عنوان مقاله:

Behavioral analysis of malware based on data mining and machine learning techniques

محل انتشار:

هفتمین کنگره ملی تازه یافته های مهندسی برق ایران (سال: 1399)

تعداد صفحات اصل مقاله: 10

نویسندگان:

Hamid Tanha - *Master of Information Technology Engineering*

Mahdi Agha Mohammady - *Department of Software Engineering,Yadegare Imam Islamic Azad University, Tehran ،Iran*

Hossein Navazesh - *Master of Software Engineering*

خلاصه مقاله:

Malware as a malicious software poses a major threat to the security of computer systems. The amount and diversity of its variants render classic security defenses ineffective, such that millions of hosts in the Internet are infected with malware in the form of computer viruses, worms , rootkit and Trojan horses. While obfuscation and polymorphism techniques employed by malware largely impede detection at file level, the dynamic analysis of malware binaries during run-time provides an instrument for characterizing and defending against the threat of malicious software.In this article, we propose a model for the automatic analysis of malware behavior using data mining and machine learning. This model allows for automatically identifying novel classes of malware (clustering) and assigning unknown malware to these discovered classes (classification). Based on both, clustering and classification, we propose an incremental approach for behavior-based analysis, capable of processing the behavior of thousands of malware binaries on a daily basis. The incremental analysis significantly reduces the run-time overhead of current analysis .methods, while providing accurate discovery and discrimination of novel malware variants

کلمات کلیدی:

Malware, Malware Detection, Data Mining, Machine Learning, Automatic Analysis, Q-gram Algorithm