وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم البرمجيات

تحليل واكتشاف البرمجيات الخبيثة بالاعتماد على الهندسة العكسية

رسالة مقدمة
الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة ماجستير علوم في
البرمجيات

من قبل

ماهر فخرالدين اسماعيل جاسم

بإشراف

أ.م.د. كرم حاتم ذنون

١٤٤٤ هـ ٢٠٢٢ م

المستخلص

في السنوات الأخيرة اكتسب الأمن السيبراني دوراً رئيسًا في علوم الحاسوب بسبب الأضرار الهائلة الناجمة عن تفشي الأمن كالاحتيال وسرقة المعلومات السرية وغيرها؛ فلذلك تُعدُّ هجمات البرمجيات الضارة مشكلة كبيرة ويتم الإبلاغ عنها بشكل متكرر، مِمَّا يؤثر سلبًا على إنتاجية المؤسسات والشركات في جميع أنحاء العالم، وتعد اهم التحديات التي تواجهها هذه المؤسسات انها لا تمتلك المعرفة ولا الاستعداد لكيفية تحليل وكشف هذه البرامج الضارة، وقد بينت الدراسات السابقة في مجال تحليل البرمجيات الضارة واكتشافها أَنَّ تقنيات الهندسة العكسية هي من أفضل التقنيات لتحليل البرمجيات الضارة.

ولأهمية الموضوع، تهدف الرسالة تصميم وتنفيذ أَداة لتحليل واكتشاف البرمجيات الضارة بالاعتماد على الهندسة العكسيَّة، فضلًا عن استخدام بعض أَدوات تحليل البرمجيات الضارة بواسطة تقنيات الهندسة العكسية، التي تهدف الى فهم سلوك هذه البرمجيات واستخراج الخصائص المميَّزة للكشف عنها. وأجريت عملية التحليل والاكتشاف على (20) عينة من البرمجيات الضارة و(2) من البرمجيات الحميدة موزعة على (8) عوائل تحتوي على خواص مختلفة، وطبقت الأدوات على هذه النماذج بثلاث طرائق من التحليل، استعملت في الطريقة الأُولى أدوات التحليل الأَساسي الساكن والديناميكي ، و في الثانية استعملت أَدوات الهندسة العكسية لطريقة التحليل المتقدم ، والطريقة الاخيرة تم تطبيق الأداة المقترحة، واستخلاص الخواص من عملية التحليل ومن ثم مقارنتها مع الدوال والمكاتب المشتبه بها للحصول على نسبة تمثل حد عتبة إذا تجاوزها الملف يتم كشفه كبرنامج ضار وإِلَّا فهو حميد. وبعد تطبيق الأداة المقترحة على (22) عينة تم اكتشاف ان (18) عينة ضارة (3) عينات حميدة، واخيراً تم تقيم نتائج الأداة ووصلت دقتها الى 91 %.

تم استنتاج أَنَّ عملية التحليل توفر رؤى لشركات مكافحة الفيروسات ولفرق الاستجابة للحوادث ومحترفي التحقيق الرقمي من أجل إيقاف المتسللين في مساراتهم وتزويد متخصصي الأمن السيبراني بالمعرفة والمهارات اللازمة لاكتشاف هجمات البرامج الضارة والرد عليها.

Ministry of Higher Education and
Scientific Research
University of Mosul
College of Computer Science and
Mathematics
Department of Software

Malicious Software Analysis and Detection Depend on Reverse Engineering

**A Thesis Submitted to the Council of the College of
Computer Science and Mathematics
University of Mosul
as a Partial Fulfillment of Requirements
for the Degree of Master of Science
in Software**

By

Maher Fakhrulddin Ismael Jasem

Supervised by

Assist. Prof .Dr. Karam Hatim Thanon

2022 A.D. **1444 A.H.**

Abstract

In recent years, cyber security has gained a major role in computer science due to the huge damage caused by the spread of malware, such as: fraud, theft of confidential information, and others. Therefore, malware attacks are a huge and frequently reported problem, which negatively affects the productivity of organizations and companies all over the world. The most important challenges faced by these institutions are that they do not have the knowledge or the willingness to analyze and detect these malicious programs. Previous studies in the field of malware analysis and discovery have shown that reverse engineering techniques are one of the best techniques for malware analysis.

Because of the importance of the topic, the thesis presented the design and implementation of a tool for analyzing and detecting malware based on reverse engineering, as well as the use of some malware analysis tools by reverse engineering techniques, which aim to understand the behavior of this software and extract the distinctive characteristics to detect it. The analysis and detection process was conducted on (20) samples of malicious software and (2) of benign software distributed over (8) families that contain different properties. The tools were applied to these models with three methods of analysis. The first method uses basic static and dynamic analysis tools. In the second, the reverse engineering tools were used for the advanced analysis method, and the last method was the application of the proposed tool, extracting the features from the analysis process and then comparing them with the suspicious functions and libraries to obtain a percentage that represents a threshold limit. If the file exceeds it, it is detected as a malicious program, otherwise it is benign. After applying the proposed tool on (22) samples, it was discovered that (18) malware samples and (3) benign samples. Finally, the results of the tool were evaluated, and its accuracy reached (91%).

It was concluded that the analysis process provides insights for antivirus companies, incident response teams, and digital investigation professionals to stop hackers in their tracks and equips cybersecurity professionals with the knowledge and skills to detect and respond to malware attacks.