ABSTRAK

Malware telah berkembang sangat pesat dan memiliki berbagai teknik untuk mengelabui *antivirus* saat menginfeksi komputer. Tujuan dari *attacker* atau pembuat *malware* ini adalah dapat memasang *malware* pada *device* tujuan dan mendapat kontrol penuh terhadap *device* tersebut. Adanya ancaman kontrol penuh terhadap *device*, korban mengalami kerugian baik dari pencurian informasi, DDoS *attack*, penyalahgunaan komputer korban, *email spam* dan kerugian yang berkaitan lainnya. Berbagai macam ancaman *malware* yang kemungkinan terjadi, harus dilakukan penelitian untuk memahami *signature* dari suatu *malware*. *Malware analysis* sangatlah dibutuhkan untuk melakukan analisis dari segi *impact*, kategori dan ciri-cirinya. Sehingga dari hasil analisis yang dilakukan dapat disimpulkan bagaimana klasifikasi *malware*, deteksi *malware* dan mitigasi *malware*. *Malware analyis* dilakukan untuk mencari beberapa informasi salah satunya pemanggilan API oleh *malware*. Kategorisasi *malware* dilakukan menggunakan *malicious activity data set* berdasarkan API *calls*. Semakin banyak keterkaitan antar *malicious activity* pada suatu *malware*, semakin besar juga dampak yang akan dihasilkan oleh *malware* tersebut. Sebaliknya, semakin sedikit keterkaitan *malicious activity* pada suatu *malware*, dampak yang dihasilkan akan kecil. Hasil dari kategorisasi dianalisis berdasarkan metode anomali. Berdasarkan kategorisasi menggunakan metode anomali, terdapat 3 (tiga) *malicious activity* yang tidak memiliki keterkaitan dengan sampel *malware* yang digunakan pada penelitian ini yaitu IAT *Hooking*, *Bind* TCP *Port* dan *Capture Network*. Terdapat juga 2 (dua) *malicious activity* yang hanya memiliki 1 keterkaitan dengan sampel *malware* yang digunakan yaitu *Process Hollowing* dan *Drop Files from* PE *Resource Section*.

Kata Kunci : *malware, malware analysis, cyber crime*, anomali, deteksi *malware, malware signature, malicious activity*.