عنوان مقاله:

Role-opcode vs. Opcode: the New method in Computer Malware Detection

محل انتشار:

دومین کنفرانس بین المللی شبکه های اطلاعاتی هوشمند و سیستم های پیچیده (سال: 1393)

تعداد صفحات اصل مقاله: 6

نویسندگان:

Zahra Ghezelbigloo - *Department of Computer Engineering Imamreza University of Mashhad Mashhad, Iran*

Majid Vafaei Jahan - *Department of Computer Engineering Mashhad Branch-Islamic Azad University Mashhad, Iran*

خلاصه مقاله:

One of the common methods in the area of combating with malwares is the use of opcodes-sequence exist in the malwares' assembly code. In this study, a new method hasbeen used based on the structural classification of opcodes to detect malwares and its efficiency has also been put intoinvestigation compared to the opcodes method. For this purpose, two different methods are to be applied for eliciting the contentbased features of the assembly files. Two approaches were, then, analyzed on an equal basis using different classifications. The results, thereof, have indicated that the efficiency and theaccuracy of different classifications do not decrease by using structural classification of opcodes. Additionally, the number offeatures, computational complexity, the time and the memory consumption would dramatically be decreased.

کلمات کلیدی: