ABSTRAK

ANALISIS DETEKSI *MALICIOUS ACTIVITY* MENGGUNAKAN METODE ANALISIS *MALWARE* DINAMIS BERBASIS ANOMALI

Oleh

DAMAR AURIGA DANISWARA

1202150007

Perkembangan teknologi yang semakin meningkat memberikan peluang terjadinya *cyber-crime* dengan memanfaatkan penggunaan internet. Salah satu kejahatan *cyber* yang dapat merugikan individu ataupun perusahaan adalah serangan dari *malware*. *Malware* merupakan *software* yang sengaja dirancang untuk pencurian data, manipulasi data serta mendapatkan akses penuh terhadap *host* yang sudah terinfeksi. Menurut situs av-test.org serangan *malware* semakin meningkat hingga 902.82 juta *malware* pada tahun 2019 dan menyebabkan kerugian hingga 11.7 juta dollar Amerika. Berdasarkan masalah tersebut, maka diperlukan analisis deteksi *malware* yang bertujuan untuk melihat *malicious activity* yang dilakukan oleh *malware* ketika *malware* dieksekusi pada komputer. Analisis dilakukan menggunakan metode analisis *malware* dinamis berbasis anomali yaitu dengan menjalankan sampel *malware* pada suatu *environment* yang sudah dirancang pada Virtual Machine. Anomali merupakan sebuah pola yang tidak sesuai dengan pola normal suatu program. Penelitian ini dilakukan dengan menguji 10 sampel *malware* yang diunduh secara random dan dianalisis menggunakan tiga *tools* yang berbeda untuk mendeteksi sampel *malware*. Anomali dari *malware* dilihat dari aktivitas yang mencurigakan, *registry* yang di akses dan API yang dipanggil oleh sampel *malware*. Hasil pengujian menggunakan *tools* akan dicocokkan dengan *malicious activity data set* yang berupa kumpulan API yang dipanggil oleh sampel *malware*, sehingga diperoleh hasil 40% dari total 10 sampel yang diuji terbukti merupakan *malware.*

Kata kunci : *malware*, analisis *malware*, *cyber-crime*, analisis *malware* dinamis, anomali