Abstract

One of the trend that follows the development period is the increasing appearance of various malwares in the internet. Trojan is a type of malware that also grows rapidly, it allows the attacker to login to the victim's system without being noticed. The use of trojan is currently moving toward cyber crime. Being fast and reliable, trojan spreads in the world of computer crime. Most trojan targets are Windows OS users. The high number of users and application providers on the internet, allows it to spread by social-engineering technique, a technique that uses human weakness that will drive the victim to download and execute that unknown program.

Malware analysis is a method to analyzing malware that is divided into two steps, static and dynamic analysis. Static analysis is done without running the malware in to the system such as disassembly and debugging, meanwhile dynamic analysis is done by running the malware in the system to see the process detail, file system activities, registry activities, and network traffic activities. Combining the results of static and dynamic analysis will produce malware's characteristic as recommendation to detect trojan malware inside windows executable file.

Keyword: *trojan, social-engineering, malware analysis, executable file*