Abstract

Malware is malicious software or programs that can damage a computer's operating system and network. A lot of research has been done to prevent malware attacks that can cause losses. Researchers have developed a malware detection and classification method based on static and dynamic methods. However, both of these methods have their respective drawbacks, such as the static method's being less effective at detecting new file types and the dynamic method's being more resource-consuming and having a higher cost. Researchers have also developed various techniques for detecting malware based on Pe-Probe's features. To overcome this problem, this final project proposes the development of a malware detection algorithm based on the Pe-Probe feature using machine learning to improve detection and classification accuracy. The method used in this research is a literature study on malware detection and classification, development of a classification algorithm for malware detection based on the Pe-Probe method, prototype development, performance testing, and analysis. This study uses a dataset of 19611 Pe-Probe files, which consist of Pe-Probe data infected and not infected with malware. By using the machine learning stacking model and tuning parameters, the validation results show an accuracy value of 0.978, a detection rate of 0.9905, and a false alarm rate of 0.057.

Keywords: Malware, Machine Learning, Pe-probe.