

Поиск вредоносной активности в DNS трафике

Студент: Меньших И.А.

Руководитель: Солодушкин С.И.

Постановка задачи

Дано:

- ❶ DNS-логи
 - source_ip
 - domain
 - rcode
- ❷ Белый список (Alexa, Quancast)
- ❸ Черный список (SkyDNS)

Необходимо:

- ❶ Найти вредоносные домены
- ❷ Выделить общие паттерны взаимодействия клиентов и вредоносных доменов
- ❸ Реализовать полученные подходы в виде программного кода и внедрить результат в производство

- ❶ Поэтапная фильтрация
- ❷ Анализ pDNS и WHOIS
- ❸ Sandbox + Reverse Engineering

- 1 Групповая активность
- 2 Ранжирование доменов
- 3 Поиск и анализ паттернов взаимодействия

Предположения:

- 1 Зараженных хостов в сети фиксированное количество.
- 2 Взаимодействие зараженных хостов и C&C сервера проявляется периодически.
- 3 Подозрительно, когда на один и тот же домен в разное время запрашивает узкий круг хостов.

Алгоритм поиска групповой активности

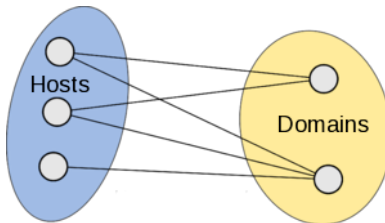
- 1 Делим логи на «окна» фиксированного размера.
- 2 Группируем хосты по домену.
- 3 Фильтруем по черным/белым спискам и количеству уникальных пользователей.
- 4 Сравниваем группы пользователей одного и того же домена в разных «окнах», если группы сильно схожи - домен подозрительный.

Ранжирование доменов

Идея - рассмотрим запросы пользователей за некоторый промежуток времени как граф.

Definition (Граф запросов)

Двудольный неориентированный граф $(H \times D, E)$, где H - множество хостов, D - множество доменных имён, $(h_i, d_j) \in E$, если пользователь h_i запрашивал домен d_j .



Ранжирование доменов

Инициализируем начальные значения, опираясь на белый/черный список и итеративно будем вычислять оценки для доменов:

$$\text{black_score}(h_i) = \sum_{d_j: (h_i, d_j) \in E} \frac{\text{black_score}(d_j)}{\deg(d_j)} \quad (1)$$

$$\text{white_score}(h_i) = \sum_{d_j: (h_i, d_j) \in E} \frac{\text{white_score}(d_j)}{\deg(d_j)} \quad (2)$$

$$\text{union_score}(d_i) = \frac{\text{black_score}(d_i)}{\text{black_score}(d_i) + \text{white_score}(d_i)} \quad (3)$$

$$\text{rank_score}(d_j) = \sum_{h_i: (h_i, d_j) \in E} \frac{\text{rank_score}(h_i)}{\deg'(h_i)} \quad (4)$$

@@ВОТ ТУТ НУЖЕН ПРИМЕР, АНИМАЦИЯ

Анализ паттернов взаимодействия

Идея - рассматривать в графе только ребра, соответствующие неудачным запросам и искать «плотные» подграфы

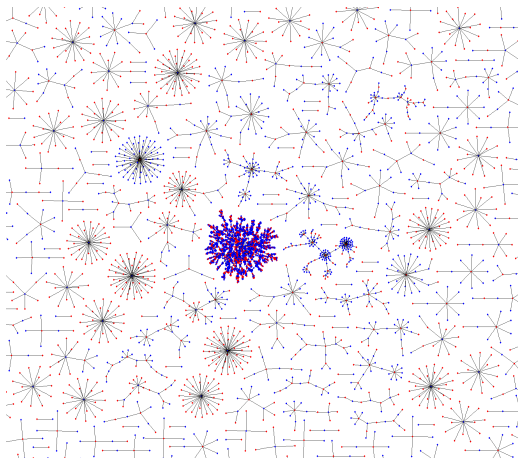


Рисунок – Граф неудачных DNS-запросов (● - хосты, ● - домены)

Алгоритм декомпозиции графа

- ❶ Удаляем ребра (DNS-Overload, SERVFAIL, etc)
- ❷ Находим все компоненты связности (BFS)
- ❸ Для каждой компоненты связности
 - ❶ Ищем плотные подграфы (3-NMF)
 - ❷ Вычисляем

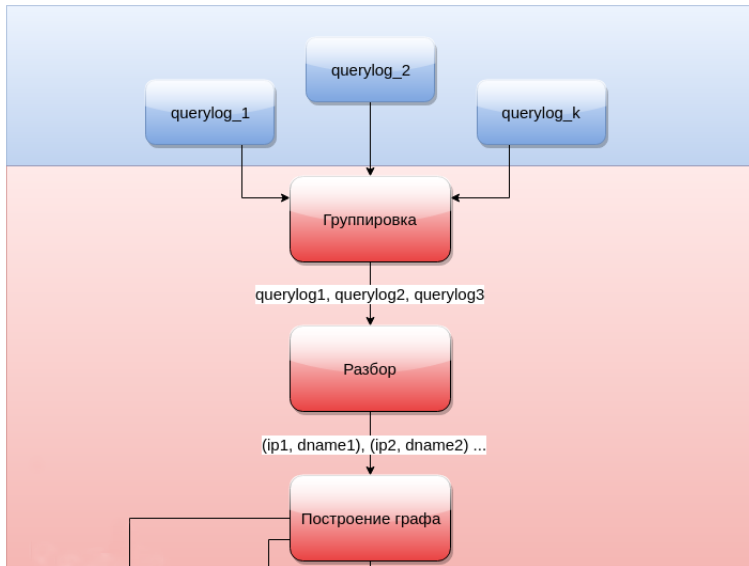
$$\text{density} = \frac{|E|}{|H| * |D|}$$

- ❸ Удаляем те подграфы, которые либо маленькие, либо недостаточно «плотные»

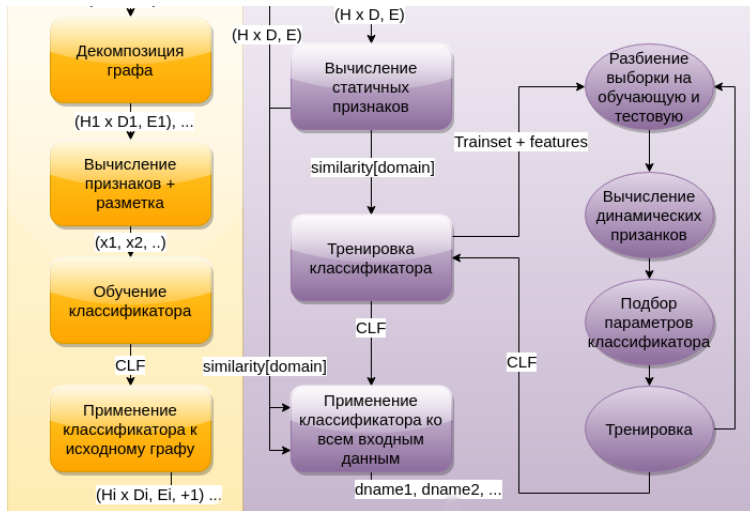
Анализ паттернов взаимодействия

@@ И тут нужен пример

Объединение подходов и автоматизация анализа



Объединение подходов и автоматизация анализа



Результаты:

- 1 Разработан программный продукт, который занимается поиском вредоносных доменов.
- 2 Продукт внедрен в эксплуатацию в компании SkyDNS и показывает хорошие результаты в «реальных» условиях.
- 3 Разработана основная часть системы для ручного анализа вредоносных подграфов.

Что дальше:

- 1 Продолжать работу над анализом «плотных» подграфов, автоматизировать этот процесс за счет дополнительной информации о доменах.
- 2 Улучшать текущий анализатор за счет более тонкой настройки на этапе подбора параметров.

Спасибо за внимание!