ABSTRAK

WannaCry adalah sebuah Malware bertipe Ransomware yang mengancam komputer data untuk dienkripsi dan dihapus sampai ransom bisa terbayarkan. WannaCry menargetkan kepada korban yang menjalankan operasi sistem Windows, dengan meminta tebusan pembayaran menggunakan mata uang digital Bitcoin. WannaCry juga menggunakan EternalBlue sebuah eksploitasi yang dibuat oleh NSA dan disebarkan oleh The Shadow Broker beberapa bulan sebelum terjadinya serangan global oleh WannaCry. NSA menggunakan *Eternalblue* untuk meretas dan mengambil alih jarak jauh komputer untuk menjalankan windows. *Eternalblue* adalah exploit kit (EK) yang mengeksploitasi kerentanan dalam implementasi Microsoft dari protokol *Server Message Block* (SMB) yang digunakan untuk berbagi file antar komputer. Kerentanan Server Microsoft Windows yang menjalankan SMB versi 1. *Malware WannaCry* menggunakan ekploit bernama *EternalBlue-Doublepulsar* untuk menginfeksi komputer yang menjalankan versi sistem operasi windows. *Malware* ini menggunakan *Eternalblue* untuk eksploitasi kerentanan SMB, jika berhasil akan menanamkan *Doublepulsar backdoor* dan menggunakannya untuk menginstal malware. WannaCry menggunakan *DoublePulsar* sebagai *backdoor* untuk melakukan pemindahan *resource WannaCry* dan menghapus *backdoor* tersebut setelah melakukan pemindahan. Dengan melakukan teknik *hybrid-analysis* yang merupakan kombinasi dari analisis statis dan dinamis. Teknik ini dilakukan dengan mengecek *signature malware* jika ditemukan kode dan memonitoring perilaku kode sehingga menghasilkan analisis lengkap. Dari hasil penelitian ini akan didapatkan aktivitas dan pola serangan *EternalBlue* dan *WannaCry Ransomware* yang beraksi pada jaringan dengan menggunakan *Hybrid-Analysis* yang menjalankan sampel *malware* ke dalam sebuah *environment.*

Kata kunci : *Ransomware, Wannacry, Eternalblue, Malware, Windows Smb, DoublePulsar.*