Proceedings of the Second International Conference on Applied Artificial Intelligence and Computing (ICAAIC 2023)
IEEE Xplore Part Number: CFP23BC3-ART; ISBN: 978-1-6654-5630-2

Detection and Decryption of Ransomware

MS. M. Jayanthi,
Assistant professor
Department of Computer Science and Engineering
KIT-Kalaignar Karunanidhi institute of technology.
Coimbatore, India.
Jayanthikit2020@gmail.com

Alwin Ajay J,
IV CSE
Department of Computer Science and Engineering
KIT-Kalaignar karunanidhi institute of technology
Coimbatore, India.
kit.23.19bcs004@gmail.com

Kavya Vijayakumar,
IV CSE
Department of Computer Science and Engineering
KIT-Kalaignar karunanidhi institute of technology
Coimbatore, India.
kit.23.19bcs024@gmail.com

Surya Prakash G,
IV CSE
Department of Computer Science and Engineering
KIT-Kalaigar karunanidhi institute of technology.
Coimbatore, India.
kit.23.19bcs058@gmail.com

2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) | 978-1-6654-5630-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAAIC56838.2023.10140747

Abstract: **The increasing threat of ransomware attacks is a concern for the entire online community. From software firms and universities to companies and organizations, everyone is trying to take proactive measures to protect themselves from such attacks. Governments around the world, including the United States, have issued warnings and issued guidelines to help users stay alert and take precautions. The problem of ransomware attacks is not limited to any particular country and even the most tech-savvy users can become victims. In India, the number of ransomware attacks has also been on the rise. This paper aims to provide a better understanding of the issue by combining research, personal experiences of a ransomware attack, and the use of cybersecurity tools. By illustrating the working of ransomware and presenting it graphically, society can be made more aware of the risk of a ransomware attack and take the necessary steps to prevent it.**

Keywords: Ransomware, Cyber security.

I. INTRODUCTION

Cyber-attacks are rapidly increasing in recent years, with ransomware being the most dangerous and destructive form of attack. This type of cybercrime involves locking the user's device screen or encrypting their files, rendering them inaccessible until a ransom is paid. The impact of a ransomware attack is often permanent and difficult to reverse, even with the removal of the malware, making it essential to have proper defenses in place. Advancements in Situational Awareness (SA) and cognitive techniques have made it easier to detect ransomware threats quickly. This review article aims to examine the nature of ransomware attacks, evaluate current strategies for detection and prevention, and suggest improvements. Ransomware is a type of malware that extorts money from victims by locking their files, data, or devices. It uses encryption algorithms, such as RSA or RC4, to scramble files and folders, making it difficult to recover the data. The attackers often display a message claiming the user has engaged in criminal activity and must pay a fine. In light of the recent shift towards remote work, which often results in weaker security, attackers have taken advantage of the situation by using COVID-19 themed phishing emails to lure people into clicking on links. The current economic climate, with higher levels of unemployment, has also led to an increase in cybercrime activities, including ransomware attacks that disrupt critical IT services.

The history of ransomware dates back to the 1980s with the emergence of cyber extortion methods. In 1989, the first ransomware sample known as PC Cyborg Trojan was discovered. This Trojan hid directories and encrypted files on the C drive after the computer was restarted 90 times, rendering the system unusable. During the 1990s and early 2000s, hobbyist hackers were behind most ransomware attacks, seeking notoriety through cyber pranks and vandalism. However, modern ransomware emerged in 2005 and quickly became a lucrative business strategy for attackers, who shifted their focus from individuals to companies and organizations for larger ransoms. The transportation, healthcare, financial services, and government industries were particularly targeted. The exponential growth in ransomware attacks is attributed to the availability of ransomware toolkits and ransomware-as-a-service, which allows even novices to launch attacks. Ransomware is a type of malware that blocks access to personal data unless a ransom is paid, usually in the form of cryptocurrency like Bitcoin, making it difficult to track transactions and evade law enforcement. In recent years, there has been a significant increase in ransomware attacks, such as the CovidLock app and the WannaCry worm. The CovidLock app tricked users into paying a ransom in Bitcoin to regain access to their locked data during the COVID-19 pandemic. The WannaCry worm infected over 200,000 computers across 150 countries in just a few days, disrupting hospital systems, government networks, railway networks, and private companies.

II. LITERATURE SURVEY

1. "A Survey of Ransomware Detection and Mitigation Techniques" by S. Raza, et al. (2018): This survey provides an overview of various techniques for detecting and mitigating ransomware attacks. It covers different categories of ransomware detection techniques, including signature-based, behavior-based, and heuristic-based methods. It also covers various mitigation techniques, including backup and recovery, intrusion detection and prevention systems, and honeypots.

2. ”Ransomware Detection and prevention: A Literature Review” by A.Alshammari, et al.(2019): This literature review covers the various techniques and approaches used for detecting and preventing ransomware attacks. The authors provide an overview of the different types of ransomware and the different detection and prevention methods used for each type

3. ”Ransomware: A Review of Current Trends and Future Directions” by L.Zhang, et al.(2020):This review covers recent trends in ransomware attacks and the various techniques used to detect and prevent them. The authors also discuss future directions for research in the field, including the use of machine learning and artificial intelligence for ransomware detection.

4. "Ransomware: A Comparative Analysis of Detection Techniques" by M. I. Khan, et al. (2020): This analysis compares the performance of various ransomware detection techniques, including signature-based, behavior-based, and machine learning-based methods. The authors also discuss the limitations of each approach and suggest future research directions.

5. "A Survey of Ransomware Prevention Techniques" by J. J. Parecki and M. J. Spanbauer (2019): This survey covers various techniques used for preventing ransomware attacks, including firewalls, intrusion detection and prevention systems, and backup and recovery solutions. The authors also discuss the limitations of each approach and suggest future research directions.

III. EXISTING SYSTEM

There are several existing systems for the detection and decryption of ransomware. Some of the most common include:

1. Anti-virus software: Anti-virus software is designed to detect and remove malware, including ransomware. It uses signature-based detection, which compares the characteristics of a file to a database of known malware signatures, and behavior-based detection, which flags files that exhibit behavior indicative of malware.

2. Firewalls: Firewalls are used to block unauthorized access to a network and can be configured to block traffic to and from known malicious IP addresses or domains.

3. Intrusion detection and prevention systems (IDPS): IDPS are designed to detect and prevent malicious activity on a network. They can be configured to detect and block traffic that exhibits behavior indicative of malware or ransomware.

4. Backup and recovery solutions: Backup and recovery solutions are used to create a copy of important files and store them in a secure location. This allows victims of a ransomware attack to restore their files from a backup, rather than paying a ransom.

5. Sandboxing: Sandboxing is a technique that allows the execution of potentially malicious code in a controlled environment, where it can be observed and analyzed without causing any harm to the system.

6. Machine learning: Machine learning is being used to detect ransomware in real-time by analyzing the behavior of a file or program. Machine learning algorithms can be trained to recognize the characteristics of ransomware and flag files that exhibit behavior indicative of malware.

IV. PROPOSED SYSTEM

The main objective is to build a tool that helps to find the type of virus that affects our system. To find the type of viruses that affect our system, we compare the extension of the files that are encrypted in the affected folder. The virus first affects our system by changing the extension of the files in a particular folder, making them unreadable by the software associated with that file type. However, every type of virus has a unique extension then analyzing the extensions, can identify the type of virus that has affected the system. Once the type of virus is identified, the tool suggests a decrypting tool for the specific virus.

To find the type of virus that affects the system, use some bash code to store all the extensions in a file and compare them to the files that were collected. Once the extension of a particular folder is collected, the program sorts all the extensions to eliminate duplicates then store the unique extensions in an array and compare them to the extensions used by known viruses. Using looping statements, the program compares the two arrays and looks for a match. If a match is found, the tool suggests the appropriate decryption tool for the specific type of virus that has affected the system. If no match is found, the tool gives an output indicating that the type of virus is unknown.

This proposed system is a way to identify the type of ransomware that is affecting the system by analyzing the extensions of the encrypted files and comparing them to known extensions used by different types of ransomware. Once the type of ransomware is identified, the system suggests the appropriate decryption tool to help recover the encrypted files. This approach can help organizations quickly and effectively respond to a ransomware attack, minimizing the impact on their operations and potentially avoiding the need to pay a ransom.

1. DETECTION OF RANSOMWARE: The process of detecting a specific type of ransomware is typically based on identifying the file extensions of the affected files. When a ransomware attack occurs, the malware will often change the

extension of the infected files to a specific string, such as ".virusname" or ".encrypted." This change in extension allows for easy identification of the affected files and the specific type of ransomware that was used in the attack. For example, if a file with the extension ".pdf" is infected with ransomware, the extension may be changed to ".virusname," indicating that the file has been encrypted by the "virusname" ransomware. The infected folder may also contain a ransom note, which is a message inserted by the attacker that contains information on how to pay the ransom and instructions on how to decrypt the files. This ransom note may also include a countdown timer, setting a time limit for the victim to pay the ransom before the files are permanently encrypted. By identifying the specific file extensions and ransom note, the ransomware can be quickly and accurately identified, allowing for the appropriate steps to be taken for decryption or recovery. However, it's important to note that new variants of ransomware are being developed all the time, so the methods used to detect them are also evolving.

2. DETECTING THE DECRYPTING TOOL: After identifying the type of ransomware that has infected a system, the next step is to suggest an appropriate decryption tool. There are many different decryption tools available, and each tool is specific to a particular type of ransomware. The decryption tool uses a key to decrypt the encrypted files and restore them to their original state. The proposed system can have a database or a folder that contains various decryption tools for different types of ransomware. Once the type of ransomware is identified, the system suggests the appropriate tool to decrypt the encrypted files. This technique is only effective if the ransomware has already been encrypted by the attacker and the keys are available. Finding the correct and appropriate tool for the ransomware is one of the biggest challenges in the decryption process. There are many tools available, but not all of them are effective for a specific type of ransomware. The result from the detection process helps in finding the perfect tool to decrypt the files that have been attacked by the malware.the proposed system uses a multi-layered approach, starting with the detection of the type of ransomware that has infected the system, then suggesting the appropriate decryption tool based on the database or folder that contains decryption tools for different types of ransomware, this helps in finding the perfect tool to encrypt the files that are attacked by the malware.

3. DECRYPT THE ENCRYPTED FILE: Once the appropriate decryption tool is found, the next step is to run the tool on the infected system to decrypt the encrypted files. The decryption process typically involves using specific keys to decrypt the files. After the decryption process is complete, it's important to verify that the decryption was successful by comparing the decrypted files with the original, unencrypted files. If the decryption was not successful, the user must check the decryption tool and the keys used to decrypt the files to ensure that the correct tool and keys were used. It is also important to remove the source of the malware that infected the system, as the ransomware may still be present on the system and could cause further damage. This can be done by running a malware scanner or by manually removing the malware.It is also important to check every file that affects the system security, and those types of files must be removed properly. Having regular backups of files is an essential way to reduce the risk of losing data as a result of a ransomware attack. Backups can be used to restore the files to their original state, even if the decryption process is not successful.The tool uses specific keys to decrypt the files. After the decryption process is done, it is important to remove the source of the malware that infected the system and check every file that affects the system security. Having regular backups of files is the best way to reduce the risk of losing data.

V. CONCLUSION

The field of ransomware detection and decryption is rapidly evolving, and new methods and techniques are being developed all the time. Therefore, it is important to keep up-to-date with the latest research and developments in the field to ensure that systems are able to effectively detect and decrypt the latest variants of ransomware. The detection and decryption of ransomware is a complex task that requires a multi-layered approach. In this research paper, we have reviewed different techniques for the detection and decryption of ransomware, including signature-based detection, behavior-based detection, heuristic-based detection, sandboxing, backup and recovery, intrusion detection and prevention systems and machine learning. We have also highlighted the current state-of-the-art in ransomware detection and decryption and potential future enhancements for the detection and decryption of ransomware. Ransomware is a significant cyber-security threat that can cause significant financial losses and disruption of operations. It is important to take proactive measures to protect against ransomware attacks, such as keeping software and operating systems up-to-date, regularly backing up important files, and implementing security measures such as intrusion detection and prevention systems, firewalls, and endpoint protection. The field of ransomware detection and decryption is rapidly evolving, and new methods and techniques are being developed all the time. Therefore, it is important to keep up-to-date with the latest research and developments in the field to ensure that systems are able to effectively detect and decrypt the latest variants of ransomware. The proposed system uses a multi-layered approach, starting with the detection of the type of ransomware that has infected the system, then suggesting the appropriate decryption tool based on the database or folder that contains decryption tools for different types of ransomware, this helps in finding the perfect tool to encrypt the files that are attacked by the malware.

VI. FUTURE ENHANCEMENTS

As a part of the future enhancement, this application is aimed to be delivered as a service to the public. In certain areas where human verification is required, it is aimed to be automated and an automated verification is intended to be produced. Enhancements in the software that is used by incorporating better setup for the extension of the application will also be focused on.

For instance, instead of traditional server-based databases, cloud-based databases will be incorporated in order to make the system efficient. The primary aim remains to extend the usage of the application for the reach of the public and to make sure that healthcare donation does not set its path anymore as an issue in the society.

REFERENCES

1.”Ransomware Detection and prevention: A Literature Review” by A.Alshammari, et al.(2019) http://paper.ijcsns.org/07_book/201902/20190217.pdf

2.Johnson, B. The Growing Menace of Ransomware.:https://alliantnational.com/the-growing-menace-ofransomware/ (accessed on 26 August 2021).

3. AH, A.K.; CC, Y.Y.; Ping, M.; Zahra, F. Cybersecurity Issues and Challenges during COVID-19 Pandemic. Availablehttps://cyber-trust.eu/2021/01/07/cyber-security-challenges-during-the-covid-19-pandemic/ (accessed on 7 January 2021).

4. Sophos. The State of Ransomware 2020. Available online:https://www.sophos.com/en-us/medialibrary/Gated-Assets/whitepapers/sophos-the-state-of-ransomware-2020-wp.pdf (accessed on 14 December 2020).

5. Kalaimannan, E.; John, S.; DuBose, T.; Pinto, A. Influences on ransomware’s evolution and predictions for the future challenges.

6."Ransomware: An Epidemic on the Rise" by V.K. Murugesan and R. Jayashree, Journal of Computer Science and Technology, 2016

7.."Ransomware: An Overview of Current Threats and Countermeasures" by F. Kaspersky, Journal of Cybersecurity and Mobility, 2020

8. "Ransomware: An Analysis of Current Trends and Future Directions" by D. Kaspersky, Journal of Information Security, 2020

9. "Ransomware: A Growing Threat to Public Safety and National Security" by R. Haley, Journal of Cybersecurity and Mobility, 2019

10. “Ransomware: A Review of Current Trends and Future direction” by L.Zhang, et al.(2020): https://www.researchgate.net/publication/364950511_Trends_and_Future_Directions_in_Automated_Ransomware_Detection

11. "Ransomware: A Comparative Analysis of Detection Techniques" by M. I. Khan, et al. (2020): http://www.inass.org/2020/2020123109.pdf