel, 2019). In 2015, TeslaCrypt or AlphaCrypt demanded a large ransom payment of roughly 200 crore INR in crypto currency to re-establish the hospital's infrastructure. All of these attacks continue to occur all over the world, so following some essential steps and guidelines can help to mitigate them and reduce the chances of being attacked by them. As a result, the project thoroughly investigates attacks involving ransomware and how they occur, and then researches ways to mitigate them and provide a protection against the attack using suggestions and recommendations in the framework (Simoiu, Bonneau, Gates, & Goel, 2019).

Some of the usual methods discussed include taking frequent backups of your essential files so all data can be readily restored if an attack occurs. Updating systems on a regular basis with critical security updates and antivirus software can also assist to mitigate assaults from known dangers to some extent. To limit the danger of losing the confidentiality of critical sensitive data, appropriate restrictions and permissions with access control must be granted. These are some of the main steps that may be taken to lower the danger of attacks and build a defense against them (Simoiu, Bonneau, Gates, & Goel, 2019).

Literature Review

According to the authors Tailor, Patel, et al., there are more modernized types of ransomware families that categorize crypto-ransomware attacks separately and encrypt a specific file inside the infected system before demanding a large ransom via online payment in order to provide them with the decryption key. A good understanding of ransomware activity can result in an efficient detection system that significantly decreases the loss of victims' data. The article also includes an examination of previous ransomware outbreaks from various sources. It then delivers detection and prevention techniques for combating these attacks, such as checking the file extensions known by users, keeping an eye out for documents being renamed multiple times, using client-based anti-ransomware agents, and other mechanisms for its prevention. The authors proposed CryptoDrop as a solution, which is essentially an early warning sign detecting system that warns the victim if there is unusual file activity. There may also be an installation of a defense mechanism in Windows, which can be done by continually monitoring the system file, registry activity, and so on. So, if the values are continuously monitored, ransomware detection is possible in this case (Tailor & Patel, 2017).

The authors Shaukat, Ribeiro, et al., convey and discuss that signature-based processes used by antivirus software are mostly insufficient for evading ransomware attacks since there are many obfuscation methods that generate new variations every day. The author also claims that generic malware attack vectors are insufficient for detecting these assaults since these approaches do not completely track and assess the behavioral patterns displayed by the various cryptographic ransomware families. In this research, the author offers RansomWall, a security solution based on comprehensive data analysis of several ransomware families. It is essentially a layered defensive mechanism for security against cryptographic ransomware assaults. This system framework uses a hybrid technique, which is a blend of static and dynamic approaches, to develop a collection of attributes that define the ransomware behavior. The author argues that if a strong trap is present afterwards, it will aid us in the early identification of these assaults. It detects intrusions and removes them using machine learning methods. When there is suspicious activity, such as ransomware, in the first levels of the RansomWall, the files that are being changed are backed up to protect the user's data until the behavior is identified as ransomware or normal. The RansomWall system was built for the Windows operating system, and it was tested against 574 samples taken from 12 distinct cryptographic ransomware variants in a real-world user scenario. The RansomWall framework was tested utilizing multiple machine learning methods and found to have a 98.25% detection rate and practically 0% false positive detection when using the Gradient Tree Boosting methodology. It was discovered that the framework successfully recognized 30 zero-day penetration samples.(having a detection rate of less than 10% with approximately 60 security engines linked to VirusTotal) (Shaukat & Ribeiro, 2018).

According to another author, Okpongete et al., ransomware has a major impact, necessitating the development of a comprehensive model for detection and mitigation of the assaults. According to the author, once the victim's system is infected, the virus takes complete control of the machine and locks or encrypts the data on it. People, organizations, and governments in numerous nations have suffered significant financial losses as a result of the assaults. The criminals seek a ransom payment in the form of Bitcoin. There are now three types of detection systems for these attacks: static, dynamic, and hybrid detection mechanisms. Because static detection is easily evaded by cryptographic techniques, the dynamic detection technique was used for the study. The ISOT ransomware dataset was used for training and testing, and it was offered as a model for a standalone endpoint detector for the assaults. This detector presented by the author was developed and then evaluated online using wild samples; also, the Cuckoo sandbox was employed for the execution and removal of malware features throughout the experiment. The online evaluation of the experiment revealed that the offline performance results were quite good, which pleased the researchers (Okpongete, 2022).

Authors Urooj, Al-Rimy, Zainal, Ghaleb, Rassam et. al state that Ransomware is a particularly infamous sort of virus that has become well-known due to its fatal and terrible impacts on victims. They claim that the harm caused by ransomware must be identified quickly. Various studies have been conducted to gather information about the ransomware attack's evolution, taxonomy, trends, threats, and countermeasures. Some are specifically designed for IoT and Android platforms. Nonetheless, there is not a single study that demonstrates the significance of dynamic analysis of ransomware detection areas. The authors of this paper, provides information about the collection of datasets from their different sources, which were primarily used for ransomware detection using multiple platforms. It also includes a survey on the detection of ransomware using machine learning, deep learning, and a combination of both of these approaches, as well as an examination of the major benefits of dynamic analysis of ransomware detection. The author's also present information regarding prior experiments on ransomware detection conducted between 2019 and 2021 in this article. It also includes a sufficient number of recommendations for future research projects (Urooj, Al-Rimy, Zainal, Ghaleb & Rassam, 2022).

According to the author, Mohammad, there is no one process or instrument that can ensure comprehensive security against ransomware assaults. The technologies that are now available identify some forms of ransomware attacks but fail to detect others and do not provide full detection. The authors of this study article outline numerous strategies, tools, and processes that may be adopted to limit the occurrence of ransomware attacks. Until date, the main technique for an attacker to infect a machine or system has been to send malicious emails and links designed to destroy the system. Following a thorough examination of multiple reports published by various anti-virus companies such as Kaspersky, McAfee, and various ransomware researches. The authors primarily conclude by advocating two primary points: first, educate users and youngsters, and second, employ strong security rules, various types of processes, and techniques for data backup in order to reduce the probability of a ransomware assault occurring. Another technique for developing particular methods to identify ransomware in the future will be through the use of artificial intelligence (Mohammad, 2020).

Methodology

Mixed approach was found to be the most relevant and suited approach for this research, as the research requires both qualitative and quantitative data.

A mixed approach of qualitative and quantitative methodology would help provide a more thorough assessment of the public's understanding of ransomware attacks and how aware they are of these attacks, and quantitatively would help us get a better and more accurate idea because anyone from all over the world can be a victim of a ransomware attack. This approach would assist in acquiring greater understanding and having a full knowledge of the issue being studied on, which is ransomware attacks and the consequences to support the study. This approach will be the most appropriate for this research, as it combines the both quantitative and qualitative methods, therefore balancing out the limitations of each method and rendering it perfectly. It will also strengthen the project with stronger evidences and give a greater trust to the project study's findings, as well as help attain a better rough idea of the results than one particular methodology. As a result, we will obtain better and more accurate replies from the audience because the questions can be closed or open ended as needed.

Data Gathering and Analysis

The study used primary and secondary data resources to gather data on the topic of Ransomware. The primary source was a survey or questionnaires and interviews with individuals from various sectors, types of employment, and different age groups. The data analyzed based on the survey will be presented in the conclusion part of the project. The secondary source was gathered from literature resources, articles, conference papers, and books. All of this helped in gathering data suitable for the research and performing analysis in a successful way.

The data gathered includes opinions and information from various sectors, which means there were respondents from various sectors which included educational sector, IT, Finance, Healthcare, Legal, Engineering backgrounds, Construction and Oilfield. This showcases that we have a wider range of audience, who responded to this questionnaire and provides us with a suitable and effective data collection and analysis for the research purpose.

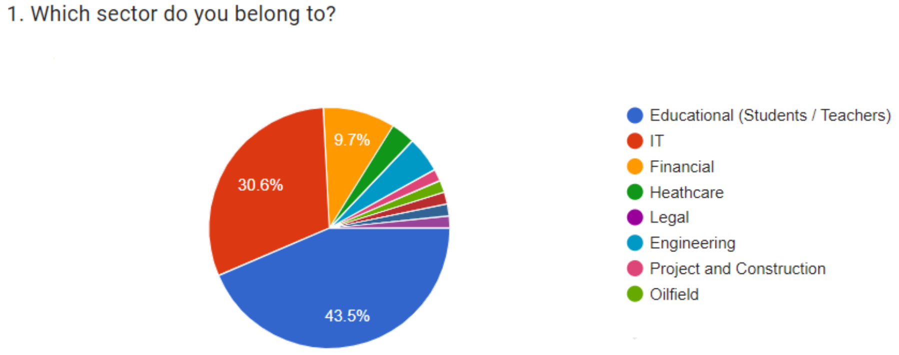

Figure1. Data Gathering (Sector)

Approximately around 70 percentages of the respondent’s state that they have been/someone they know have been a victim to ransomware attack/cyber attacks. This is a huge amount in today’s world and makes the need of a robust and better prevention and defense mechanism framework more essential. Keeping this into consideration, development of a much more enhanced and robust framework for the Ransomware Defense is required as soon as possible due to its growing threat.

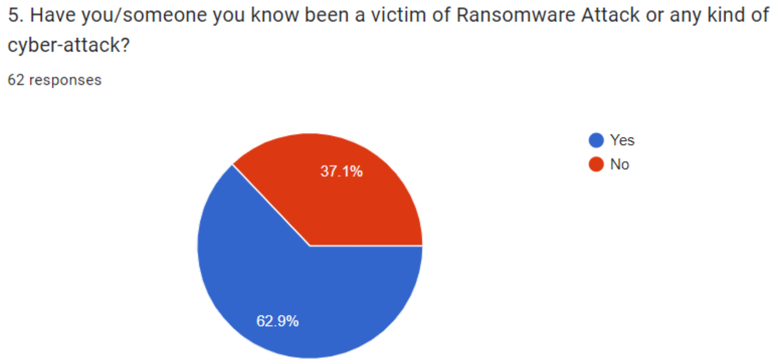

Figure2. Data Gathering (Victim of Ransomware)

Almost about 82 percentage of the audience, have received phishing emails according to the survey done. This indicates that the hackers still use phishing attack as one of the important attacks to gain access and information, and also use it as a pre attack for ransomware assaults. Phishing attack which is one of the most commonly used attack by cyber criminals, is a type of cyber assault in which an attacker impersonates a reliable entity or organization, such as a bank, social media site, or email provider, in order to trick the victim into disclosing sensitive information such as passwords, credit card numbers, or other personal information. This is often accomplished through the use of email, text messaging, or social media communications that look legitimate but are actually aimed to obtain personal information from the victim.

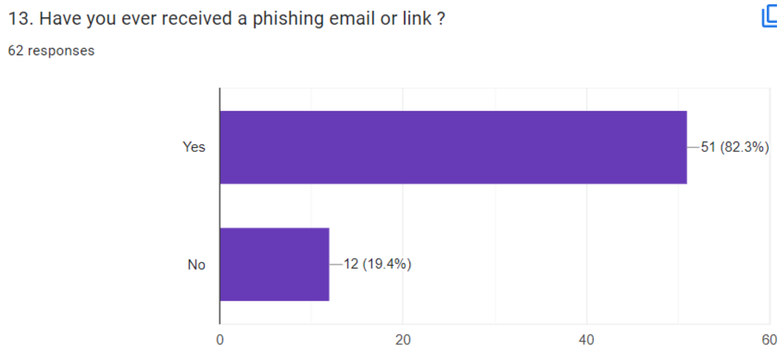

Figure3. Data Gathering (victim to phishing attack)

Approximately, 82 percentage of the respondents from the survey think that yes, there is a need of much stronger detection and prevention plan for Ransomware Assaults. These attacks have become more prevalent and complex in recent years, causing enormous disruptions to businesses, organizations, and individuals all around the world. These assaults involve cybercriminals encrypting important data or systems and demanding a ransom payment in order for access to be restored. While some victims choose to pay the ransom, doing so only encourages further attacks and fails to ensure the safe return of their personal information. Also, there is no specific type of mechanism discovered which can comprehensively protect and defend these Ransomware Attacks. As a result, there is an obvious need for more comprehensive and efficient security systems to resist the danger of ransomware by proposing a suitable framework for serving this purpose.

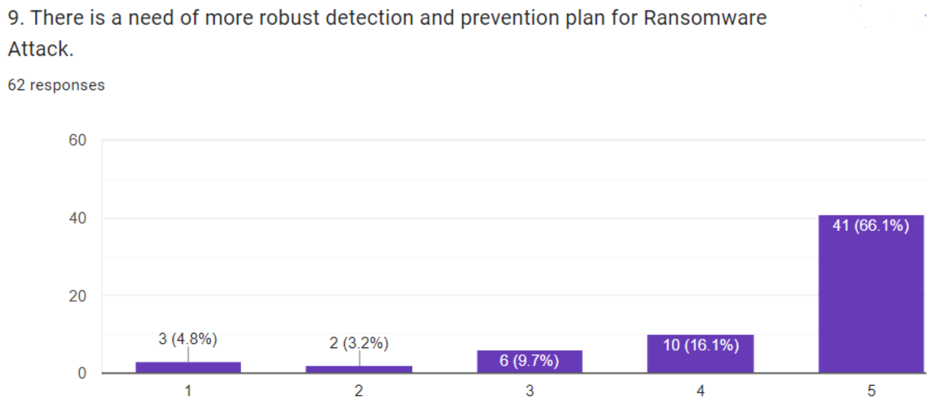

Figure4. Data Gathering (need of more robust planning for ransomware defense)

Proposed Framework

Organizations will have a complete plan to protect or preserve their systems and data against ransomware attacks if they build a strong Ransomware Security plan or a defensive architecture. They will also be able to improve their overall security posture and reduce the likelihood of a costly and destructive ransomware attack by using

Ransomware Defense Framework. Additionally, having an effective defense framework in place can help firms recover from an attack as quickly as possible while minimizing the impact on their business operations and company reputation. All of this highlights the need of having a robust and improved Defense Framework in place.

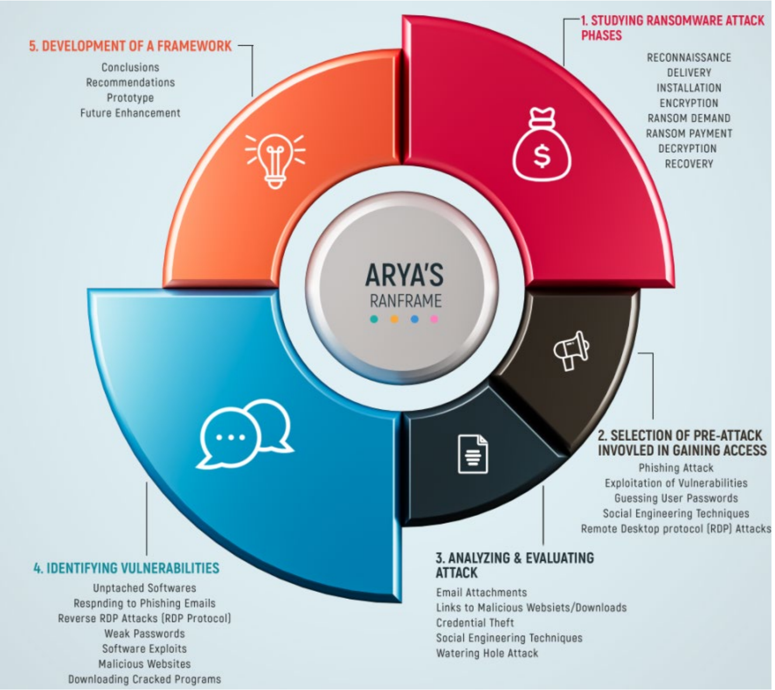
ARYA'S
RANFRAME
1. STUDYING RANSOMWARE ATTACK PHASES
RECONNAISSANCE
DELIVERY
INSTALLATION
ENCRYPTION
RANSOM DEMAND
RANSOM PAYMENT
DECRYPTION
RECOVERY
2. SELECTION OF PRE-ATTACK INVOVLED IN GAINING ACCESS
Phishing Attack
Exploitation of Vulnerabilities
Guessing User Passwords
Social Engineering Techniques
Remote Desktop protocol (RDP) Attacks
3. ANALYZING & EVALUATING ATTACK
Email Attachments
Links to Malicious Websiets/Downloads
Credential Theft
Social Engineering Techniques
Watering Hole Attack
4. IDENTIFYING VULNERABILITIES
Unptached Softwares
Respnding to Phishing Emails
Reverse RDP Attacks (RDP Protocol)
Weak Passwords
Software Exploits
Malicious Websites
Downloading Cracked Programs
5. DEVELOPMENT OF A FRAMEWORK
Conclusions
Recommendations
Prototype
Future Enhancement

Figure5. The Proposed Design of the Framework

Result and Conclusion

According to the research and analysis, guarding against ransomware attacks necessitates a multifaceted approach. Keeping software up to date, making data backups, employing antivirus software, training users, and building an incident response strategy are among the important considerations. These precautions can help avoid ransomware attacks or lessen their damage if they do occur up to a certain limit.

❖ Implementing a secured private mail servers can help organizations protect themselves from ransomware attacks up to a certain extend. Private and secured mail servers can help prevent ransomware from spreading through an organization's network by screening out doubtful emails and attachments before they reach employees' inboxes.

❖ Closing emails from outside personal email users and placing them in the spam folder can serve as an effective method for defending enterprises against ransomware threats. Organizations may dramatically minimize the danger of employees mistakenly clicking on harmful links or downloading malware-laden files and documents by eliminating emails from anonymous senders.

❖ Blocking particular file types is another effective ransomware protection method. Organizations could reduce their vulnerability to these forms of attacks by prohibiting the download and execution of files that are widely used to spread ransomware. To effectively implement this approach, firms should consider the following recommendations: Configure email filtration systems, block particular file types, utilize antivirus software, train staff, monitor the flow of emails, and update software on a regular basis. Organizations may dramatically lower the risk of ransomware attacks from unknown or suspected email senders by following these precautions.

- Reducing or limiting administrator user access and giving certain individuals domain account capabilities can be a successful approach for defending enterprises against ransomware attacks. Organizations may dramatically lower the possibility of ransomware attacks spreading throughout the network by restricting the number of individuals with admin-level privileges.
- Denying the transmission of file extensions to encrypted formats can be a useful technique for safeguarding enterprises against ransomware attacks. Organizations may dramatically lower the risk of infection by prohibiting users from transferring data to encrypted formats typically utilized by ransomware.
- Another recommendation is, to protect against brute force and John the Ripper attacks, strong and complex passwords, two-factor authentication, and limiting login attempts are effective measures. Intrusion detection and prevention systems can also help identify and prevent suspicious login attempts, and keeping software up-to-date can defend against known vulnerabilities. Adopting these safety measures can reduce the risk of successful attacks, which could lead to ransomware and other illegal activities, for both individuals and companies.
- The Zero Trust Model is a type of security architecture that makes assumptions that all network communication is dangerous and says that there is no device, software, or any human that should be trusted by standard. This particular kind of ransomware protection or defense mechanism can be effective by restricting the user access and detecting any kind of suspicious activity using procedures such as multiple-factor authentication techniques, the segmentation of network, and continuous surveillance. The above technique can be executed by identifying the various types of network assets, establishing strict access controls mechanisms, and providing personnel with appropriate type of security training. Using this model which is a Zero Trust Model can help companies reduce their exposure to malicious attacks like ransomware and other cyber attacks which has a growing threat among the individuals all around the globe..
- Adequate mechanisms, such as robust access control is of the utmost importance for protecting against attacks involving ransomware. Access control mechanisms provide confidence that sensitive data and systems are only accessed by authorized persons or operations, lowering the risk of possible attacks. Access may be restricted depending upon roles assigned to users, two-factor authorization implemented, and along with the strong password restrictions enforced. Access control, used in combination with other safety precautions, can dramatically minimize the probability of ransomware attacks from happening and limit the damage if the attack happens anytime.

As a summary, defending against ransomware attacks is an important consideration for businesses and individuals throughout the entire globe. Companies can more effectively protect themselves from the devastating effects of ransomware attacks by following the recommendations and adopting a multi-layered security plan which is proposed.

References

Kelley, K. (2022, December 8). *What is Cybersecurity and Why It is Important?* Simplilearn. Retrieved January 4, 2023, from https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

Simoiu, C., Bonneau, J., Gates, C., & Goel, S. (2019). " I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)* (pp. 155-174).

Tailor, J. P., & Patel, A. D. (2017). A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control. *International Journal of Research and Scientific Innovation (IJRSI)*, *4*(6), 116-121. https://www.rsisinternational.org/IJRSI/Issue42/116-121.pdf

S. K. Shaukat and V. J. Ribeiro, (2018) "RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning," *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, pp. 356-363, doi: 10.1109/COMSNETS.2018.8328219.

Okpongete, F. (2022). Intelligent Endpoint-based Ransomware Detection Framework

Urooj, U., Al-rimy, B. A. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2022). Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. *Applied Sciences*, *12*(1), 172.

Mohammad, A. H. (2020). Ransomware evolution, growth and recommendation for detection. *Modern Applied Science*, *14*(3), 68. https://doi.org/10.5539/mas.v14n3p68.

Simoiu, C., Bonneau, J., Gates, C., & Goel, S. (2019). " I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)* (pp. 155-174).

Tailor, J. P., & Patel, A. D. (2017). A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control. *International Journal of Research and Scientific Innovation (IJRSI)*, *4*(6), 116-121. https://www.rsisinternational.org/IJRSI/Issue42/116-121.pdf