STM JOURNALS

Recent Trends in
Electronics & Communication Systems

ISSN: 2393-8757
Volume 11, Issue 1, 2024
DOI (Journal): 10.37591/RTECS

http://engineeringjournals.stmjournals.in/index.php/RTECS/index

Review RTECS

Ransomware Detection and Prevention Using Honeypot

Rutesh Bharat Autade[1], Yash Ashok Shinde[2], Snehal Shinde[3], Mayur Maruti Kumbhar[4,*]

Abstract

The significance of network security and explores the details of ransomware attacks, highlighting the crucial parameters essential to fortifying defences against this pernicious cyber threat. Network security involves safeguarding computer networks against unauthorized access, data breaches, and cyberattacks. Ransomware attack, a specific type of cyberattack, entail malicious software encrypting a computer system, making them unavailable to use in return attacker asks for ransom in form of cryptocurrency like Bitcoin or Ethereum These attacks can result in significant data loss and financial harm to individuals and organizations alike. In response to this vulnerability and to prevent data loss caused by such attacks, This specialized tool is meticulously designed to swiftly identify and mitigate ransomware threats in real-time. It conducts through ransomware analysis by examining ransom notes, file extensions, and ransomware-specific codes, allowing for accurate identification of ransomware variants and facilitating data recovery. Furthermore, the tool aids in classifying various ransomware families. With help of Honeypot this tool will lure attackers away from real systems. This tool aligns with network security principles, including Confidentiality, Integrity, and Availability.

Keywords: Ransomware, cybersecurity, honeypot

INTRODUCTION

In today's digitally interconnected landscape, the significance of network security has reached unprecedented levels. Safeguarding confidential data and defending against sophisticated cyber threats have become paramount concerns for organizations and individuals alike. One particularly menacing threat in recent years is ransomware, a form of malicious software designed to encrypt files or systems, demanding payment for their release. The continuous evolution of ransomware makes traditional signature-based detection techniques ineffective, necessitating innovative approaches for detection and prevention.

***Author for Correspondence**
Mayur Maruti Kumbhar
E-mail: mayurmk20comp@student.mes.ac.in

[1]Student, Department of Computer Engineering Pillai HOC College of Engineering and Technology, University of Mumbai, Rasayani, Maharashtra, India
[2]Student, Department of Computer Engineering Pillai HOC College of Engineering and Technology, University of Mumbai Rasayani, Maharashtra, India
[3]Assistant Professor Department of Computer Engineering Pillai HOC College of Engineering and Technology University of Mumbai Rasayani, Maharashtra, India
[4]Student, Department of Computer Engineering Pillai HOC College of Engineering and Technology, University of Mumbai Rasayani, Maharashtra, India

Received Date: April 18, 2024
Accepted Date: May 14, 2024
Published Date: May 25, 2024

Citation: Rutesh Bharat Autade, Yash Ashok Shinde, Snehal Shinde, Mayur Maruti Kumbhar. Ransomware Detection and Prevention Using Honeypot. Recent Trends in Electronics & Communication Systems. 2024; 11(1): 8–13p.

Ransomware attacks have become a major concern in cybersecurity, resulting in substantial financial losses and the exposure of sensitive data. To combat this ongoing threat, there's a rising focus on innovative strategies, including the adoption of honeypots for ransomware detection and prevention. Honeypots are simulated systems created to attract and mislead attackers, serving as a proactive defense against ransomware. By observing and analyzing malicious behavior within a controlled environment, honeypots offer valuable insights for enhancing cybersecurity measures.

Traditional security measures often struggle to detect and mitigate ransomware attacks due to the

malware's dynamic nature. The continuous evolution of ransomware signatures makes it challenging for standard methods to identify and thwart these threats effectively. Machine learning algorithms have emerged as a promising avenue for enhancing ransomware detection, as evidenced by studies such as "Ransomware detection using machine learning algorithms"[8].

According to the U.S. Department of Homeland Security, ransomware represents the fastest-growing malware threat to both individuals and organizations. The infamous WannaCry ransomware attack in May 2017, which affected over 200,000 computers running Microsoft Windows, underscored the urgency of addressing this escalating threat [9].

Malware, in general, is defined as software aiming to perform unauthorized operations that negatively impact the CIA triad of cyber security i.e. confidentiality, integrity and availability, a crucial aspect of cybersecurity is detection of malicious software in system, requiring analysis based on the software's functionality and methods of operation. Honeypots [10] play a crucial role in capturing the attack strategies employed by attackers. Honeypots do not prevent or mitigate attacks; instead, they remain silent, mimicking real environments to trap attackers ("Honeypots: Tracking Hackers" by L. Spitzner). There are two main types of honeypots-research and production honeypots. Research honeypots focus on gathering maximum information about attackers in a research context, allowing them access to security systems. On the other hand, production honeypots are strategically placed within production networks to enhance overall company security.

In conclusion, as ransomware continues to evolve into a sophisticated and pervasive cyber threat, the role of honeypots in detecting and preventing such attacks becomes increasingly crucial. Innovative solutions, coupled with advancements in machine learning, provide a promising path forward in the ongoing battle against ransomware and other forms of malicious software.

MOTIVATION

The motivation for using honeypots in ransomware attack detection and prevention is to achieve early threat detection, gain insights into attacker tactics, proactively defend against ransomware, strengthen cybersecurity, reduce potential financial losses, and serve as a legal deterrent to attackers. Incorporating honeypots into our project for ransomware detection and prevention aligns with our commitment to robust cybersecurity practices, enabling us to detect threats early, understand attacker behavior, and proactively defend against ransomware attacks. It is in this context that honeypots emerge as a powerful and innovative solution. Honeypots are security mechanisms deliberately designed to emulate vulnerable systems, services, or networks, acting as attractive targets for potential attackers. By deploying honeypots strategically within a network, organizations can gain invaluable insights into the methods, motivations, and behaviors of malicious actor.

FUNDAMENTAL CONCEPTS

Ransomware

Ransomware is a malicious software designed to encrypt files or entire computer systems, rendering them inaccessible to users. The primary characteristic of ransomware lies in its extortion strategy – it demands payment, usually in cryptocurrency, from the victim in exchange for a decryption key to restore access. The operation of ransomware involves infiltrating a system, encrypting files using advanced encryption techniques, and subsequently displaying a ransom demand. Notable examples of ransomware attacks include WannaCry in 2017 [9], which affected over 200,000 computers running Microsoft Windows, and impact ranges from financial losses to compromised sensitive data.

Honeypots

Honeypots are decoy systems strategically deployed to detect and analyze malicious activities within a network. In cybersecurity, honeypots play a crucial role in understanding and studying the

tactics, techniques, and procedures (TTPs) employed by attackers. They serve as bait, attracting cyber threats, and can be categorized into two types low-interaction and high-interaction simulate certain vulnerabilities to gather information without exposing the system to significant risk, while high-interaction honeypots provide a more realistic environment, allowing for deeper analysis. Real-world examples of honeypot deployments include using them to identify new malware variants or understand specific attack patterns.

Ransomware Detection Challenges

Detecting ransomware poses significant challenges for traditional security measures. Signature-based detection techniques struggle due to continuous evolution of ransomware, rendering static signatures ineffective. Behavioral analysis, while useful, has limitations in distinguishing normal from malicious behavior. Ransomware often employs evasion tactics, such as polymorphic malware that changes its code to evade signature-based detection, making it challenging to identify and mitigate these threats effectively.

Honeypots for Ransomware Detection

Honeypots offer a proactive approach to ransomware detection and prevention. By mimicking real environments, honeypots attract and analyze malicious activity, allowing for the capture of ransomware samples and a deeper understanding of attacker behavior. The advantages of using honeypots include the ability to study evolving tactics, identify new strains of ransomware, and enhance overall cybersecurity awareness. Deploying honeypots for ransomware detection involves careful planning, emulation of realistic scenarios, and continuous monitoring to capture and analyze potential threats effectively.

LITERATURE SURVEY

A recent survey highlights the critical importance of addressing ransomware attacks, which have emerged as significant threats targeting individuals, enterprises, healthcare industries, and the Internet of Things (IoT) [1-3]. Traditional security measures such as Intrusion Detection and Prevention Systems and antivirus software are often insufficient for effective ransomware detection due to their complexity and time-consuming nature. To overcome these limitations, a robust solution called Intrusion Detection Honeypot (IDH) has been proposed. The IDH comprises three main components: Honey folder, Audit Watch, and Complex Event Processing (CEP). The Honey folder serves as a decoy folder, strategically designed using the Social Leopard Algorithm (SoLA), to lure and detect suspicious file activities, thereby providing early warnings to users. Audit Watch, on the other hand, employs an Entropy module to verify the entropy of files and folders, enhancing the system's ability to identify potential ransomware threats [4–8] The CEP engine aggregates data from various security systems to analyze ransomware behavior and attack patterns promptly. Experimental testing of the proposed IDH in a secure test environment, involving over 20 variants of recent ransomware, demonstrates significant improvements in ransomware detection time, rate, and accuracy compared to existing models. Furthermore, another research initiative aims to experiment with encryptor and locker ransomware, combined with goodware, to generate dynamic parameters using a sandbox environment. The objective is to analyze and identify relevant dynamic features for distinguishing between ransomware and legitimate software. This effort culminates in the creation of a dynamic features dataset, encompassing various parameters for different artifacts. Machine learning algorithms are then employed to develop detection models using this dataset. Evaluation on five platforms, involving 20 ransomware samples and 20 goodware artifacts, results in a final feature dataset comprising 2000 records with 50 characteristics each. Notably, machine learning-based detection achieves an average accuracy exceeding 0.99 across different algorithms, including gradient boosted regression trees, random forest, and neural networks. These research endeavors collectively underscore the importance of innovative approaches, such as honeypot- based systems and machine learning-driven analysis, in effectively combating ransomware threats.

After an extensive analysis of recent research papers, it is evident that ransomware detection methodologies have become a burgeoning area of study. Among the various approaches investigated, it has been observed that honeypot and network analysis techniques exhibit superior efficacy compared to traditional key backup methods. This analysis serves as a foundational step in an ongoing research endeavor aimed at developing an open-source tribrid ransomware detection system. The ultimate goal is to address existing gaps identified through this review and subsequently design and implement an innovative solution. One potential advantage of this proposed system is the consolidation of various functionalities into a single solution, [9] resulting in streamlined operations and enhanced user convenience. Additionally, it is anticipated that the system will demonstrate optimal resource utilization, characterized by minimal memory and processor usage. Furthermore, the system's open-source nature facilitates collaborative development and continuous improvement, ensuring its relevance and effectiveness in the dynamic landscape of cybersecurity. However, it is imperative to acknowledge potential drawbacks associated with the proposed approach. Notably, it has been suggested that conventional key backup systems may prove ineffective in thwarting future ransomware attacks, as threat actors may exploit alternative methods for key generation, circumventing established security measures such as Windows crypto APIs. A recent survey conducted in this domain evaluated files collected using Cowrie Honeypot deployed on Google Cloud, with subsequent analysis performed through Virus Total integration. The study included the development of a program script to assess 50 files acquired from the Cowrie system, utilizing signature-based detection methods and comparing the efficacy of various antivirus tools [10]. The findings revealed that AVG exhibited the highest success rate among the tested antivirus applications, followed by Avast and Dr Web. However, it was noted that 19 antivirus applications failed to provide responses for the evaluated files, attributed to either outdated databases or database sizes impeding timely responses. One advantage of signature-based detection highlighted by this study is its continued relevance as a standard method for malware detection. Nonetheless, the study underscored the insufficiency of relying solely on signature-based detection, emphasizing the importance of implementing complementary approaches. In summary, this analysis underscores the evolving nature of ransomware detection methodologies and highlights the importance of comprehensive, multifaceted solutions in combating emerging cyber threats [11–13]. While certain challenges and limitations persist, ongoing research efforts hold promise for advancing the efficacy and resilience of ransomware detection systems.

A recent survey highlights the critical importance of addressing ransomware attacks, which have emerged as significant threats targeting individuals, enterprises, healthcare industries, and the Internet of Things (IoT). Traditional security measures such as Intrusion Detection and Prevention Systems (IDPS) and antivirus (AV) software are often insufficient for effective ransomware detection due to their complexity and time- consuming nature. To overcome these limitations, a robust solution called Intrusion Detection Honeypot (IDH) has been proposed. The IDH comprises three main components: Honey folder, Audit Watch, and Complex Event Processing (CEP). The Honey folder serves as a decoy folder, strategically designed using the Social Leopard Algorithm (SoLA), to lure and detect suspicious file activities, thereby providing early warnings to users. Audit Watch, on the other hand, employs an Entropy module to verify the entropy of files and folders, enhancing the system's ability to identify potential ransomware threats. The CEP engine aggregates data from various security systems to analyze ransomware behavior and attack patterns promptly. Experimental testing of the proposed IDH in a secure test environment, involving over 20 variants of recent ransomware, demonstrates significant improvements in ransomware detection time, rate, and accuracy compared to existing models. Furthermore, another research initiative aims to experiment with encryptor and locker ransomware, combined with goodware, to generate dynamic parameters using a sandbox environment. The objective is to analyze and identify relevant dynamic features for distinguishing between ransomware and legitimate software. This effort culminates in the creation of a dynamic features dataset, encompassing various parameters for different artifacts. Machine learning algorithms are then employed to develop detection models using this dataset. Evaluation on five platforms,

involving 20 ransomware samples and 20 good ware artifacts, results in a final feature dataset comprising 2000 records with 50 characteristics each. Notably, machine learning-based detection achieves an average accuracy exceeding 0.99 across different algorithms, including gradient boosted regression trees, random forest, and neural networks. These research endeavors collectively underscore the importance of innovative approaches, such as honeypot-based systems and machine learning-driven analysis.

PROPOSED SYSTEM

This section outlines an overview of the system architecture visualized in Figure 1. This detailed elaboration will delve into each component of the methodology, highlighting the technical intricacies, the user experience, and the system's capabilities.

The proposed system has three stages: the first stage includes deployment of the honeypot; second stages include built-in ransomware malware attack on deployed honeypot system and the last stage includes detection and prevention of malware attack.

First the system is initiated by overviewing all the network required requirements for the deployment of the honeypot to mimic the system. Although the honeypot is difficult to setup we have to set up and fulfill all its modules we can use low interaction honeypots which can make our system less vulnerable and more secured.

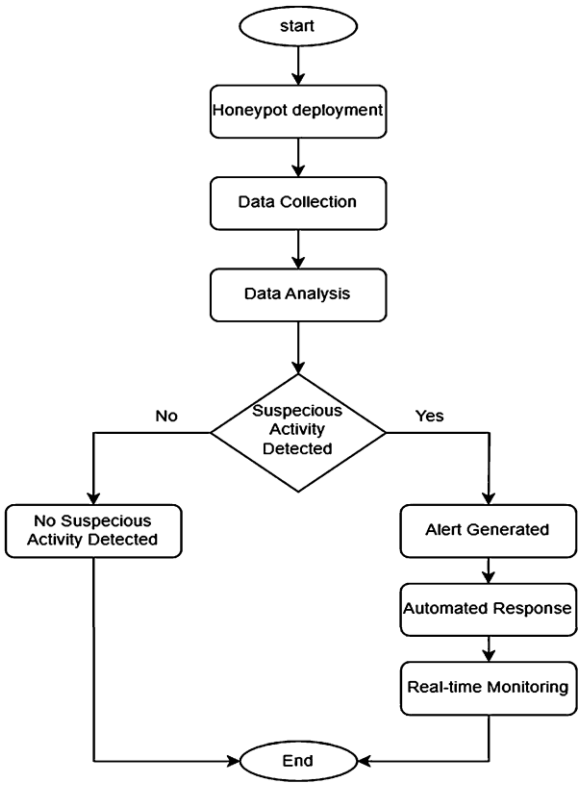

Figure 1. Proposed system.

Secondly, ransomware malware will encrypt system files and make system vulnerable ,using actual ransomware malware can put system under huge risk of cyber attack and it will be intolerable to detect and prevent. In python there are various libraries for cryptography such as fernet, cryptography pycrptography. By use of this built-in malware we attack on system files and then encrypt the files. He key is also generated by using key generation method.

Lure the attacker and save our real data from data loss and modification.

This system can Detect ransomware malware attack also helps to lure cyber attackers we can Analyze honeypot data to identify suspicious activity.

CONCLUSION

In conclusion, the utilization of honeypots for ransomware attack detection and prevention is a proactive and invaluable strategy in fortifying an organization's cybersecurity defenses. This approach empowers organizations to detect ransomware threats in their nascent stages, providing a vital window of opportunity for mitigation. Through the deployment of honeypots, we gain insights into attacker tactics and procedures, enhancing our overall understanding of ransomware threats.

REFERENCES

1. Seamlessly safeguarding data against Ransomware attacks by Abu Elkhail, Nada lachtar Duha lbdh, January 2023, Vol no 20.
2. Honeypot in Network Security: A Survey by Abhishek Mairh, Debabrat Barik Kanchan Verma, Oct 2015
3. Ransomware Threat, Attack, Prevention and Cure on Window Platform by Shubham Sharma and Satwinder Singh, February 2020.
4. A Review on Ransomware Detection Systems by Chamupathi Gigara Hettige, June 2023.
5. Dynamic Feature Dataset for Ransomware Detection Using Machine Learning Algorithms by Juan A. Herrera-Silva and Myriam Hernandez Alvarez, January 2023.
6. Analysis of Malicious Files Gathering via Honeypot Trap System and Benchmark of Anti-Virus Software, Ebu Yusuf Guven and M.Ali Aydin, Decmber2023.
7. Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks by S. sibi chakkaravarthy, D. Sangeetha, Meenalosini Vimal Cruz, V. Vaidehi and Balasubramanian Raman, September 23,2020
8. S. il Bae, G. bin Lee, and E. G. Im, "Ransomware detection using machine learning algorithms," Jun. 2019, doi: 10.1002/cpe.5422.
9. S. Mohurle and M. Patil, "A Brief Study of WannaCry Threat: Ransomware Attack 2017," International Journal of Advanced Research in Computer Science (IJARCS).
10. Spitzner, L. 2002. Honeypots: Tracking Hackers. 1st ed. Boston,MA, USA: Addison Wesley.
11. Design_of_Intrusion_Detection_Honeypot_Using_Social Engineering.
12. Survey of malware detection techniques by Aditya P.Mathur, Nwokedi Idika, Feb2007.
13. PDF Malware Detection: Towards Machine Learning Modeling with Explainability Analysis, G.M. Sakhawat Hossain, Kaushik Deb, Helge Janicke and Iqbal H.Sarker, January 2024.

