ABSTRAK

Pada paper ini terfokus pada *malicious software* atau *malware* APT1 (*Advance Presistent Threat*) dengan *code name WEBC2-DIV* yang menjadi salah satu varian *malware* yang mewakili sifat dari *Virus, Worm, Trojan, Adware, Spyware Backdoor* Ataupun *Rootkit.* Meski *malware* dapat menghindari *scanning* antivirus namun dengan teknik *reverse engineering* dapat dilakukan meski menyita waktu karena dengan teknik ini dapat mengetahui seberapa bahaya *malware* yang menginfeksi. Penyerangan menggunakan *malware hacker* menjadi *trend espionage* dari sebuah negara (*cyberwar)*, karena memiliki dampak begitu besar dari sisi materil dan non materil. *forensic malware* menjadi tolak ukur keberhasilan bahwa setiap pengguna Komputer akan sadar bahaya *malware*. Pada penelitian ini terfokus pada *reverse engineering malware*. Beberapa langkah analisis diantaranya berawal dari pindai aplikasi yang menyerupai *malware*, mencurigai paket yang bergerak pada jaringan, analisis tingkah laku *malware*.

Kata kunci : *forensic malware*, *Analysis*, *Advance Presistent Threat*, *Cyberwar*, *dissambler*