*An ontology-based representation of knowledge for specifying ransomware behavior*

|  |  |  |  |
| --- | --- | --- | --- |
| Manh-Duc Hoang ICT Department FPT University Hanoi 10000, Vietnam [duchm29@fe.edu.vn](mailto:duchm29@fe.edu.vn) | Duc-Anh Nguyen Information Assurance FPT UniversityHanoi 10000, Vietnam [anhndhe160785@fpt.edu.vn](mailto:anhndhe160785@fpt.edu.vn) | Nhat-Huy Nguyen Information Assurance FPT UniversityHanoi 10000, Vietnam  huynnhe161198@fpt.edu.vn | Viet-Chien Nguyen Information Assurance FPT UniversityHanoi 10000, Vietnam  chiennvhe163660@fpt.edu.vn |
| Duy-Huy Doan Information Assurance FPT UniversityHanoi 10000, Vietnam [huyddhe163583@fpt.edu.vn](mailto:huyddhe163583@fpt.edu.vn) | Viet-Nam Ta Information Assurance FPT UniversityHanoi 10000, Vietnam namtvhe160666@fpt.edu.vn | Manh-Linh Pham  Information Technology  UET University  Hanoi 10000, Vietnam  linhmp@vnu.edu.vn |  |

*Abstract—* *This paper introduces CyberRanto, an ontology-based framework for analyzing ransomware behavior. As ransomware attacks grow more sophisticated, structured knowledge representation becomes crucial. CyberRanto, developed from a thorough review of ransomware lifecycle stages, categorizes actions into phases like infiltration, Behavior detail properties, and ransom demand. This aids in early detection, prevention, and investigation of cyber threats. Leveraging real-world instances and diverse behavioral patterns, the framework enhances threat intelligence, supports digital forensics, and is useful for cybersecurity training. Future research may adapt this framework to emerging ransomware variants, maintaining its relevance in dynamic threat landscapes.*

Keywords— Ontology, Ransomware Behavior, Ransomware.

# Introduction

## Project’s Background

Cyberattacks are becoming increasingly complex, with ransomware emerging as a major threat to global information security. Ransomware encrypts data or systems until a ransom is paid, but even payment does not guarantee data recovery, and attackers may continue to demand more payments.

The first ransomware attack, the “AIDS Trojan,” appeared during the AIDS pandemic in the early 1980s. By 2012, ransomware had evolved significantly, becoming more complex and dangerous. In late 2016, the U.S. Department of Justice reported over 4,000 daily ransomware attacks, a 300% increase from 2015 [1].

In 2018, although the number of attacks decreased, the threats intensified as attackers began using cryptocurrencies like Bitcoin, leading to fewer but more profitable attacks [2, 3]. By early 2020, ransomware attacks targeted high-profile entities. For instance, on March 25, 2024, VNDirect, a Vietnamese securities brokerage, was forced to shut down its trading system after a ransomware attack, resulting in significant financial losses, including an 18% drop in net profit and a loss of VND 538 billion (USD 21.27 million) [4, 5].

Cybersecurity Ventures predicts that ransomware damages will reach $265 billion by 2031, including ransom payments, data recovery costs, business downtime, and other expenses [6]. The actual number of attacks may be higher than reported due to underreporting by victims [7].

## Problem Statement

According to Gartner, the first cybersecurity trend of 2023 is the adoption of human-centric security design, emphasizing employee roles in the cybersecurity lifecycle. By 2027, 50% of CISOs at large enterprises are expected to implement these measures to mitigate risks and optimize controls [8]. This aligns with the Integrated Information Assurance Framework, which highlights the importance of technical and human elements in Security Countermeasures [9]. The framework identifies three key components: Security Services, Information States, and Security Countermeasures, focusing on Technology, Policy & Practice, and People [10].

Addict noted that traditional cybersecurity awareness programs have failed to reduce insecure employee behavior significantly [8]. Organizations need a flexible approach, treating training as a continuous process to equip employees with the skills to respond to threats, enhancing overall security [11].

Despite the growing threat of ransomware, there is no comprehensive knowledge base for extortionate ransomware [7]. Understanding crucial aspects for monitoring, investigation, or prevention requires deep analysis of malware behavior and system interactions. Developing an ontology for extortion-based attacks can provide a standardized vocabulary for describing ransomware and related components [7].

As threats evolve, new methods for understanding ransomware behavior are essential [7]. Botacin and his partner presented a longitudinal analysis of security solutions, evaluating them using six metrics [12]. Identifying common characteristics across ransomware strains helps distinguish them from benign software [7]. An ontology-based representation can provide a structured framework for analyzing ransomware, enhancing understanding and response strategies.

## Research Objectives

The main objective of this research is to develop a knowledge representation using ontology to describe the behavior of ransomware. Specifically, the research aims to:

* Develop an ontology framework capable of representing concepts and behaviors related to ransomware.
* Promote widespread awareness to develop effective solutions, including early threat detection systems, digital forensics, and especially ransomware awareness training for engineers and end users. Enhancing understanding of ransomware behavior serves as the foundation for prevention strategies.

## Significance of the Study

This research enhances knowledge about ransomware, addressing the scarcity and inaccessibility of market information [7]. Training users to understand ransomware behavior enhances their ability to detect and respond to threats effectively. By utilizing ontology-based knowledge representation, this study contributes to cybersecurity by helping individuals grasp specifying ransomware characteristics. This understanding enables security professionals to predict and infer the future trajectory of ransomware, thereby preventing attacks, conducting digital investigations, and training personnel, ultimately minimizing future risks and damages.

## Scope and Limitations

This research centers on constructing and utilizing an ontology to represent knowledge about ransomware, particularly focusing on file-encrypting ransomware behavior for easier analysis and to mitigate system encryption disruptions. The study primarily examines ransomware employing hybrid encryption methods, which are commonly used by many ransomware variants today. Additionally, it delves into the most complex ransomware types that leverage C&C servers and Tor networks to enhance anti-tracking measures. The propagation of ransomware underscores its increasing threat level, demanding more sophisticated analysis to address its dangers.

The rest of this paper is organized as follows. In Section II, the related work is provided. Then, we describe in detail the overall architecture of our proposed model in Section III. Next, the experiments and results are reported in Section IV. Finally, we conclude in Section V.

# LITERATURE REVIEW

## Review of Previous Studies

Ontology-based frameworks are increasingly recognized as powerful tools for representing and analyzing ransomware behavior. Previous studies have emphasized the need for structured knowledge representation in cybersecurity to enhance the detection, prevention, and mitigation of ransomware threats. A significant study by **Keshavarzi and Ghaffary (2022)** explored the potential of ontology in representing knowledge about digital extortion attacks, providing a foundational framework that can be applied to ransomware [7]. Their approach demonstrates that ontology can define stages, attack methods, and relationships between malware behaviors, contributing to the advancement of digital forensics. However, their work primarily focuses on general extortion frameworks and does not delve deeply into the evolving nature of ransomware, leaving room for further exploration.

**Nair and Ramesh (2024)** proposed a novel semantic model that uniquely represents ransomware’s behavioral characteristics, addressing inconsistencies in traditional ransomware labeling methods, which often lead to conflicting aliases and hinder unified analysis. [13]. However, the model fails to clarify the specific actions and commands involved in connecting to the victim's server via Tor as well as the use of encryption methods, whether symmetric or asymmetric, for encrypting the data files on the compromised machine.

**Mourad Benmalek (2024)** focuses on classifying ransomware threats targeting Cyber-Physical Systems (CPS). Ransomware attacks on CPS can disrupt both physical infrastructure and network operations, posing significant risks to critical sectors. Their work presents a static taxonomic approach that categorizes ransomware based on the types of CPS it targets [14]. Their static taxonomic approach categorizes ransomware based on CPS types but lacks an ontology or knowledge graph to visually represent ransomware knowledge and does not address specific behavioral aspects.

**Ipshita Roy Chowdhury and Deepayan Bhowmik (2023)** introduced a multi-layered ontology framework to optimize ransomware detection strategies [15]. This framework identifies ransomware behaviors from early stages, aiding early detection. However, it focuses on identifying characteristics rather than providing specific defense measures.

**Craig Beamana, et al. (2021)** developed an ontology-driven model combining knowledge graphs with malware behavior analysis to enhance ransomware traceability [16]. Their model tracks interactions among malware elements, enabling quick identification of attack vectors. However, it focuses on broader malware interactions rather than ransomware-specific strategies.

## Summary of the Literature Review

Despite advances in traditional cybersecurity methods, ransomware attacks continue to grow in complexity, outpacing current detection techniques. Ontology-based frameworks offer significant flexibility and scalability in representing and analyzing ransomware behavior. However, further development is needed to address the sophisticated deployment tactics of modern ransomware variants. Including traceability models adds a new dimension to tracking and mitigating ransomware attacks.

## Contribution of Research

This research develops an ontology-based framework to represent ransomware behavior, supporting early threat detection, digital forensics, and ransomware training. It bridges the gap between theory and practice, enhancing understanding and prevention of ransomware threats.

# METHODOLOGY

## Research Design

This study analyzes and models the lifecycle of a typical ransomware attack, focusing on three primary stages: Phishing, Behavior, and Payment. Each stage includes unique aspects that contribute to the overall function of ransomware, capturing both overt and covert actions.

In the **Phishing** phase:

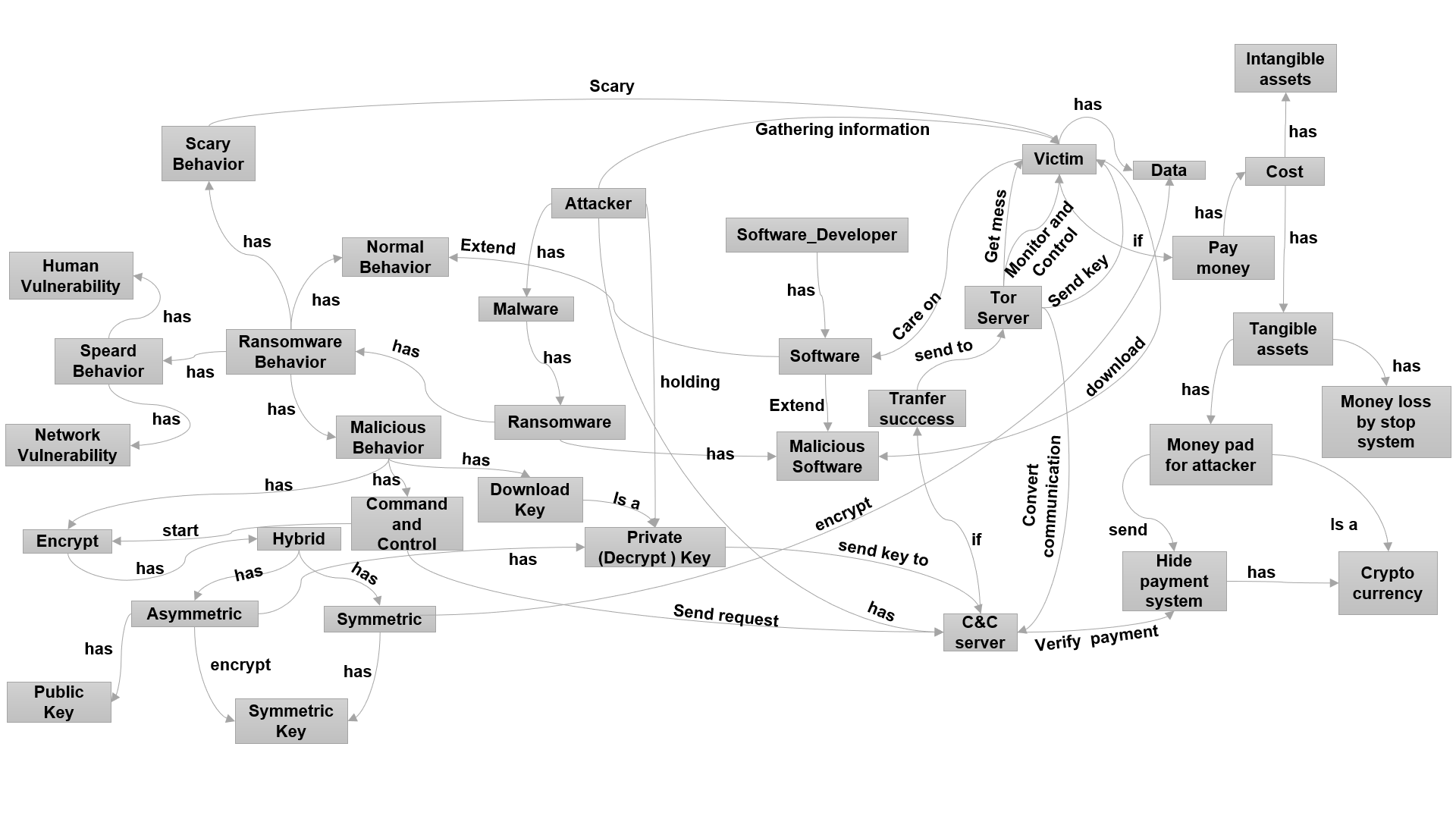
* Collecting information about the victim (email, online behavior, and interests). This helps them craft more convincing phishing messages.
* Using the gathered information, attackers create a deceptive message, often an email, designed to trick the victim.
* Attackers send the phishing message to the victim. This may involve sending emails, text messages, or other forms of communication.

The **Behavior** phase:

* Normal behavior: completely inherited from the application that the victim is interested in.
* Abnormal behavior:
* Connecting to C2 to be able to control the victim's computer through Tor Server to avoid tracking.
* Encrypting the victim's data with symmetry and using asymmetric encryption to encrypt the symmetric encryption key.
* Spreading behavior:
* Through user vulnerabilities: such as clicking on phishing emails or copying malicious files from one computer to another.
* Through network vulnerabilities.
* Threatening behavior to users: Change the screen and display a ransom demand

The **Payment** phase:

* The attacker demands payment in cryptocurrency so that the system can transfer money anonymously.
* Attackers may use various communication channels, including the C2 server, email, or chat applications to check the payment and then send the decryption key back to the victim.
* Damages suffered by the victim:
* Invisible: Loss of customer trust, damage to brand image, lost productivity, psychological impact on employees...
* Tangible: Ransom payment, recovery costs, legal fees, and lost revenue.



1. *Ontology Knowledge Graph.*

This ontology captures specific details across each phase, allowing for a systematic representation of ransomware behaviors and stages within an ontology framework. In addition to encrypting files, ransomware can also access the C2 server in order to keep control. Activities that entail just authorized access are considered normal behavior, and they inherit the characteristics of the applications that the victim is interested in.

## Sampling Data Analysis Techniques

Creating a ransomware knowledge base helps cybersecurity analysts categorize, understand, and respond to different types of ransomwares more effectively. By building a structured database with details on ransomware families, sample sizes, first appearances, and behavior patterns, security professionals can streamline analysis and enhance threat detection. Our knowledge base includes data from sources like VirusTotal and Malware Bazaar, focusing on a comprehensive view of each ransomware family’s characteristics and evolution.

1. Ransomware Statistics by Year and Sample Size.

|  |  |  |  |
| --- | --- | --- | --- |
| Ransomware Family | Sample size | First Year of Appearance | Last Year of Appearance |
| Locky | 28 | 2016 | 2017 |
| Cerber | 25 | 2016 | 2019 |
| CryptoBit | 12 | 2016 | 2017 |
| Lockbit | 31 | 2019 | 2024 |
| WannaCry | 22 | 2017 | 2024 |
| Petya | 13 | 2016 | 2017 |
| TeslaCrypt | 15 | 2015 | 2016 |
| Babuk | 23 | 2020 | 2021 |

Each of these ransomware families presents distinct characteristics, infection methods, and encryption techniques that make them valuable for study and inclusion in a comprehensive cybersecurity knowledge base.

Ransomware has gone through several iterations, each with its own set of characteristics, key inflection points, and advanced encryption techniques. TeslaCrypt (2015-2016) was a ransomware that targeted game files, but it quickly stopped working after the inventor provided a public decryption key. Petya (2016-2017) was known for overwriting the Master Boot Record (MBR), rendering machines unbootable, but declined as patches and decryption tools were discovered. Locky (2016-2017) spread by phishing emails, however its influence faded as security awareness improved. Cerber (2016-2019), with its "Ransomware-as-a-Service" (RaaS) model, facilitates large-scale attacks, but was eventually weakened by the availability of free decryption tools. CryptoBit (2016-2017) and WannaCry (2017-2024) both showed their power by exploiting security flaws, with WannaCry launching a global attack in 2017.

Additionally, Lockbit (2019-2024) distinguished out for its fast encryption speed and dual threat strategy (encryption and data theft), making it the most formidable ransomware today. Babuk (2020-2021) targeted large corporations but was quickly weakened as its source code was leaked. Technically, these ransomware often employ strong encryption techniques such as AES, RSA, or ChaCha20, rendering the encrypted data nearly impossible to decrypt without the decryption key. Significant inflection points are often reached when ransomware causes large-scale attacks or when the security community develops effective protections, which diminish or disappear.

## Limitations of the Methodology

This methodology has several limitations. Constructing an ontology based on a fixed timeline may not capture evolving ransomware techniques, resulting in an incomplete representation. Reliance on simulated data may not reflect real-world complexities, affecting accuracy. The focus on typical attack techniques might omit advanced methods like multi-extortion tactics. Dependency on a single data source may limit representativeness, suggesting future research should incorporate real-world data, multiple sources, and dynamic timelines to better capture the evolving ransomware landscape.

# EXPERIMENTAL AND RESULTS

## Introduction

This project focuses on developing an ontology-based schema to depict the relationships and processes in a ransomware attack. Ontology diagrams visualize complex systems by representing concepts and their interconnections. For ransomware, an ontology diagram illustrates how vulnerabilities, malicious behaviors, encryption methods, and assets interact, providing a comprehensive view of the cyber-attack lifecycle.

Key methods include identifying primary entities (e.g., “Attacker,” “Victim,” “Malware”) and establishing their relationships. These entities are broken down into actions and attributes (e.g., “Encrypt,” “Command and Control,” “Pay Money”), representing the attack’s sequential steps. The diagram differentiates between types of vulnerabilities (e.g., human, network) and their role in spreading ransomware.

The project aims to offer a framework for understanding ransomware mechanisms, aiding cybersecurity professionals in identifying vulnerabilities and developing mitigation strategies. The ontology diagram serves as show ransomware attacks flow and study their impact on assets.

## Presentation of Data

This section presents the classes and properties Group developed within the ontology to clearly model the elements and relationships involved in a ransomware attack. Designed to thoroughly analyze ransomware behavior, this ontology, named **CyberRanto**, includes key classes and properties that accurately represent the attack cycle.

### **Metrics Summary**

* **Class Count**: 35
* **Object Property Count**: 23
* **Axioms: 2**

The classes and object attributes form the foundation for the CyberRanto ontology, enabling the detailed modeling and analysis of relationships and behaviors within a ransomware attack. This serves as a powerful tool for in-depth ransomware research as well as supporting the development of effective countermeasures in the field of cybersecurity.

## Analysis of Results

This section delves into an in-depth analysis of the gathered data, aimed at assessing the effectiveness and implications of each observed phase of the ransomware attack. The analysis is structured to address each stage, beginning with the initial phase of Phishing and Exploitation.

This version provides a smooth transition into a detailed breakdown, setting up the analysis as a critical step in interpreting the experimental results.

### Axioms:

#### Encryption as Normal Behavior:

In analyzing ransomware behavior, we observe that encryption itself is not inherently malicious, as it is a standard functionality in many legitimate applications. If no references explicitly affirm this, we can demonstrate it by showing that numerous applications, such as file compression tools, secure messaging apps, and cloud storage services, rely on encryption for normal operations [17]. This supports the argument that encryption alone cannot definitively indicate ransomware activity without considering its context and execution patterns.

#### The Role of Payment Methods in Ransomware Evolution:

The adoption of Cryptocurrency marked a turning point in ransomware operations, enabling anonymous, decentralized transactions that fueled its rise as a scalable criminal industry. As Bitcoin becomes more traceable, ransomware operators are likely to shift to alternative payment methods like decentralized finance (DeFi) systems or privacy-focused cryptocurrencies [18]. These alternatives, powered by smart contracts and decentralized structures, could offer greater anonymity and flexibility, allowing ransomware to evolve further. Tracking and regulating these systems is crucial to mitigating future ransomware threats.

## Interpretation of Results

### Instances

Corresponding to the Ransomware samples we have applied to our Ontology diagram; our Ontology diagram reflects what the Ransomware Samples can do.

### Benefits

Enhanced framework empowering employees to identify and respond to security threats through comprehensive security training and advanced ransomware data analysis.

## Comparison with Literature

### Clarifying the Detailed Lifecycle of Ransomware Attacks:

Our research provides a comprehensive view of each stage in the ransomware lifecycle, covering information gathering, malware deployment through phishing, data encryption, and ransom demands. This detailed approach is often overlooked in existing studies, which primarily focus on classification or offer an overview. For example, some studies emphasize classification and security challenges in Cyber-Physical Systems (CPS) but do not delve deeply into each step of the ransomware lifecycle [14]. Similarly, a semantic framework standardizes ransomware information but does not detail each deployment phase [13].

### In-depth Analysis of Ransomware Encryption Techniques:

CyberRanto describes hybrid encryption mechanisms used by ransomware, combining symmetric encryption for speed and asymmetric encryption for key protection. This analysis highlights the complexity of ransomware’s encryption techniques and victim dependency. In contrast, existing studies rarely explore these technical details. For instance, one study focuses on the ransomware landscape during the COVID-19 pandemic and prevention measures but lacks a deep analysis of encryption methods [16]. Another study examines malware behavior and evolution but does not describe specific encryption mechanisms [15].

### Identifying Detailed Ransomware Behaviors through Ontology-based Mapping:

This study thoroughly analyzes ransomware’s deceptive behaviors, including masquerading as legitimate software and establishing command-and-control (C2) connections through the Tor network. This provides insights into how ransomware conceals its actions and maintains control. Existing studies often lack specifics on these behaviors. Some research classifies ransomware by targets and objectives but does not elucidate deceptive strategies [14]. Another paper introduces a knowledge-organizing system for ransomware but does not analyze evasion and control tactics [7].

### Comprehensive View of Ransomware Impact on Victims:

CyberRanto offers a thorough analysis of ransomware’s impact on victims, including financial and non-financial consequences such as reputational loss and loss of customer trust. This aspect is often insufficiently addressed in other studies. For instance, one publication introduces the “Rantology” system to organize ransomware-related knowledge but lacks a detailed analysis of real-world impacts on victims [7]. In contrast, CyberRanto provides a more comprehensive view of these consequences, enhancing understanding of ransomware’s long-term effects on victims.

## Implications of the Results

This study yielded a clear and detailed ontology-based framework for understanding and interpreting the stages of a ransomware attack lifecycle. This framework has potential applications across various corporate security domains. Key implications of this research include:

### Application in Security Drills within Organizations:

### The framework can be used in internal drills to help employees understand each stage of a ransomware attack, enhancing their response capabilities and reducing real-world risks.

### Providing Detailed Insights into Ransomware Behavior:

### The study clarifies specific ransomware behaviors, such as masquerading as legitimate software, establishing C2 connections, and deploying hybrid encryption. These insights help analysts identify and monitor ransomware indicators, improving response capabilities

### Enhancing Cybersecurity Awareness Training:

### The framework aids in post-attack investigations and digital forensics, helping analysts track each stage of ransomware within a compromised system and identify attack methods.

### Supporting Digital Forensics:

### The framework aids in post-attack investigations and digital forensics. Analysts can use the model to track each stage of ransomware within a compromised system, identifying and documenting attack methods for source detection.

# DICUSSION

## Restate the Research Problem or Objectives

This study aimed to develop an ontology-based framework to describe the lifecycle and behaviors of ransomware attacks, addressing limitations of prior frameworks that focused only on classification or static stages. Despite providing a comprehensive view, limitations include the absence of real-world data, lack of real-time updates, and the need for manual data integration. Future research should focus on integrating recent attack data, enabling continuous updates, and automating data collection using AI techniques.

## Summarize Key Findings

Key findings include the construction of a detailed ontology-based framework describing each stage of a ransomware attack, from information gathering to ransom demands. The study clarified complex encryption techniques, providing insights into ransomware’s deceptive tactics and control behaviors. This framework aids cybersecurity analysts in identifying attack signs and can be used in security drills and training to enhance awareness and preventive skills among employees:

* Stage of Ransomware Attack: Description from phishing to payment.
* Complex Encryption Techniques: Hybrid encryption technique.
* Framework helps employees: Preventive skills training.

# CONCLUSION AND FUTURE WORK

## Conclusion

This study highlights the increasing sophistication of ransomware and its ability to evade detection by mimicking legitimate applications. Traditional antivirus (AV) systems face challenges, especially during file encryption stages. A comprehensive ransomware prevention strategy must address various attack phases.

The study outlines a phased detection approach to improve ransomware identification, starting from the initial **Phishing or Exploit Phase**. Here, monitoring systems should detect unusual data-gathering activities and alert users to suspicious emails or unverified downloads. Automation potential through AI-powered phishing detection can further enhance early intervention. In the **Behavior Phase**, identifying both normal and malicious behaviors, such as abnormal Command and Control (C2) connections, hybrid encryption actions, and spread mechanisms, can help differentiate ransomware from legitimate applications. Lastly, in the **Ransom Demand Phase**, immediate alerts on ransom requests and anonymous payment systems should be triggered, with automated warnings for any suspicious cryptocurrency-related transactions post-encryption.

Human vigilance is crucial in early detection, particularly against phishing and social engineering tactics. Educating users to identify phishing emails and malicious links can reduce ransomware infiltration opportunities. Demonstrations show that standard AV systems often struggle to detect novel ransomware strains until significant damage occurs, highlighting the need for a multi-layered approach combining AV, behavioral monitoring, and human awareness. The absence of real-time data integration from actual ransomware attacks limits the model’s accuracy.

A proactive, multi-phase approach to ransomware detection and prevention, encompassing advanced AV tools, human awareness, and real-time behavioral analysis, is crucial in safeguarding organizational networks and critical data assets against ransomware threats.

## Future Work

Future research could explore leveraging large language models (LLMs) for ransomware detection by analyzing actions leading up to or following encryption, rather than focusing solely on the encryption phase. Integrating data from real-world ransomware attacks into LLM training could improve the framework's accuracy and adaptability. Additionally, developing a real-time update mechanism for this LLM-powered framework would enhance its effectiveness in identifying and mitigating emerging threats. Finally, expanding the scope to enable cross-organizational information sharing and collaboration would contribute to a robust knowledge base, benefiting the broader cybersecurity community.

##### Acknowledgment

We extend our sincere gratitude to **Mr. Hoang Manh Duc** for his invaluable guidance and support throughout our Capstone Project. His feedback has been instrumental in shaping our project's direction and content.

We also thank **FPT University** and the **Ministry of Education and Training** for providing the facilities and academic environment that enabled us to complete this initial phase.

Additionally, we acknowledge the valuable **reference materials** and **research papers** that significantly contributed to our work, particularly the insights from the referenced paper.

Lastly, we appreciate the dedication and collaboration of all team members: **Nguyen Duc Anh, Nguyen Huy Nhat, Nguyen Viet Chien, Doan Duy Huy, and Ta Viet Nam**.

##### References

[1] U.S. Government, "How to protect your networks from ransomware," The U.S. Department of Justice. [Online]. Available: <https://www.justice.gov/criminal/criminal-ccips/file/872771/dl>

[2] S. Frankoff and B. Hartley, "Big game hunting: The evolution of INDRIK SPIDER from Dridex wire fraud to BitPaymer targeted ransomware," CrowdStrike, Nov. 14, 2018. [Online]. Available: <https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/>

[3] M. Osena, "Cryptocurrency-mining malware: 2018’s new menace?," TrendMicro, Feb. 28, 2018. [Online]. Available: <https://www.trendmicro.com/en_us/research/18/b/a-mining-malware-2018-new-menace.html>

[4] L. Robert, "Ransomware, junk bank accounts: Cyber threats proliferate in Vietnam," DarkReading, Apr. 3, 2024. [Online]. Available: <https://www.darkreading.com/cyber-risk/ransomware-junk-bank-accounts-cyberthreats-proliferates-in-vietnam>

[5] N. Diem and H. Yen, "Ransomware attack-hit VNDirect Securities sees 18% drop in Q2 net profit," The Investor, Jul. 26, 2024. [Online]. Available: <https://theinvestor.vn/ransomware-attack-hit-vndirect-securities-sees-18-drop-in-q2-net-profit-d11439.html>

[6] S. Morgan, "Global ransomware damage costs predicted to exceed $265 billion by 2031," Cybersecurity Ventures, Jul. 7, 2023. [Online]. Available: <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>

[7] M. Keshavarzi and H. R. Ghaffary, "An ontology-driven framework for knowledge representation of digital extortion attacks," Islamic Azad University of Ferdows Branch, Iran, Oct. 18, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0747563222003405>

[8] Gartner, "Gartner identifies the top cybersecurity trends for 2023," Stamford, Connecticut, Apr. 12, 2023. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023>

[9] A. Darwish, P. Choe, “A Framework of Information Security Integrated with Human Factors,” in Proceedings of the International Conference on Information Security, 12 June 2019, pp. 217–229. [Online]. Available: [https://link.springer.com/chapter/10.1007/978-3-030-22351-9\_1](https://link.springer.com/chapter/10.1007/978-3-030-22351-9_15)5

[10] D. Kim and M. Solomon, Fundamentals of Information Systems Security, FPT University: Jones & Bartlett Learning, 2014. [Online]. Available: <http://ds.libol.fpt.edu.vn/handle/123456789/2554>

[11] E. Ukwandu, M. A. B. Farah "A Review of Cyber-Ranges and Test-Beds: Current and Future Trends," Sensor Networks, 13 December 2020. [Online]. Available: <https://www.mdpi.com/1424-8220/20/24/7148>

[12] M. Botacin, F. D. Domingues, F. Ceschin, R. Machnicki, M. A. Z. Alves, P. L. de Geus, and R. Grégio, "AntiViruses under the microscope: A hands-on perspective," A. Brazil, Nov. 5, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/abs/pii/S0167404821003242>

[13] A. R. Nair and G. Ramesh, “Ontology-Driven Behavioral Model for Ransomware Traceability,” 2024. [Online]. Available: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4779064>

[14] Mourad Benmalek "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges" Internet of Things and Cyber-Physical Systems 4, 6 January 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2667345223000561>

[15] Ipshita Roy Chowdhury, Deepayan Bhowmik "Capturing Malware Behaviour with Ontology-based Knowledge Graphs" Division of Computing Science & Mathematics, University of Stirling, April 01,2023. [Online]. Available: https://www.researchgate.net/publication/363872971\_Capturing\_Malware\_Behaviour\_with\_Ontology-based\_Knowledge\_Graphs

[16] Craig Beamana, et al. "Ransomware: Recent advances, analysis, challenges and future research directions “Computers & Security, December 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S016740482100314X>

[17] José. H, et al. " Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges" Electronics 2023, 12(21), 4494, 1 November 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/21/4494

[18]  [Masarah Paquet-Clouston](https://arxiv.org/search/cs?searchtype=author&query=Paquet-Clouston,+M), et al. "Ransomware Payments in the Bitcoin Ecosystem" Cryptography and Security (cs.CR),Wed, 11 Apr 2018 . [Online]. Available: https://arxiv.org/abs/1804.04080