1. **Journal**

|  |  |
| --- | --- |
| ديدان الإنترنت باستخدام تقنيات التعدين الكشف عن البيانات | Research Title (Arabic) |
| Detecting Internet Worms Using Data Mining Techniques | Research Title (English) |
| البيانات والتعدين ، وكشف عن البرامج الضارة | Research Topic (Arabic) |
| Data mining, malware detection | Research Topic (English) |
| المعهد الدولي للمعلوماتية وعلم التحكم الآلي | Publisher (Arabic) |
| International Institute of Informatics and Cybernetics | Publisher (English) |
| 2009 | Publishing Year (Arabic) |
| 2009 | Publishing Year (English) |
| ISSN: 1690-4524 | ISBN |
| استخراج البيانات والكشف دودة والتصنيف الثنائي، تحليل ساكنة، التفكيك تسلسل التعليمات، | Key Words (Arabic) |
| Data Mining, Worm Detection, Binary Classification, Static Analysis, Disassembly, Instruction Sequences | Key Words (English ) |
| Journal of Systemics, Cybernetics and Informatics | Journal Name, or (Conference + place and date being held) |
| Vol. 6, No. 6, pp. 48-53 | Volume No. or Issue No. and the Number of Pages in case it has been published in a scientific journal |
| ديدان الإنترنت تشكل تهديدا خطيرا للأمن الكمبيوتر. النهج التقليدية باستخدام التوقيعات للكشف عن الديدان تشكل خطرا كبيرا على هجمات اليوم صفر. تركيز البحوث الخبيثة هي التحول من أنماط استخدام التوقيع في تحديد سلوك ضار عرضها بواسطة ملورس. تقدم هذه الورقة فكرة جديدة لاستخراج متغير تسلسل التعليمات التي يمكن أن تحدد طول الديدان من برامج تنظيف باستخدام تقنيات استخراج البيانات. ومما يسهل وتحليل تدفق المعلومات الواردة في برنامج مكافحة تسلسل التعليمات. استنادا إلى الإحصاءات العامة التي تم جمعها من هذه التعليمات متواليات ضعنا المشكلة باعتبارها مشكلة تصنيف ثنائي والتصنيف شجرة شجرة بنيت بما في ذلك القرار ، والتعبئة والغابات العشوائية. وأظهرت نهجنا 95،6 ٪ في معدل اكتشاف الديدان الرواية التي لم تكن البيانات المستخدمة في عملية بناء نموذج. | Research Abstract (Arabic) |
| Internet worms pose a serious threat to computer ecurity. Traditional approaches using signatures to detect worms pose little danger to the zero day attacks. The focus of malware research is shifting from using signature patterns to identifying the malicious behavior displayed by the malwares. This paper presents a novel idea of extracting variable length instruction sequences that can identify worms from clean programs using data mining techniques. The analysis is facilitated by the program control flow information contained in the instruction sequences. Based upon general statistics gathered from these instruction sequences we formulated the problem as a binary classification problem and built tree based classifiers including decision tree, bagging and random forest. Our approach showed 95.6% detection rate on novel worms whose data was not used in the model building process. | Research Abstract (English) |