Article

Not peer-reviewed version

Analyzing Data Theft Ransomware Traffic Patterns Using BERT

Gabriela Almeida * and Felipe Vasconcelos

Posted Date: 4 December 2023

doi: 10.20944/preprints202312.0158.v1

Keywords: Ransomware Evolution; Data Theft; Network Traffic Analysis; BERT Model; Cybersecurity Adaptation

Article

Analyzing Data Theft Ransomware Traffic Patterns Using BERT

Gabriela Souza Almeida [1,*,†] and Felipe Eduardo Vasconcelos [2,‡]

[1] Instituto Politécnico de São Paulo
* Correspondence: AlmeidaGabriela2020@outlook.com
† Current address: Instituto Politécnico de São Paulo, São Paulo, 05508, São Paulo State, Brazil.

Abstract: This research looks into the evolving dynamics of ransomware, shifting from conventional encryption-based attacks to sophisticated data exfiltration strategies. Employing the Bidirectional Encoder Representations from Transformers (BERT) model, the study analyzes network traffic patterns to detect ransomware activities, offering new insights into their covert operations. The findings emphasize the need for advanced AI tools in cybersecurity, highlighting the significance of adapting and innovating defense strategies to counter the changing landscape of ransomware threats. The study contributes to a deeper understanding of ransomware evolution and underscores the importance of integrating AI in cybersecurity practices.

Keywords: ransomware evolution; data theft; network traffic analysis; BERT model; cybersecurity adaptation

1. Introduction

Ransomware, a form of malicious software meticulously crafted to block access to a computer system or its data until a ransom demand is met, has evolved substantially over the years [1–3]. In its early stages, ransomware attacks predominantly involved crypto-ransomware, known for encrypting user files, thus making them unreachable for the victims [4,5]. This approach to cyber extortion gained widespread attention through infamous instances like Petya and WannaCry [6]. However, more recent trends have indicated a notable shift in the tactics employed by ransomware perpetrators [3,7]. Contemporary ransomware groups, moving beyond the sole reliance on file encryption, are progressively focusing on data exfiltration [8,9]. This progression has been recognized as a significant transformation in the threat landscape posed by ransomware [10,11].

The progression from crypto-ransomware to ransomware that prioritizes data exfiltration signifies a more complex and menacing threat environment [4,5,12]. Data exfiltration, which entails the unauthorized copying, transferring, or retrieving of data from a computer or server, represents a ransomware variant that is frequently carried out through network channels [11,13,14]. Such methods pose a formidable challenge to existing cybersecurity measures as they directly target the core of organizational data confidentiality [2,15]. The ramifications of these attacks are extensive, impacting not only the availability of data but also its integrity and confidentiality [16,17].

In light of these evolving ransomware techniques, traditional cybersecurity measures focusing solely on preventing access breaches have become inadequate [11,18,19]. The need for advanced analytical tools capable of detecting and interpreting complex and subtle patterns of network traffic indicative of ransomware activities has become more critical [15,20,21]. Here, the Bidirectional Encoder Representations from Transformers (BERT) model emerges as a potent tool [22,23]. BERT's ability to process and analyze large volumes of unstructured data through its deep learning capabilities makes it uniquely suited for this task [24]. Unlike conventional models, BERT's bidirectional nature allows for a more nuanced understanding of context within data, a feature crucial for detecting the sophisticated methods employed by modern ransomware groups [16,25]. By leveraging BERT, researchers and cybersecurity professionals can better identify and respond to the subtle signs of data exfiltration, a task that traditional methods might overlook [26,27].

 doi:10.20944/preprints202312.0158.v1

The primary objective of this research is to explore the effectiveness of BERT in analyzing and identifying network traffic patterns associated with data exfiltration activities by contemporary ransomware groups [5,16,28–30]. The study focuses on the top 10 ransomware groups of 2023 (Table 1), including LockBit, AlphV/BlackCat, Cl0p, and others, recognized for their shift from traditional crypto-ransomware tactics to strategies centered around data theft [31,32]. The scope of this research encompasses the development of a BERT-based analytical framework, the collection and processing of relevant network traffic datasets, and the application of this framework to detect and analyze patterns indicative of data exfiltration activities by these ransomware groups [33,34]. By achieving these objectives, the study aims to contribute to the broader understanding of modern ransomware tactics and advance the capabilities of cybersecurity defenses in detecting and mitigating such threats [35,36].

Table 1. Top 10 Ransomware Groups of 2023

Name	Active Year	Estimated Loss ($M)	Usual Attack Style
LockBit	2019	$315.7M	Aggressive Tactics, Sophisticated Techniques
AlphV/BlackCat	2021	$280.4M	Double Extortion, Large Ransoms
Cl0p	2019	$190.2M	Data Leaks, Targeting Large Organizations
Black Basta	2022	$170.3M	Critical Infrastructure Attacks
Royal	2018	$225.5M	High-Value Targets, Sophisticated Tools
MalasLocker	2020	$95.6M	Ransomware-as-a-Service
Karkakurt	2021	$150.7M	Financial Institutions, Critical Infrastructure
BlackByte	2021	$132.9M	Social Engineering, RaaS
Ragnar Locker	2020	$110.4M	Varied Targets, Inactivity Periods
Hive/L0cked	2021	$187.8M	Rebranding, Persistent Threat

Our three major contributions in this research include:

1. The development of a comprehensive framework for analyzing ransomware network traffic patterns using the BERT model, highlighting its effectiveness in identifying subtle signs of ransomware activity.
2. An in-depth analysis of the evolving strategies of ransomware groups, particularly the shift from encryption-based attacks to covert data exfiltration methods.
3. The presentation of significant insights into how contemporary ransomware operates, emphasizing the need for advanced AI tools and methods in cybersecurity.

The rest of this research is organized as follows. Section 2 provides a detailed literature review, discussing the evolution of ransomware and previous approaches in ransomware network traffic analysis. Section 3 elaborates on the methodology adopted for data collection, ransomware group profiles, and network traffic datasets. Section 4 presents the results of our study, focusing on communication frequencies, data exfiltration volumes, and network bandwidth usage. Section 5 discusses the key findings, implications for cybersecurity practices, limitations, and future research directions. Finally, Section 6 concludes the research, summarizing the key contributions and implications of the study.

2. Literature Review

We review related literature in this section.

2.1. Ransomware Evolution and Trends

The progression of ransomware over the years has been marked by a significant shift from crypto-ransomware, which primarily focused on encrypting user files, to a more advanced form of ransomware that emphasizes data theft [1,2]. Initially, ransomware attacks were characterized by their use of encryption schemes that effectively locked user files, with infamous examples such as CryptoLocker and TeslaCrypt spearheading this trend [4,5]. These encryption-based ransomware

 doi:10.20944/preprints202312.0158.v1

types initially posed a substantial threat; however, their impact gradually waned as organizations strengthened their backup and recovery strategies, thereby diminishing the leverage these ransomware variants held [6]. This development in cybersecurity prompted the rise of more advanced ransomware variants like Locky and Cerber, which not only employed more sophisticated encryption algorithms but also integrated evasion tactics to circumvent traditional cybersecurity measures [3,7]. Yet, as cyber defenses continued to advance, particularly with the enhancement of backup and recovery solutions, the potency of ransomware relying solely on encryption began to decline [8,9]. This led to a notable transition in the ransomware landscape, where recent trends have witnessed a pivot towards ransomware strategies that prioritize data exfiltration [10,11]. This new breed of ransomware, exemplified by groups like Royal and Ragnar Locker, has adopted a dual-threat approach that combines the conventional method of encryption with the additional threat of exposing stolen data [5,12].

2.2. Previous Approaches in Ransomware Network Traffic Analysis

The analysis of network traffic associated with ransomware has played an essential role in both comprehending and counteracting these threats [4,5]. Various methodologies have been employed to scrutinize distinct facets of network activities linked to ransomware [13,37]. A prominent strategy includes the detection of interactions with command and control (C&C) servers, integral for coordinating the assault and transmitting directives [8,9]. Furthermore, the generation of encryption keys stands as a critical element, wherein ransomware frequently initiates contact with external servers for the creation or exchange of cryptographic keys [38–40]. The investigation into the existence of a "kill switch" within ransomware, a mechanism purposefully crafted to discontinue the attack under specific scenarios, has also been a focal point [11,13]. An additional area of significant interest has been the detection of sandbox environments; a considerable number of ransomware variants are designed to detect such virtualized environments as a means to elude analysis [14,15,41]. The process of encrypting files located on network drives has garnered notable attention, as this requires ransomware to execute conspicuous network operations [2,16]. There were also proposals to trace the bitcoin transactions of ransomware ransom payments over the network, for example, [13,22,29], but not all ransomware variants use bitcoins, and bitcoin-network-based forensic methods have their own reliability issues to address [38,40]. Finally, the shift towards data exfiltration has drawn heightened scrutiny towards identifying network activities indicative of file transfer operations, a hallmark of contemporary ransomware tactics [17,18].

2.3. Other Ransomware Detection Methods

In addition to the analysis of network traffic, a diverse range of methods for detecting ransomware has been investigated and developed. Behavioral analysis stands out as a fundamental strategy, where systems are tasked with monitoring activities that are typically indicative of ransomware, such as swift alterations in file structures or modifications in registry settings [34,36,42]. The adoption of machine learning for ransomware detection has been increasingly prominent, with these techniques harnessing algorithms to discern patterns characteristic of ransomware actions, drawing upon a wealth of historical data [3,14]. While signature-based detection continues to be extensively utilized, its efficacy tends to wane in the face of new or carefully obscured ransomware variants [2,6]. Heuristic analysis, which is centered around the recognition of ransomware based on its general characteristics rather than distinct signatures, has found broad application in recent times [25,26]. Furthermore, the deployment of decoy files or honeypots, which serve to entice and subsequently analyze ransomware in a secure environment, represents another innovative approach [28,43]. But all of those studies only focus on optional features of ransomware not required to perform its extortion functions. This study will look into how the principles of distributed ledger technology could be leveraged to bolster cybersecurity defenses against the ever-evolving threats posed by ransomware.

 doi:10.20944/preprints202312.0158.v1

3. Methodology

In this section, we detail the methodology of our study.

3.1. Data Collection

The data collection process for this research is two-fold, involving both the compilation of ransomware group profiles and the accumulation of network traffic datasets.

3.1.1. Ransomware Group Profiles

To understand the specific behaviors and tactics of the ransomware groups under study, comprehensive profiles were created, based on the analysis of ransomware samples collected from various sources. The following Table 2 outlines the ransomware families included in this study, the number of samples collected for each, and their sources.

Table 2. Ransomware Families and Sample Collection

Ransomware Family	No. of Samples	Source
LockBit	35	VirusTotal, Datasets
AlphV/BlackCat	18	VirusShare
Cl0p	12	Public Datasets, VirusShare
Black Basta	30	VirusTotal
Royal	25	VirusShare, VirusTotal
MalasLocker	40	Public Datasets, VirusShare
Karkakurt	38	VirusTotal, VirusShare
BlackByte	33	VirusShare
Ragnar Locker	26	Public Datasets, VirusShare
Hive/L0cked	14	VirusShare

3.1.2. Network Traffic Datasets

Constructing network traffic datasets is a cornerstone for analyzing ransomware's behavioral patterns, where a simulated network environment is crucial. In this controlled environment, ransomware samples, particularly from prominent families as outlined in Table 2, are executed, and their network behaviors are carefully monitored for a period of 12 hours from the initiation of execution. This setup utilizes isolated virtual machines, each configured with diverse operating systems and settings to mirror real-world network scenarios.

Network traffic capturing is conducted using sophisticated tools like Wireshark, which enables the detailed collection of data packets transmitted during various phases of ransomware activity [22]. This process captures a broad spectrum of activities, starting from the initial infection phase, encompassing command and control communications, and extending to data exfiltration attempts. Special attention is focused on identifying anomalous network behaviors indicative of ransomware operations, such as sudden spikes in data transfer volumes, transfers to suspicious sites, new network connections, and unusual port usage [17,22]. Once captured, the data undergoes rigorous preprocessing to filter out background network noise, thereby accentuating the characteristics unique to ransomware traffic. This preprocessing includes techniques such as signature-based analysis to identify known ransomware patterns, file integrity monitoring for detecting unauthorized alterations, and entropy scanning to identify randomness in encrypted files [17,22,28,44]. The result is a comprehensive dataset that embodies a diverse array of ransomware activities, laying the groundwork for subsequent analysis using the BERT model.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 December 2023 doi:10.20944/preprints202312.0158.v1

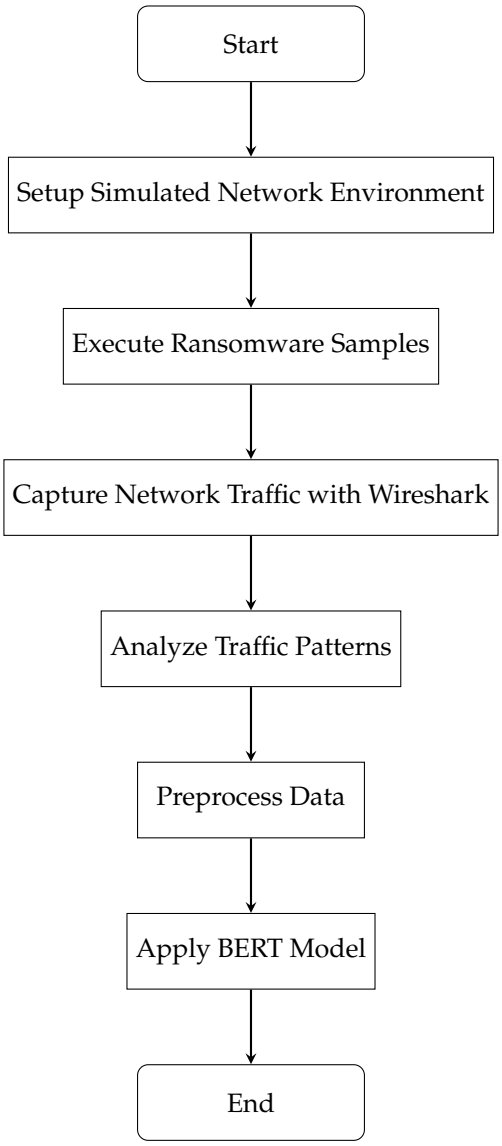

Figure 1. Network Traffic Analysis Flowchart

3.2. BERT Model Configuration and Training

The configuration and training of the BERT (Bidirectional Encoder Representations from Transformers) model for analyzing ransomware network traffic involve several critical steps. This process is pivotal for ensuring the model effectively interprets the complex patterns in the data.

1. *Data Preparation:* The preprocessed network traffic data, as described in the previous sections, is structured into a format suitable for BERT analysis. This involves tokenizing the data and converting it into tensors.
2. *Model Selection:* A pre-trained BERT model is selected as the foundation. Because of the complexity of the data, BERT Base is chosen.
3. *Fine-Tuning Parameters:* The model is fine-tuned to adapt to the specifics of the ransomware network traffic. This includes adjusting hyperparameters like learning rate, batch size, and the number of training epochs.
4. *Feature Engineering:* Features specific to ransomware behaviors, such as data exfiltration patterns and communication with C&C servers, are integrated into the model.
5. *Training:* The model undergoes training with the prepared dataset. During this phase, the BERT model learns to identify and interpret the various patterns and anomalies characteristic of ransomware traffic.

 doi:10.20944/preprints202312.0158.v1

6. *Validation:* Post-training, the model is validated on a separate set of data to assess its accuracy and effectiveness in detecting and analyzing ransomware-related network activities.
7. *Model Optimization:* Based on the validation results, the model may be further optimized to enhance its precision and reduce false positives or negatives.

The outcome is a BERT model specifically trained and optimized to analyze ransomware network traffic, capable of identifying subtle and complex patterns that traditional analysis methods might overlook. This model forms an integral part of the study's approach to advancing cybersecurity defenses against modern ransomware tactics.

3.3. Feature Extraction and Analysis Methods

In the realm of network traffic analysis for ransomware detection, extracting relevant features is crucial. These features are instrumental in identifying potential ransomware activities. The following Table 3 lists key features extracted from the network traffic data, along with their cybersecurity significance.

Table 3. Extracted Network Traffic Features and Their Significance

Feature	Cybersecurity Significance
Frequency of Communications	High frequency may suggest regular check-ins with C&C servers or automated data exfiltration activities.
Amount of Data Exfiltrated	Large volumes of data transfer, especially from sensitive directories, can indicate active data theft.
Network Bandwidth Percentage	Anomalous spikes in bandwidth usage can signal ongoing ransomware activities like file encryption or data upload to external servers.

Each of these features plays a vital role in the broader context of ransomware detection. By analyzing the destination IPs against databases like AbuseIPDB, we gain insights into potentially malicious network connections. The frequency of communications can unveil periodic patterns typical in ransomware operations, while the amount of data exfiltrated helps in assessing the scale of a breach. Lastly, overall network bandwidth usage offers a macro-level view of the network's health, where unusual spikes may indicate ransomware activity.

4. Results

We are presenting our results in this section.

4.1. Frequency of Communications

This metric highlights the regularity and patterns of network communication associated with ransomware activities. The analysis revealed frequent communication spikes with certain external IPs, which were flagged for suspicious activities, which often coincided with the initial stages of ransomware deployment or data exfiltration phases. As illustrated in Figure 2, the frequency of communications for each ransomware group varied significantly over the observed period, indicating different patterns of activity and potential stages of the ransomware attack cycle.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 December 2023 doi:10.20944/preprints202312.0158.v1

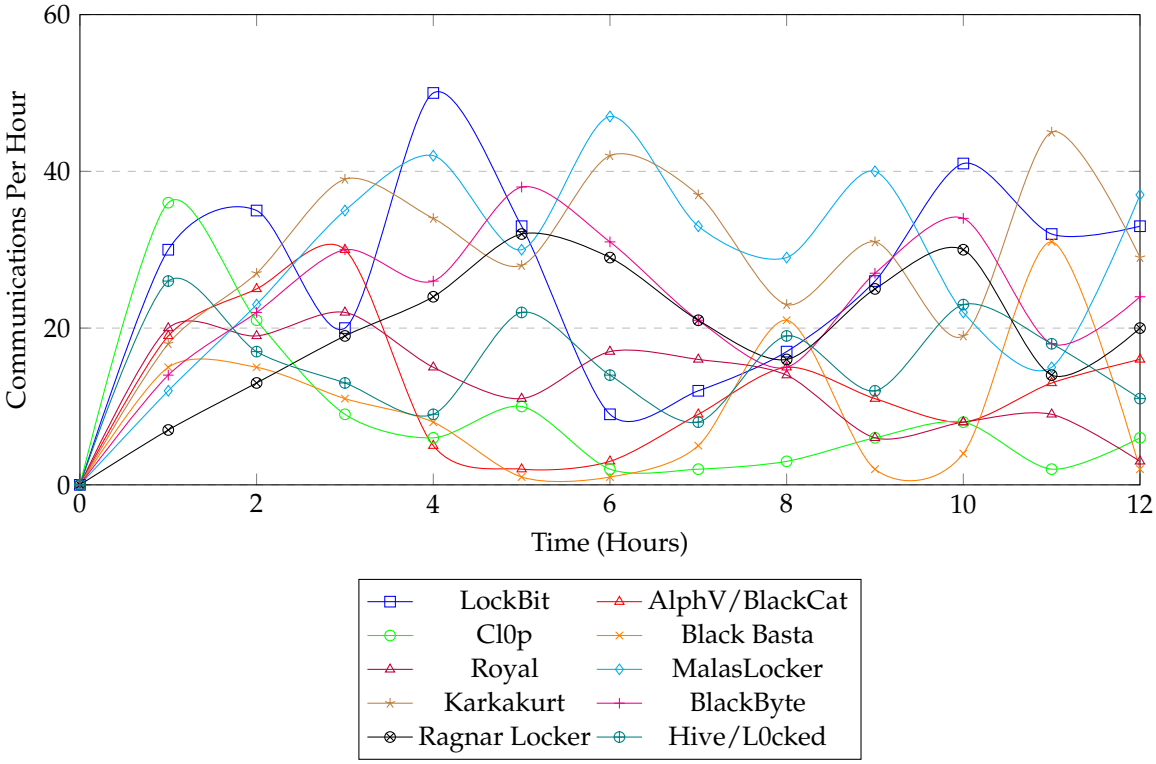

Figure 2. Frequency of communications for different ransomware groups over a 12-hour period

4.2. Amount of Data Exfiltrated

The assessment of data exfiltration volume, as displayed in Figure 3, is a critical component in understanding ransomware impacts. Our system, containing 20GB of customer data, encountered significant data theft. The extraction was especially pronounced in directories with sensitive data. This observation underscores how data theft ransomware operates tactically, choosing to discreetly siphon data rather than executing aggressive, large-scale exfiltrations. Such a strategy allows the ransomware to evade detection, as massive data movements are more likely to trigger security protocols. By exfiltrating smaller, selective amounts of data, ransomware can maintain a covert presence, increasing the challenge of early detection and response.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 4 December 2023 doi:10.20944/preprints202312.0158.v1

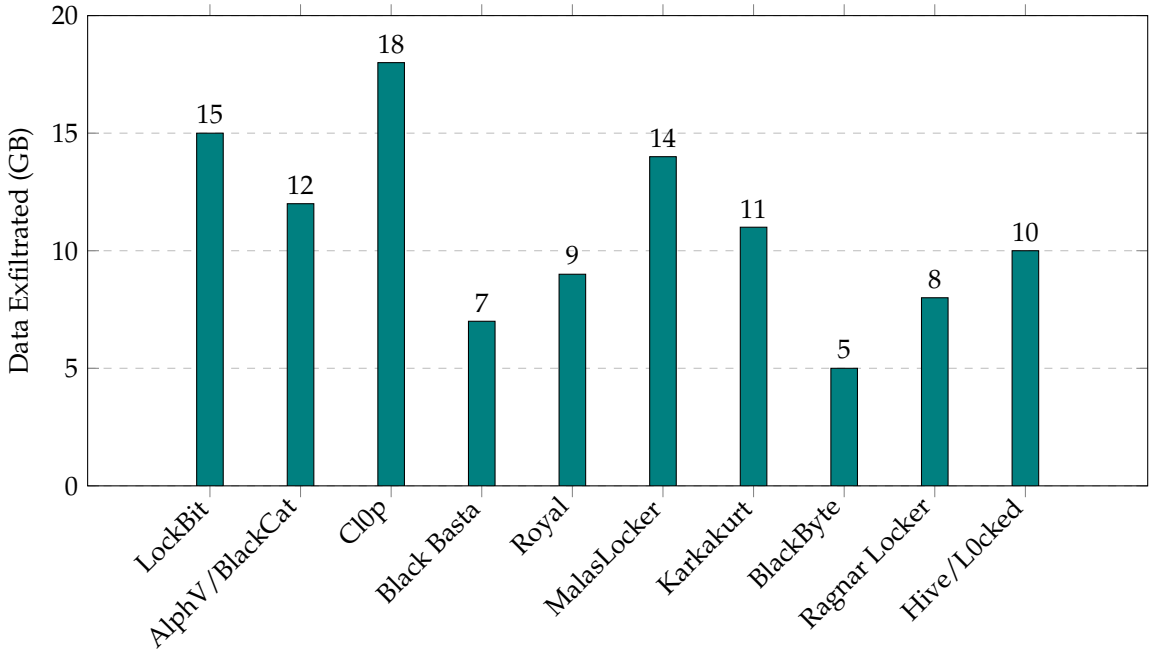

Figure 3. Data Exfiltration Volume by Ransomware Group

4.3. Network Bandwidth Usage Percentage

Monitoring bandwidth usage is crucial for detecting unusual spikes characteristic of ransomware activities. Our analysis, as depicted in Figure 4, showed a marked increase in bandwidth usage during ransomware attacks, particularly during the data encryption and exfiltration stages. However, it's important to note that sophisticated ransomware often employs low bandwidth for data exfiltration to remain undetected. Covert data exfiltration strategies aim to mimic normal network traffic patterns, thereby avoiding triggering network security alarms. This subtle approach is crucial for ransomware to successfully operate under the radar, prolonging its presence in the network and increasing the likelihood of a successful attack.

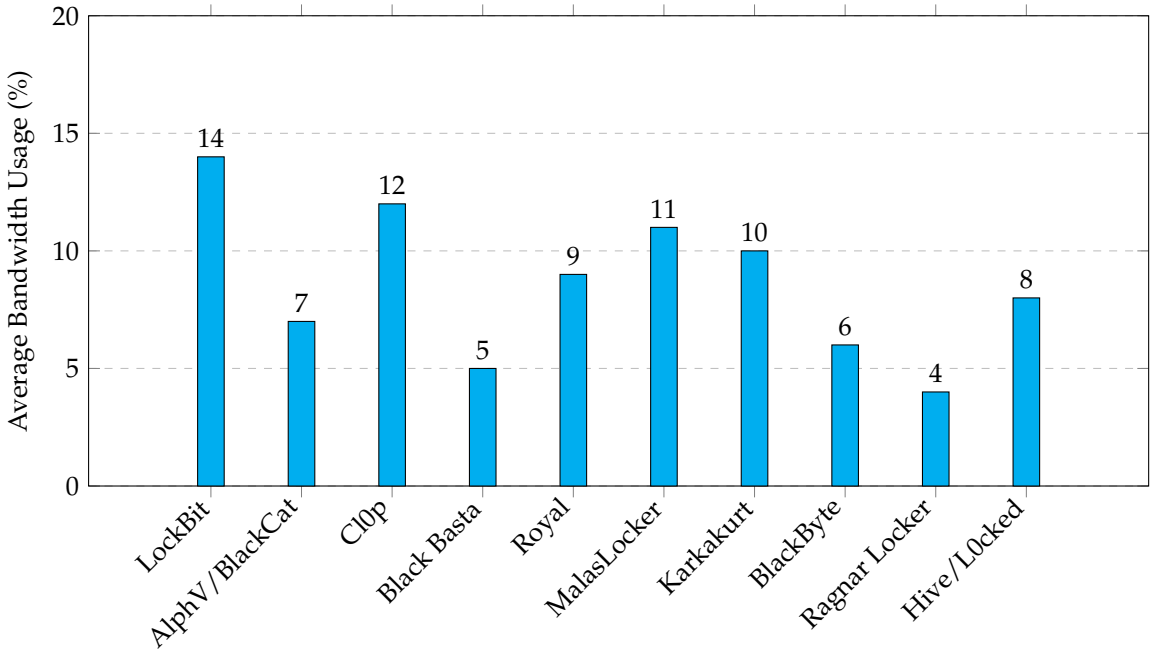

Figure 4. Network Bandwidth Usage Percentage by Ransomware Group

 doi:10.20944/preprints202312.0158.v1

5. Discussion

In this section, we discuss our findings in depth.

5.1. Key Findings

The study has uncovered pivotal insights into the sophisticated evolution of ransomware strategies. A notable transition from encryption-based attacks to more stealthy data exfiltration methods reflects ransomware groups' adaptation to enhanced defensive measures like robust backup and recovery processes. This subtle shift in tactics suggests a strategic response to circumvent traditional cybersecurity defenses, emphasizing the need for dynamic and advanced detection methods.

In-depth analysis of network traffic, facilitated by the BERT model, has proven highly effective in detecting nuanced ransomware activities. For instance, our observation of communication frequencies reveals that ransomware groups meticulously time their network activities, often correlating with initial deployment phases or crucial data exfiltration stages. These findings, depicted in Figure 2, indicate diverse operational patterns and attack stages among different ransomware groups, offering crucial insights into their *modus operandi*. The volume of data exfiltrated, as shown in Figure 3, provides a tangible measure of the impact of ransomware attacks. Notably, the study has observed that ransomware tends to target and exfiltrate data from sensitive directories selectively. This tactical approach of stealing smaller, more critical data sets, rather than large-scale, indiscriminate data dumps, aligns with ransomware's objective to remain undetected and maintain a prolonged presence within compromised networks. By doing so, ransomware can evade detection systems designed to flag significant, abrupt data movements, further complicating early detection and response efforts. Moreover, our analysis of network bandwidth usage, illustrated in Figure 4, has identified substantial increases during ransomware attacks, especially during data encryption and exfiltration phases. This finding is critical for early ransomware detection; however, it is imperative to recognize that sophisticated ransomware often employs low-bandwidth data exfiltration methods. This strategy is designed to blend in with normal network traffic, thus avoiding the activation of standard network security protocols. The adoption of such covert tactics by ransomware significantly challenges traditional cybersecurity approaches, necessitating more advanced, AI-driven detection methodologies.

These key findings have demonstrated the evolving complexity of ransomware attacks and highlight the necessity for continuous adaptation and enhancement of cybersecurity strategies to effectively combat these sophisticated threats.

5.2. Implications for Cybersecurity Practices Enhanced

The study's revelations have significant ramifications for current and future cybersecurity approaches. The shift in ransomware strategies towards discreet data exfiltration calls for a reassessment of network monitoring techniques. Traditional security systems focusing on detecting overt anomalies may not suffice; instead, there's a pressing need to identify and analyze subtle, covert activities that hint at ransomware presence.

Integrating sophisticated machine learning models like BERT into cybersecurity arsenals is no longer optional but a necessity. These models' capacity to discern intricate patterns and anomalies in network traffic makes them invaluable in the fight against advanced ransomware. This integration would not only bolster detection capabilities but also enhance predictive measures, allowing for proactive rather than reactive responses. The dynamic nature of ransomware threats underscores the importance of continuous learning and adaptation within cybersecurity teams. Regularly updating defense mechanisms, training in new detection technologies, and staying abreast of ransomware evolution are crucial steps in building resilience against these evolving threats. Cybersecurity strategies must evolve concurrently with the threats they aim to thwart, emphasizing agility, advanced analytics, and a thorough understanding of emerging ransomware behaviors and techniques. This holistic

approach will be pivotal in fortifying defenses against sophisticated ransomware attacks in the digital age.

5.3. Limitations and Future Research Directions

The current research, despite its valuable insights, has its constraints. A primary limitation is the dependence on specific network traffic patterns, which might not be universally applicable to all ransomware variants. To address this, future research should aim to diversify the dataset, encompassing a wider spectrum of ransomware behaviors. This expansion would enhance the robustness and generalizability of the findings. Another avenue for future exploration is to assess various AI models against each other. This comparative analysis could unveil strengths and weaknesses unique to each model, guiding the selection of the most effective tools for ransomware detection. Another important step would be the practical application of this research in real-time monitoring systems. Testing the model in live environments would provide invaluable insights into its operational effectiveness and adaptability. This real-world application could also reveal unforeseen challenges or additional factors that may influence the model's performance, thus providing a more comprehensive understanding of its practical utility in dynamic cybersecurity contexts. Such endeavors will be instrumental in advancing the field of cybersecurity, offering more sophisticated tools and strategies to combat the ever-evolving threat of ransomware.

6. Conclusion

This research has shed light on the evolving landscape of ransomware, underscoring the shift from traditional encryption-based attacks to more sophisticated data exfiltration methods. The study's application of the BERT model for analyzing ransomware network traffic patterns has demonstrated the potential of advanced AI in enhancing cybersecurity measures. Our findings highlight the necessity for continual adaptation and innovation in cybersecurity practices to effectively counter the dynamic nature of ransomware threats. As ransomware continues to evolve, so must our strategies and tools to defend against it. This research paves the way for future investigations, emphasizing the integration of AI technologies in cybersecurity and the exploration of new detection methodologies. Ultimately, our study contributes to the ongoing effort to strengthen digital defenses against the ever-adapting threat of ransomware.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Umar, R.; Riadi, I.; Kusuma, R.S. Analysis of conti ransomware attack on computer network with live forensic method. *IJID (International Journal on Informatics for Development)* **2021**, *10*, 53–61.
2. Moreira, C.C.; Moreira, D.C.; de Sales Jr, C.d.S. Improving ransomware detection based on portable executable header using xception convolutional neural network. *Computers & Security* **2023**, *130*, 103265.
3. Singh, J.; Sharma, K.; Wazid, M.; Das, A.K. SINN-RD: Spline interpolation-envisioned neural network-based ransomware detection scheme. *Computers and Electrical Engineering* **2023**, *106*, 108601.
4. Moussaileb, R.; Cuppens, N.; Lanet, J.L.; Le Bouder, H. Ransomware network traffic analysis for pre-encryption alert. Foundations and Practice of Security: 12th International Symposium, FPS 2019, Toulouse, France, November 5–7, 2019, Revised Selected Papers 12. Springer, 2020, pp. 20–38.
5. McIntosh, T.; Kayes, A.; Chen, Y.P.P.; Ng, A.; Watters, P. Applying staged event-driven access control to combat ransomware. *Computers & Security* **2023**, *128*, 103160.
6. Monge, M.A.S.; Vidal, J.M.; Villalba, L.J.G. A novel self-organizing network solution towards crypto-ransomware mitigation. Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018, pp. 1–10.
7. Almousa, M.; Osawere, J.; Anwar, M. Identification of Ransomware families by Analyzing Network Traffic Using Machine Learning Techniques. 2021 Third International Conference on Transdisciplinary AI (TransAI). IEEE, 2021, pp. 19–24.

 doi:10.20944/preprints202312.0158.v1

8. Manzano, C.; Meneses, C.; Leger, P. An empirical comparison of supervised algorithms for ransomware identification on network traffic. 2020 39th International Conference of the Chilean Computer Science Society (SCCC). IEEE, 2020, pp. 1–7.
9. Shemitha, P.; Dhas, J.P.M. Research perceptions on ransomware attack: a complete analysis on conventional authentication protocols in network. *Evolutionary Intelligence* **2020**, pp. 1–16.
10. Ketzaki, E.; Toupas, P.; Giannoutakis, K.M.; Drosou, A.; Tzovaras, D. A behaviour based ransomware detection using neural network models. 2020 10th International Conference on Advanced Computer Information Technologies (ACIT). IEEE, 2020, pp. 747–750.
11. Xia, T.; Sun, Y.; Zhu, S.; Rasheed, Z.; Shafique, K. Toward a network-assisted approach for effective ransomware detection. *arXiv preprint arXiv:2008.12428* **2020**.
12. Reidys, B.; Liu, P.; Huang, J. Rssd: Defend against ransomware with hardware-isolated network-storage codesign and post-attack analysis. Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, 2022, pp. 726–739.
13. Cahyani, N.D.W.; Nuha, H.H.; others. Ransomware detection on bitcoin transactions using artificial neural network methods. 2021 9th International Conference on Information and Communication Technology (ICoICT). IEEE, 2021, pp. 1–5.
14. Nurnoby, M.F.; El-Alfy, E.S.M. Overview and Case Study for Ransomware Classification Using Deep Neural Network. 2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM). IEEE, 2019, pp. 1–6.
15. Owolafe, O.; Thompson, A.F. Analysis of Crypto-Ransomware Using Network Traffic. *Journal of Information Security and Cybercrimes Research* **2022**, *5*, 76–83.
16. Ankita, A.; Rani, S. Machine learning and deep learning for malware and ransomware attacks in 6G network. 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT). IEEE, 2021, pp. 39–44.
17. Kusuma, R.S.; Umar, R.; Riadi, I. Network forensics against ryuk ransomware using trigger, acquire, analysis, report, and action (TAARA) method. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control* **2021**.
18. Gazzan, M.; Sheldon, F.T. An Enhanced Minimax Loss Function Technique in Generative Adversarial Network for Ransomware Behavior Prediction. *Future Internet* **2023**, *15*, 318.
19. 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.
20. Rodriguez-Bazan, H.; Sidorov, G.; Escamilla-Ambrosio, P.J. Android Ransomware Analysis Using Convolutional Neural Network and Fuzzy Hashing Features. *IEEE Access* **2023**.
21. Berrueta, E.; Morato, D.; Magaña, E.; Izal, M. Ransomware encrypted your files but you restored them from network traffic. 2018 2nd Cyber security in networking conference (CSNet). IEEE, 2018, pp. 1–7.
22. Nalinipriya, G.; Balajee, M.; Priya, C.; Rajan, C. Ransomware recognition in blockchain network using water moth flame optimization-aware DRNN. *Concurrency and Computation: Practice and Experience* **2022**, *34*, e7047.
23. Khalid Alkahtani, H.; Mahmood, K.; Khalid, M.; Othman, M.; Al Duhayyim, M.; Osman, A.E.; Alneil, A.A.; Zamani, A.S. Optimal Graph Convolutional Neural Network-Based Ransomware Detection for Cybersecurity in IoT Environment. *Applied Sciences* **2023**, *13*, 5167.
24. Sangher, K.S.; Noor, A.; Sharma, V. Holistic Cyber Threat Hunting Using Network Traffic Intrusion Detection Analysis for Ransomware Attacks. International Conference on Information Security, Privacy and Digital Forensics. Springer, 2022, pp. 199–212.
25. PA, S.; Dhas, J.P.M. Crow Search with Adaptive Awareness Probability-Based Deep Belief Network for Detecting Ransomware. *International Journal of Pattern Recognition and Artificial Intelligence* **2022**, *36*, 2251010.
26. Al Duhayyim, M.; Mohamed, H.G.; Alrowais, F.; Al-Wesabi, F.N.; Hilal, A.M.; Motwakel, A. Artificial Algae Optimization with Deep Belief Network Enabled Ransomware Detection in IoT Environment. *Computer Systems Science & Engineering* **2023**, *46*.
27. Srivastava, A.; Kumar, N.; Handa, A.; Shukla, S.K. Ransomware Detection based on Network Behavior using Machine Learning and Hidden Markov Model with Gaussian Emission. 2023 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2023, pp. 227–233.

28. Tafkov, S. Cloud Intelligence Network for Ransomware Detection and Infection Effect Reversing,". Proc. of 12th International Conference on Business Information Security (BISEC-2021), Belgrade, Serbia, December 3rd, 2021, pp. 23–26.
29. Nalinipriya, G.; Maram, B.; Vidyadhari, C.; Cristin, R. Optimized deep stacked autoencoder for ransomware detection using blockchain network. *International Journal of Wavelets, Multiresolution and Information Processing* **2021**, *19*, 2150022.
30. Susnjak, T. Beyond Predictive Learning Analytics Modelling and onto Explainable Artificial Intelligence with Prescriptive Analytics and ChatGPT. *International Journal of Artificial Intelligence in Education* **2023**, pp. 1–31.
31. Singh, M.P.; Karkhur, Y. Portable Executable Header Based Ransomware Detection using Power Iteration and Artificial Neural Network. 2023 6th International Conference on Information Systems and Computer Networks (ISCON). IEEE, 2023, pp. 1–6.
32. Wang, F. A Few-Shot Learning Approach with a Twin Neural Network Utilizing Entropy Features for Ransomware Classification **2023**.
33. Tsai, W.T.; Lin, S.R.; Liu, T.M.; Chou, C.L. Ransomware Detection Technique by using Network Packet Analysis and Machine Learning. *Communications of the CCISA* **2022**, *28*, 36–57.
34. Kumar, G.; Nagu, V. Recurrent Neural Network Deep Learning Approach for Classifying Early-Stage Malicious Ransomware Malware. International conference on Variability of the Sun and sun-like stars: from asteroseismology to space weather. Springer, 2022, pp. 641–652.
35. 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.
36. Kanumuri, S.; Kantipudi, V.T.; Mary, A.V.A.; Selvan, M.P. Detection of Ransomware Based on Recurrent Neural Network (RNN). Advances in Smart Grid and Renewable Energy: Select Proceedings of ETAEERE 2020. Springer, 2021, pp. 569–575.
37. 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.
38. Halgamuge, M.N. Estimation of the success probability of a malicious attacker on blockchain-based edge network. *Computer Networks* **2022**, *219*, 109402.
39. Abdella, J.; Tari, Z.; Anwar, A.; Mahmood, A.; Han, F. An architecture and performance evaluation of blockchain-based peer-to-peer energy trading. *IEEE Transactions on Smart Grid* **2021**, *12*, 3364–3378.
40. Halgamuge, M.N.; Munasinghe, G.K.; Zukerman, M. Time Estimation for a New Block Generation in Blockchain-Enabled Internet of Things. *IEEE Transactions on Network and Service Management* **2023**.
41. Jin, Y.; Tomoishi, M.; Matsuura, S.; Kitaguchi, Y. A secure container-based backup mechanism to survive destructive ransomware attacks. 2018 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2018, pp. 1–6.
42. Scaife, N.; Carter, H.; Traynor, P.; Butler, K.R. Cryptolock (and drop it): stopping ransomware attacks on user data. 2016 IEEE 36th international conference on distributed computing systems (ICDCS). IEEE, 2016, pp. 303–312.
43. Lei, I.S.; Tang, S.K.; Chao, I.K.; Tse, R. Self-recovery Service Securing Edge Server in IoT Network against Ransomware Attack. IoTBDS, 2020, pp. 399–404.
44. Peddoju, S.K.; Upadhyay, H.; Lagos, L. File integrity monitoring tools: Issues, challenges, and solutions. *Concurrency and Computation: Practice and Experience* **2020**, *32*, e5825.