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

Domain Name

- antivirusecurity[.]com
- flrefoxupdater[.]com
- itsupportsecuruty[.]com

MD5

- 79d1427fa201854efa13dd5546297d3e
- 56ef03d07da7b9ea1f9c2aae4c2ad27b

SHA-256

- 10d3af2c724604fb85f3480be97da62b695c002fa116b5d2adf5cacc0666eb4f
- bf918055d62b3ef4d7fe8cd6a9cca7900d874688d43d09a641d1ab1283955ef9

SHA-1

- 610e951e8268b630b2360f9f2bb2f6378a4061d7
- 75e828674e491ce47b32232e2a26d5f00ecd8ec0

Remediation

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