Abstract

Study the behavior of malicious software, understand the security challenges, detect the malware behavior automatically using dynamic approach. Study various classification techniques and to group these malwares and able to cluster different malware into unknown group whose characteristics are not known. The classifiers used in this research are k-Nearest Neighbors (kNN), J48 Decision Tree, and n-grams. Based on the analysis of the tests and experimental results of all the 3 classifiers, the overall best performance was achieved by J48 decision tree with a recall of 96.3%.

References

11. Hengli Zhao, Ming Xu, Ning Zheng, Jingjing Yao, Qiang Hou Malicious executables classification based on behavioral factor analysis.
12. J. Han, M. Kamber, Data Mining: Concepts and Techniques, Morgan Kaufmann, August 2000.

Index Terms

Computer Science Artificial Intelligence

Keywords

Malware, Opcode n-grams, Bytecode n-grams, malware behaviors; malware classification.