عنوان الرسالة: تحسين تقنية اقتناص التهديدات السبرانية لمنع هجمات فيروس الفدية : نهج استباقي

اسم الطالب: إبراهيم محمد باعباد

اسم المشرف: د. عمر عبدالله باطرفي

المستخلص

البرمجيات الضارة في الحاسب الآلي هي برامج تحتوي على أوامر غير آمنة هدفها الإستيلاء على أنظمة وبيانات المستخدم الحساسة. في الآونة الأخيرة انتشرت العديد من البرمجيات الضارة ومنها فيروس الفدية. فيروس الفدية هو برنامج ضار يقوم بقفل نظام الضحية المستهدَفة من مستخدمي الإنترنت (أفراد أو مؤسسات) أو يشفر بياناته الحساسة بهدف الحصول على رسم الفدية. مؤخرًا تم إجراء العديد من الأبحاث لمنع هجمات فيروس الفدية واكتشافها مبكرًا. تُستخدم تقنيات الذكاء الاصطناعي للتنبؤ الاستباقي ومع ذلك فإن خوارزميات التعلم الآلي والتعلم العميق التقليدية تستهلك الوقت وتقلل من أداء مراقبة الشبكة في دقة وزمن التصنيف. في هذه الدراسة، سنطبق تقنيات التنقيب عن البيانات المتدفقة للكشف المبكر عن هجمات فيروس الفدية ومنعها. وبالتالي سيتم تحسين أداء تقنية اقتناص التهديدات السبرانية عن طريق اكتشاف هجمات فيروس الفدية بشكل استباقي في الزمن الأمثل مع الدقة في التصنيف. علاوة على ذلك ، سيساعد هذا على حماية بيانات المستخدم الحساسة كما أنه يزيد من مستويات الأمان لنظام مستخدمي الإنترنت. كنتيجة لهذا البحث وبعد استخدام خوارزمية أشجار القرار فائقة السرعة ، تم الحصول على دقة تصنيف تقدر ب ١٤,٩٩ نسبة مئوية وذلك في زمن قصير يقدر ب٦٦ ملي ثانية.

Thesis Title: ENHANCING CYBER THREAT HUNTING TECHNIQUE FOR PREVENTING RANSOMWARE ATTACKS: A PROACTIVE APPROACH

Student Name: Ibrahim Mohammed Baabbad

Advisor Name: Dr. Omar Abdullah Batarfi

Abstract:

Software that contains destructive commands intended to damage user data and systems is known as malware. The malware objective is to take over the system without authorization, view important data, or even corrupt it. Over the years, several malware forms have threatened systems and data. Ransomware is among the most damaging malware since it results in significant losses. In order to get a ransom, ransomware is software that locks the victim's machine or encrypts his personal information. Numerous research has been conducted to stop and quickly recognize ransomware attacks. For proactive forecasting, Artificial Intelligence (AI) techniques are used. Traditional machine learning / deep learning (ML/DL) techniques, however, take a lot of time and decrease the accuracy and latency performance of network monitoring. In this study, we will utilize three algorithms of the Hoeffding trees classifier as one of the stream data mining classification techniques to detect and prevent ransomware attacks. Consequently, when ransomware attacks are identified as early as possible, cyber threat hunting technique performance is improved. In conclusion, the 99.41 percent classification accuracy was the highest result achieved by the extremely fast decision trees (EFDT) algorithm in 66 ms.