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

- 753343f7e482c53bf20a73322d9617c5
- cf97b12d745bacd0c472da1675eee43e

SHA-256

- e68e45111b8863637a81e29eeec9b89f4844c617a6a78db919c43a47fa00d870
- 51f3948bccd0bea7cb9d6f7e33a636be3200cbaf01cd3de42806ac1e1946289b

SHA-1

- 3f1ba666dd0ce2a0a402e424320716833515f298
- bb2831b06c0599d0c940da39fd8a9efb35b33759

Remediation

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