ABSTRAK

ANALISIS DAMPAK *MALWARE* TERHADAP TRAFIK JARINGAN DENGAN TEKNIK DETEKSI *BEHAVIOR-BASED*

Oleh

ADIB FAKHRI MUHTADI

1202154192

Malware merupakan sebuah perangkat lunak atau program komputer yang digunakan untuk menjalankan *malicious activity*. *Malware* dibuat dengan tujuan merugikan *users* karena dapat menghabiskan sebagian bahkan seluruh *bandwidth* yang ada pada trafik jaringan. Oleh karena itu, dibutuhkan penelitian analisis dampak *malware* terhadap trafik jaringan dengan teknik deteksi *behavior-based*. Penelitian ini bertujuan untuk mengetahui bagaimana dampak *malware* terhadap trafik jaringan. Teknik ini menganalisis *malware* dengan menjalankan sampel *malware* ke dalam sebuah *environment* untuk memantau aktivitas yang ditimbulkan oleh sampel *malware*. Untuk memperoleh hasil yang akurat, analisis dilakukan dengan mengambil informasi API *call network* dan aktivitas trafik jaringannya. Dari analisis API *call network malware*, akan dihasilkan informasi mengenai urutan API *call network* yang digunakan oleh *malware*. Kemudian dari trafik jaringannya, diperoleh aktivitas-aktivitas *malware* dengan menganalisis *behavior* trafik jaringan *malware, payload*, dan *bandwidth* trafik yang terinfeksi. Selanjutnya dari hasil urutan API *call network* yang digunakan *malware* dan hasil analisis trafik jaringannya, dianalisis sehingga dapat diketahui apa dampak *malware* terhadap trafik jaringan serta penyebab terjadinya dampak tersebut.

Kata kunci: *malware, dynamic analysis, behavior-based*, trafik jaringan, API *call network*