ABSTRAK

Kejahatan dunia maya setiap tahunnya mengalami peningkatan yang sangat pesat, hal ini dikarenakan semakin berkembangnya teknologi komputer yang berdampak dikehidupan manusia. Objek yang digunakan pada penelitian ini adalah *WannaCry* yang memiliki jenis *malware Ransomware* 2.0 yang saat *malware* ini berjalan, pembuatnya menginginkan keuntungan besar. Cara kerja *malware* ini mengeksploitasi kerentanan yang ada dalam protokol SMB (Server Message Block) di OS Windows lalu sistem target mencari file-file yang relevan untuk di enkripsi, termasuk dokumen, gambar, video, dan file-file penting, setelah itu menyebar kesistem lain setelah target awal berhasil, menggunakan EternalBlue pada protokol SMB. Hasil yang diperoleh terhadap *malware WannaCry* berupa pola *byte* dan kode instruksi yaitu "aWanarry" , "c.wnry" dan "WNcry@2oI7". Analisis lain berupa *hash* nilai MD5 A64F30812A25A75A71BE38452D21C718 ,hasil *signature networ*king didapatkan http://192.168.122.1:9200/_bulk yang berupa IP lokal jaringan pribadi , diketahui juga pemanggilan fungsi khusus seperti RegSetValueExA, RegCreateKeyExA, fopen, memcpy, dan lainnya. Fungsi-fungsi ini digunakan dalam operasi *malware*, seperti memanipulasi registri, membuka file, melakukan penggandaan memori, instruksi assembly, yang menandakan ciri khas bahwa termasuk *malware wannacry*. Hasil total *actions* yang dilakukan memperoleh hasil total action sebanyak 8.367 dipenelitian pertama dan 111.976 penelitian kedua, dengan terdapat 7 parameter yang digunakan.

Kata Kunci: *Malware, Ransomware, Signature, WannaCry*