ABSTRAK

ANALISIS DAMPAK *MALWARE* BERDASARKAN API *CALL NETWORK* DENGAN METODE *HEURISTIC DETECTION*

Oleh

ONE TIKA SURYATI

1202154320

Malware adalah sebuah program yang memiliki pengaruh negatif pada sistem komputer yang tidak memiliki *user permission*. Semakin berkembangnya dunia internet, semakin berkembang pula jumlah maupun jenis dari *malware*. Tujuan dari dibuatnya *malware* oleh para peretas ialah untuk menghasilkan uang dengan cara yang tidak sah. Dengan adanya bahaya tersebut membuat para *user* komputer merasa terancam. Oleh karena itu diperlukan suatu *malware analysis*. *Malware analysis* bertujuan untuk mengetahui spesifik dari *malware* sehingga dapat meningkatkan keamanan pada suatu sistem komputer. Banyak metode yang dapat digunakan dalam menganalisis *malware,* salah satunya adalah metode *heuristic detection*. *Heuristic detection* merupakan metode analisis yang memungkinkan untuk menemukan *malware* jenis baru dengan mencari perintah atau instruksi yang seharusnya tidak terdapat pada suatu aplikasi. Dengan adanya kemajuan teknologi, maka semakin banyak pula orang-orang yang akan mengakses internet, sehingga banyak *malware* yang dibuat untuk menyerang melalui jaringan internet. Berdasarkan kondisi tersebut, maka dilakukanlah *malware analysis* menggunakan API *call network* dengan metode *heuristic detection*. Hal ini bertujuan untuk mengidentifikasi bagaimana kecendrungan dari *malware-malware* yang menyerang dari sisi jaringan. Hasil analisis dari penelitian ini adalah *malware* dengan API *network* cendrung bersifat sebagai *spyware*, yaitu mengintai aktivitas dan mengambil data *user* tanpa seizin *user*. Selain itu, terdapat pula *malware* yang bersifat sebagai *adware*, yaitu menampilkan iklan-iklan melalui jendela *pop-up* pada perangkat komputer yang dapat mengganggu aktivitas *user*. Sehingga dengan adanya hasil tersebut, dapat diidentifikasi pula tindakan-tindakan yang harus dilakukan oleh *user* untuk melindungi perangkat komputernya, seperti dengan memasang *antivirus* atau *antimalware*, tidak mengunduh aplikasi yang tidak sah serta tidak mengakses *website* yang tidak aman.

Kata Kunci : *malware, malware analysis, heuristic detection,* API *call network.*