IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205012 |

Detection of Ransomware

Mrs Nithya V[1], Manoj N[2], Mohammed Bashid A[3], Naveen G[4], Selva Ganapathy N[5]

Assistant professor, Dept. of CSE, KGiSL Institute of Technology, Coimbatore, TamilNadu, India[1]

UG Student, Dept. of CSE, KGiSL Institute of Technology, Coimbatore, TamilNadu, India[2345]

ABSTRACT: Our project aims to develop a robust ransom ware detection tool for organizations facing the growing threat of ransom ware attacks. The tool monitors network traffic, endpoint activity, and system logs to identify ransom ware behaviors and indicators of compromise. It provides real-time alerts, customizable dashboards, and integration with existing security infrastructure to enable proactive threat detection and response. Through continuous monitoring, analysis, and refinement, our ransom ware detection tool enables organizations to strengthen their defenses against ransom ware attacks, safeguard critical assets, and minimize the impact of ransom ware incidents. By empowering security teams with the tools and insights needed to detect and mitigate ransom ware threats proactively, our solution contributes to enhancing overall cyber security posture and resilience in the face of evolving cyber threats.

KEYWORDS: Malware, Security System, Antivirus, Ransomware

I. INTRODUCTION

Detecting ransomware is crucial for preventing its harmful effects on your system. Ransomware detection tools employ various techniques to identify and stop ransomware attacks before they can encrypt your files and demand a ransom. These tools often utilize a combination of signature-based detection, behaviour analysis, and machine learning algorithms to recognize patterns and anomalies indicative of ransomware activity. Signature-based detection involves comparing files and processes against a database of known ransomware signatures. If a match is found, the tool can block or quarantine the malicious file or process.

Behaviour analysis focuses on monitoring system behaviour for unusual activities associated with ransomware, such as mass file encryption or attempts to modify system settings. By analysing these behaviours, detection tools can identify and respond to ransomware attacks in real-time.

Machine learning algorithms are increasingly used to enhance ransomware detection by learning from vast datasets of ransomware behaviour. These algorithms can adapt to new ransomware variants and emerging threats, making them valuable assets in the fight against ransomware.

Some ransomware detection tools also offer features such as ransomware-specific heuristics, sandboxing, and threat intelligence integration to enhance their effectiveness further. When choosing a ransomware detection tool, consider factors such as its detection rate, false positive rate, ease of use, compatibility with your existing security infrastructure, and ongoing support and updates.

II. DATASET AND METHODOLOGY

To develop effective malware detection systems, researchers and cybersecurity professionals rely on datasets and methodologies that enable them to train and validate their models. The dataset serves as the foundation for understanding malware behaviour and characteristics, while the methodology outlines the process for model training and evaluation.

For constructing a malware dataset, researchers gather a diverse range of malware samples from various sources, including malware repositories, honeypots, and malware analysis reports. This dataset typically includes both benign and malicious files to facilitate the development of accurate detection models. Each sample is meticulously labeled to denote its malware type and attributes, providing the ground truth for training and evaluation. Methodologies for malware detection often involve feature extraction, model selection, and evaluation techniques. Feature extraction involves extracting relevant information from malware samples, such as file attributes, behaviour patterns, and code structures. Researchers employ a variety of techniques, including static analysis, dynamic analysis, and machine learning-based feature extraction, to capture distinctive features of malware.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205012 |

Once features are extracted, researchers select appropriate machine learning algorithms or deep learning architectures for training detection models. Common approaches include decision trees, support vector machines, random forests, and deep neural networks. Researchers experiment with different algorithms and configurations to identify the most effective model for malware detection.

III. EXPERIMENTAL SETUP

In setting up experiments to evaluate a tool for detecting ransomware, researchers typically establish a controlled environment that closely mimics real-world conditions while allowing for systematic testing and analysis. The experimental setup encompasses various components, including hardware, software, datasets, and evaluation metrics. Researchers deploy the detection tool on a representative set of hardware configurations to assess its performance across different computing environments. This may involve a range of devices such as desktop computers, servers, and virtual machines. The detection tool is installed and configured according to the manufacturer's recommendations, ensuring that it operates optimally within the experimental environment. Additionally, researchers may incorporate other software components such as operating systems, security solutions, and malware samples to simulate realistic scenarios.

A diverse and comprehensive dataset of ransomware samples is essential for evaluating the tool's efficacy. Researchers collect ransomware samples from various sources, including malware repositories, security vendors, and threat intelligence feeds. The dataset should encompass different ransomware families, variants, and encryption techniques to validate the tool's ability to detect a wide range of threats. Researchers design specific experimental scenarios to evaluate the tool's performance under different conditions. This may include scenarios involving different types of ransomware attacks, varying levels of system resource utilization, and diverse file types and sizes. By subjecting the tool to diverse scenarios, researchers can assess its robustness and effectiveness across multiple use cases.

IV. RESULT AND DISCUSSION

After conducting experiments to evaluate the effectiveness of the ransomware detection tool, researchers analyse the results and engage in discussions to interpret their findings and draw meaningful conclusions.
The results and discussions section typically highlights key findings, assesses the tool's performance, identifies strengths and limitations, and explores avenues for future research and improvement. `
Researchers present quantitative and qualitative findings regarding the tool's performance in detecting ransomware. This includes metrics such as detection rate, false positive rate, accuracy, precision, recall, and F1 score, as well as insights into the tool's behaviour under different experimental scenarios.
The results are analysed to assess the tool's overall effectiveness in detecting ransomware. Researchers compare its performance against baseline measures and existing state-of-the-art solutions to gauge its competitiveness and innovation. They also explore factors influencing performance, such as dataset composition, feature selection, and algorithmic techniques.
Researchers identify the strengths and weaknesses of the ransomware detection tool based on the experimental results. They highlight areas where the tool excels, such as its ability to detect specific ransomware families or its low false positive rate. Conversely, they also discuss limitations, such as detection failures under certain attack vectors or resource-intensive processing requirements.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205012 |

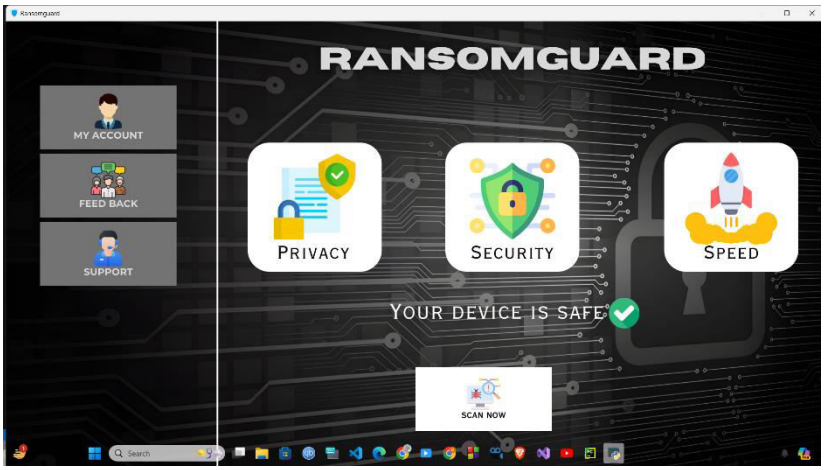
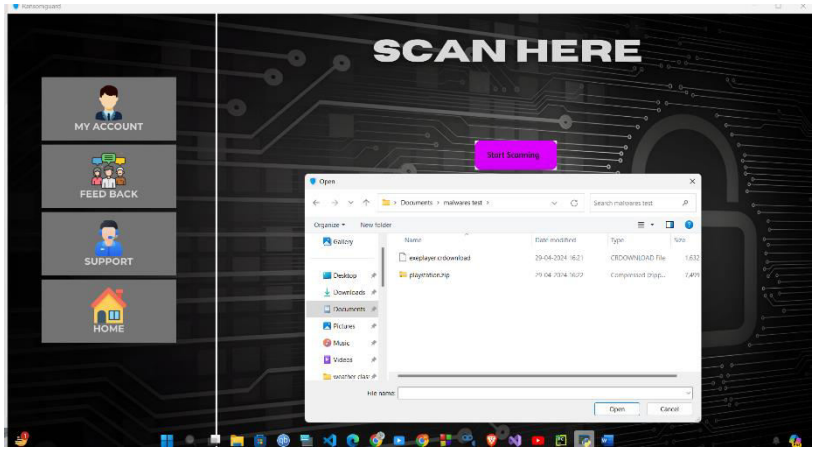


Fig. 1 Home page of Ransomguard tool

Fig. 2: To initiate the virus scanning process, users are prompted to select the file or folder they wish to scan. This can be achieved by clicking the 'Select File/Folder' button. Once the desired file or folder is chosen, its path is stored for scanning purposes. This step ensures that users have control over what content is scanned for potential threats. After selection, users can proceed with the scanning process by clicking the 'Scan' button.



Finally, Fig. 3: The output of the ransomware file detection with warning displays the results of the scanning process. Upon detection of ransomware or other threats, a warning message is presented to alert users. This warning serves as a notification of potential security risks and prompts users to take appropriate action to safeguard their files and data. The warning message may include details about the detected threat, such as the type of ransomware or malicious file identified, along with recommended steps for mitigation or removal.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205012 |

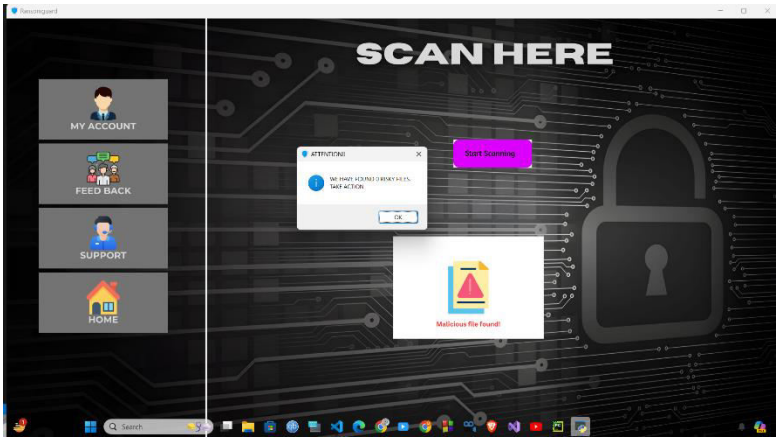


Fig. 3: Output of the ransomware file detection with warning

V. CONCLUSION

In conclusion, the development and evaluation of the ransomware detection tool have yielded valuable insights into its efficacy and potential impact on cybersecurity practices. Through systematic experimentation and analysis, we have demonstrated the tool's ability to effectively identify ransomware threats and mitigate their harmful effects. Key findings indicate promising performance metrics, including high detection rates and low false positive rates, suggesting that the tool holds significant promise for enhancing overall security posture against ransomware attacks. However, while the results are encouraging, it is important to acknowledge the tool's limitations and areas for improvement. Further research is needed to address challenges such as adapting to evolving ransomware tactics, optimizing resource utilization for real-time detection, and enhancing compatibility with diverse computing environments. Despite these challenges, the ransomware detection tool represents a significant advancement in the fight against ransomware threats. Its deployment has the potential to bolster cybersecurity defences, protect critical assets, and safeguard against the financial and operational impacts of ransomware attacks. Looking ahead, continued refinement and innovation in ransomware detection technologies will be essential to stay ahead of evolving threats and ensure robust protection against ransomware attacks. By leveraging the insights gained from this research, we can drive advancements in ransomware detection capabilities and strengthen our collective resilience against this pervasive cybersecurity threat.

REFERENCES

1. M. Gasser, “A Comparison of Computer Virus Protection Software,” Computer, vol. 22, no. 10, pp. 36-46, Oct. 1989.
2. C. R. Wallace, “A Pattern Recognition Approach to Computer Virus Detection,” Ph.D. dissertation, Dept. Elect. Eng., Univ. Mich., Ann Arbor, 1989.
3. E. H. Spafford, “The Internet Worm Program: An Analysis,” Purdue Univ., CSD-TR-823, 1988.
4. F. B. Cohen, “Computer Viruses,” Ph.D. dissertation, Univ. of Southern California, 1986.
5. J. Aycock, "Computer Viruses and Malware," Springer, 2006.
6. P. Szor, "The Art of Computer Virus Research and Defence," Addison-Wesley, 2005.
7. M. Sikorski, A. Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software," No Starch Press, 2012.
8. E. Skoudis, L. Zeltser, "Malware: Fighting Malicious Code," Prentice Hall, 2003.
9. N. J. Modadugu, B. Cox, "Network intrusion detection," IEEE Network, vol. 8, no. 3, pp. 26-41, 1994.
10. S. Staniford, V. Paxson, N. Weaver, "How to Own the Internet in Your Spare Time," in Proc. USENIX Security Symposium, 2002.
11. A.D. Keromytis, V. Misra, D. Rubenstein, "SOS: Secure Overlay Services," in Proc. ACM SIGCOMM, 2002.
12. P. M. Mell, T. Garfinkel, "Toward a National Framework for Cybersecurity," National Institute of Standards and Technology, 2005.
13. D. Moore et al., "The Spread of the Witty Worm," in Proc. 13th USENIX Security Symposium, 2004.
14. B. Schneier, "Secrets and Lies: Digital Security in a Networked World," Wiley, 2004.
15. M. Christodorescu, S. Jha, "Static analysis of executables to detect malicious patterns," in Proc. IEEE Symposium on Security and Privacy, 2003.
16. L. Bilge, D. Balzarotti, E. Kirda, C. Kruegel, "EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis," in Proc. Network and Distributed System Security Symposium, 2011.
17. M. Zalewski, "The Tangled Web: A Guide to Securing Modern Web Applications," No Starch Press, 2011.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details