1. **Conference**

|  |  |
| --- | --- |
| مسح البيانات التعدين تقنيات لاكتشاف البرمجيات الخبيثة باستخدام ملف ميزات | Research Title (Arabic) |
| A Survey of Data Mining Techniques for Malware Detection using File Features | Research Title (English) |
| مسح واستخراج البيانات والكشف عن البرامج الضارة | Research Topic (Arabic) |
| Survey, data mining, malware detection | Research Topic (English) |
| ACM | Publisher (Arabic) |
| ACM | Publisher (English) |
| 2008 | Publishing Year (Arabic) |
| 2008 | Publishing Year (English) |
| 978-1-60558-105-7 | ISBN |
| المسح كشف عن البرامج الضارة، واستخراج البيانات والتعلم الآلي، ن غراما، متواليات التعليم، ويدعو النظام | Key Words (Arabic) |
| survey, malware detection, data mining, machine learning, n-grams, instruction sequences, system calls | Key Words (English ) |
| ACM-SE 46 Proceedings of the 46th Annual Southeast Regional Conference | Journal Name, or (Conference + place and date being held) |
| Pp 509-510 | Volume No. or Issue No. and the Number of Pages in case it has been published in a scientific journal |
| وتعرض هذه الورقة دراسة استقصائية للتقنيات استخراج البيانات للكشف عن البرامج الضارة باستخدام ميزات الملف. وتصنف تستند تقنيات بناء على التسلسل الهرمي ثلاثة الطبقة التي تتضمن ميزات الملف، نوع التحليل والكشف عن نوع. ملف الميزات هي ميزات المستخرجة من البرامج الثنائية، نوع التحليل هو ثابت أو حيوي، واقترضت من نوع الكشف عن كشف التسلل إما سوء استخدام أو الشاذة. ويقدم للقارئ مع تقدم كبير في الأبحاث الخاصة بالبرمجيات الخبيثة باستخدام التنقيب عن البيانات على ميزات الملف ويصنف العمل شملهم الاستطلاع على أساس التسلسل الهرمي هو مذكور أعلاه. خدم هذا كمساهمة كبيرة من هذه الورقة. | Research Abstract (Arabic) |
| This paper presents a survey of data mining techniques for malware detection using file features. The techniques are categorized based upon a three tier hierarchy that includes file features, analysis type and detection type. File features are the features extracted from binary programs, analysis type is either static or dynamic, and the detection type is borrowed from intrusion detection as either misuse or anomaly detection. It provides the reader with the major advancement in the malware research using data mining on file features and categorizes the surveyed work based upon the above stated hierarchy. This served as the major contribution of this paper. | Research Abstract (English) |