FORTRA | bakotech

Cobalt Strike —

інструмент емуляції загроз, який ідеально підходить для проведення постексплуатаційних завдань Red Team на основі прихованого агента і оновлюваної бази атакувальних скриптів.

КЛЮЧОВІ ОСОБЛИВОСТІ

КОРИСНЕ НАВАНТАЖЕННЯ ПІСЛЯ ЕКСПЛУАТАЦІЇ

Моделюйте атакуючого суб'єкта за допомогою Beacon. Це корисне навантаження Cobalt Strike, яке виконує сценарії PowerShell, реєструє натискання клавіш, робить знімки екрана, завантажує файли і створює інші корисні навантаження.

BROWSER PIVOTING

Використовуйте Browser Pivot, щоб обійти двофакторну аутентифікацію й отримати доступ до сайтів як кінцеву мету.

СПІЛЬНА РОБОТА

Декілька Red Teamers можуть увійти на сервер команди для спільної роботи, спілкуючись у режимі реального часу. На додаток до загальних сеансів, члени команди також можуть спільно використовувати хости та захоплені.

ПРИХОВАНА КОМУНІКАЦІЯ

Імітуйте внутрішнього зловмисника, використовуючи асинхронний «низький і повільний» зв'язок. Гнучку мову управління і контролю Beacon, Malleable C2, можна використовувати для зміни мережевих індикаторів для сумісності зі звичайним трафіком або для приховування своєї діяльності шляхом імітації різних типів шкідливих програм.

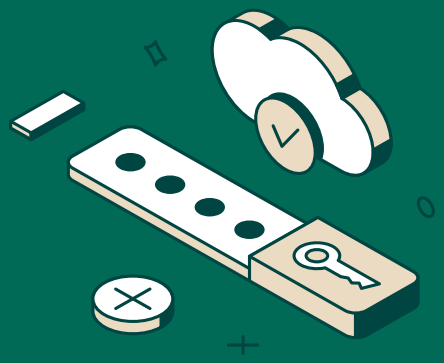
РОЗВІДКА НА СТОРОНІ КЛІЄНТА

Системний профайлер Cobalt Strike ідеально підходить для розвідки на стороні клієнта. Він може визначити внутрішню IP-адресу, застосунки, плагіни, а також інформацію про версію відвідувача.

ЗВІТНІСТЬ І ВЕДЕННЯ ЖУРНАЛУ

Звіти Cobalt Strike містять часову шкалу і список індикаторів діяльності Red Team. Cobalt Strike експортує звіти як у форматі PDF, так і у форматі MS Word.

ПЕРЕВІРТЕ ЗАХИЩЕНІСТЬ ВАШОЇ КОМПАНІЇ



від цільових атак за допомогою одного з найпотужніших наборів, доступних пентестерам.

УДОСКОНАЛЕНЕ МОДЕЛЮВАННЯ ПРОТИВНИКА

Використовуйте Beacon, корисне навантаження Cobalt Strike після експлуатації, щоб контролювати мережу вашої цілі, залишаючись при цьому непоміченим.

ДИНАМІЧНА ВЗАЄМОДІЯ З RED TEAM

Red Team може використовувати спільний командний сервер для взаємодії над реалістичними атаками і створення детальних звітів для документування всіх дій після експлуатації.

ГНУЧКА СТРУКТУРА І ВЕЛИЧЕЗНЕ COMMUNITY

Змінюйте вбудовані скрипти і пишіть свої власні, а також створюйте і діліться своїми розширеннями в Community Kit.

ІНДИВІДУАЛЬНІ СКРИПТИ.
Створюйте скрипти, використовуючи Aggressor Script — мови сценаріїв Cobalt Strike. Нові сценарії легко завантажуються і управляються в консолі, де можна виконувати подальшу взаємодію.

НАБОРИ РЕГУЛЬОВАНИХ АТАК.
Змінюйте набори, завантажені з арсеналу Cobalt Strike, відповідно до потреб кожної атаки. Наприклад, можна перевизначити шаблони скриптів із набору ресурсів, який використовується в робочих процесах, а також створити свій власний Beacon Object File (BOF).

СУМІСНІСТЬ ІЗ CORE IMPACT.
Скористайтеся можливостями передавання сеансів і тунелювання під час використання Cobalt Strike і Core Impact.

COMMUNITY KIT.
Community Kit слугує центральним репозиторієм для проєктів користувачів, тому колеги-професіонали в галузі безпеки також можуть скористатися цими розширеннями.

FORTRA | bakotech®

fortra@bakotech.com