1. **Book Chapter**

|  |  |
| --- | --- |
| الكشف عن حصان طروادة باستخدام تقنيات التعدين البيانات | Research Title (Arabic) |
| Detecting Trojans Using Data Mining Techniques | Research Title (English) |
| البيانات والتعدين ، وكشف عن البرامج الضارة، والكشف عن طروادة | Research Topic (Arabic) |
| Data mining, malware detection, trojan detection | Research Topic (English) |
| Springer | Publisher (Arabic) |
| Springer | Publisher (English) |
| 2009 | Publishing Year (Arabic) |
| 2009 | Publishing Year (English) |
| DOI: 10.1007/978-3-540-89853-5\_43 | ISBN |
| استخراج البيانات والكشف طروادة ، والتصنيف الثنائي، تحليل ساكنة، التفكيك تسلسل التعليمات، | Key Words (Arabic) |
| Data Mining, Trojan Detection, Binary Classification, Static Analysis, Disassembly, Instruction Sequences | Key Words (English ) |
| Communications in Computer and Information Science | Journal Name, or (Conference + place and date being held) |
| Volume 20, pp 400-411 | Volume No. or Issue No. and the Number of Pages in case it has been published in a scientific journal |
| حصان طروادة هو البرنامج الذي ينفذ خلسة عملها تحت ستار برنامج المشروعة. النهج التقليدية باستخدام التوقيعات للكشف عن هذه البرامج يشكل خطرا يذكر لعينات جديدة والغيب الذي التواقيع غير متوفرة. تركيز البحوث الخبيثة هي التحول من أنماط استخدام التوقيع في تحديد سلوك ضار أبداه هؤلاء ملورس. تقدم هذه الورقة فكرة الرواية استخراج متغير تسلسل التعليمات التي يمكن أن تحدد المدة من برامج حصان طروادة نظيفة باستخدام تقنيات استخراج البيانات. ومما يسهل وتحليل تدفق المعلومات الواردة في برنامج مكافحة تسلسل التعليمات. استنادا إلى الإحصاءات العامة التي تم جمعها من هذه المتتاليات التعليم، وضعنا هذه المشكلة باعتبارها مشكلة تصنيف ثنائي وبناء عشوائي للغابات، وتعبئة الدعم التصنيف آلة متجه. وأظهرت نهجنا بمعدل 94،0 ٪ على الكشف عن حصان طروادة الرواية التي لم تكن البيانات المستخدمة في عملية بناء نموذج. | Research Abstract (Arabic) |
| A trojan horse is a program that surreptitiously performs its operation under the guise of a legitimate program. Traditional approaches using signatures to detect these programs pose little danger to new and unseen samples whose signatures are not available. The focus of malware research is shifting from using signature patterns to identifying the malicious behavior displayed by these malwares. This paper presents the novel idea of extracting variable length instruction sequences that can identify trojans from clean programs using data mining techniques. The analysis is facilitated by the program control flow information contained in the instruction sequences. Based on general statistics gathered from these instruction sequences, we formulated the problem as a binary classification problem and built random forest, bagging and support vector machine classifiers. Our approach showed a 94.0% detection rate on novel trojans whose data was not used in the model building process. | Research Abstract (English) |