ABSTRACT

Malware is a kind of software that, if installed on a malware victim's device, might carry malicious actions. The malicious actions might be data theft, system failure, or denial of service. Malware analysis is a process to identify whether a piece of software is a malware or not. However, with the advancement of malware technologies, there are several evasion techniques that could be implemented by malware developers to prevent analysis, such as polymorphic and oligomorphic. Therefore, in this research we propose an automatic malware detection system. In our system, the malware characteristics data were obtained through both static and dynamic analysis processes. Data from the analysis process were classified using Naive Bayes algorithm to identify whether the software is malware or not. The process of identifying malware and goodware files using the Naive Bayes machine learning method has an accuracy value of 93 percent for the detection process using static characteristics and 85 percent for detection through dynamic characteristics.

Keyword: *Malware, Naive Bayes, Static Analysis, Dynamic Analysis, Portable Executable, API Call Sequence.*