ПРАКТИЧЕСКАЯ РАБОТА

Что нужно сделать?

Постройте цепочку атак по MITRE TTP с указанием тактик и техник, используя следующее описание инцидента:

Злоумышленник развернул удалённый C&C сервер и подготовил ВПО для кражи данных, сделал фишинговую рассылку по заранее собранным почтовым ящикам, содержащую требование немедленно скачать обновление, после чего произвел дамп конфиденциальных данных жертв, открывших письмо и установивших вложение.

Выполнение задания

1. Подробнее рассмотрим действия злоумышленника и разобьём их на более детальные процессы:

a) Подготовка Command and Control сервера:
   - Приобретение инфраструктуры(T1583);
   - Размещение средств(T1608).

b) Подготовка вредоносного программного обеспечения для кражи данных:
   - Сбор информации об атакуемых узлах(T1592);
   - Поиск технической информации в открытых источниках(T1596);
   - Поиск в закрытых источниках(T1597);
   - Подготовка необходимых средств(T1588);
   - Разработка собственных средств(T1587).

c) Рассылка по заранее собранным почтовым ящикам, содержащая требование немедленно скачать обновления:
   - Сбор бизнес — информации об атакуемой организации(T1591);
   - Сбор информацииоб атакуемых пользователях(T1589);
   - Поиск на сайтах организации(T1594);
   - Фишинг(T1566).

d) Открытие письма и установка вложения:
   - Выполнение с участием пользователя(T1204);
   - Внешние службы удаленного доступа(T1133);
   - Сценарии инициализации при загрузке или входе в систему(T1037);
   - Автозапуск при заргузке или входе в систему(T1547);
   - Руткит(T1014);
   - Сокрытие артефактов(T1564).

e) Произвел дапм конфиденциальных данных жертвы:
    - Данные со съемных носителей(T1025);
    - Автоматизированный сбор данных(T1125);
    - Архивация собранных данных(T1560);
    - Эксфильтрация через веб-службу(T1567);
    - Автоматизированная эксфильтрация(T1020).

2. Перенесём техники на модель MITRE TTP и выстроим цепочку атаки:

Разведка

- Сбор информации об атакуемых узлах(T1592);
- Поиск технической информации в открытых источниках(T1596);
- Поиск в закрытых источниках(T1597);
- Сбор бизнес — информации об атакуемой организации(T1591);
- Сбор информацииоб атакуемых пользователях(T1589);
- Поиск на сайтах организации(T1594).

Подготовка ресурсов

- Приобретение инфраструктуры(T1583);
- Размещение средств(T1608);
- Подготовка необходимых средств(T1588);
- Разработка собственных средств(T1587).

Первоначальный доступ

- Фишинг(T1566).

Выполнение

- Выполнение с участием пользователя(T1204).

Закрепление

- Внешние службы удаленного доступа(T1133);
- Сценарии инициализации при загрузке или входе в систему(T1037);
- Автозапуск при заргузке или входе в систему(T1547).

Предотвращение обнаружения

- Руткит(T1014);
- Сокрытие артефактов(T1564).

Сбор данных

- Данные со съемных носителей(T1025);
- Автоматизированный сбор данных(T1125);

- Архивация собранных данных(T1560).

Эксфильтрация данных

- Эксфильтрация через веб-службу(T1567);
- Автоматизированная эксфильтрация(T1020).

В ходе структуризации информации были пропущены следующие этапы атаки по матрице MITTRE:

- Повышение привелегий
- Получение учетных данных
- Изучение
- Перемещение внутри периметра
- Организация управления
- Деструктивное воздействие

Так как основной целью злоумышленника была: заполучение конфиденциальных данных корпоративных пользователей.

Но также их не следует исключать из цепи и стоит рассматривать при наличии дополнительной информации.

Для выполнения данного задания была использованна руссифицированная матрица Mittre ATT&CK от компании Positive Technologies https://mitre.ptsecurity.com/ru-RU.