معماری و مهندسی سیستم های هوشمند

Content list available at tspixplore.ir

پژوهشکده پردازشگر علم و فن

Journal homepage: http://journal.tspi.ir

# روشی جدید در تشخیص بدافزارها مبتنی بر دنباله نقش-آپکد و روش‌های داده‌کاوی

زهرا قزل بیگلو[۱]، مجید وفایی جهان[۲]

[۱] گروه کامپیوتر، دانشگاه بین‌المللی امام رضا(ع)، مشهد، ایران

zahra.ghezelbigloo@yahoo.com

[۲] استادیار، گروه کامپیوتر، دانشگاه آزاد اسلامی مشهد، مشهد، ایران

Vafaeijahan@mshdiau.ac.ir

## چکیده

بدافزارها طیف وسیعی از خطرات و تهدیدات کامپیوتری، از قبیل ویروس‌ها، کرم‌ها، تروجان‌ها و نرم‌افزارهای جاسوسی را در برمی‌گیرند. در این مقاله از روشی جدید مبتنی بر دسته‌بندی معنایی آپکدها برای تشخیص بدافزارها استفاده شده است و کارایی و دقت آن با استفاده از دسته‌بندهای مختلف مورد ارزیابی قرار گرفته است. برای این منظور آپکدهای استخراج شده از هر نمونه مطابق با نقش‌های آن‌ها طبقه‌بندی می‌شوند. سپس به جای آنالیز دنباله آپکدها، از دنباله نقش-آپکدها استفاده می‌شود. نتایج آزمایشات نشان می‌دهد با استفاده از دنباله نقش-آپکدها می‌توان به دقت و صحت مطلوب ۹۴٫۵٪ دست یافت، علاوه بر این تعداد ویژگی‌ها، حجم محاسبات و حافظه مصرفی به طور قابل توجهی کاهش می‌یابد.

## کلمات کلیدی:

بدافزارها، آپکد(opcode)، نقش-آپکد، فراوانی، داده‌کاوی.

# A New Approach to Malware Detection Sequence Based on the Role-opcode and Data Mining Methods

Zahra Gezel Beyglo[1], Majed Vafayi Jahan, Assistant Professor[2]

1- Faculty of Computer, Imam Reza International University, Mashhad, Iran, Email:zahra.ghezelbigloo@yahoo.com

2- Faculty of Computer, Islamic Azad University of Mashhad, Mashhad, Iran, Email:Vafaeijahan@mshdiau.ac.ir

**Abstract:** Malwares include wide range of computer threats like viruses, worms, Trojans and spywares. In this article a new method based on semantic classification of is proposed to detect malwares. Different classifications used to evaluate performance and accuracy of this method. For this purpose, extracted opcodes of each sample, classified according to their role. Then opcode-role sequence used instead of analyzing opcode sequence. Experimental results show 94.5% accuracy when opcode-role sequence has been used. Furthermore, number of properties, calculation amount and memory use have been decreased.

**Keywords:** malware، opcode، Role-opcode، Abundance،Data Mining.

تاریخ ارسال مقاله:۹۳/۰۲/۰۲

تاریخ پذیرش مقاله:۹۳/۰۷/۵

نام نویسنده مسئول: زهرا قزل بیگلو

نشانی نویسنده مسئول: دانشگاه بین‌المللی امام رضا مشهد(ع)