FORTRA | bakotech®

Cobalt Strike —

инструмент эмуляции угроз, который идеально подходит для проведения постэксплуатационных задач Red Team на основе скрытого агента и обновляемой базы атакующих скриптов.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

ПОЛЕЗНАЯ НАГРУЗКА ПОСЛЕ ЭКСПЛУАТАЦИИ

Моделируйте атакующего субъекта с помощью Beacon. Это полезная нагрузка Cobalt Strike, которая выполняет сценарии PowerShell, регистрирует нажатия клавиш, делает снимки экрана, загружает файлы и создает другие полезные нагрузки.

BROWSER PIVOTING

Используйте Browser Pivot, чтобы обойти двухфакторную аутентификацию и получить доступ к сайтам в качестве конечной цели.

СОВМЕСТНАЯ РАБОТА

Несколько Red Teamers могут войти на сервер команды для совместной работы, общаясь в режиме реального времени. В дополнение к общим сеансам, члены команды также могут совместно использовать хосты и захваченные данные, а также загружать файлы.

СКРЫТАЯ КОММУНИКАЦИЯ

Имитируйте внутреннего злоумышленника, используя асинхронную «низкую и медленную» связь. Гибкий язык управления и контроля Beacon, Malleable C2, можно использовать для изменения сетевых индикаторов для совмещения с обычным трафиком или для скрытия своей деятельности путем имитации различных типов вредоносных программ.

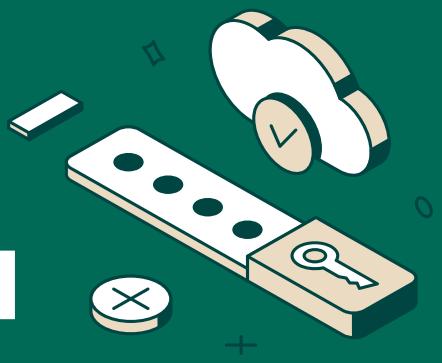
РАЗВЕДКА НА СТОРОНЕ КЛИЕНТА

Системный профайлер Cobalt Strike идеально подходит для разведки на стороне клиента. Он может определить внутренний IP-адрес, приложения, плагины, а также информацию о версии посетителя.

ОТЧЕТНОСТЬ И ВЕДЕНИЕ ЖУРНАЛА

Отчеты Cobalt Strike содержат временную шкалу и список индикаторов деятельности Red Team. Cobalt Strike экспортирует отчеты как в формате PDF, так и в формате MS Word.

ПРОВЕРЬТЕ ЗАЩИЩЕННОСТЬ ВАШЕЙ КОМПАНИИ



от целевых атак с помощью одного из самых мощных наборов, доступных пентестерам.

УСОВЕРШЕНСТВОВАННОЕ МОДЕЛИРОВАНИЕ ПРОТИВНИКА

Используйте Beacon, полезную нагрузку Cobalt Strike после эксплуатации, чтобы контролировать сеть вашей цели, оставаясь при этом незамеченным.

ДИНАМИЧНОЕ ВЗАИМОДЕЙСТВИЕ С RED TEAM

Red Team может использовать общий командный сервер для совместной работы над реалистичными атаками и создания подробных отчетов для документирования всех действий после эксплуатации.

ГИБКАЯ СТРУКТУРА И ОГРОМНОЕ COMMUNITY

Изменяйте встроенные скрипты и пишите свои собственные, а также создавайте и делитесь своими расширениями в Community Kit.

ИНДИВИДУАЛЬНЫЕ СКРИПТЫ.
Создавайте скрипты, используя Aggressor Script — языка сценариев Cobalt Strike. Новые сценарии легко загружаются и управляются в консоли, где можно выполнять дальнейшее взаимодействие.

НАБОРЫ РЕГУЛИРУЕМЫХ АТАК.
Изменяйте наборы, загруженные из арсенала Cobalt Strike, в соответствии с потребностями каждой атаки. Например, можно переопределить шаблоны скриптов из набора ресурсов, который используется в рабочих процессах, а также создать свой собственный Beacon Object File (BOF).

СОВМЕСТИМОСТЬ С CORE IMPACT.
Воспользуйтесь возможностями передачи сеансов и туннелирования при использовании Cobalt Strike и Core Impact.

COMMUNITY KIT.
Community Kit служит центральным репозиторием для проектов пользователей, поэтому коллеги-профессионалы в области безопасности также могут воспользоваться этими расширениями.

FORTRA | bakotech®

fortra@bakotech.com