AYI NEDJIMI Consultants

Cobalt Strike : Plateforme C2 Red Team de R

10 mai 2026 • Mis à jour le 17 mai 2026 • 21 min de lecture • 4349 mots

Cobalt Strike est la plateforme commerciale de Command and Control la p
monde pour les operations red team et la simulation d'adversaires. Concue
Raphael Mudge, fondateur de Strategic Cyber LLC, elle a ete rachetee en 2
HelpSystems puis integree au portefeuille Fortra en 2022. Cobalt Strike fou
Server collaboratif qui orchestre des implants nommes Beacons (HTTP, HT
TCP, External C2), un moteur de profils Malleable C2 permettant de model
pour mimer des APT connus, ainsi qu'un langage de scripting Aggressor S
Sleep pour automatiser les tactiques.

Cobalt Strike est la plateforme commerciale de **Command and Control** (C2) la plus
pour les operations **red team** et la simulation d'adversaires (*adversary simulation*)
Raphael Mudge, fondateur de Strategic Cyber LLC, elle a ete rachetee en 2020 pa
integree au portefeuille **Fortra** en 2022. Cobalt Strike fournit un **Team Server** colla
des implants nommes *Beacons* (HTTP, HTTPS, DNS al C2), un m
Malleable C2 permettant de modeler le trafic reseau PT connus,

de scripting **Aggressor Script** base sur Sleep pour automatiser les tactiques. Deve
des consultants offensifs, Cobalt Strike est aussi malheureusement l'outil prefere
rancongiciels (Conti, LockBit, BlackCat) et de groupes APT etatiques apres la fuite
sur GitHub en 2020. Cette page entity couvre l'architecture Team Server / Beacon
techniques de **lateral movement**, les profils Malleable C2, la detection cote **EDR**, l
Sliver, Empire, Mythic et Brute Ratel C4, ainsi que les aspects legaux d'utilisation p
comprendre l'ecosysteme C2 commercial moderne.

À RETENIR

L'essentiel a retenir

Cobalt Strike est la plateforme C2 commerciale dominante pour les operati
editee par Fortra (ex-HelpSystems) au prix d'environ $3 540 par utilisateu

Architecture en trois couches : Team Server (Java, port 50050), Beacons
en C) et Listeners (HTTP/HTTPS/DNS/SMB/TCP/External C2) orchestres v
Aggressor.

Les Malleable C2 profiles permettent de mimer le trafic d'APT connus (APT
contourner les signatures reseau via personnalisation de chaque header H
metadata.

Cobalt Strike est massivement abuse depuis la fuite GitHub de novembre 2
dans plus de 66 % des incidents ransomware selon le rapport Cisco Talos

Concurrents serieux : Sliver (BishopFox, open source Go), Mythic (modula
Empire (open source PowerShell/Python), Brute Ratel C4 (commercial, OPS

Réponse sous 24h

Devis gratuit →