Abstrak

Salah satu tren yang mengikuti perkembangan masa adalah jenis - jenis *malware* yang muncul di dunia maya semakin beragam. Trojan adalah salah satu jenis *malware* yang ikut berkembang di dalamnya, yang memungkinkan *attacker* masuk ke dalam sistem tanpa diketahui oleh pemilik. Penggunaan trojan saat ini lebih ke arah kejahatan dunia maya (*cyber crime*). Cara kerja trojan yang cepat dan handal menjadi penyebab penggunaan *trojan* semakin marak dalam dunia kejahatan komputer. Sasaran terbanyak penyebaran *trojan* adalah pengguna sistem operasi Windows. Jumlah pengguna dan penyedia aplikasi di internet yang banyak, memungkinkan penyebaran *trojan* ini dilakukan dengan metode *social-engineering*, teknik yang menggunakan kelemahan manusia, sehingga user tanpa curiga langsung mengeksekusi sebuah *program* yang tidak dikenal.

Malware analysis adalah metode untuk mengetahui keberadaan *malware* (*malicious software*) dalam suatu *executable file* yang dibagi dalam dua buah tahap yaitu *static analysis* dan *dynamic analysis*. *Static analysis* dilakukan tanpa menjalankan *malware* tersebut ke dalam sistem seperti *disassembly* dan *debugging*, sedangkan *dynamic analysis* dilakukan dengan menjalankan *malware* dalam sistem untuk melihat *process detail*, *file system activity*, *registry activities*, dan *network traffic*. Dengan menggabungkan hasil dari *static malware analysis* dan *dynamic malware analysis* diperoleh karakteristik malware yang dijadikan data rekomendasi untuk mendeteksi keberadaan *trojan malware* pada *executable file* Windows.

Kata Kunci: *Trojan, social engineering, malware analysis, executable file*