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

- 229a758e232aeb49196c862655797e12

SHA-256

- 49ba10b4264a68605d0b9ea7891b7078aeef4fa0a7b7831f2df6b600aae77776

SHA-1

- 73067102a6b37818f83121b9033087e291c667db

Remediation

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