Malware Analysis And Detection

N. Swathi[1], T. Pooja[2], D. Srihari[3], R. Kiran[4], N. Sainath[5]

Assistant Professor, Computer Science Engineering[1]

Students, Computer Science Engineering[2-5]

ACE Engineering College, Ghatkesar, India.

Abstract: *The Malware Analysis and Detection System aims to develop a five-stage process for analyzing and detecting malware in virtualized environments. The process includes installing virtual machines, setting up a controlled laboratory, detonating malware samples, conducting static analysis, executing malware, and developing a web interface for monitoring malware activity. The goal is to enhance cyber defense mechanisms by isolating, studying, and assessing malware behavior. The system will provide a detailed summary of the processes, findings, and future applications of the system, ensuring a user-friendly tool for ongoing detection and analysis efforts.*

Keywords: Hypervisors; FlareVM; strings; reverse engineering; static analysis; dynamic analysis; Process Monitor; Procmon