Abstract

Development of the internet causes a major problem to the privacy and security of an organization and to personal systems. Security communities receive the huge number of malware every day, Categorization of malware to their corresponding families based on their behaviour is a complex task is to the computer security community. Traditional anti-virus systems based on the signature extraction procedures fail to classify the new malware. Therefore we propose a machine learning model to classify the malware to their corresponding families using the properties of the malware.

In this paper, we present a Review of Mansour Ahmadi et al.’s Feature fusion for effective Malware Family Classification system, Liu et al.’s Automatic Malware classification and detection system, Bashari et al.’s Malware classification and detection system using ANN. Ashu Sharma et al.’s Classification of advanced Malware system. Finally, we have done a comparative analysis of all the above-mentioned methods.
References

1. Mansour Ahmadi, Dmitry Ulyanov, Stanislav Semenov, Mikhail Trofimov, Giorgio Giacinto: Novel Feature Extraction, Selection, and Fusion for Effective Malware Family Classification. CODASPY 2016: 183-194

Index Terms

Computer Science  Artificial Intelligence
Keywords

Windows Malware, Computer Security, Machine Learning, Static Analysis, Malware Classification, Microsoft Malware Data.