Severity

High

Analysis Summary

Cobalt Strike first appeared in 2012 in response to alleged flaws in the Metasploit Framework, an existing red team (penetration testing) tool. Cobalt Strike 3.0 was released in 2015 as a stand-alone opponent emulation platform. However, researchers began observing threat actors using Cobalt Strike by 2016. Cobalt Strike's use in hostile activities was previously connected with huge cybercriminal operations like TA3546 and APT40. Two-thirds of detected Cobalt hit efforts from 2016 to 2018 were attributable to well-resourced cybercrime organizations or APT groups, according to researchers.

Cobalt Strike lets the attacker install a 'Beacon' agent on the target PC which provides the attacker with a plethora of capabilities, including command execution, file transfer, keylogging, mimikatz, port scanning, and privilege escalation. Cobalt Strike includes a toolkit called Artifact Kit that is used to create shellcode loaders

Impact

- Data Exfiltration
- Information Theft

Indicators of Compromise

MD5

- 1e41e05a849bf47240c50220dae5d1c0

SHA-256

- 0203fa232d0eb3da7aa08e29eaa0bec6b5ac700d6d4b6100a285a58ecf271db8

SHA-1

- c7c670c61cdc2b3c7b5c5df504fd54fc5205ae69

Remediation

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