ABSTRACT

Cyber crime has increased very rapidly every year, this is due to the growing development of computer technology which has an impact on human life. The object used in this research is WannaCry which has a type of Ransomware 2.0 malware which when this malware is running, the creators want big profits. The way this malware works exploits a vulnerability in the SMB (Server Message Block) protocol on Windows OS and then the target system looks for relevant files to be encrypted, including documents, images, videos, and important files, after which it spreads to other systems. after initial target success, using EternalBlue on SMB protocol. The results obtained for the WannaCry malware are in the form of byte patterns and instruction codes, namely "aWanarry", "c.wnry" and "WNcry@2oI7". Another analysis is the hash value of MD5 A64F30812A25A75A71BE38452D21C718 , the results of signature networking obtained http://192.168.122.1:9200/_bulk which is the local IP of the private network , it is also known that special function calls such as RegSetValueExA, RegCreateKeyExA, fopen, memcpy, and others. These functions are used in malware operations, such as manipulating the registry, opening files, duplicating memory, assembly instructions, which are the hallmarks that belong to the wannacry malware. The results of the total actions taken resulted in a total of 8,367 actions in the first study and 111,976 in the second study, with 7 parameters used.

***Keywords**: Malware, Ransomware, Signature, WannaCry*