Разбор атак с эксфильтрацией

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цели урока

- Узнать подробнее про техники эксфильтрации
- Рассмотреть атаки и защиту от техник

Техники атак

Вспомним техники:

- автоматизированная эксфильтрация
- сжатие данных
- шифрование данных
- ограничение размера передаваемых данных
- эксфильтрация через альтернативный протокол
- эксфильтрация через командный сервер
- эксфильтрация через альтернативный канал связи
- физическая эксфильтрация
- передача по расписанию

Автоматизированная эксфильтрация данных

Описание: конфиденциальная информация, полученная на этапе сбора данных, передаётся злоумышленникам с использованием специально созданных автоматизированных сценариев (скриптов).

Защита: защититься от подобных атак сложно, поскольку в каждой системе они будут иметь свои индивидуальные черты, будут иметь векторы, основанные на конфигурации и окружении этой конкретной системы.

Обнаружение: рекомендуется отслеживать нетипичные обращения к файлам и сетевую активность.

Сжатие данных

Описание: злоумышленники могут сжимать собранные данные перед их эксфильтрацией, чтобы минимизировать трафик, передаваемый по сети.

Защита: использовать любую доступную систему предотвращения сетевых вторжений или утечки данных, способную блокировать отправку определённых типов файлов.

Обнаружение: можно обнаружить, отслеживая соответствующие процессы и известные аргументы, которые используются при запуске утилит из командной строки.

Ограничение размера передаваемых данных

Описание: злоумышленники могут проводить эксфильтрацию данных блоками фиксированного размера, а не целыми файлами, или задавать размер пакетов ниже определённого порога.

Защита: рекомендуется использовать системы обнаружения и предотвращения сетевых вторжений.

Обнаружение: анализировать сетевую активность на предмет необычных потоков данных.

Эксфильтрация с помощью физического устройства

Описание: при определённых обстоятельствах, например в случае физической изоляции атакуемой сети, эксфильтрация данных может осуществляться с помощью физического устройства, например внешнего жёсткого диска, флеш-карты, мобильного телефона или MP3-плеера.

Защита: отключение или удаление ненужной функции или программы.

Обнаружение: контроль доступа к файлам на носителе и контроль процессов, которые запускаются на данном носителе.

Эксфильтрация данных: рекомендации

Чтобы выявлять присутствие злоумышленника до того, как он причинит ущерб компании, важно постоянно:

- следить за безопасностью инфраструктуры
- оперативно реагировать на подозрительные события
- строить гипотезы о компрометации и проверять их в инфраструктуре

Выводы урока

- Узнали, что такое эксфильтрация и чем она опасна
- Рассмотрели несколько техник, предложенных матрицей Mitre