ABSTRAK

ANALISIS *MALWARE* PADA *TRAFFIC* JARINGAN MENGGUNAKAN NETWORKMINER

Oleh

JAYSYURAHMAN

1202154199

Malware merupakan program yang memiliki kode berbahaya yang menjadi ancaman bagi setiap pengguna. *Malware* dibuat dengan tujuan mengumpulkan informasi pribadi atau membuat kerusakan di trafik jaringan. Penyebaran *malware* umumnya terjadi melalui *file attachment* yang tanpa disadari pengguna telah mengunduh *file* berisikan *malware* ketika menggunakan layanan *email* ataupun *website. Malware* tidak selalu berada pada *end-host*, bisa juga berada pada trafik jaringan, di mana menyebabkan dampak kepada jaringan. Oleh karena itu, mendeteksi dan menganalisis *malware* pada trafik jaringan merupakan hal yang penting karena sebelum sampai pada *end-host malware* awalnya akan melalui trafik jaringan. Untuk mendeteksi *malware* pada trafik jaringan, maka diperlukan *file* PCAP yang berisikan hasil *capture* dari pemantauan trafik jaringan Di mana *file* tersebut dianalisis menggunakan perangkat lunak *packet analyzer* yaitu NetworkMiner untuk dicek apakah terdapat *malware* yang berada pada trafik jaringan. Hasil yang didapatkan dari deteksi dan analisis adalah perilaku atau aktivitas *malware* ketika berada di jaringan seperti *port* yang digunakan untuk melakukan penyerangan, dan layanan apa yang menjadi sasaran dari *malware*. Berdasarkan analisis tersebut, maka hasil yang didapatkan adalah kategori *malware* berdasarkan dampak yang dihasilkan dan mengacu pada aspek *access control system* , baik pada trafik jaringan maupun *host* yang berada di jaringan. Selanjutnya dari kategori *malware* tersebut dapat dibuat *controlling* terhadap dampak yang dihasilkan.

Kata Kunci: *malware*, *malware analysis,* anomali jaringan, *traffic analysis*, *packet capture, packet analyzer*.