C2 (Command and Control) сервер.

telegra.ph/S2-Command-and-Control-server-07-20

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint July 20, 2024

Успешная кибератака — это не просто проникновение в компьютерные системы ничего не подозревающей организации. Для достижения реальной выгоды злоумышленник должен обеспечить непрерывное функционирование вредоносного ПО в целевой среде, обмениваться данными с зараженными или скомпрометированными устройствами в сети, а также извлекать конфиденциальную информацию. Всё это требует надежной инфраструктуры управления и контроля, также известной как C2.

Инфраструктура управления и контроля, также называемая C2 или C&C, включает в себя различные инструменты и методы, которые злоумышленники используют для взаимодействия с скомпрометированными устройствами после их первоначального взлома. В большинстве случаев C2 подразумевает наличие одного или нескольких скрытых каналов связи между устройствами в целевой организации и платформой, управляемой злоумышленником, разработчики C&C постоянно стараются придумать новый уникальный способ сввязи агента с командным сервером для сокрытия от антивирусного ПО. Эти каналы связи служат для передачи команд взломанным устройствам, загрузки дополнительных вредоносных программ и передачи украденных данных злоумышленникам. Распространенной стратегией является смешивание с другими типами легитимного трафика, например, HTTP/HTTPS или DNS. Злоумышленники могут предпринять другие действия для маскировки канала связи, например, использовать шифрование или нестандартные типы кодирования данных.

Платформы управления и контроля могут быть полностью персонализированными или стандартными. Киберпреступники и пентестеры используют такие популярные платформы, как Cobalt Strike, Covenant, Havoc, Sliver, Powershell Empire и Metasploit.

В контексте C2 или C&C часто можно услышать ряд терминов, перечисленных ниже:

- **beacon / implant / payload** - нагрузка, работающая в режиме маяка, обеспечивающая регулярное подключение к серверу (reverse shell) и доступа к компьютеру жертвы.
- **stage** - метод загрузки, поэтапный или сразу целиком.
- **beaconing** - данный процесс предполагает отправку вызова в инфраструктуру Command and Control с целью проверки дополнительной информации и инструкций. Во избежание обнаружения сигналы могут какое-то время бездействовать или отправляться через определенные временные промежутки.
- **ботнет** - представляет собой сеть скомпрометированных устройств, которые хакеры используют для определенной цели. Это может быть отключение ресурса через DDoS-атаки, майнинг криптовалюты и т. п.

Рассмотри ключевые возможности C&C:

- **reverse shells** - возможность настраивать обратные соединения, которые создают постоянный канал связи от скомпрометированной машины к атакующему. Это дает возможность злоумышленнику передавать команды удаленному устройству.
- **модули постэксплуатации** - разработчики C&C стараются включить в свой продукт максимальное количество модулей, которые можно использовать для выполнения различных задач после успешного проникновения, например: сбор данных, установка дополнительных бэкдоров или удаление следов атаки.
- **устойчивость** - обеспечение постоянного доступа к зараженным машинам, используя автозагрузку или службы системы.
- **туннелирование и перенаправление портов** - позволяет атакующим туннелировать трафик через скомпрометированные системы и перенаправлять порты, обеспечивая им доступ к ресурсам, к которым они иначе не смогли бы подключиться напрямую.
- **загрузка / выгрузка** - позволяет доставлять дополнительное ПО на целевое устройство или выгружать данные с него.

Эффективность и удобство C&C решений делают их популярным выбором как для специалистов по кибербезопасности, так и для злоумышленников. Важно применять такие технологии исключительно для обеспечения безопасности и повышения ее уровня, избегая их неправомерного использования.