ABSTRAK

ANALISIS *MALWARE* BERDASARKAN *API CALL MEMORY* DENGAN METODE DETEKSI *SIGNATURE-BASED*

Oleh

JULIAN DWI NUGRAHA

1202154120

Malware merupakan sebuah perangkat lunak atau program komputer yang digunakan untuk melakukan tindakan kejahatan. *Malware* pada dasarnya dirancang untuk menginfeksi sistem komputer penguna tanpa persetujuan pemiliknya. *Trojan*, *Worms*, *Virus*, *Spyware*, dan *Keylogger* adalah kategori *malware* yang dapat merugikan pengguna yang telah terinfeksi. Berdasarkan hal tersebut maka dari itu diperlukan *malware analysis* menggunakan API *call memory* dengan metode *signature based detection*. *Signature based detection* adalah teknik deteksi yang berdasarkan *pattern matching*, *string*, *mask*, atau teknik *fingerprinting*. *Signature* adalah teknik persamaan *bit* yang disuntikkan dalam program aplikasi oleh *attacker*, yang secara unik mengidentifikasi jenis *malware* tertentu. Hal ini digunakan dengan tujuan untuk mengidentifikasi *malware* tersebut menggandung program yang dapat mengambil data pengguna tanpa sepengetahuan pengguna. Maka dari itu didalam penelitian ini dilakukan *malware analysis* menggunakan sebanyak 150 *sample malware* dan yang melakukan *import* API *memory* terindikasi mengandung 30 *malware.* Penelitian ini berfokus untuk melakukan analisis pada API *Memory* yang telah didapatkan. Dari semua *malware* akan menjalankan satu API *memory* yang sama ketika dijalankan pertama kali. Hasil pada penelitian ini untuk melihat API *call memory* dan hasil *signature* yang telah dilakukan menggunakan metode *signature based detection* dan melihat hubungan antara API *call memory* dengan hasil *signature* pada setiap *malware*.

Kata Kunci : *malware, malware analysis, static analysis, dynamic analysis, signature-based*