Abstrak

Penggunaan Metode *Behavior Based Detection* Untuk Deteksi Ransomware Dengan Cara Mengawasi Perilaku Aplikasi Pada Data

Malware merupakan program yang sengaja dibuat untuk membahayakan dan merugikan sistem operasi atau data pada komputer, langkah untuk deteksi terhadap serangan malware telah dilakukan dengan menerapkan metode-motode terkini yang dirasa mampu untuk deteksi malware masuk dan merusak sistem, salah satu metode tersebut adalah *behavior based detection*. Penelitian yang berkembang saat ini lebih fokus pada *behavior operation* dimana sistem sebagai *target behavior operations,* Namun sayangnya penelitian berbasis *behavior based detection* untuk deteksi malware yang ada saat ini belum membahas secara spesifik tentang data user seperti file .docx, .pdf dan .jpeg sebagain *target behavior operations* padahal, beberapa tahun belakangan malware yang menjadi topik utama dalam dunia keamanan komputer adalah malware yang manargetkan data user sebagai sasaran seperti ransomware, oleh karena itu diperlukan penelintian yang membahas penggunaan metode *behavior* untuk deteksi malware berdasarkan perilaku aplikasi pada data. Metode yang digunakan adalah metode *behavior based detection,* karena itu penelitian ini membahas tentang penerapan metode *behavior based detection* untuk deteksi malware berdasarkan perilaku applikasi terhadap data, hal lain yang juga dibahas yaitu kinerja *behavior based detection* dalam mendeteksi malware berdasarkan perilaku applikasi terhadap data. Berdasarkan hasil pengujian terhadap sistem deteksi menunjukkan bahwa penggunaan metode *behavior* sebagai metode deteksi malware memperlihatkan indikasi keberhasilan, hal ini ditunjukkan pada hasil pengujian dimana angka *true positive* mencapai angka 99% dan *false positive* 1%, dengan demikian data menunjukkan angka keberhasilan mendeteksi malware adalah 99% akurat. Tingginya perbedaan data *behavior* malware dan aplikasi normal tersebut dapat digunakan untuk menentukan sebuah aplikasi itu sebagai malware atau aplikasi normal.

Kata kunci

Malware, Ransomware, Behavior Based Detection, Data User

Abstract

Use Of Behavior Based Detection Method To Detect Ransomware By Monitoring The Behavior Of Applications To Data

Malware is a program that is intentionally made to harm and harm the operating system or data on the computer, steps to detect malware attacks have been carried out by applying the latest methods that are considered capable of detecting malware entering and damaging the system, one of these methods is behavior based detection. Research that is currently developing is more focused on the behavior operation where the system is targeted for behavior operations, but unfortunately behavior-based detection-based research for malware detection currently does not specifically address user data such as .docx, .pdf and .jpeg files as targets operations behavior, whereas in recent years malware has become the main topic in the world of computer security is malware that targets user data as targets such as ransomware, therefore this study discusses the use of behavior methods for malware detection based on application behavior to data. The method used is behavior based detection, therefore this study describes the application of the behavior based detection method for detection of malware based on application behavior towards data, another thing that is also explained is the behavior based detection performance in detecting malware based on application behavior towards data. Based on the test results on the detection system, it shows that the use of the behavior method as a malware detection method shows an indication of success, this is shown in the test results where the true positive number is 99% and the false positive is 1%, thus the data shows the success of detecting malware is 99% accurate. The high differences in malware behavior data and normal applications can be used to determine an application as a malware or normal application.

Keywords

Malware, Ransomware, Behavior Based Detection, Data User.