

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Уральский федеральный университет имени
первого Президента России Б. Н. Ельцина»

Институт математики и компьютерных наук
Кафедра вычислительной математики

Поиск вредоносной активности в DNS трафике

Студент: Меньших И.А.

Руководитель: к.ф.-м.н., доцент Солодушкин С.И.

Екатеринбург
2016

Постановка задачи

Дано

- 1 DNS-логи
- 2 Белый список (Alexa, Quancast)
- 3 Черный список (SkyDNS)

Необходимо

- 1 Найти вредоносные домены
- 2 Выделить общие паттерны взаимодействия клиентов и вредоносных доменов
- 3 Реализовать полученные подходы в виде программного кода и внедрить результат в производство

- ① Поэтапная фильтрация
- ② Анализ pDNS и WHOIS
- ③ Sandbox

Методы решения

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

Групповая активность

Предположения:

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

Групповая активность

Алгоритм поиска групповой активности

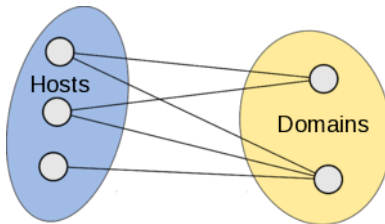
- 1 Делим логи на «окна» фиксированного размера.
- 2 Группируем хосты по домену.
- 3 Фильтруем по черным/белым спискам и количеству уникальных пользователей.
- 4 Сравниваем группы пользователей одного и того же домена в разных «окнах», если группы сильно схожи - домен подозрительный.

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:

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

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

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

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

Ранжирование доменов

Процесс, который скрывается за формулами 1 – 4

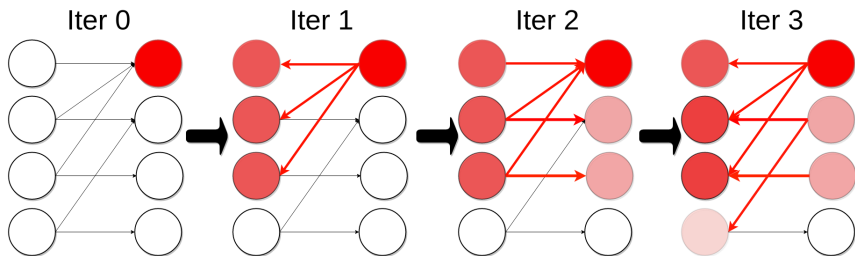


Рисунок – Схематичный пример вычисления ранга

Анализ паттернов взаимодействия

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

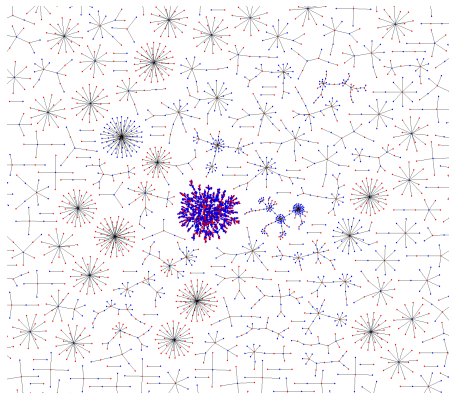


Рисунок – Граф DNS-запросов (● - хосты, ● - домены)

Анализ паттернов взаимодействия

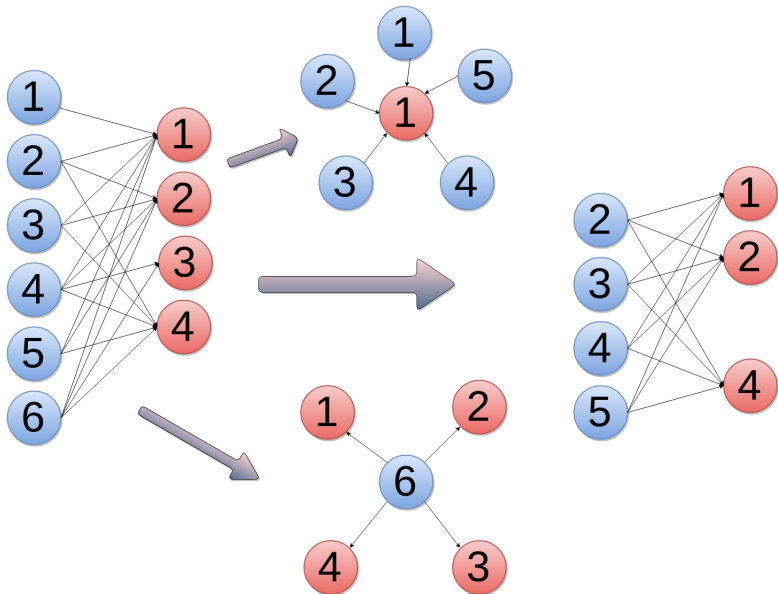
Алгоритм декомпозиции графа

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

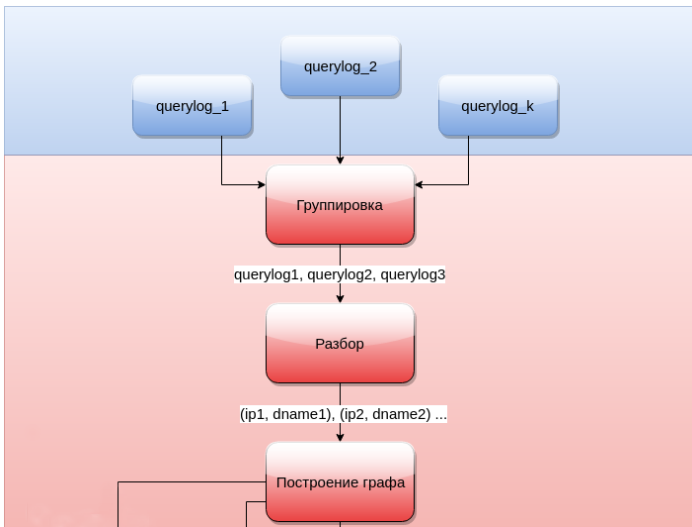
$$\text{density} = \frac{|E|}{|H| * |D|}$$

- c) Удаляем те подграфы, которые либо маленькие, либо имеют малый density

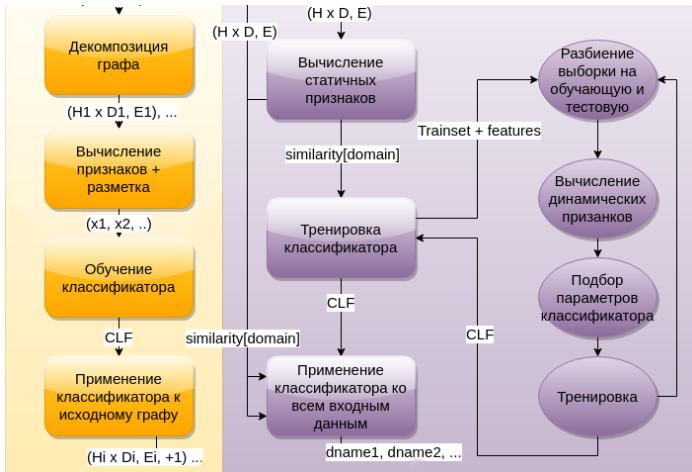
Анализ паттернов взаимодействия



Объединение подходов и автоматизация анализа



Объединение подходов и автоматизация анализа



Результаты работы

- ❶ Разработан программный продукт, который занимается поиском вредоносных доменов.
- ❷ Продукт внедрен в эксплуатацию в компании SkyDNS и показывает хорошие результаты в реальных условиях.
- ❸ Разработана основная часть системы для ручного анализа вредоносных подграфов.

Планы на будущее

- 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!