Severity

High

Analysis Summary

SystemBC malware is recently being distributed through Emotet and SmokeLoader. The malware has been used in multiple ransomware attacks over the past few years. SystemBC acts as a Proxy Bot and if an infected system has SystemBC on it, then the system can be used as a passage to access the victim's address. The earlier versions of the malware were distributed using Fallout exploit kit and RIG exploit kit. The 2020 version was used with Egregor or Ryuk-associated ransomware attacks. DarkSide ransomware group also used the malware. SystemBC is mainly used as a proxy and to download and install additional payloads. It might be installed in internal networks to perform the role of a proxy or download and execute malicious payloads.

Impact

- Credential Theft
- Information Theft
- Financial Loss

Indicators of Compromise

MD5

- 4a987f518a86e8a058b0d7f41febd4c5

SHA-256

- 57eccf5d61a8ca0b2bea78e57df2c987ae07232f2e7ed43bb90314e73aeae543

SHA-1

- 5d6bc86394c1b90775bc6dd64ff9f19847d8748d

Remediation

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