Review

A Survey on Ransomware Threats: Contrasting Static and Dynamic Analysis Methods

Qian Kang [*] and Yuanyuan Gu

Posted Date: 13 November 2023

doi: 10.20944/preprints202311.0798.v1

Keywords: ransomware detection; static analysis; dynamic analysis; cybersecurity; threat mitigation

Article

A Survey on Ransomware Threats: Contrasting Static and Dynamic Analysis Methods

Qian Kang [1,*,†] **and Yuanyuan Gu** [1,*,†]

[1] Xinshiji Cyber Academy
[*] Correspondence: xinshiji_academy_kang@outlook.com
[†] Current address: Xinshiji Cyber Academy, Shanghai, China. 200000

Abstract: The proliferation of ransomware poses a significant threat to global cybersecurity. This study presents a comprehensive review of the methodologies employed in the detection and analysis of ransomware, emphasizing the dichotomy between static and dynamic analysis approaches. It introduces the historical context and the necessity for robust cybersecurity measures, followed by an outline of the methodological framework used to evaluate existing ransomware analysis techniques. The results detail the effectiveness and limitations of various analysis strategies, identifying key features and patterns that aid in the detection and classification of ransomware threats. The study concludes by summarizing the primary achievements, including the identification of gaps in current research and proposing future research directions aimed at enhancing ransomware detection and mitigation strategies. The synthesis provided in this survey offers a consolidated view of the state-of-the-art in ransomware threat analysis and serves as a resource for cybersecurity professionals and researchers.

Keywords: ransomware detection; static analysis; dynamic analysis; cybersecurity; threat mitigation

1. Introduction

Recently, there has been an observable surge in ransomware incursions aimed at healthcare infrastructures, particularly during the heights of the COVID-19 pandemic [1–3]. Such institutions encountered substantial disruptions in medical services along with enduring ramifications due to these ransomware intrusions [4,5]. Additionally, ransomware incursions have targeted both individuals and organizations, with the primary intention of extracting increased financial gains [6,7]. A survey conducted in 2021 revealed that twice the number companies had been victims of ransomware attacks, than in 2020 [8]. Ransomware, a form of malicious software, employs encryption techniques to either encrypt users' non-replaceable files or lock the entire system [9,10]. The ultimate goal of ransomware attacks is to coerce payments from the victim to either unlock the system or decrypt the affected data files [11–13]. The inception of ransomware can be traced back to 1989 when Joseph Popp introduced a ransomware strain named AIDS or PC Cyborg, disseminating it through floppy disks to various AIDS researchers along with malicious scripts [14]. As time progressed, ransomware attacks evolved, adopting myriad tactics and methodologies [15,16]. Crypto-ransomware and locker-ransomware emerged as the two primary variants of this threat [17,18]. Crypto-ransomware involves the encryption of the victim's critical data by applying strong encryption algorithms such as the AES or RSA, whereas locker ransomware simply locks the victim's system, demanding a ransom to restore access [19,20]. Cryptocurrencies like Bitcoin have become the predominant medium for such transactions due to their anonymity and ease of transfer [21,22].

The security research community has dedicated significant efforts towards understanding the progression of various ransomware families [23–26]. Notable among these are WannaCry and Petya. For instance, CryptoWall, which appeared in 2014, was primarily disseminated via phishing emails, exploit kits, and infected attachments [27]. TeslaCrypt, which emerged in 2015, utilized the AES encryption algorithm to encrypt user data and was distributed through exploit kits [28]. Conversely, Cerber, often distributed via exploit kits and hacker forums as Ransomware-as-a-Service (RaaS), initiates the encryption of user data using the AES algorithm without requiring connection to a command and control center (C&C) [8]. Locky ransomware, first seen since 2016, propagated through embedded macros within Microsoft Office documents and facilitated encrypted communications for Tor and Bitcoin transactions [29]. The infamous WannaCry attack in 2017, which leveraged the Microsoft Windows EternalBlue security vulnerability to target the Server Message Block protocols, affected over 300,000 computers across more than 100 countries and encrypted files using the AES algorithm [30]. The spectrum of ransomware attacks is not limited to personal computers, but also includes mobile devices and Internet of Things (IoT) [31,32]. Since 2017, ransomware attacks on mobile devices have been on the rise, resulting in data theft or device lockdown [11]. Attacks on IoT devices pose a growing challenge [33]. The concept of Ransomware-as-a-Service (RaaS) has further simplified the process for adversaries to launch ransomware attacks, even for those with limited expertise [10].

The majority of ransomware countermeasures that exist today are reactive in nature [4,26,34]. Known indicators such as file hashes, IP addresses, and DNS records are typically employed in such reactive strategies [20]. However, these approaches have often led to data and system damages. In contrast, a proactive defense mechanism stands as the most secure alternative against ransomware incursions [35]. Proactive methodologies utilize behavioral clues and indicators to identify malicious activities, including system calls and Registry changes [17,36]. Such knowledge is essential to take preemptive action and aids in decision-making [6]. The frequency and sophistication of ransomware attacks have been escalating, garnering considerable attention due to their impact on individuals, businesses, and government entities globally [3]. These attacks are increasingly complex and require meticulous study [37,38]. From this standpoint, this study conducts a literature review focused on static and dynamic analysis, highlighting their limitations and gaps, and also examines the current techniques and the application of methods. Through a review of related studies and available datasets, the main trends in ransomware research are emphasized in this survey, along with potential future research directions.

The major contributions of this study include:

1. We examined the latest ransomware definition
2. We surveyed studies of static analysis and dynamic analysis of ransomware, and critiqued their shortcomings.
3. We listed and discussed major insights of this surveys.

2. Ransomware history and definition

This section explores ransomware history and definition.

2.1. Ransomware History

Ransomware, the extortion-based cyber threat, has evolved to target a diverse array of systems including computers, mobile and cloud-based platforms, Internet of Things (IoT) devices, and Industrial Control Systems (ICS) [23,28]. Historically, ransomware has progressed through a myriad of phases, each characterized by the development of various taxonomies aimed at deciphering its operational framework [8,39]. In its infancy, ransomware simply locked users out of their systems without compromising data integrity [20]. Over time, the threat metamorphosed, and ransomware began encrypting data resources, escalating the stakes of cyber extortion [4,40]. Such encryption procedures have bifurcated into three distinct types: symmetric, asymmetric, and a combination known as hybrid encryption [34]. Each method has been associated with varying degrees of encryption complexity and has been a factor in shaping the defensive strategies against ransomware [41,42]. The forensic investigation into these attacks has unveiled a sequence of ransomware attack steps, consisting of infection, installation, communication, execution, extortion, and emancipation phases [12,33]. Each phase represents a critical juncture in the lifecycle of a ransomware attack, from the initial breach to the final release of the encrypted assets [43,44].

2.2. Ransomware Definition

The persistent escalation of ransomware as a cyber threat has compelled security professionals to intensively analyze and develop various defensive techniques [27,35]. These methodologies are broadly categorized into signature-based and behavior-based defenses. The key features or attack patterns of ransomware and the corresponding defense strategies are summarized in Table 1.

Both strategies are integral components in the cyber defense arsenal, with behavior-based defenses increasingly favored for their adaptability and proactive capabilities [41,45]. The dynamic method, in particular, underscores the necessity of continual behavioral analysis to effectively counteract the evolving nature of ransomware threats [46,47].

Table 1. Key Features or Attack Patterns of Ransomware and Corresponding Defense Strategies.

Feature/Attack Pattern	**Defense Strategy**	**Sources**
Static properties inspection	Signature-Based Defenses	[48,49]
Complex anti-forensic tactics (code packing, obfuscation)	Signature-Based Defenses (limitations)	[8,9]
Dynamic behavior monitoring	Behavior-Based Defenses	[19,50]
Subtle behavioral signatures identification	Proactive Defense Mechanism	[2,51]

3. Static Analysis of Ransomware

Static analysis involves examining ransomware without executing it, focusing instead on characteristics like file metadata, byte frequency, opcode sequences, and static features extracted through disassembly. This section reviews key themes in static ransomware analysis.

3.1. File Metadata Analysis

Historical examinations of ransomware encrypted files have predominantly utilized static analysis, scrutinizing file metadata characteristics such as extensions, dimensions, entropy values, and headers [12,19,52]. Initial investigations conducted by researchers, such as Davies and colleagues in the early 2020s, undertook assessments of file entropy as a distinctive indicator for ransomware identification, meticulously contrasting various methodologies for calculating entropy [12,19,52]. Additionally, metadata analysis has been ingeniously integrated with machine learning algorithms to augment classification accuracy. Notably, some authors extracted static attributes including file extensions and dimensions to cluster and classify ransomware threats effectively [53]. Furthermore, statistical byte frequency analysis has been employed, exemplified by Kim and colleagues in 2022, who leveraged indicators of byte frequency to pinpoint crypto-ransomware incidents [25]. Nonetheless, a limitation of file metadata analysis is its susceptibility to obfuscation techniques employed by sophisticated ransomware. Techniques such as entropy measurement for detection can be circumvented when ransomware employs complex encoding strategies [54]. Moreover, machine learning models that depend on static attributes might not exhibit the flexibility to generalize across the spectrum of ransomware families, resulting in potential shortcomings [29]. Consequently, metadata analysis often concentrates on recognized ransomware families, encountering challenges in detecting novel or zero-day threats with advanced obfuscation techniques [39].

The ongoing development of ransomware presents an escalating challenge to static analysis methods [8,12]. Advanced ransomware variants are capable of manipulating file metadata in such a way that they masquerade as benign entities, effectively bypassing traditional static analysis [39,54]. This obfuscation can take various forms, including the strategic alteration of file extensions, the adjustment of file sizes to common document formats, and the manipulation of entropy levels to mimic non-encrypted files [52,55]. It has been observed that even when machine learning is applied to the analysis of metadata, there is a significant challenge in adapting to the continuous evolution of ransomware [9,29]. The static nature of file metadata means that once ransomware developers understand the features being analyzed, they can modify their code to avoid raising red flags [4,20]. In light of these limitations, there has been a shift towards dynamic analysis techniques [46,50]. These methods do not solely rely on pre-attack characteristics of files but also on behavioral patterns observed during the execution of ransomware [2,41]. Dynamic analysis simulates an environment where ransomware can execute, allowing security systems to observe its behavior in real time [36,51]. By monitoring system changes, network traffic, and other runtime behaviors, dynamic analysis provides a more robust and adaptable approach to ransomware detection [42,56]. This shift underscores the necessity for continuous innovation in cybersecurity defenses, moving towards more proactive and adaptable systems that can keep pace with the rapid development of ransomware tactics [47,57].

3.2. Disassembly Analysis

The examination of ransomware binary code through disassembly procedures has traditionally facilitated the extraction of informative static features [24]. The process involves the meticulous analysis of Portable Executable (PE) headers and operation code (opcode) sequences obtained from the disassembly, a technique that has been effectively used for the detection of ransomware such as the Locky strain [10]. The integration of machine learning models with these static features has proven to be effective in identifying the presence of ransomware [35]. The application of machine learning algorithms to the features derived from static disassembly has seen a marked increase over the past years [58]. Researchers have employed various approaches, such as the utilization of the XceptionNet Architecture, to analyze the patterns within PE headers [27]. The Class Feature Weighting (CFW) technique has also been adopted to enhance the predictive capability of these models when dealing with the binary code of ransomware [28]. Despite its contributions, static disassembly analysis comes with significant limitations [48]. The absence of runtime behavioral data is a major drawback, as static features can be manipulated by ransomware through techniques such as obfuscation, polymorphism, and metamorphism [49]. These advanced evasion tactics can render static analysis ineffective, as they enable ransomware to circumvent detection mechanisms that rely solely on pre-execution code inspection [5].

3.3. Bytecode Analysis

Researchers have methodically examined ransomware by disassembling the executable files into an intermediate format, commonly referred to as bytecode [31]. This approach was instrumental in identifying and extracting static characteristics from the hexadecimal codes of the bytecode, which were then analyzed through sophisticated machine learning algorithms for the detection of ransomware [35,58]. The utilization of bytecode is advantageous due to its inherent portability, which facilitates the deployment of defensive mechanisms across a multitude of platforms [20,27]. Nevertheless, the absence of behavioral data during the execution phase constitutes a significant limitation [17,36]. This shortfall is primarily because static analysis is confined to pre-execution attributes, which does not account for the dynamic nature of ransomware execution within a system [48,59]. As a consequence, machine learning models meticulously trained on static features derived from bytecode analysis may exhibit limitations in their efficacy, particularly when confronted with new and previously unseen ransomware variants [21,49]. These models have been tailored to identify patterns within the static code, yet the constantly evolving landscape of ransomware poses a substantial challenge [5,23]. The polymorphic and metamorphic characteristics of contemporary ransomware strains enable them to adeptly evade static detection, underscoring the need for enhanced detection strategies that incorporate dynamic analysis to observe the ransomware's behavior in a live and controlled sandbox environment [24,60].

3.4. Summary of Static Analysis Limitations

Advanced obfuscation can circumvent static indicators, requiring analysis of dynamic runtime behavior. Machine learning models relying solely on static features also have difficulties covering the extensive ransomware threat landscape. Hence, dynamic ransomware analysis is often more robust and generalizable (Table 2).

Table 2. Summary of the Main Inadequacies in Static Ransomware Analysis.

Limitation	Relevant Citations
Focus on known strains	[8,12,39]
Evasion techniques	[5,39,54]
Lack of runtime behavior	[2,41,46,50]
Generalization issues	[4,9,20,29]
Non-executable analysis	[23,24,60]

4. Dynamic Analysis of Ransomware

Dynamic analysis involves executing and monitoring ransomware to analyze its runtime behavior and effects. This provides insight into actions like file encryption, network activity, registry changes, API calls, and more. Dynamic ransomware analysis has focused on several key themes.

4.1. System Call Analysis

The practice of tracing system calls has been established as a critical method for the monitoring of ransomware behavior. Research in this domain has demonstrated that ransomware can be detected by profiling system calls [4,20,27]. Through the application of sophisticated algorithms, significant features have been extracted that are crucial for the identification process [17,36,46]. The chronology of system call sequences represents a pattern that has been harnessed using probabilistic models to discern the presence of ransomware [21,28,49]. Insights into low-level interactions with the operating system are gleaned through system calls, providing a granular view of the software's behavior [47,50,57]. Despite this, the challenge of interpreting such data at a high level remains formidable [2,25,41]. Ransomware, with its ever-increasing sophistication, has been known to employ a variety of obfuscation techniques to cloak its activity, thereby eluding detection methods that are reliant on system call patterns [29,54,55].

The cybersecurity landscape is in a state of perpetual flux, with ransomware consistently manifesting in ever more sophisticated forms [15,61,62]. Historical reliance on the analysis of system call patterns to detect such malicious software has, over time, proven to have its limitations [1,4,27]. These methodologies have been largely predicated on the identification of known ransomware strains, leveraging the static signatures and characteristics of these established threats [8,19,63]. Yet, the efficacy of such approaches is increasingly being called into question as the perimeter of ransomware innovation expands [30,42,64]. Predominantly, the methodologies employed for system call analysis have been rooted in the identification of ransomware strains that have already been documented [9,16,39]. This retrospective focus has yielded substantial insights into the behavioral patterns and signatures associated with these specific ransomware variants [12,52,65]. However, it has been observed that the detection of new or advanced threats, which often deploy sophisticated evasion techniques, presents a considerable challenge [23,24,60]. These advanced threats exhibit a dynamic nature, with adversaries continuously refining their methods to circumvent traditional detection systems [34,40,61]. The limitations inherent in the traditional system call analysis methodologies underscore the pressing need for the development of more sophisticated detection mechanisms [18,33,66]. These mechanisms must be capable of contending with the complexities of modern ransomware [7,12,19]. In response to this need, cybersecurity experts have begun advocating for the adoption of strategies that synergize both static and dynamic analysis techniques [43,67,68]. The integration of these approaches, particularly when underpinned by machine learning models trained on a comprehensive spectrum of ransomware behaviors, holds promise [11,44,69]. Such models, informed by a broad dataset reflective of the diverse tactics employed by ransomware developers, could provide a more robust defense against the broad array of ransomware attacks witnessed today [51,70,71]. The development and training of these models require a meticulous approach, accounting for the ever-changing tactics that ransomware developers employ to avoid detection [37,41,72]. As ransomware continues to evolve, so too must the methodologies designed to detect and mitigate its impact, with the goal of providing a fortified defense against an array of sophisticated ransomware attacks [2,25,73].

4.2. API Call Analysis

Monitoring high-level Windows API interactions through API call tracing has surfaced as a pivotal method in the cybersecurity domain for identifying potential ransomware activity [20,35,58]. Initial studies in this area, such as the work conducted by Continella and colleagues, revolved around the identification of ransomware through the observation of sequences of API calls deemed suspicious [17,27,36]. This approach was predicated on the assumption that ransomware, in its quest to execute its malicious payload, would inevitably interact with the operating system in a manner that could be classified as anomalous [48,49,59,74]. Further advancements have seen the application of sophisticated machine learning techniques, such as Long Short-Term Memory (LSTM) networks, which have been trained to discern patterns within API call data that might suggest the presence of ransomware [5,21,23].

Despite the initial successes, the task of accurately detecting ransomware via API call analysis has encountered significant hurdles [10,24,60]. Advanced strains of ransomware have demonstrated a capacity to obfuscate or modify their API call sequences, thereby undermining the effectiveness of detection mechanisms that rely on specific patterns [34,61,75]. Additionally, machine learning models, while powerful, often face challenges in generalizing their detection capabilities across the increasingly diverse families of ransomware [40,76,77]. The issue is further compounded when considering the detection of zero-day threats—newly emerging ransomware for which no prior knowledge exists [18,50,66]. These novel threats can exploit unknown vulnerabilities and, as such, may not exhibit the API call patterns that models have been trained to recognize [7,12,33,74]. Similarly, web-based ransomware, which executes within the context of a web browser rather than directly within the operating system environment, eludes API call analysis with its unique execution vectors [19,52,67].

4.3. File Activity Monitoring

The inspection of file operations has become a critical component in the arsenal against ransomware attacks, focusing specifically on the detection of unauthorized encryption activities [4,29,78]. The methodology involves a meticulous examination of file access patterns, scrutinizing the nature of read-write operations, and observing the fluctuations in file entropy—a quantitative measure that often signals the onset of encryption [12,19,79]. A novel approach in this domain is the deployment of decoy files, acting as honeypots, to lure and subsequently identify ransomware activity [33,80]. This technique not only aids in the early detection of encryption processes typically associated with ransomware but also serves as a means to study the behavior of such malicious entities [1,10,60]. However, sophisticated ransomware variants have evolved to adopt more covert operations, rendering traditional file activity monitoring less effective [23,45,76]. These advanced threats possess the ability to mask their encryption activities, blending in with legitimate processes to evade detection [9,27,39]. The prevalent emphasis on local file interactions also presents a limitation, as it neglects the increasing prevalence of cloud storage services—a domain where ransomware can execute encryption remotely, away from the prying eyes of local monitoring tools [34,61,81]. Another critical challenge lies in distinguishing between the encryption activities of ransomware and those of legitimate encryption utilities, which can exhibit similar file manipulation behaviors [41,51,55].

The analysis of file activity as a means to detect ransomware necessitates a comprehensive understanding of typical user behavior and encryption routines, as the subtleties in file access patterns can be indicative of a ransomware infection [17,44,49]. As such, cybersecurity specialists are tasked with the ongoing development of refined monitoring systems that can adapt to the evolving nature of ransomware strategies [30,42,64]. These systems must not only discern between benign and malicious encryption activities but also extend their vigilance to emerging cloud-based vectors that are increasingly being exploited by ransomware [25,62]. The continuous refinement of these monitoring techniques is an essential endeavor in the fight against ransomware, requiring an agile and forward-thinking approach to stay ahead of the sophisticated evasion strategies employed by attackers [6,65,82]. The ultimate objective remains to craft a robust defense mechanism that can withstand the multifaceted and dynamic nature of ransomware threats, ensuring the integrity and security of digital assets in an ever-connected world [14,32,83].

4.4. Network Traffic Analysis

Despite the demonstrated efficacy in various contexts, the approach of network traffic analysis does not come without its challenges [4,27]. One significant hurdle is the increasing sophistication of ransomware tactics, particularly their use of encryption and obfuscation techniques to conceal their network activity [9,23]. This evolution in strategy effectively camouflages the ransomware's network footprint, making it indistinguishable from legitimate network behavior to the unaided eye [61]. As a consequence, reliance solely on network indicators for the detection of such threats has been cast into doubt [18]. Moreover, the advent of web-based ransomware introduces additional complexities [34]. This form of ransomware, which operates through web protocols and services, seamlessly blends its communication within the vast sea of benign traffic that typifies web interactions [77]. The challenge is further amplified by the resilient and adaptable nature of web-based ransomware, which continuously evolves to exploit the dynamic web ecosystem [33].

4.5. Summary of Dynamic Analysis Limitations

The process of dynamic analysis, while providing valuable insights into the operations of ransomware, presents several limitations. These limitations are summarized in Table 3, along with citations from the literature that have contributed to the understanding of these challenges.

Table 3. Summary of the Main Limitations in Dynamic Ransomware Analysis.

Limitation	Description	Relevant Citations
Evasion Tactics	Susceptible to runtime obfuscation and anti-analysis evasion, making detection difficult.	[4,20,27]
Local Focus	Concentrates on local file activities, with limited consideration for cloud-based environments.	[9,23,61]
Activity Attribution	Challenges in distinguishing ransomware encryption from legitimate encryption tools.	[18,34,74,77]
Web-based Strains	Difficulty in detecting ransomware that operates within web browsers or through web services.	[12,19,33]
Model Generalization	Machine learning models struggle to generalize across the broad and evolving ransomware landscape.	[4,29,36]

Dynamic analysis remains an invaluable tool in the cybersecurity arsenal. However, the effectiveness of current methods is often compromised by sophisticated evasion techniques, necessitating a multi-faceted approach that combines various analysis techniques to improve the detection and prevention of ransomware attacks.

5. Discussions

In this section, we discuss the key insights of this survey.

5.1. Emergence of Ransomware-as-a-Service

The recent expansion of Ransomware-as-a-Service (RaaS) has significantly transformed the threat landscape [8,57]. RaaS platforms have emerged, offering a user-friendly interface, complete with dashboards that streamline the process of initiating ransomware campaigns [10,20,61]. These services are not only accessible to seasoned cybercriminals but also to those with minimal technical know-how, enabling a broader range of individuals to orchestrate ransomware attacks with ease [35,58]. The commodification of ransomware through this subscription-based model has led to a democratization of cybercrime, where sophisticated attack capabilities are available to the masses [17,23].

The industrialization of ransomware has not stopped at mere service offerings. It has maturely evolved into a full-fledged economy, comprising affiliates and partnerships that mirror legitimate business practices [5,21,49]. This burgeoning underground economy has systematized ransomware deployment, transforming it into a service that is disturbingly akin to mainstream SaaS (Software-as-a-Service) models [24,60]. This shift is further evidenced by the prevalent use of commodity ransomware, which capitalizes on the RaaS infrastructure to perpetrate extensive, automated attacks that indiscriminately target a wide range of victims [29,62,70]. Such ransomware campaigns are meticulously designed to maximize reach and impact, leveraging the scale and automation afforded by the service-based model [9,39].

The implications of the RaaS model's proliferation are profound, signaling an era where the frequency and sophistication of ransomware attacks could potentially escalate [2,25,41]. It necessitates an in-depth examination of the RaaS infrastructure, the stratagems employed, and the economic foundations that sustain its existence [54,55]. Scrutiny into these domains is imperative for the development of countermeasures that are both effective and adaptive [30,42,64]. The cybersecurity community must, therefore, allocate resources toward understanding the mechanics of RaaS operations, the economic incentives that drive their adoption, and the collaborative networks that underpin the model's success [6,32,78].

5.2. Escalating Sophistication of Evasion Techniques

In the realm of cybersecurity, the evolution of ransomware has evolved with increased complexity, rendering traditional detection mechanisms less effective [27,42,47,74]. The latest strains have exhibited a plethora of sophisticated tactics, such as utilizing advanced obfuscation techniques that have been meticulously designed to thwart analysis tools [5,9,67]. Cyber adversaries have not only employed cryptographic measures to conceal command and control communications but have also engineered their attacks to exploit supply chain vulnerabilities [36,46,61]. Furthermore, these threat actors have adeptly utilized social engineering to deceive unsuspecting users and harnessed known vulnerabilities to infiltrate systems with devastating efficiency [4,23,62]. The dynamic nature of these threats has posed a significant challenge to the development of machine learning models [20,29,55]. These models have been found wanting in their ability to generalize and adapt to the diverse and innovative attack methodologies employed by ransomware [19,39,45]. The research community has recognized the imperative need to enrich training datasets with more granular data and to explore ensemble methods that can offer a more nuanced understanding of the ransomware landscape [35,44,81].

Ransomware has also demonstrated a disturbing capability to evolve, with new variants appearing that can alter their behavior and signatures to slip past established defense mechanisms [24,48,60]. This has necessitated an ongoing investment in research aimed at uncovering new behavioral indicators that can signal the presence of these threats [2,15,54]. Analysts find themselves in a constant battle to stay ahead of these increasingly evasive and adaptive threats [1,6,37]. The challenge lies not just in detection but also in improving the generalization capabilities of security systems to anticipate and mitigate the impact of these attacks [8].

5.3. Limitations of This Survey

Although this survey offers an extensive examination of ransomware and its technical aspects, it presents certain limitations that must be acknowledged. The emphasis on technical dissection of ransomware, while rigorous, has overshadowed the exploration of the human element, such as the psychological tactics used by attackers, and the economic ramifications these attacks have on individuals and enterprises. The intricate financial incentives driving the ransomware economy, a vital piece of understanding the full scope of the problem, have received relatively less attention. This oversight leaves a gap in grasping the complete picture of ransomware's influence on global cybersecurity. The interconnections and collaborative networks that exist between various ransomware syndicates are not thoroughly investigated. Such alliances play a critical role in the dissemination and evolution of ransomware threats and are instrumental in devising more effective countermeasures. The survey's concentration on ransomware that targets Windows operating systems means that the nuances of ransomware attacks on alternative platforms, such as mobile devices and embedded systems, are not as prominently featured. Given that these platforms are becoming increasingly popular targets, this represents a significant area for further inquiry. The landscape of ransomware is one that is in constant flux, with tactics, techniques, and procedures evolving at a rapid pace. Consequently, any survey can only offer a momentary glimpse into the state of ransomware, which may quickly become outdated. Acknowledging this, the survey has compiled critical advancements in the technical analysis of ransomware and has underscored areas that hold potential for impactful research moving forward. This serves to chart a course for future investigations that could enhance the cybersecurity field's ability to preempt, understand, and neutralize ransomware threats.

6. Conclusions

This study has extensively surveyed the current landscape of ransomware threats, with a particular focus on contrasting static and dynamic analysis methods. It has systematically reviewed the progression of ransomware attack methodologies, the evolution of defensive strategies, and the challenges that persist in the face of this menacing cyber threat. The findings underscore the limitations of current analytical methods, particularly in adapting to the ever-evolving complexities of ransomware tactics. Through meticulous examination, this survey has highlighted the critical developments in both static and dynamic ransomware analysis and underscored the need for robust, adaptable defense mechanisms that can anticipate and respond to advanced ransomware strategies.

Looking ahead, the study pinpoints several avenues for future research that are crucial for advancing the field of cybersecurity in ransomware mitigation. The need for enriched training datasets, the exploration of ensemble methods for improved detection, and the development of new behavioral indicators are identified as key areas for investigation. Moreover, as ransomware adversaries refine their techniques, future research must pivot towards creating more sophisticated machine learning models that can generalize across various ransomware families and effectively counteract zero-day threats. The continuous innovation in cybersecurity defenses is paramount, and this study serves as a foundational reference for future endeavors aimed at enhancing the capability of security systems to protect against the dynamic and sophisticated nature of ransomware attacks.

Conflicts of Interest: The authors declare that there is no conflict of interest.

doi:10.20944/preprints202311.0798.v1

References

1. Tariq, U.; Ullah, I.; Yousuf Uddin, M.; Kwon, S.J. An Effective Self-Configurable Ransomware Prevention Technique for IoMT. *Sensors* **2022**, *22*, 8516.
2. Iqbal, M.J.; Aurangzeb, S.; Aleem, M.; Srivastava, G.; Lin, J.C.W. RThreatDroid: A Ransomware Detection Approach to Secure IoT Based Healthcare Systems. *IEEE Transactions on Network Science and Engineering* **2022**.
3. Wazid, M.; Das, A.K.; Shetty, S. BSFR-SH: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare. *IEEE Transactions on Consumer Electronics* **2022**.
4. McIntosh, T.; Kayes, A.; Chen, Y.P.P.; Ng, A.; Watters, P. Dynamic user-centric access control for detection of ransomware attacks. *Computers & Security* **2021**, *111*, 102461.
5. Al-Dwairi, M.; Shatnawi, A.S.; Al-Khaleel, O.; Al-Duwairi, B. Ransomware-Resilient Self-Healing XML Documents. *Future Internet* **2022**, *14*, 115.
6. Ryan, P.; Fokker, J.; Healy, S.; Amann, A. Dynamics of targeted ransomware negotiation. *IEEE Access* **2022**, *10*, 32836–32844.
7. Connolly, A.Y.; Borrion, H. Reducing ransomware crime: analysis of victims' payment decisions. *Computers & Security* **2022**, *119*, 102760.
8. McIntosh, T.; Kayes, A.; Chen, Y.P.P.; Ng, A.; Watters, P. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys (CSUR)* **2021**, *54*, 1–36.
9. Zahoora, U.; Khan, A.; Rajarajan, M.; Khan, S.H.; Asam, M.; Jamal, T. Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier. *Scientific Reports* **2022**, *12*, 15647.
10. Almeida, F.; Imran, M.; Raik, J.; Pagliarini, S. Ransomware Attack as Hardware Trojan: A Feasibility and Demonstration Study. *IEEE Access* **2022**, *10*, 44827–44839.
11. Faghihi, F.; Zulkernine, M. RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware. *Computer Networks* **2021**, *191*, 108011.
12. Davies, S.R.; Macfarlane, R.; Buchanan, W.J. Evaluation of live forensic techniques in ransomware attack mitigation. *Forensic Science International: Digital Investigation* **2020**, *33*, 300979.
13. Davies, S.R.; Macfarlane, R.; Buchanan, W.J. Majority Voting Ransomware Detection System. *Journal of Information Security* **2023**, *14*.
14. Yilmaz, Y.; Cetin, O.; Arief, B.; Hernandez-Castro, J. Investigating the impact of ransomware splash screens. *Journal of Information Security and Applications* **2021**, *61*, 102934.
15. Zuhair, H.; Selamat, A.; Krejcar, O. A Multi-Tier Streaming Analytics Model of 0-Day Ransomware Detection Using Machine Learning. *Applied Sciences* **2020**, *10*, 3210.
16. Zhang, Y.; Li, M.; Zhang, X.; He, Y.; Li, Z. Defeat Magic with Magic: A Novel Ransomware Attack Method to Dynamically Generate Malicious Payloads Based on PLC Control Logic. *Applied Sciences* **2022**, *12*, 8408.
17. Ahmed, U.; Lin, J.C.W.; Srivastava, G. Mitigating adversarial evasion attacks of ransomware using ensemble learning. *Computers and Electrical Engineering* **2022**, *100*, 107903.
18. Bold, R.; Al-Khateeb, H.; Ersotelos, N. Reducing False Negatives in Ransomware Detection: A Critical Evaluation of Machine Learning Algorithms. *Applied Sciences* **2022**, *12*, 12941.
19. Davies, S.R.; Macfarlane, R.; Buchanan, W.J. Differential area analysis for ransomware attack detection within mixed file datasets. *Computers & Security* **2021**, *108*, 102377.
20. Ahmed, Y.A.; Koçer, B.; Al-rimy, B.A.S. Automated Analysis Approach for the Detection of High Survivable Ransomware. *KSII Transactions on Internet and Information Systems (TIIS)* **2020**, *14*, 2236–2257.
21. Al-Haija, Q.A.; Alsulami, A.A. High performance classification model to identify ransomware payments for heterogeneous bitcoin networks. *Electronics* **2021**, *10*, 2113.
22. Wang, K.; Pang, J.; Chen, D.; Zhao, Y.; Huang, D.; Chen, C.; Han, W. A large-scale empirical analysis of ransomware activities in bitcoin. *ACM Transactions on the Web (TWEB)* **2021**, *16*, 1–29.
23. Albulayhi, K.; Al-Haija, Q.A. Early-stage Malware and Ransomware Forecasting in the Short-Term Future Using Regression-based Neural Network Technique. 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN). IEEE, 2022, pp. 735–742.

24. Almashhadani, A.O.; Kaiiali, M.; Sezer, S.; O'Kane, P. A multi-classifier network-based crypto ransomware detection system: a case study of Locky ransomware. *Ieee Access* **2019**, *7*, 47053–47067.
25. Kara, I.; Aydos, M. The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems with Applications* **2022**, *190*, 116198.
26. Davies, S.R.; Macfarlane, R.; Buchanan, W.J. Review of Current Ransomware Detection Techniques. In Proceedings of the Proc. of the 7 th International Conference on Engineering and Emerging Technologies (ICEET). Institute of Electrical and Electronics Engineers, 2022.
27. Ahmed, Y.A.; Koçer, B.; Huda, S.; Al-rimy, B.A.S.; Hassan, M.M. A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection. *Journal of Network and Computer Applications* **2020**, *167*, 102753.
28. Ahmed, Y.A.; Huda, S.; Al-rimy, B.A.S.; Alharbi, N.; Saeed, F.; Ghaleb, F.A.; Ali, I.M. A weighted minimum redundancy maximum relevance technique for ransomware early detection in industrial IoT. *Sustainability* **2022**, *14*, 1231.
29. Smith, D.; Khorsandroo, S.; Roy, K. Machine Learning Algorithms and Frameworks in Ransomware Detection. *IEEE Access* **2022**, *10*, 117597–117610.
30. McDonald, G.; Papadopoulos, P.; Pitropakis, N.; Ahmad, J.; Buchanan, W.J. Ransomware: Analysing the impact on Windows active directory domain services. *Sensors* **2022**, *22*, 953.
31. A. Alissa, K.; H. Elkamchouchi, D.; Tarmissi, K.; Yafoz, A.; Alsini, R.; Alghushairy, O.; Mohamed, A.; Al Duhayyim, M. Dwarf mongoose optimization with machine-learning-driven ransomware detection in internet of things environment. *Applied Sciences* **2022**, *12*, 9513.
32. Saeed, S.; Jhanjhi, N.; Naqvi, M.; Humayun, M.; Ahmed, S. Ransomware: A framework for security challenges in internet of things **2020**. pp. 1–6.
33. Chakkaravarthy, S.S.; Sangeetha, D.; Cruz, M.V.; Vaidehi, V.; Raman, B. Design of intrusion detection honeypot using social leopard algorithm to detect IoT ransomware attacks. *IEEE Access* **2020**, *8*, 169944–169956.
34. Baksi, R.P. Pay or Not Pay? A Game-Theoretical Analysis of Ransomware Interactions Considering a Defender's Deception Architecture **2022**. pp. 53–54.
35. Abbasi, M.S.; Al-Sahaf, H.; Mansoori, M.; Welch, I. Behavior-based ransomware classification: A particle swarm optimization wrapper-based approach for feature selection. *Applied Soft Computing* **2022**, *121*, 108744.
36. Ahmed, M.E.; Kim, H.; Camtepe, S.; Nepal, S. Peeler: Profiling kernel-level events to detect ransomware. In Proceedings of the Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part I 26. Springer, 2021, pp. 240–260.
37. Herrera-Silva, J.A.; Hernández-Álvarez, M. Dynamic Feature Dataset for Ransomware Detection Using Machine Learning Algorithms. *Sensors* **2023**, *23*, 1053.
38. Davies, S.R.; Macfarlane, R.; Buchanan, W.J. Exploring the Need For an Updated Mixed File Research Data Set. In Proceedings of the 2021 International Conference on Engineering and Emerging Technologies (ICEET). IEEE, 2021, pp. 1–5.
39. Zhang, X.; Wang, J.; Zhu, S. Dual Generative Adversarial Networks Based Unknown Encryption Ransomware Attack Detection. *IEEE Access* **2021**, *10*, 900–913.
40. Beaman, C.; Barkworth, A.; Akande, T.D.; Hakak, S.; Khan, M.K. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security* **2021**, *111*, 102490.
41. Hwang, J.; Kim, J.; Lee, S.; Kim, K. Two-stage ransomware detection using dynamic analysis and machine learning techniques. *Wireless Personal Communications* **2020**, *112*, 2597–2609.
42. Marais, B.; Quertier, T.; Morucci, S. AI-based Malware and Ransomware Detection Models **2022**.
43. Eliando, E.; Purnomo, Y. LockBit 2.0 Ransomware: Analysis of infection, persistence, prevention mechanism. *CogITo Smart Journal* **2022**, *8*, 232–243.
44. Fernando, D.W.; Komninos, N. FeSA: Feature selection architecture for ransomware detection under concept drift. *Computers & Security* **2022**, *116*, 102659.
45. Li, Z.; Liao, Q. Preventive portfolio against data-selling ransomware—A game theory of encryption and deception. *Computers & Security* **2022**, *116*, 102644.
46. McIntosh, T.; Kayes, A.; Chen, Y.P.P.; Ng, A.; Watters, P. Applying Staged Event-Driven Access Control to Combat Ransomware. *Computers & Security* **2023**, p. 103160.

47. Urooj, U.; Al-rimy, B.A.S.; Zainal, A.; Ghaleb, F.A.; Rassam, M.A. Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. *Applied Sciences* **2022**, *12*, 172.
48. Al-rimy, B.A.S.; Maarof, M.A.; Alazab, M.; Alsolami, F.; Shaid, S.Z.M.; Ghaleb, F.A.; Al-Hadhrami, T.; Ali, A.M. A Pseudo Feedback-Based Annotated TF-IDF Technique for Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation and Features Extraction. *IEEE Access* **2020**.
49. Al-Hawawreh, M.; Sitnikova, E.; Aboutorab, N. Asynchronous peer-to-peer federated capability-based targeted ransomware detection model for industrial IoT. *IEEE Access* **2021**, *9*, 148738–148755.
50. Celdrán, A.H.; Sánchez, P.M.S.; Scheid, E.J.; Besken, T.; Bovet, G.; Pérez, G.M.; Stiller, B. Policy-based and Behavioral Framework to Detect Ransomware Affecting Resource-constrained Sensors **2022**. pp. 1–7.
51. Ganfure, G.O.; Wu, C.F.; Chang, Y.H.; Shih, W.K. RTrap: Trapping and Containing Ransomware With Machine Learning. *IEEE Transactions on Information Forensics and Security* **2023**.
52. Davies, S.R.; Macfarlane, R.; Buchanan, W.J. Comparison of Entropy Calculation Methods for Ransomware Encrypted File Identification. *Entropy* **2022**, *24*, 1503.
53. Yamany, B.; Elsayed, M.S.; Jurcut, A.D.; Abdelbaki, N.; Azer, M.A. A New Scheme for Ransomware Classification and Clustering Using Static Features. *Electronics* **2022**, *11*, 3307.
54. Lee, J.; Lee, K. A method for neutralizing entropy measurement-based ransomware detection technologies using encoding algorithms. *Entropy* **2022**, *24*, 239.
55. Li, Z.; Rios, A.L.G.; Trajkovic, L. Machine Learning for Detecting the WestRock Ransomware Attack using BGP Routing Records. *IEEE Communications Magazine* **2022**.
56. Olani, G.; Wu, C.F.; Chang, Y.H.; Shih, W.K. Deepware: Imaging performance counters with deep learning to detect ransomware. *IEEE Transactions on Computers* **2022**.
57. McIntosh, T.; Liu, T.; Susnjak, T.; Alavizadeh, H.; Ng, A.; Nowrozy, R.; Watters, P. Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Computers & Security* **2023**, *134*, 103424.
58. Adamov, A.; Carlsson, A. Reinforcement learning for anti-ransomware testing. In Proceedings of the 2020 IEEE East-West Design & Test Symposium (EWDTS). IEEE, 2020, pp. 1–5.
59. Al-rimy, B.A.S.; Maarof, M.A.; Alazab, M.; Shaid, S.Z.M.; Ghaleb, F.A.; Almalawi, A.; Ali, A.M.; Al-Hadhrami, T. Redundancy coefficient gradual up-weighting-based mutual information feature selection technique for crypto-ransomware early detection. *Future Generation Computer Systems* **2020**.
60. AlMajali, A.; Qaffaf, A.; Alkayid, N.; Wadhawan, Y. Crypto-Ransomware Detection Using Selective Hashing. *2022 International Conference on Electrical and Computing Technologies and Applications (ICECTA)* **2022**, pp. 328–331.
61. Axon, L.; Erola, A.; Agrafiotis, I.; Uuganbayar, G.; Goldsmith, M.; Creese, S. Ransomware as a Predator: Modelling the Systemic Risk to Prey. *Digital Threats: Research and Practice*.
62. Khan, R.A.S.; Rahman, D.M.N.A. Efficiency of surveillance of TCP packet in IoT in reducing the risk of ransomware attacks. *Journal of Theoretical and Applied Information Technology* **2023**, *101*.
63. Yilmaz, Y.; Cetin, O.; Grigore, C.; Arief, B.; Hernandez-Castro, J. Personality Types and Ransomware Victimisation. *Digital Threats: Research and Practice* **2022**.
64. Malik, A.W.; Anwar, Z.; Rahman, A.U. A novel framework for studying the business impact of ransomware on connected vehicles. *IEEE Internet of Things Journal* **2022**.
65. Lang, M.; Connolly, L.Y.; Taylor, P.; Corner, P.J. The Evolving Menace of Ransomware: A Comparative Analysis of pre-pandemic and mid-pandemic Attacks. *Digital Threats: Research and Practice* **2022**.
66. Borah, P.; Bhattacharyya, D.K.; Kalita, J.K. Cost effective method for ransomware detection: an ensemble approach **2021**. pp. 203–219.
67. De Gaspari, F.; Hitaj, D.; Pagnotta, G.; De Carli, L.; Mancini, L.V. Evading behavioral classifiers: a comprehensive analysis on evading ransomware detection techniques. *Neural Computing and Applications* **2022**, *34*, 12077–12096.
68. Du, J.; Raza, S.H.; Ahmad, M.; Alam, I.; Dar, S.H.; Habib, M.A. Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection. *Security and Communication Networks* **2022**, *2022*, 1–16.
69. Filiz, B.; Arief, B.; Cetin, O.; Hernandez-Castro, J. On the effectiveness of ransomware decryption tools. *Computers & Security* **2021**, *111*, 102469.

70. Goodell, J.W.; Corbet, S. Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. Elsevier, 2023, Vol. 51, p. 103329.
71. Haner, M.; Sloan, M.M.; Graham, A.; Pickett, J.T.; Cullen, F.T. Ransomware and the Robin Hood effect?: Experimental evidence on Americans' willingness to support cyber-extortion. *Journal of Experimental Criminology* **2022**, pp. 1–28.
72. Hernandez-Castro, J.; Cartwright, A.; Cartwright, E. An economic analysis of ransomware and its welfare consequences. *Royal Society open science* **2020**, *7*, 190023.
73. Jaya, M.I.; Razak, M.F.A. Dynamic Ransomware Detection for Windows Platform Using Machine Learning Classifiers. *JOIV: International Journal on Informatics Visualization* **2022**, *6*, 469–474.
74. McIntosh, T.; Watters, P.; Kayes, A.; Ng, A.; Chen, Y.P.P. Enforcing situation-aware access control to build malware-resilient file systems. *Future Generation Computer Systems* **2021**, *115*, 568–582.
75. Aurangzeb, S.; Rais, R.N.B.; Aleem, M.; Islam, M.A.; Iqbal, M.A. On the classification of Microsoft-Windows ransomware using hardware profile. *PeerJ Computer Science* **2021**, *7*, e361.
76. Bekkers, L.; van't Hoff-de Goede, S.; Misana-ter Huurne, E.; van Houten, Y.; Spithoven, R.; Leukfeldt, E.R. Protecting Your Business against Ransomware Attacks? Explaining the Motivations of Entrepreneurs to Take Future Protective Measures against Cybercrimes Using an Extended Protection Motivation Theory Model. *Computers & Security* **2023**, *127*, 103099.
77. Berrueta, E.; Morato, D.; Magaña, E.; Izal, M. Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic. *Expert Systems with Applications* **2022**, *209*, 118299.
78. Sharmeen, S.; Ahmed, Y.A.; Huda, S.; Koçer, B.Ş.; Hassan, M.M. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. *IEEE Access* **2020**, *8*, 24522–24534.
79. Sheen, S.; Asmitha, K.; Venkatesan, S. R-Sentry: Deception based ransomware detection using file access patterns. *Computers and Electrical Engineering* **2022**, *103*, 108346.
80. Wang, S.; Zhang, H.; Qin, S.; Li, W.; Tu, T.; Shen, A.; Liu, W. KRProtector: Detection and Files Protection for IoT Devices on Android Without ROOT Against Ransomware Based on Decoys. *IEEE Internet of Things Journal* **2022**, *9*, 18251–18266.
81. Fang, R.; Xu, M.; Zhao, P. Determination of ransomware payment based on Bayesian game models. *Computers & Security* **2022**, *116*, 102685.
82. Tripathy, S.; Sahoo, D.; Satpathy, M.; Mutyam, M. Formal Modeling and Verification of Security Properties of a Ransomware-Resistant SSD. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* **2022**.
83. Molina, R.M.A.; Torabi, S.; Sarieddine, K.; Bou-Harb, E.; Bouguila, N.; Assi, C. On ransomware family attribution using pre-attack paranoia activities. *IEEE Transactions on Network and Service Management* **2021**, *19*, 19–36.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.