Severity

Medium

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

- ce4f5903bb3109933416b7aa6e6531fb

SHA-256

- fe6d6d15e0ffa8717c2a5ac80b7f117e853c05cd642c746bb2eab0f70416150d

SHA-1

- aab9f3c01cc753371b93e5c8880ecafa16e4b10f

Remediation

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