ABSTRAK

ANALISIS DETEKSI *MALWARE REMOTE ACCESS TROJAN* MENGGUNAKAN *DYNAMIC MALWARE ANALYSIS DETECTION TOOLS* BERBASIS *BEHAVIOUR*

Oleh

EPIFANIO JUANG VICTORIUS

1202150100

Semakin berkembangnya suatu teknologi, semakin besar pula peluang terjadinya *cybercrime* melalui penyerangan *malware*. *Malicious software* (*malware*) merupakan sebuah *software* berbahaya sengaja dirancang untuk menjalankan muatan asing yang merugikan atau merusak sistem korban tanpa sepengetahuannya. Dengan banyak kategori *malware* yang tersebar, membuat semua sistem rentan terhadap serangan *malware*. Salah satu kategori *malware* yang paling berbahaya adalah *Remote Access Trojan* (RAT) yang dapat mengendalikan sistem secara menyeluruh untuk mencuri informasi pribadi, menghapus *file*, memodifikasi *file*, mengganggu kinerja *user*, dan memasang *malware* atau *backdoor* di dalam sistem. Terbukti dengan adanya 557 serangan *malware* RAT yang terjadi atau terdeteksi antara 1 September 2017 hingga 31 Agustus 2018 di beberapa instansi atau individu di United Kingdom. Oleh karena itu, diperlukan *malware analysis* berbasis *behaviour* untuk mengetahui dan menganalisis *malware behaviour* yang unik berupa Windows API dan *Registry* dari *malware* RAT. Penelitian ini menggunakan 3 dari 10 sampel *malware* RAT yang telah didapatkan yaitu DarkComet-RAT, njRAT, dan QuassarRAT untuk diuji dan dianalisis *malware behaviour*-nya *Malware behaviour* yang dianalisis adalah Windows API dan Windows *Registry* ketika *malware* RAT diinisiasi, dan mengeksekusi *Keylogger*, *File* Transfer dan *Remote.* Desktop menggunakan *dynamic malware analysis detection tools* berbasis *behaviour*. Penelitian ini juga membandingkan *behaviour* inisiasi antara *remote access software* yaitu AeroAdmin dan *malware* RAT untuk mengetahui perbedaan Windows API dan Windows *Registry* yang digunakan. Hasil *malware behaviour* yang didapatkan menjelaskan bahwa *malware* RAT akan menggunakan Windows API dan Registry yang berkaitan dengan RPC dan OLE untuk membuat koneksi dengan sistem yang ditarget, lalu menggunakan Windows API dan Windows *Registry* yang berhubungan dengan *Keyboard Input, Data Access and Storage, Graphic and Gaming* ketika beberapa fitur dieksekusi. *Malware* RAT tidak akan memvalidasi segala aktivitas yang dilakukan dan segala fitur *malware* RAT dapat dijalankan secara manual oleh *attacker*-nya.

Kata Kunci: *malware, malware rat, malware analysis, dynamic malware analysis, malware behaviour.*