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

- 84c82835a5d21bbcf75a61706d8ab549
- 4632c90fc12fca77aee70b6995bbacaa
- db349b97c37d22f5ea1d1841e3c89eb4

SHA-256

- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- 869204f63f3abb98feed1a151358beed11699d636d973a33e8cf775911c9619a
- 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

SHA-1

- 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
- cc0bdffa26e697c767e32b79a3aa23f03f162a9c
- e889544aff85ffaf8b0d0da705105dee7c97fe26

URL

- http[:]//iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com/

Remediation

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