Abstract

In recent years, malware (malicious software) has greatly evolved and has become very sophisticated. The evolution of malware makes it difficult to detect using traditional signature-based detection. There are basically two main types of detection techniques : signature-based detection and anomaly-based detection. Signature-based detection method cannot detect unknown malware because a signature from that malware has not been written. To overcome this issue, anomaly-based detection method have been developing to detect unknown malware. This method observe behavior on a system. There are two types of behavior : normal behavior and abnormal behavior. Abnormal behavior is malware.

Anomaly-based detection method issue is false positive and false negative. This issue because rule not effective. So parameter must be analysed before use it on rule. That rule will be testing on malware sample. Compare data testing on signature-based detection. Anomaly-based detection method can detect 77% of malware sample otherwise signature-based detection only 51%. The results show that our approach has high detection accuracy than signature-based detection method.

Keywords : Malware, Anomaly-based Detection, Signature-based Detection, Rule, Accuracy