ABSTRACT

WannaCry is a Ransomware type malware that threatens computer data to be encrypted and deleted until ransom can be paid for. WannaCry targets victims who operate Windows systems, by requesting ransom payments using the digital currency Bitcoin. WannaCry also uses EternalBlue, an exploitation made by the NSA and spread by The Shadow Broker several months before the global attack by WannaCry. NSA uses Eternalblue to hack and remotely take over computers to run Windows. Eternalblue is an exploit kit (EK) that exploits vulnerabilities in Microsoft's implementation of the Server Message Block (SMB) protocol that is used to share files between computers. Vulnerability of a Microsoft Windows Server running SMB version 1. The WannaCry malware uses an exploit called EternalBlue-Doublepulsar to infect computers running versions of the Windows operating system. This malware uses Eternalblue to exploit SMB vulnerabilities, if successful it will embed Doublepulsar backdoor and use it to install malware. WannaCry uses DoublePulsar as a backdoor to move WannaCry resources and delete the backdoor after removal. By doing hybrid-analysis techniques which are a combination of static and dynamic analysis. This technique is done by checking the malware signature if found code and monitoring code behavior so as to produce a complete analysis. From the results of this study will get the activity and attack patterns of EternalBlue and WannaCry Ransomware that act on the network using Hybrid-Analysis which runs malware samples into an environment.

Keyword : *Ransomware, Wannacry, Eternalblue, Malware, Windows Smb, DoublePulsar*.