ABSTRAK

Setiap hari muncul berbagai jenis *malware* baru di Internet. Di mana teknologi yang digunakan *malware* sudah semakin berkembang. *Malware* sudah menggunakan berbagai teknik dan cara untuk mengelabui antivirus ketika menginfeksi korban. Perkembangan *malware* harus diimbangi dengan melakukan penelitian tentang deteksi malware. Maka dari itu, pada penelitian ini dilakukan kegiatan *malware analysis* menggunakan sebanyak 170 *malware* untuk melakukan kategoriasi berdasarkan *malicious activity* yang digunakan. *Malicious activity* dapat dilihat dari jenis API *call* yang digunakan. Pada penelitian ini menggunakan 3 (tiga) jenis API *call* yaitu API *file*, API *process* dan API *registry*. Teknik yang digunakan untuk mendapatkan informasi API *call* adalah *Static Analysis* dan *Dynamic Analysis*. Sehingga hasil yang diperoleh terdapat 5 kategorisasi dengan minimum 0 kombinasi dan maksimum 5 kombinasi *malicious activity*. Dimana pada anlisis ini menggunakan metode *clustering* sehingga dibagi menjadi 3 cluster yang memiliki lebih dari 1 (satu) kombinasi *malicious activity*. Analisis *impact* yang diberikan tergantung dari banyaknya kombinasi, semakin banyak kombinasi API *call* akan semakin besar dampaknya pada komputer yang terinfeksi. Pada penelitian ini *impact* yang diberikan adalah *high* karena terdapat malware yang memiliki 2 (dua) kombinasi sampai 5 (lima) kombinasi *malicious activity*.

Kata Kunci : *malware, malware analysis, static analysis, dynamic analysis, clustering*