Abstract

Recent years have encountered massive growth in malwares which poses a severe threat to modern computers and internet security. Existing malware detection systems are confronting with unknown malware variants. Recently developed malware detection systems investigated that the diverse forms of malware exhibit similar patterns in their structure with minor variations. Hence, it is required to discriminate the types of features extracted for detecting malwares. So that potential of malware detection system can be leveraged to combat with unfamiliar malwares. We mainly focus on the categorization of features based on malware analysis. This paper highlights general framework of malware detection system and pinpoints strengths and weaknesses of each method. Finally we presented overview of performance of present malware detection systems based on features.

References

Comparative Analysis of Feature Extraction Methods of Malware Detection


- M. Z. Shafiq, S. M. Tabish, F. Mirza, and M. Farooq, Pe-miner: Mining structural information to detect malicious executables in realtime, in Proceedings of the 12th International Conference on Novo Tellus:


Comparative Analysis of Feature Extraction Methods of Malware Detection


- Mikhail Zolotukhin, Timo Hamalainen, Support Vector Machine Integrated with Game-Theoretic Approach and Genetic Algorithm for the Detection and Classification of Malware, Globecom 2013 IEEEWorkshop - First InternationalWorkshop on Security and Privacy in Big Data


- Park, Y., Reeves, D., Mulukutla, V. and Sundaravel, Fast Malware Classification by Automated Behavioral Graph Matching. Proceedings of the 6th Annual Workshop on Cyber Security and Information Intelligence Research, Article No. 45,2010.


**Index Terms**

Computer Science

Security
Keywords

Feature Extraction  Malware Detection  Opcodes  Static Analysis  Dynamic Analysis  Machine Learning.