Раздел: Реагирование и расследование инцидентов.
Модуль 1. Расследование инцидентов с использованием встроенных средств защиты Kali Linux
Выполнил: Александр Ганицев.

Постройте цепочку атак по MITRE TTP с указанием тактик и техник.

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.

Реализация: для построения цепочки атак по MITRE TTP (Tactics, Techniques, and Procedures) мы разберем данный инцидент (постфактум).

Вот как выглядит цепочка атак, основанная на MITRE ATT&CK Matrix и Tactic, Technique, Procedure (TTP):

1. Инициация (Initial Access):
Тактика: Initial Access
Техника: Phishing (T1566)
Процедура: Злоумышленник осуществил фишинговую кампанию, посредством письма с вредоносным вложениям на ящики электронной почты, выявленные в результате реализации тактик первой группы.

2. Использование зараженного программного обеспечения (Execution, вторая группа):
Тактика: Execution
Техника: User Execution (T1204)
Процедура: Открытые пользователями письма с запущеным (использование ссылки) ВПО.

3. Закрепление на захваченном устройстве (Persistence, вторая группа):
Тактика: Persistence
Техника: Valid Accounts (T1078)
Процедура: Используя взломанные учётные записи злоумышленник настроил Remote Services на зараженных системах.

4. Захват других внутренних устройств (Lateral Movement, третья группа):
Тактика: Lateral Movement
Техника: Internal Spearphising (T1564)
Процедура: Злоумышленник осуществил рассылку фишинговых писем с учётной записи пользователя, на захваченной системе.

5. Взаимодействие с сервером C&C :
Тактика: Command and Control
Техника: Remote Access Tools (T1219)
Процедура: Злоумышленник взаимодействует с заражёнными системами посредством сконфигурированного C&C сервера.

6. Слив конфиденциальных данных жертвы (Collection):
Тактика: Collection
Техника: Data from Local System (T1005)
Процедура: Злоумышленник осуществил дамп конфиденциальных данных с зараженных систем.

Вывод: Исследованная цепочка атак включала в себя подготовку C&C сервера и создание вредоносного ПО, фишинг по заранее добытым, в процессе разведки, адресам электронной почты. После, злоумышленник разослал фишинговые письма со ссылкой на ВПО, и в результате открытия писем и активации ссылок, он осуществил дамп конфиденциальных данных с локальных дисков данных жертв.