2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS) | 979-8-3503-4023-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICACRS58579.2023.10404203

Targeted Ransomware Attacks and Detection to Strengthen Cybersecurity Strategies

Chinmaya B J
Artificial Intelligence and Machine Learning Engineering
RV College of Engineering®
Bengaluru, India

Sujay Arun Kudtarkar
Artificial Intelligence and Machine Learning Engineering, RV College of Engineering® Bengaluru, India

Mohana
Computer Science and Engineering (Cyber Security)
RV College of Engineering®
Bengaluru, India
mohana@rvce.edu.in

Abstract— **Ransomware attacks have emerged as the most trending malware in recent eras. Ransomware attacks hold data and devices hostage until a ransom is paid. The proposed methodology involves virtual or practical demonstration of ransomware attacks using tools like TeamViewer and 7z, aiming to raise awareness on cybercriminal tactics. The main objective is to educate and empower individuals and organizations to protect against such threats. HostedScan, with its robust features, efficiently detects and categorizes risks, providing actionable insights to prioritize security efforts. Detailed reports sent to registered emails include information on risk levels, vulnerabilities, IPs, ports, and hostnames, enabling proactive system and data protection. This work promotes cybersecurity awareness, fostering proactive defense and helping users to mitigate the risk of ransomware and other cyber threats.**

Keywords— Ransomware, Malware, Vulnerabilities, Cybersecurity, TeamViewer, Hostname, Targeted Ransomware.

I. INTRODUCTION

Ransomware presents a significant threat in the digital realm, creating substantial financial and data security challenges for individuals and organizations. This study delves deeply into ransomware, employing simulation techniques and online threat assessment tools to enhance comprehension of its dangers and promote heightened cybersecurity awareness. The proposed methodology involves the utilization of TeamViewer and 7z to conduct ransomware attack simulations. These simulations offer practical demonstrations of how such attacks can compromise data and systems. The main objective is to clarify the inner workings of ransomware and the potential consequences, emphasizing the critical nature of taking preventive measures as soon as possible. Additionally, HostedScan, a widely recognized online scanning tool, is employed to assess the ransomware threat landscape and educate users on protecting their digital assets. HostedScan provides a valuable platform for individuals and organizations to measure their vulnerability to ransomware and proactively engage in risk mitigation. In this research study, the ransomware simulations are carefully analyzed to reveal the tactics employed by ransomware cyber criminals and the vulnerabilities they exploit. Additionally, HostedScan is presented, explaining its functionalities, capabilities, and how it provides essential insights to users concerned about ransomware threats. Also, the literature survey provides a critical step in shaping the direction and quality of research endeavors. Proposed research contributes to the growing body of knowledge about preventing and detecting ransomware. It equips individuals and organizations with practical insights and tools to strengthen their cybersecurity defenses. In a landscape where ransomware is constantly changing and evolving, taking proactive measures and being highly aware is crucial to protect the digital realm. Also. to empower individuals and organizations to enhance their defenses against this formidable adversary.

II. LITERATURE SURVEY

S. R. B. Alvee *et al* [1] introduces a method for extensive malware analysis through hashed matrix feature extraction and automated signature creation using Bayesian signature selection within clusters. While it offers efficient speed and accuracy, it relies on complex mathematics, makes assumptions about data distribution, and may face scalability issues with large datasets. G. Usha *et al* [2] suggests a framework for dynamic malware analysis with real-time monitoring and resource tracking. It tackles challenges posed by packed malware, with three key processes: runtime analysis, resource monitoring, and behaviour definition. However, the primary issue lies in effectively disassembling heavily packed malware codes. K. Thummapudi *et al* [3] This research study explores the lifecycle and analysis of Windows-based ransomware, tracking its evolution. It employs MD5 and Cuckoo Sandbox for malware analysis, while RSA and AES are used for encryption. The primary goal is ransomware detection through monitoring abnormal file system and registry activities, emphasizing the importance of incremental online and offline data backups to prevent data loss. S. Alzahrani *et al* [4] CryptoDrop employs Teslacrypt, CTB-Locker, and GP code for ransomware detection, aiming to counter this nuisance. Instead of paying ransoms, it prevents ransomware execution, minimizing loss to a median of just 10 files and rendering the malware ineffective. S. Lee *et al* [5] demonstrated ransomware prevention method for the Android platform, consisting of three modules: Configuration, Monitoring, and Processing. The method effectively monitors file events when ransomware accesses and copies files and categorizes ransomware into Scareware, Lock-Screen, and Encrypting.

E. Berrueta *et al* [6] To mitigate ransomware risks, this approach employs Remote Desktop Protocol (RDP) and Software Restriction Policies (SRP). Ransomware poses a threat to various sectors, including home users, businesses, and government networks, potentially resulting in the loss of sensitive data. F. M. Alotaibi *et al* [7] HelDroid is an automated system for identifying both known and unknown scareware and ransomware in mobile applications. It focuses on detecting threats to users, device locking, and data encryption. It uses a classifier with Natural Language Processing (NLP) features, lightweight emulation to spot locking strategies, and ruin tracking to detect file-encrypting behaviours. HelDroid excels in identifying unknown ransomware samples. S. Sibi Chakkaravarthy *et al* [8] Ransomware operates in five phases. through five phases. The key to Défense against ransomware lies in preparedness and the capability to detect, shut down, and contain suspicious activities effectively. Daryle Smith *et al* [9] This research study discusses ransomware detection frameworks, highlighting various ML algorithms. Machine learning approaches outperform traditional methods, showing promising results in ransomware detection. M. Al-Hawawreh *et al* [10] emphasizes the need for external cyber threat intelligence, internal data integration, and advanced analysis to identify abnormal patterns and combat both known and new ransomware attacks. The study examines prior research on Cyber Threat Intelligence (CTI) and CTH, highlighting their limitations and gaps. This research study underscores the importance of developing effective CTH techniques capable of detecting both known and unknown ransomware threats.

I. Kara *et al* [11] employs methods like Inbound traffic analysis, detection of DDoS activities, and direct attacks, using Snort software as a tool. It utilizes two sniffers, implemented with open-source Snort, for malware detection. The primary objective is to develop a practical network protection solution by investigating the feasibility of analyzing outbound traffic. It notes that Sniffer-2, with more rules in its database, takes longer for analysis compared to Sniffer-1. N. Aldaraani *et al* [12] Honeypot operations involve setting up deceptive resources to entice malware, allowing for monitoring of their behaviour. The access router serves as both a DHCP server and DNS server, with IP assignments that generate minimal ARP traffic. M. Alam *et al* [13] explores ransomware detection using an Intrusion Detection Honeypot system, introducing the innovative "Social Leopard" algorithm inspired by collective behaviour in IoT environments. It mimics how leopards cooperate in nature to catch prey. While this concept is intriguing, scaling it for numerous devices may pose challenges and could potentially misinterpret harmless actions as attacks. M. Baykara *et al* [14] focuses on crypto-ransomware detection techniques, analyzing 63 ransomware samples from 52 families. It categorizes input data sources and timing for detection algorithms and classifies them based on input parameters and classification methods. Machine learning is popular, but evaluation results are limited and challenging to compare, highlighting a need for more reproducible research in security. The survey concludes by addressing open issues in ransomware detection to encourage better research and algorithm validation in this field. H. Madani *et al* [15] examines the Conti ransomware's leaked source code, revealing its advanced techniques and evasion strategies. It analyses the code's structure, anti-detection mechanisms, encryption method, and API obfuscation. The concern is the potential for other ransomware groups to adopt Conti-like tactics. Future research will delve into Conti's internal operations and develop a detection system tailored to Conti-like ransomware based on the findings.

The impact of ransomware attacks on organizations using data from 55 cases across the UK and North America. It finds organizations significantly affect attack severity, with private sector entities facing more severe consequences and weaker security postures leading to harsher outcomes. Targeted attacks are more damaging than opportunistic ones. Factors like organization size, attack type, and target do not significantly influence attack severity. The study highlights the importance of cybersecurity measures, particularly for private organizations, and introduces terminology and assessment tools to aid in understanding ransomware's impact. Ransomware surged in early 2023, targeting manufacturing and professional services. The US was the top target, and mid-sized companies were often hit. Key ransomware groups included LockBit, AlphaVM, and Black Basta. Encryption-less attacks rose, and many victims were susceptible due to poor security practices, including weak email configurations and outdated systems.

Early detection of threats, for response- The baddies can see troubles early and respond to them in a timely manner by getting real-time information on evolving risks via a threat intelligence feed. In this respect, this tool gives organizations the potential to identify and react to potential threats as soon as possible; thus, minimizing damage and mitigating the effects of ransomware attacks.

Developing a response plan based on TTP- Ransomware attackers' tactical techniques are explained through threat intelligence. By doing that, teams can create tailored response plans for different types of attacks that are classified according to their features.

Proactive mitigation of vulnerabilities- Organizations can identify and deal with vulnerabilities before they become known if they use threat intelligence. In this regard, the application of such an approach increases the cyber defences, reduces the chances of being attacked, and shows dedication towards risk elimination.

III. DESIGN AND IMPLEMENTATION

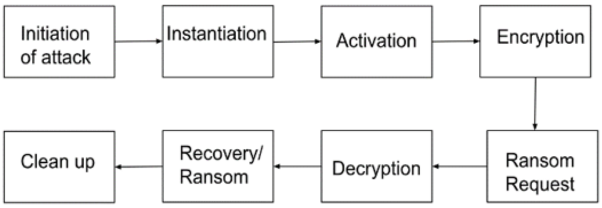


Fig.1. Block diagram of implementation

Figure 1 shows the block diagram of implementation methodology. It starts with the initiation of the attacks which includes planning the process and the steps to be taken if anything goes wrong. Then comes Instantiation which is the beginning of this master plan. This is where social engineering comes in place to convince the users of the next phase. Activation is where you install the software on the target's computer and have him give the target's ID and password for remote access. then move into the main stage which is inputting malicious payload into the target's computer for the ransomware to take control. This is where this study uses the 7z zip file and AES-256 encryption algorithm to safeguard confidential data. Now come to the ransom note/ ransom request. Where, after encryption, a ransom note is displayed to the victim demanding ransom payment usually in the form of cryptocurrency as transactions are impossible to trace back to the user by means of cryptocurrency. Here also mention a time limit in the ransom note, so that they feel compelled to take immediate decision or all their files will be lost. After ransom payment and confirmation of the amount received, then move on to the decryption stage where the attacker provides the targetted user a decryption key to get all the files back. Post-attack activity includes recovery and clean-up. It is important that the attacker should not leave any traces, as the targetted computer will be sent to cyber security professionals after the attack. From the victim's perspective, He should first report to the cyber police and send his laptop for inspection for any clues regarding the attacker.

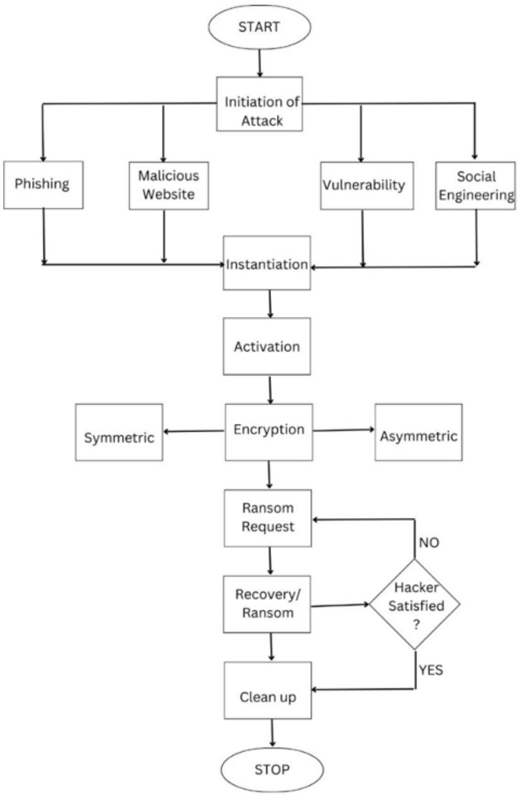
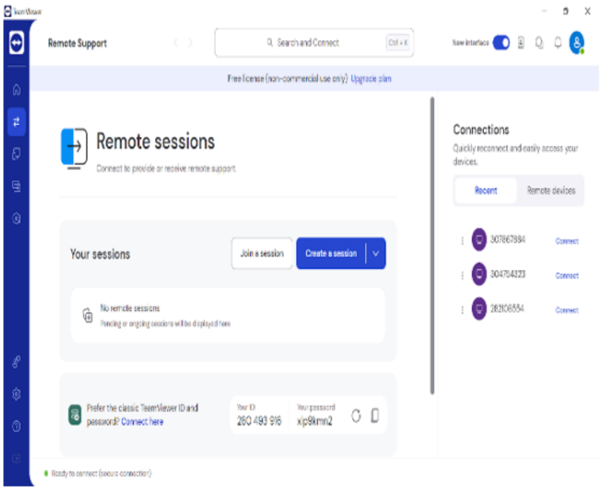


Fig. 2. Detailed Flowchart of implementation

Figure 2 shows a detailed flowchart of design and implementation from selecting the type of social engineering to whether the attacker wants to repeat the attack or not. We can choose several social engineering hacks to convince the user such as Phishing, Malicious Websites, and Vulnerability messages (based on the victim's personal data a curated message can be created to force the victim). For the encryption stage, there are two main ways to handle this, symmetric encryption and asymmetric encryption. Symmetric encryption makes it a faster encryption method than asymmetric where there exist 2 separate keys for encryption and decryption. We have a loop here in the flowchart which depicts the greediness of the attacker. The attacker can choose to play with the victim even after the decryption until he/she is satisfied. Lastly, we come to the cleanup stage where the victim has to avoid any kind of attacks like these in the future because even after decryption, the victim's computer still remains compromised.

IV. SIMULATION RESULTS AND ANALYSIS

Proposed implementation simulated primary version of the ransomware attack by using tools such as TeamViewer for accessing a targeted computer remotely and 7z file for encryption of the files once gain access to desired computer. The purpose of this demonstration is to shed light on the harmful tactics implemented by cybercriminals all over the world and to underline the importance of cybersecurity awareness. By this simulation, this study aimed to educate and empower individuals and organizations to protect and safeguard themselves against such threats. Let's now dwell on understanding this better with images that portray the usage of TeamViewer and 7z software.


TeamViewer

Remote Support

Search and Connect Ctrl + K

New Interface

Free license (non-commercial use only) Upgrade plan

Remote sessions

Connect to provide or receive remote support

Your sessions

Join a session

Create a session

No remote sessions

Pending or ongoing sessions will be displayed here

Prefer the classic TeamViewer ID and password? Connect here

Your ID: 280 493 916

Your password: xip9kmn2

Connections

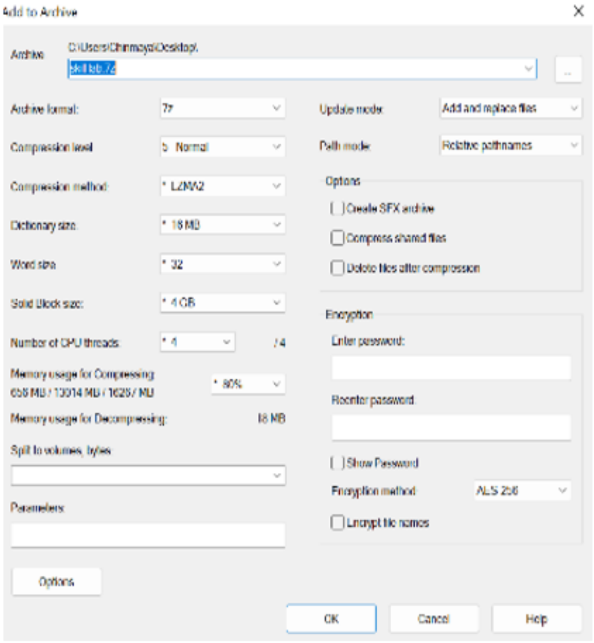
Quickly reconnect and easily access your devices.

Recent | Remote devices

307867884 Connect
304754323 Connect
282106554 Connect

Ready to connect (secure connection)

Fig. 3. Starting a Remote Session



Archive: C:\Users\Chinmaya\Desktop\ skill lab.7z

Archive format: 7z

Compression level: 5 - Normal

Compression method: * LZMA2

Dictionary size: * 16 MB

Word size: * 32

Solid Block size: * 4 GB

Number of CPU threads: * 4 / 4

Memory usage for Compressing: 656 MB / 13014 MB / 1625 / MB * 80%

Memory usage for Decompressing: 18 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

□ Create SFX archive

□ Compress shared files

□ Delete files after compression

Encryption

Enter password:

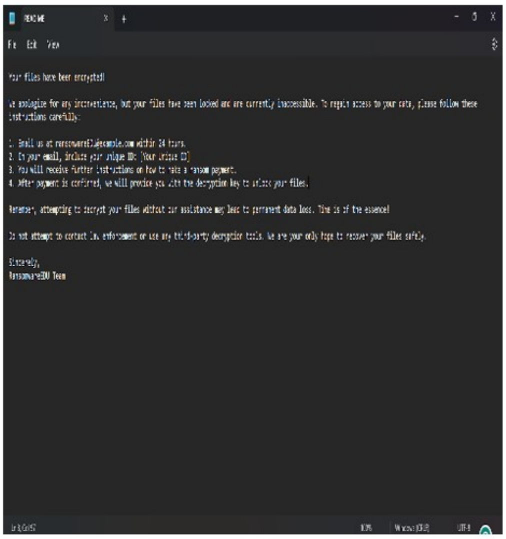
Reenter password:

□ Show Password

Encryption method: AES-256

□ Encrypt file names

Fig. 4. Setting an encryption



Your files have been encrypted!

We apologize for any inconvenience, but your files have been locked and are currently inaccessible. To regain access to your data, please follow these instructions carefully:

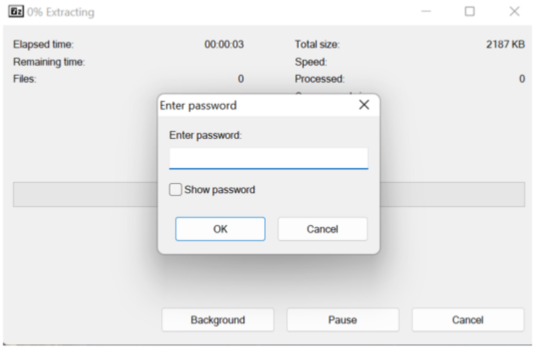
1. Email us at ransomwareEDU@example.com within 24 hours.
2. In your email, include your unique ID: [Your Unique ID]
3. You will receive further instructions on how to make a ransom payment.
4. After payment is confirmed, we will provide you with the decryption key to unlock your files.

Remember, attempting to decrypt your files without our assistance may lead to permanent data loss. Time is of the essence!

Do not attempt to contact law enforcement or use any third-party decryption tools. We are your only hope to recover your files safely.

Sincerely,
RansomwareEDU Team

Fig. 5. Sending a Ransom note



Elapsed time: 00:00:03

Remaining time:

Files: 0

Total size: 2187 KB

Speed:

Processed: 0

Enter password

Enter password:

□ Show password

Fig. 6. User fails to access files.

Figure 3 to 6 shows the detailed steps of implementation details.

Establishing Remote access with TeamViewer - By means of social engineering, install the TeamViewer application on the target computer. Install TeamViewer on the computer and ensure that both computers have a stable internet connection. Obtain the ID and password of the target computer by convincing the targeted user. Click the connect button on the controlling computer and you have successfully established a remote connection.

Encrypting Files using 7z Compression and encryption- Locate target files or the folders you need to encrypt, right-click on the folder and select more options, then select 7z zip, and finally select “add to archive”. A white window will appear as shown in the picture above. Select all the checkboxes in the options section, enter your desired password and click OK. Now the selected files are encrypted and can only be accessed with the password you have given.

Ransomware note display - Following the successful encryption of files, add a ransomware note on the victim's desktop. This note is designed to evoke a sense of urgency and fear, demanding a ransom payment in cryptocurrency in exchange for the decryption key. This particular image drives home the devastating impact of ransomware attacks. Collectively the above steps serve as a powerful teaching tool for understanding the steps involved in such attacks and the critical need for proactive cybersecurity measures.

Using modern technology such as advanced threat Intelligence to collaborate with interested peers in the industry and stay updated on the latest attack tactics. Machine learning and AI have significantly leveraged pattern identification regarding ransomware attacks, avoiding attacks and hence improving performance. This helps keep the user safe from an attack that has never occurred before. Continuous monitoring of network traffic, system logs and user activity to quickly find out and respond to uncommon behavior also keeps the user’s system at high speed.

One key factor for achieving reliability is to maintain constant backup and recovery and to make sure that data is stored in a secure and reliable place. Implementing SIEM (Security Information and Event Management) to analyze relevant data and to detect signs of unusual activity. Deploying advanced end-point protection with endpoint detection and response (EDR) is useful for monitoring real-time achieving high levels of reliability.

V. REAL TIME IMPLEMENTATION CHALLENGES

The potential reasons for the challenges faced when using HostedScan or any vulnerability assessment method can be multifaceted. Several factors may contribute to its shortcomings. First, incomplete coverage of vulnerabilities in the tool's database can lead to missed threats, especially if it lacks updates or fails to recognize newly discovered vulnerabilities. Second, high rates of false positives or negatives can hinder efficiency and require continuous fine-tuning of detection algorithms and result validation. Additionally, the limited scope of the tool, misconfigurations, or reliance on outdated signatures can compromise the assessment's accuracy. Compatibility issues, resource constraints, and inadequate remediation guidance can also impact its effectiveness. Lastly, the rapidly evolving threat landscape demands constant vigilance and adaptation. Success in vulnerability assessment relies on a combination of factors, including proper configuration, resource allocation, and integration with an organization's cybersecurity strategy. Educating and

Training users often dealing with sensitive data to learn and adapt methods of precaution to avoid cyberattacks. Using e-mail authentication tools such as DMARC and SPF to prevent spoofing and phishing attempts is also a prominent method. This research study should make sure to Ensure very few people have key access to perform tasks and change the system data, therefore implementing the principle of least privilege [16] [17] [18].

Behavioral Anomaly Detection-Implementing behavioral analysis allows for the identification of anomalies(abnormality) in the model's predictions and user interactions. By continuously monitoring the unexpected patterns in the system or program, the system can detect potential ransomware attacks based on deviations from normal behavior [19].

Continuous Model Training-Regular updates and continuous training of machine learning models are crucial to adapt to evolving ransomware threats. This ensures that the models are equipped and adapted to recognize new patterns associated with ransomware attacks, improving their overall detection capabilities and their efficiency towards detection.

Ensemble Models for Improved Detection-The use of ensemble models, which combine multiple machine learning algorithms or models, enhances the overall robustness of the system. This approach leverages the strengths of different algorithms, making it more difficult for attackers to escape detection and increase the accuracy of identifying ransomware threats.

VI. APPLICATIONS

Creating applications for ransomware simulations is an effective way to educate organizations and individuals about it. Here are some applications for ransomware simulation:

Penetration Testing and Vulnerability Assessment-Organizations hire white hat hackers to conduct controlled ransomware simulations as part of penetration tests. This helps to identify vulnerabilities in their systems, networks, and processes. By providing a comprehensive list of security threats and weaknesses, it is essential for keeping software up-to-date and secure. They provide a documented record of the organization's security efforts and history. This demonstrates compliance with the current security standards and regulatory requirements.

Security Awareness Training - One of the primary applications is teaching individuals how to recognize and respond to phishing and social engineering attacks. Training programs also instruct employees on how to handle sensitive data securely. It educates users on password practices such as avoiding common passwords, changing passwords regularly, and enabling multi-factor authentication(MFA). Organizations should extend security awareness training to include third-party vendors and supply chain partners to ensure there is no scope for a cyber threat.

Research and Development - Researchers can learn the methods to implement encryption, access controls and backup solutions to protect valuable data. Through this application, this study also identify new vulnerabilities and weaknesses leading to more robust security measures. Ransomware Simulations can be used to develop advanced threat research to create custom ransomware variants to understand the evolving attack techniques.

VI. CONCLUSION

This research study demonstrated the practical or virtual simulation of targeted ransomware using TeamViewer and 7z, coupled with the comprehensive insights provided about HostedScan, offers a considerable contribution to realm of cybersecurity. This effort acts as a valuable wake-up call, emphasizing the critical need for individuals and organizations to fortify their digital defenses. HostedScan's remarkable features, including its efficient risk detection and clear categorization into high, medium, and low-risk levels, empower users with actionable knowledge to prioritize their security efforts effectively. The detailed reports generated by HostedScan, sent directly to registered email addresses, provide a wealth of information, encompassing risk levels, vulnerabilities, IP addresses, port names, hostnames, and open TCP ports. This data equips users with the insights required to proactively safeguard their systems and data. Ultimately, this work fosters cybersecurity awareness and encourages proactive defense, enabling users to mitigate the risk of falling victim to ransomware attacks and other cyber threats. Future enhancements for the described cybersecurity approach could include integrating machine learning to advance threat detection and risk assessment, automating remediation, and improving reporting. Incorporating behavioral analysis, predictive modeling, and user anomaly detection would enhance proactive threat identification. Integration with threat intelligence feeds, SIEM systems, and addressing cloud and IoT security concerns would expand the system's scope. Additionally, using machine learning for personalized user education can empower individuals and organizations to better understand and respond to cyber threats, ensuring a more robust defense against evolving challenges.

REFERENCES

[1] S. R. B. Alvee *et al* "Ransomware Attack Modeling and Artificial Intelligence-Based Ransomware Detection for Digital Substations," *IEEE Workshop on the Electronic Grid (eGRID)*, 2021, pp. 01-05.

[2] G. Usha *et al* "Enhanced Ransomware Detection Techniques using Machine Learning Algorithms," *International Conference on Computing and Communications Technologies (ICCCT)*, 2021, pp. 52-58.

[3] K. Thummapudi *et al* "Detection of Ransomware Attacks Using Processor and Disk Usage Data," *IEEE Access*, vol. 11, pp. 51395-51407, 2023.

[4] S. Alzahrani *et al* "An Analysis of Conti Ransomware Leaked Source Codes" *IEEE Access*, vol. 10, pp. 100178-100193, 2022.

[5] S. Lee *et al* "Hiding in the Crowd: Ransomware Protection by Adopting Camouflage and Hiding Strategy With the Link File," *IEEE Access, vol. 11*, pp. 92693-92704, 2023.

[6] E. Berrueta *et al* "A Survey on Detection Techniques for Cryptographic Ransomware" *IEEE Access, vol. 7,* pp. 144925-144944, 2019.

[7] F. M. Alotaibi *et al* "SDN-Based Detection of Self-Propagating Ransomware: The Case of BadRabbit," *IEEE Access*, vol. 9, pp. 28039-28058, 2021.

[8] S. Sibi Chakkaravarthy *et al* "Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks," *IEEE Access*, vol. 8, pp. 169944-169956, 2020.

[9] X. Zhang *et al* "Dual Generative Adversarial Networks Based Unknown Encryption Ransomware Attack Detection," *IEEE Access*, vol. 10, pp. 900-913, 2022.

[10] M. Al-Hawawreh *et al* "Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7137-7151, 2019.

[11] I. Kara et al "Static and Dynamic Analysis of Third Generation Cerber Ransomware," *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT),* 2018, pp. 12-17.

[12] N. Aldaraani *et al* "Understanding the impact of Ransomware: A Survey on its Evolution, Mitigation and Prevention Techniques," *National Computer Conference (NCC),* 2018, pp. 1-5.

[13] M. Alam *et al* "RATAFIA: Ransomware Analysis using Time And Frequency Informed Autoencoders," *IEEE International Symposium on Hardware Oriented Security and Trust (HOST),* 2019, pp. 218-227.

[14] M. Baykara *et al*"A novel approach to ransomware: Designing a safe zone system," *International Symposium on Digital Forensic and Security (ISDFS),* 2018, pp. 1-5.

[15] H. Madani *et al* "Classification of ransomwaresusing Artificial Neural Networks and Bayesian Networks," *International Conference on Intelligent Computing in Data Sciences (ICDS),* 2019, pp. 1-6.

[16] V. Dharani *et al* "Spam SMS (or) Email Detection and Classification using Machine Learning," *5th International Conference on Smart Systems and Inventive Technology (ICSSIT),*2023, pp. 1104-1108.

[17] A. Vikram *et al* "Blockchain Technology and its Impact on Future of Internet of Things (IoT) and Cyber Security," *6th International Conference on Electronics, Communication and Aerospace Technology,* 2022, pp. 444-447.

[18] Upendra Shetty D R *et al* "Malicious URL Detection and Classification Analysis using Machine Learning Models," *International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT),* 2023, pp. 470-476.

[19] A. Vikram *et al* "Anomaly detection in Network Traffic Using Unsupervised Machine learning Approach*," International Conference on Communication and Electronics Systems (ICCES),*2020, pp. 476-479.