**UNIVERSITY OF ZIMBABWE**

****

**FACULTY OF COMPUTER ENGINEERING INFORMATICS AND COMMUNICATION**

**DEPARTMENT OF INFORMATICS AND ANAYLTICS**

STUDENT NAME: ELTON TANAKA MUKARATI

REG NUMBER: R217057T

DEGREE PROGRAMME: BACHELOR OF SCIENCE HONORS IN CYBERSECURITY AND FORENSIC AUDIT (HCF)

MODULE: CAPSTONE PROJECT HCF460

TOPIC: BEHAVIORAL PROFILING FRAMEWORK FOR RANSOMWARE DETECTION: A CONTROLLED ENVIRONMENT STUDY

AREA of RESEARCH: MALWARE ANALYSIS

Contents

[**1** **CHAPTER 1: INTRODUCTION** 4](#_Toc192974531)

[1.1 Introduction 4](#_Toc192974532)

[1.2 Background of the Study 5](#_Toc192974533)

[1.3 Problem Statement 6](#_Toc192974534)

[1.4 Research Objectives 7](#_Toc192974535)

[1.5 Research Questions 7](#_Toc192974536)

[1.6 Significance of Research 7](#_Toc192974537)

[1.7 Scope or Limitations of the Study 7](#_Toc192974538)

[1.8 Structure of the Dissertation 10](#_Toc192974539)

[*Figure 1: Predicted damage cost of Ransomware attack* [1][7]*.* 5](#_Toc192974428)

# **CHAPTER 1: INTRODUCTION**

## Introduction

Ransomware is a type of malicious software that encrypts a victim’s data and demands payment for its release and has become one of the most common and damaging threats in the world of cybercrime [1]. What began as isolated incidents carried out by individual hackers has now transformed into a sophisticated, large-scale operation orchestrated by organised crime groups. These crime groups leverage ransomware to extort large sums of money, exploiting widespread cybersecurity weaknesses and causing billions of losses financial. This research article plunge deep into the evolution of ransomware, its role as a primary tool used for organised crime, and the far-reaching consequences of its continued consequences. [2] Although ransomware is a growing threat, many individuals are still short-informed and do not implement and practice necessary security precautions for them not to be victims and the financial damages could result up to 1 billion from this malicious software, which locks victims from accessing their devices or data until a ransom is paid [3]. [2]Cybercriminals take advantage of this information gap to use automated methods to extort money from unwary individuals. [4]The risks are made worse by the state of technology that contains many vulnerabilities, which has increased ransomware assaults worldwide. [5]The staggering 600% rise in Locky and Crypto illustrates how widespread this threat is worldwide as shown on Figure 1 with a predicted damage costs of up to 200billion dollars in 2021 [5].

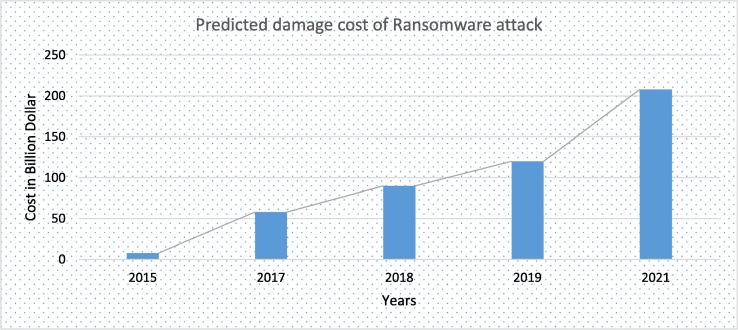
Ransomware has rapidly increased in both scale and impact, largely due to the expansion of the internet and the widespread adoption of cloud platforms, which have made it easier for attackers to exploit vulnerabilities. This worrying trend highlights the urgent need to educate employees and organisations about ransomware risks to strengthen cybersecurity defences [6]. As businesses continue to face the growing threat of ransomware, it is essential to explore all necessary strategies for effective defence. One promising approach involves analysing the psychological and behavioral characteristics of cybercriminals to develop a behavioural profiling framework, which could significantly enhance cybersecurity measures [7] and by implementing such a framework, experts and researchers can gain deeper insights into the tactics used and intentions of ransomware attackers, enabling the development of more targeted and effective preventative measures.

This research aims to address existing knowledge gaps and explore strategic approaches to understanding ransomware including both its attack methodologies and variants, with a specific focus on behavioral profiling as a proactive cybersecurity mechanism. By emphasising the significance of enhancing awareness and implementing robust security measures, the study seeks to contribute to the mitigation of risks associated with ransomware attacks. Through this lens, the research underscores the critical role of proactive strategies in strengthening cybersecurity frameworks and reducing the impact of ransomware on individuals, organisations, and broader digital ecosystems

## Background of the Study

Ransomware has emerged as a significant and escalating global threat, exploiting vulnerabilities in digital systems to cause widespread disruption and financial losses. The Covid-19 pandemic exacerbated this issue, with ransomware attacks doubling during this period, as cybercriminals capitalised on the rapid shift to remote work and increased reliance on digital infrastructure [9]. In 2021, a new vulnerability was recorded every 24 minutes, highlighting the growing attack surface for ransomware operators [8]. Incident response engagements related to ransomware surged by 240% over the past two years, with web applications and application-specific attacks accounting for 72% of all incidents [8]. These attacks are not confined to developed nations; even countries like Zimbabwe have faced significant impacts, as evidenced by the 2017 WannaCry ransomware attack, which affected systems in 104 countries, including Zimbabwe, Russia, the UK, Ukraine, and China [9]. The attack exploited a known Microsoft vulnerability leaked by the Shadow Brokers group, demanding $300 in Bitcoin for file restoration and doubling the ransom after three days [9]. The consequences were catastrophic, underscoring the urgent need for robust cybersecurity measures and proactive strategies to mitigate the risks posed by ransomware.

Despite the increasing frequency and impact of ransomware attacks, many individuals and organisations remain inadequately prepared to defend against them. While awareness of ransomware and its devastating impact has grown, particularly in region counties like Zimbabwe, significant barriers for effective prevention and response persist. In the developing countries, challenges such as the high cost of mobile data and limited access to cybersecurity resources often hinder users from implementing basic protective measures, such as enabling regular software updates. For businesses, the lack of prioritisation of cybersecurity, together with limited knowledge of available tools, worsen the problem. Many organisations remain unaware of straightforward prevention techniques, such as sandboxes, which can mitigate the risk of catastrophic losses [9]. These gaps in preparedness highlight the urgent need for improved education, resource allocation, and proactive cybersecurity strategies to address the growing ransomware threat.



*Figure 1: Predicted damage cost of Ransomware attack* [1][7]*.*

## Problem Statement

[10]Ransomware attacks are becoming more frequent and sophisticated worldwide, revealing major weaknesses in traditional cybersecurity defenses. [11]Many of these defenses rely on outdated methods like static and signature-based detection, which struggle to keep up with the constantly changing nature of ransomware. Despite the severe damages both in operation and financially caused by the ransomware attacks, many organisations and individuals, especially in developing countries and regions like Zimbabwe are still unprepared [12]. Limited resources, lack of awareness, and insufficient access to advanced cybersecurity tools leave them vulnerable. The 2017 WannaCry attack, which impacted Zimbabwe and over 100 other countries, is a stark reminder of how urgent it is to find better ways to fight this growing threat [13].  
  
This research focuses on tackling these challenges by developing and testing a behavioral profiling framework for ransomware detection. [14]The aim is to identify key behavioral patterns in a controlled environment that can differentiate between different ransomware variants and normal system activity and by doing so, the framework improves the detection capabilities and strengthen overall cybersecurity resilience against ransomware attacks.

## Research Objectives

1. To develop a behavioral profiling framework for ransomware detection.
2. To evaluate the effectiveness of the framework in identifying ransomware variants.
3. To identify key indicators that differentiate various ransomware strains and types.

## Research Questions

1. What techniques are needed to develop a behavioral profiling framework for ransomware detection?
2. How well does the suggested framework differ from already existing techniques.
3. What markers are going to be used to differentiate various ransomware strains.
4. How do the various ransomware strains affect the frameworks’ ability to identify and distinguish

## Significance of Research

Businesses, cybersecurity experts, and individual users are among the many stakeholders who stand to gain from applying behavior profiling to counter and reduce ransomware incidents. Organizations can reduce the financial effect of ransomware attacks, because its effect causes major operational interruptions, and they better secure their sensitive data by strengthening cybersecurity procedures [15]. Cybersecurity teams will be better equipped to recognize and react to new ransomware strains thanks to enhanced detection systems based on behavioral profiling, guaranteeing a proactive defense approach. Additionally, encouraging innovation in cybersecurity by investigating novel technologies can result in the development of cutting-edge solutions that improve overall resistance to ransomware attacks. In addition to protecting important assets, this team effort makes the digital world safer.

## Scope or Limitations of the Study

This research will mainly focus on the development and evaluation of a behavioral profiling framework that will be used analyse ransomware strains because traditional signature-based methods have proved inadequate in the ever-evolving world, However, the research will not involve an attack being conducted on anyone as it will be done in a controlled environment. It will not also consider the economic or legal implications of ransomware and the ethical implications of ransomware. The research and study will focus on automated tests rather than the manual methods. It will also consider the impact of ransomware attacks on individuals and companies. Lastly, it will also include future research gaps that can be partaken in

Ransomware attacks have become a significant global threat, exposing the limitations of traditional cybersecurity defenses, particularly the static and signature-based detection methods. This research focuses on addressing the limitations by the development and evaluation of a behavioral profiling framework for ransomware detection. The framework aims to identify key behavioral markers that distinguish ransomware activity from normal system operations, providing a more effective solution to combat evolving ransomware variants. However, the study is bound by specific scopes and limitations, which are essential to understand its focus and potential constraints.  
  
The scope of this research is primarily centered on the development and testing of a behavioral profiling framework in a controlled environment and unlike traditional methods, which rely on known signatures, this framework analyses the behavioral patterns of ransomware strains to detect and mitigate the threats. To ensure ethical and safe experimentation, the study will not involve conducting actual ransomware attacks on any individuals or organisations. Instead, simulations will be used to replicate ransomware behavior in a secure, isolated setting. This approach allows for the safe analysis of ransomware without risking harm to real systems or data.  
  
Additionally, the research will prioritise automated testing methods over manual techniques. Automated testing ensures scalability, consistency, and efficiency in analysing ransomware behavior, making it a practical choice for large-scale applications. The study will also consider the impacts both operationally and psychologically on individuals and organizations, providing insights into how the proposed framework can mitigate these effects. The research will also identify gaps in current knowledge and suggest areas for future studies, contributing to the ongoing development of ransomware detection and prevention strategies.   
  
Physically, the research depends on simulated ransomware attacks and synthetic data, which may not fully capture the complexity and unpredictability of real-world threats. Although simulations offer a safe and ethical way to study ransomware behavior, they might lack the dynamic and evolving nature of actual attacks. Methodologically, the use of automated testing, despite being efficient, could miss some behavioral details that manual analysis might catch. Additionally, the framework’s reliance on predefined behavioral markers might limit its ability to detect entirely new or unconventional ransomware tactics.  
  
Theoretically, the study is guided by its narrow focus on behavioral profiling. It does not explore the economic, legal, or ethical aspects of ransomware attacks, which could limit the broader applicability of its findings. Moreover, the proposed framework is specifically for ransomware and may need adjustments to address other types of malware or cyber threats.  
  
Data for the study will come from three main sources namely simulated ransomware attacks, publicly available datasets, and synthetic data generation. Simulations will be carried out using sandboxing tools and virtual machines, ensuring a controlled and secure environment. Publicly available datasets from cybersecurity repositories like VirusTotal or CICMalDroid will be used to validate the framework’s effectiveness. In cases where real-world data is insufficient, synthetic data will be generated to mimic ransomware behavior. While these methods ensure ethical and practical research, they may introduce limitations in terms of real-world applicability.  
  
In conclusion, this research aims to develop a behavioral profiling framework to address the growing threat of ransomware. The study provides a strong also foundation for improving ransomware detection and prevention despite its limitations. By identifying key behavioral markers and using automated testing in a controlled environment, the framework offers a proactive approach to strengthening cybersecurity resilience. Future research can build on these findings to address the identified gaps and further refine the framework for real-world use.

## Structure of the Dissertation

The dissertation is composed of five chapters named Chapter 1 to Chapter 5. Chapter 1 introduces the study, followed by Chapter 2 which contains the Literature Review. This is followed by Chapter 3 which contains the methodology that was used to carry out the study and then Chapter 4 provides the results of the study. Chapter 5 provides the study’s conclusion, recommendations and areas of further study.

**REFERENCES**

[1]Jabid, T., Masum, S., Shams, R.A., Chowdhury, A., Islam, M.M., Ferdaus, M.H., Ali, M.S. and Islam, M., 2025. A Brief History of Ransomware. In *Ransomware Evolution* (pp. 3-17). CRC Press.

[2]Sharma, Nikhil, and Ravi Shanker. "Analysis of ransomware attack and their countermeasures: A review." In *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, pp. 1877-1883. IEEE, 2022.

[3]Khaliq, Khowla, Nor Zairah Ab Rahim, Khalid Hamid, Muhammad Ibrar, Uzair Ahmad and Muhammad Ubaid Ullah. “Ransomware Attacks: Tools and Techniques for Detection.” 2024 2nd International Conference on Cyber Resilience (ICCR) (2024): 1-5.

[4]., 2020, July. The growing influence of ransomware. In *2020 IEEE International Conference on Electro Information Technology (EIT)* (pp. 643-647). IEEE.

[5]., 2023, March. Security Analysis of Ransomware: A Deep Dive into WannaCry and Locky. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 285-294). IEEE.

[6]Urooj, Umara, Bander Ali Saleh Al-rimy, Anazida Zainal, Fuad A. Ghaleb, and Murad A. Rassam. 2022. "Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions" Applied Sciences 12, no. 1: 172. <https://doi.org/10.3390/app12010172>

[7]Kang, Qian & Gu, Yuanyuan.(2023). A Survey on Ransomware Threats: Contrasting Static and Dynamic Analysis Methods. 10.20944/preprints202311.0798.v1.

[8]Farion-Melnyk, A., Rozheliuk, V., Slipchenko, T., Banakh, S., Farion, M. and Bilan, O., 2021, September. Ransomware attacks: risks, protection and prevention measures. In *2021 11th international conference on advanced computer information technologies (ACIT)* (pp. 473-478). IEEE.

[9][L.S.M Kabweza](https://www.techzim.co.zw/author/kabweza/). WannaCry Ransomware: Zimbabwe among countries hit by the massive cyber-attack. <https://www.techzim.co.zw/2017/05/wannacry-ransomware-zimbabwe-amoung-countries-targeted/#:~:text=Zimbabwe%20is%20one%20of%20the,the%20cancellation%20of%20medical%20appointments>. Accessed 22 August 2024

[10]Arabo, Abdullahi & Dijoux, Remi & Poulain, Timothee & Chevalier, Gregoire. (2020). Detecting Ransomware Using Process Behavior Analysis. Procedia Computer Science. 168. 289-296. 10.1016/j.procs.2020.02.249.

[11]. (2024). Enhancing Cybersecurity: Ransomware Detection - A Proof of Concept Study. Journal of Advanced Research in Applied Sciences and Engineering Technology. 252-268. 10.37934/araset.54.2.252268.

[12]Martineau, M., Spiridon, E. and Aiken, M., 2023. A comprehensive framework for cyber behavioral analysis based on a systematic review of cyber profiling literature. *Forensic Sciences*, *3*(3), pp.452-477

[13]Ransomware: Recent advances, analysis, challenges and future research directions. Comput Secur. 2021 Dec;111:102490. doi: 10.1016/j.cose.2021.102490. Epub 2021 Sep 24. PMID: 34602684; PMCID: PMC8463105.

[14](2024). Ransomware Detection through Dynamic Behavior-Based Profiling Using Real-Time Crypto-Anomaly Filtering. 10.31219/osf.io/nvg65

[15]Yuryna Connolly, L., Wall, D.S., Lang, M. and Oddson, B., 2020. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, *6*(1), p.tyaa023.

[16],Internet of things and ransomware: Evolution, mitigation and prevention,Egyptian Informatics Journal,Volume 22, Issue 1,2021,Pages 105-117,ISSN 1110-8665, <https://doi.org/10.1016/j.eij.2020.05.003>.

[17]Fitzgerald, M., 2022. *Tactics, Techniques, and Procedures (TTPs) of Ransomware Groups and the Threats Posed to United States National Security* (Master's thesis, Utica University).

.