C&C

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цель урока

Узнать, что такое C&C.

Немного воспоминаний

Кибератака — это не просто вторжение в систему. Чтобы получить профит, злоумышленник должен поддерживать постоянное функционирование вредоноса в целевой системе.

Необходим механизм, позволяющий удалённо обновить «прошивку под капотом» вируса для его более длительного пребывания в целевой системе.

C&C

C&C — структура управления и контроля, также известная как C2, или C&C, представляет собой набор инструментов и методов, которые злоумышленники используют для обмена данными со скомпрометированными устройствами после первоначального получения доступа.

Готовые решения C&C

- Cobalt Strike
- Covenant
- Powershell Empire
- Armitage

Зомби

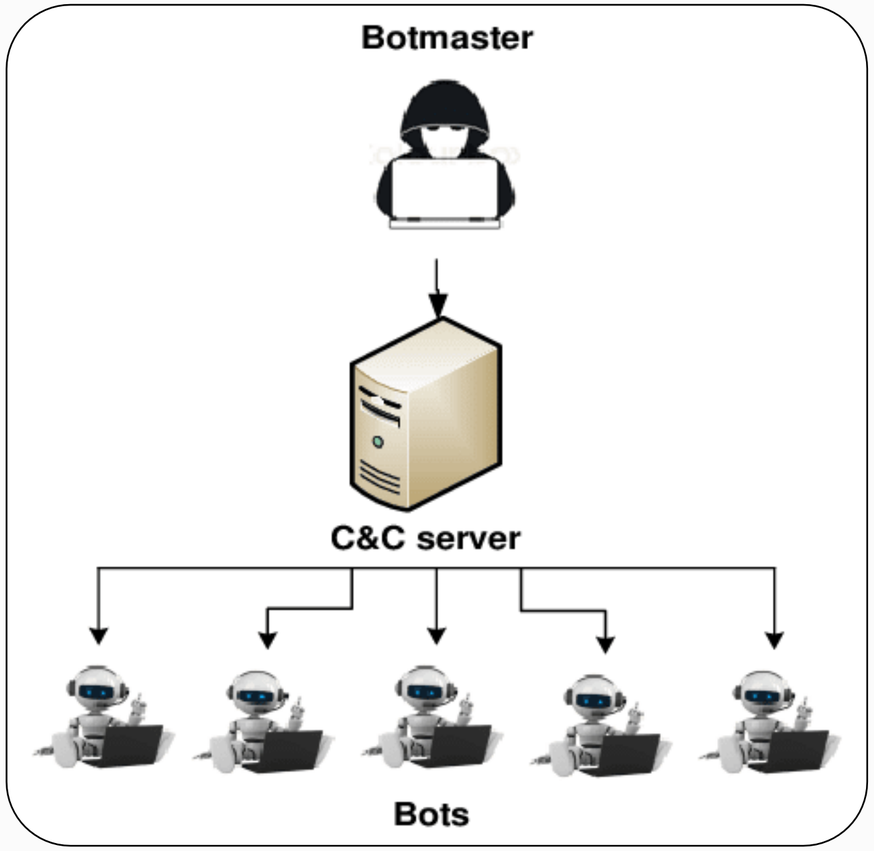
Зомби — это компьютер или иное устройство (IoT), которое заражено вредоносной программой и может удалённо управляться злоумышленником без ведома или согласия истинного владельца.

Ботнет

Много «зомби-машин», используемых для единой цели — это ботнет. Целью этих машин может быть что угодно: от майнинга до отключения веб-сайта с помощью DDoS-атаки. Ботнеты обычно объединяются в единой инфраструктуре C2.

C&C

Command and Control (C&C) — это централизованные машины, которые могут отправлять команды и получать обратную связь от компьютеров из бот-сети.



Beaconing

Beaconing — это процесс, в ходе которого заражённое устройство отправляет вызов в командный центр для проверки инструкций или дополнительных данных (например, за обновлением).

Чего могут достичь хакеры с помощью C2?

Исходящие данные часто не подлежат контролю и ограничениям. За счёт этого вредоносное ПО, внедрённое через другой канал, например, фишинговое письмо или взломанный веб-сайт, устанавливает исходящий канал связи.

Модели C2

- Централизованная модель
- Одноранговая модель P2P
- Модель с внешним управлением
  и случайными каналами связи

Выводы урока

- Command and Control (C&C) —
это централизованные машины, которые могут отправлять команды и получать обратную связь от компьютеров из бот-сети
- Существует 3 модели C&C: централизованная, одноранговая и модель с внешним управлением