Severity

High

Analysis Summary

WannaCry is also called WCry or WanaCrptor ransomware malware, this ransomware can encrypt all your data files and demands a payment to restore the stolen information, usually in bitcoin with a ransom amount. WannaCry is one of the most dangerous malware ever used for cyberattacks. The attackers behind WannaCry ransomware uses a tool called Eternal Blue to exploit a vulnerability in the Windows Server Message Block, or SMB Protocol. WannaCry ransomware have caused serious disruptions in healthcare sector and financial sector and locked out users from their data.

Impact

- File Encryption

Indicators of Compromise

MD5

- 2110ff5fc3c8e62b878150e7d1416be1

SHA-256

- a6a584dbe82106cd32f028811a815f3d82dc654a62e6178e47005de2e5e56835

SHA-1

- d2877862a4c93faa336c50365f44b84f50a49b42

Remediation

- Block all threat indicators at your respective controls
- Search for IOCs in your environment.