(1)

Behavior-based features model for malware detection

Hisham Shehata Galal Yousef Bassyouni Mahdy Mohammed Ali Atiea

Abstract:

The sharing of malicious code libraries and techniques over the Internet has vastly increased the release of new malware variants in an unprecedented rate. Malware variants share similar behaviors yet they have different syntactic structure due to the incorporation of many obfuscation and code change techniques such as polymorphism and metamorphism. The different structure of malware variants poses a serious problem to signature-based detection technique, yet their similar exhibited behaviors and actions can be a remarkable feature to detect them by behavior-based techniques. Malware instances also largely depend on API calls provided by the operating system to achieve their malicious tasks. Therefore, behavior-based detection techniques that utilize API calls are promising for the detection of malware variants. In this paper, we propose a behavior-based features model that describes malicious action exhibited by malware instance. To extract the proposed model, we first perform dynamic analysis on a relatively recent malware dataset inside a controlled virtual environment and capture traces of API calls invoked by malware instances. The traces are then generalized into high-level features we refer to as actions. We assessed the viability of actions by various classification algorithms such as decision tree, random forests, and support vector machine. The experimental results demonstrate that the classifiers attain high accuracy and satisfactory results in the detection of malware variants.

Keywords:

Malware, Dynamic-Analysis, Classification

Published In:

Journal of computer virology and hacking techniques , ,