Abstrak

Dalam beberapa tahun ini, *malware (malicious software)* telah berevolusi dan menjadi pintar. Dengan berevolusinya *malware* semakin sulit melakukan deteksi dengan menggunakan cara tradisional *signature-based detection*. Secara garis besar terdapat dua jenis metode deteksi malware yaitu *signature-based detection* dan *anomaly-based detection*. Metode *signature-based detection* tidak dapat digunakan untuk melakukan pendeteksian terhadap *malware* baru karena *signature* dari *malware* tersebut belum diketahui. Untuk mengatasi masalah ini maka dikembangkanlah metode *anomaly-based detection* untuk melakukan pendeteksian terhadap *malware* baru. Metode *anomaly-based detection* melakukan monitoring aktivitas pada sebuah sistem. Kemudian aktivitas dibagi menjadi dua kelompok dari hasil analisis yaitu aktivitas yang normal dan aktivitas yang tidak normal. Jika aktivitas sebuah aplikasi dikategorikan tidak normal, maka aplikasi tersebut dianggap sebagai *malware*.

Masalah yang muncul pada metode *anomaly-based detection adalah false positif* dan *false negatif*. masalah ini muncul karena tidak efektifnya penerapan metode ini pada rule yang telah dibuat. Untuk itu diperlukan analisa terhadap pemakaian parameter yang digunakan pada sebuah *rule*. Kemudian dilakukan pengujian terhadap *rule* dengan cara melakukan pendeteksian terhadap sampel *malware*. Hasil dari pengujian kemudian dibandingkan dengan metode *signature-based detection*. Dari 100 sampel *malware*, dengan menggunakan metode *anomaly-based detection* dapat dilakukan pendeteksian sebanyak 77% sedangkan menggunakan metode *signature-based detection, malware* yang terdeteksi hanya 51%. Dengan demikian metode *anomaly-based detection* memiliki tingkat akurasi yang lebih baik daripada metode *signature-based detection*.

Kata Kunci : *Malware, Anomaly-based Detection, Signature-based Detection, Rule, Akurasi*