1. **Conference**

|  |  |
| --- | --- |
| استخراج البيانات عن طرق الكشف عن البرامج الضارة باستخدام التعليمات متواليات | Research Title (Arabic) |
| Data Mining Methods for Malware Detection using Instruction Sequences | Research Title (English) |
| البيانات والتعدين ، وكشف عن البرامج الضارة، تسلسل التعليمات | Research Topic (Arabic) |
| Data mining, malware detection, instruction sequences | Research Topic (English) |
| ACTA Press | Publisher (Arabic) |
| ACTA Press | Publisher (English) |
| 2008 | Publishing Year (Arabic) |
| 2008 | Publishing Year (English) |
| 978-0-88986-710-9 | ISBN |
| استخراج البيانات، كشف عن البرامج الضارة، التصنيف الثنائي، تحليل ساكنة، التفكيك تسلسل التعليمات | Key Words (Arabic) |
| Data Mining, Malware Detection, Binary Classification, Static Analysis, Disassembly, Instruction Sequences | Key Words (English ) |
| AIA '08 Proceedings of the 26th IASTED International Conference on Artificial Intelligence and Applications | Journal Name, or (Conference + place and date being held) |
| Pp 358-363 | Volume No. or Issue No. and the Number of Pages in case it has been published in a scientific journal |
| البرامج الخبيثة تشكل تهديدا خطيرا للأمن الكمبيوتر. النهج التقليدية باستخدام التوقيعات للكشف عن البرامج الخبيثة يشكل خطرا يذكر لبرامج جديدة والغيب الذي التواقيع غير متوفرة. محور البحث هو التحول من استخدام أنماط التوقيع لتحديد برنامج محدد ضار و / أو مشتقاته لاكتشاف السلوك العام في البرامج الخبيثة. تقدم هذه الورقة فكرة جديدة لتحديد تسلسل تلقائيا التعليمات الهامة التي يمكن أن تصنف بين البرامج الخبيثة ونظيفة باستخدام تقنيات استخراج البيانات. استنادا إلى الإحصاءات العامة التي تم جمعها من هذه التعليمات متواليات ضعنا المشكلة باعتبارها مشكلة تصنيف ثنائي وبنى الانحدار اللوجستي، والشبكات العصبية والنماذج شجرة القرارات. وأظهرت نهجنا 98،4 ٪ في معدل اكتشاف برامج جديدة لم تكن البيانات التي استخدمت في عملية بناء نموذج. | Research Abstract (Arabic) |
| Malicious programs pose a serious threat to computer security. Traditional approaches using signatures to detect malicious programs pose little danger to new and unseen programs whose signatures are not available. The focus of the research is shifting from using signature patterns to identify a specific malicious program and/or its variants to discover the general malicious behavior in the programs. This paper presents a novel idea of automatically identifying critical instruction sequences that can classify between malicious and clean programs using data mining techniques. Based upon general statistics gathered from these instruction sequences we formulated the problem as a binary classification problem and built logistic regression, neural networks and decision tree models. Our approach showed 98.4% detection rate on new programs whose data was not used in the model building process. | Research Abstract (English) |