**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 ANALYSIS: A CONTROLLED ENVIRONMENT STUDY

AREA of RESEARCH: MALWARE ANALYSIS

Cybersecurity field is always changing, and ransomware has become a serious issue that is affecting not only individuals but organisations and governments worldwide. With the inability of traditional detection techniques to handle the dynamic and complicated nature of ransomware attacks, adaptable and advanced detection systems and mechanisms are needed to be developed. In the same context, the base research paper titled “Automated Ransomware Detection Using Dynamic Behavior Trace Profiling” presents a new method that is very important to the area of research known as “Behavioral Profiling for Ransomware Analysis.” By focusing more on real-time activity analysis over static signatures, the method that was suggested, Dynamic Behavioral Trace Profiling (DBTP) made a huge shift in the ransomware detection mechanism. Dynamic Behavioral Trace Profiling (DBTP) creates more detailed behavioral profiles by the continuous observation of system-level events that include Input or Output Operations, Process manipulation, and network irregularities.

DBTP creates more detailed behavioral profiles that are able to distinguish between benign and harmful activity. With many thanks to the approach of automation and adaptability, which is more important for real time deployment in a large sum of operational scenarios, the system can effectively handle the large volumes of data whilst retaining low detection latency. DBTP can detect unrecognized patterns suggestive of ransomware activity by monitoring the interactions between system resource, network communication, other system level events and software interactions. Improved detection accuracy is the main advantage because even against more advanced ransomware strains that use invasion techniques that undermine conventional detection approaches the use of behavior-based analysis is effective.

The paper also emphasizes how DBTP can be adjusted to new ransomware threats variants without requiring human involvement. It is important that detection models are updated dynamically because ransomware attacks are dynamic, and attackers are always coming up with new ways to avoid detection. By discussing the gaps of existing detection methods, especially static and signature-based approaches, the research stress on the importance of more sophisticated and dynamic methodologies, such as DBTP, for ransomware analysis.

Inconclusion, Dynamic Behavior Trace Profiling offering as an automated and adaptable method described in the publication, offers an advance in the field of ransomware. The research paper highlights the importance of behavior-based analysis in the cybersecurity domain with efforts of providing improved resistance, speed, and accuracy against new ransomware attack strains. Use of automised and real-time behavior analysis, DBTP is a promising development in the ongoing battle against ransomware strains, showcasing its potential to improve the detection method and has significantly impacted my research because there was an outline for the need of a profiling framework that is able copy with the ever-evolving world.