FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Александр Щербаков

Технический анализ возможности использования доменов после повторной регистрации

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

В случае, если домен ранее использовался для WEB-сайта, то после перерегистрации при повторном делегировании на новый WEB-сайт продолжит идти HTTP-трафик

Плохо это или хорошо ?

FAITID

Фонд содействия развитию технологий и инфраструктуры Интернета

В ноябре 2015г. FAITID начал исследование

Метод: перенаправление всех запросов к неделегированным доменам на статическую WEB-страницу с информацией о том, что домен не делегирован либо не зарегистрирован.

В DNS для 72 доменов 2-го уровня типа tula.su, spb.su … были внесены записи вида:

*.ru.net. 3600 IN A 178.210.89.119

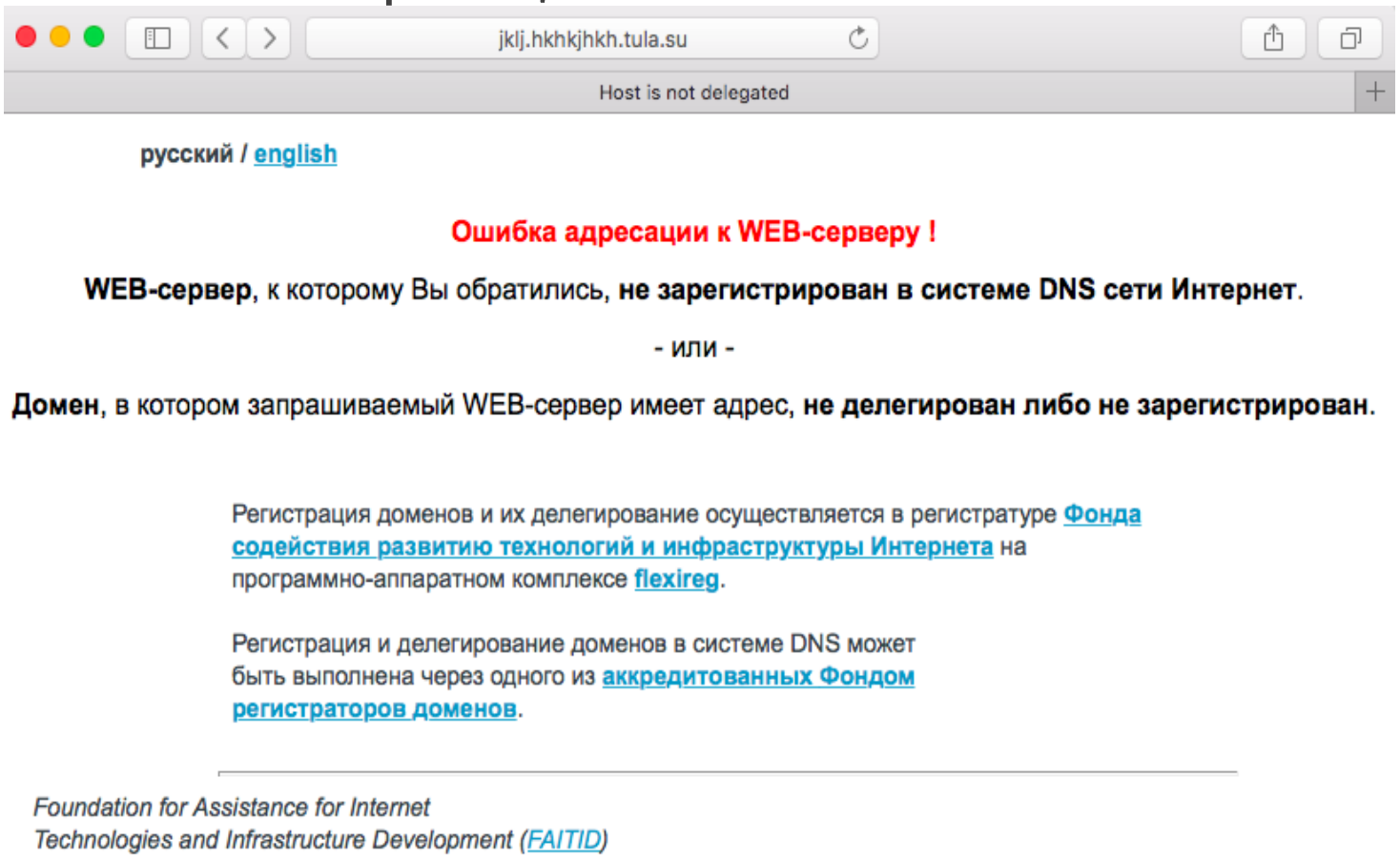
В результате трафик к неделегированным сайтам направлялся на единый IP адрес:

dig -t A ahjkj.spb.ru +short ->178.210.89.119
dig -t A pooioiop.ru.net +short ->178.210.89.119
dig -t A hjhjhyyyy.com.ru +short ->178.210.89.119

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Страница с ответом WEB-сайта:



FAITID

Фонд содействия развитию технологий и инфраструктуры Интернета

Почему были выбраны домены 2-го уровня?

- В связи с программой newGTLD популярность регистрации доменов 3-го уровня уменьшается, ранее зарегистрированные домены освобождаются.
- Количество зарегистрированных доменов третьего уровня всё ещё велико и достаточно для получения объективной картины:

Имя домена	Зарегистрировано	Делегировано
spb.ru	35284	34035
com.ru	18694	17023
msk.ru	11838	10374
…	…	…

FAITID

Фонд содействия развитию технологий и инфраструктуры Интернета

Риски установки “*”

Опасения напрасны, всего 7 обращений:

- 3 WEB-студии
- 4 физлица

Благодарность за помощь в настройке

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Анализ обращений по HTTP

Анализировался стандартный access.log с добавлением имени хоста %{Host}I к которому идёт обращение:

```
LogFormat "%a %l %u %{Host}i %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
```

Информация из файла:

```
162.255.160.109 - - teambuildingap.com.ru [31/Aug/2016:00:01:00 +0300] "GET
/img/h_bg.gif HTTP/1.0" 200 3971 "http://teambuildingap.com.ru/index.html"
"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727)"
37.153.47.213 - - aquaviva.spb.ru [31/Aug/2016:00:01:00 +0300] "GET
/bitrix/spread.php?s=QklUUklYX1NNX0dVRVNUX0lEATM2Mjk2MjMBMTUwMzY5NDc4NA
EvAQEBAkJJVFJJWF9TTV9MQVNUX1ZJU0lUATMxLjA4LjIwMTYgMDA6NTk6NDQBMTUwMz
Y5NDc4NAEvAQEBAg%3D%3D&k=b44d3103800fb6c964bbcefd32a980f5 HTTP/1.0" 200
3971 "http://mitropolia.spb.ru/news/mitropolit/?id=105778" "Mozilla/5.0 (Linux; Android
6.0.1; SAMSUNG SM-G925F Build/MMB29K) AppleWebKit/537.36 (KHTML, like Gecko)
SamsungBrowser/4.0 Chrome/44.0.2403.133 Mobile Safari/537.36"
```

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Количество запросов к странице

Ежемесячная статистика										
Месяц	В среднем за день				Всего за месяц					
	запросов	файлов	страниц	посещений	сайтов	Кбайт	посещений	страниц	файлов	запросов
Сен 2016	1710491	1386933	422364	38714	60736	10364008	77429	844729	2773866	3420982
Авг 2016	3277378	2896655	1191834	71605	830457	334753867	2219767	36946870	89796325	101598728
Июл 2016	3501025	2883992	2231747	63130	781635	334853961	1957037	69184159	89403779	108531776
Июн 2016	4249445	3800051	2557519	63862	900355	424899394	1915874	76725583	114001542	127483356
Май 2016	5111949	4360213	2999169	74313	1202493	505901038	2303711	92974243	135166632	158470419
Апр 2016	4416579	3885269	1639663	73972	1056123	425182988	2219165	49189905	116558088	132497382
Мар 2016	5105443	4376976	1877241	75510	1102896	497250147	2340822	58194471	135686279	158268747
Фев 2016	9018213	8434135	6151405	78192	1130278	920409483	2267579	178390760	244589938	261528205
Янв 2016	3714713	3419803	2051878	29417	319063	207218638	470673	32830061	54716852	59435420
Дек 2015	6215820	5606220	3417233	44243	666420	608278419	973346	75179146	123336859	136748060
Ноя 2015	6002296	3250339	3424097	186658	1372286	655962650	3546504	65057848	61756459	114043641
Всего						4925074593	20291907	735517775	1167786619	1362026716

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Анализ частоты обращений

К каким страницам чаще всего обращались:

#	запросов		Кбайт		URL
1	8274976	14.92%	74870163	30.40%	/search
2	2530251	4.56%	21113743	8.57%	/
3	1857366	3.35%	17120179	6.95%	/wpad.dat
4	1696462	3.06%	43016	0.02%	/robots.txt
5	905689	1.63%	8183205	3.32%	/java/api.php
6	557400	1.00%	5083210	2.06%	/announce
7	361560	0.65%	3322256	1.35%	/retracker/announce.php
8	288849	0.52%	2649146	1.08%	/bitrix/spread.php
9278185	0.50%		2570862	1.04%	/retracker/scrape.php

Отметим, что только 4.56% запросов обращались к корневому документу несуществующего сайта.
Именно эти запросы можно считать запросами пользователей при условии, что обращения повторялись не более 2-х раз и выполнялись стандартным броузером.

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Анализ броузеров

Первые 15 из 50388 броузеров:

#	запросов	Броузер	
1	9776556	17.63%	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2)
2	9041737	16.30%	uTorrent/345(109814002)(41202)
3	6906745	12.45%	Bittorrent
4	1354953	2.44%	Kaspersky Proxy-Server detection agent
5	958268	1.73%	Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; ru; rv:1.9.2.9)
6	795975	1.43%	WHR
7	712938	1.29%	Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
8665253	1.20%	BitTorrent/795(254517491)(41203)	

Запросы можно разделить на категории, направляемые:

- Торрент-клиентами
- Прочими ботами и роботами.
- Пользователями в ручном режиме (по ссылкам, по закладкам)

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Torrent-клиенты или пару слов об anisource и evolution

Вычислим, к каким адресам наибольшее в час количество обращений:

119000 anisource.spb.ru
54783 evolution.tula.su
77 mp3.free-stuff.com.ru
12 wsus.admtu.spb.ru

Но при этом делегирование было снято:

evolution.tula.su 31-JAN-2012
anisource.spb.ru 22-NOV-2013

FAITID

Фонд содействия развитию технологий и инфраструктуры Интернета

Паразитный torrent-трафик к сайту

Каждый запрос «весомый»:

182.131.12.233 - - anisource.spb.ru [31/Aug/2016:00:10:06 +0300] "GET /announce?info_hash=%9E%2C%EE4%04%8CBx%89%0CQ%A4%A99%3D%F4%26%FA9S&peer_id=-lt0C60-%F8%8E%89%AB%B0X%27%04%E9%AF%3F0&key=3f1e78c7&compact=1&port=2380&uploaded=0&downloaded=0&left=16750731341&event=started HTTP/1.0" 403 1633 "-" "rtorrent/0.8.6/0.12.6"

Вывод: повторная регистрация доменов, на которых работали сайты из сети torrent-серверов, приведёт к тому, что пользователь, вновь зарегистрировавший домен, при организации WEB-сайта столкнётся с проблемами загрузки своего сайта «паразитными» запросами и огромным трафиком.

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Что делать с torrent-трафиком?

На уровне регистратуры есть метод:

- помещение домена в «отстойник»
- делегирование домена на 127.0.0.1

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Прочие боты и роботы

Выборочно иллюстрация:

==========

IP: 79.134.192.18 Count: 1010033 PTR: 79-134-192-18.obit.ru.
79.134.192.18 - - wpad.kronos.spb.ru [31/Aug/2016:00:00:58 +0300] "GET /wpad.dat HTTP/1.0" 200 3971 "-" "Kaspersky Proxy-Server detection agent»

==========

IP: 79.25.115.107 Count: 144975 PTR: host107-115-dynamic.25-79-r.retail.telecomitalia.it.
79.25.115.107 - - broadcast.com.ru [31/Aug/2016:10:26:30 +0300] "GET /DISK_3/Focus_8_2002/03_-_Fretless_Love.mp3 HTTP/1.0" 206 3971 "-" "Lavf/56.40.101»

В общем случае:

- если ранее на домене был сервер, раздающий какую-либо информацию, то паразитный трафик на вновь зарегистрированный и делегированный домен гарантирован;
- объем трафика может быть измерен только экспериментально, а для этого домен должен быть делегирован.

FAITID

Фонд содействия развитию технологий и инфраструктуры Интернета

Запросы пользователей

Безусловно зависят от ТИЦ, и разница может быть весьма существенной.

От 1% - 4% в общем объеме трафика к ранее делегированным WEB-сайтам (в среднем по больнице).

FAITID

Фонд содействия развитию технологий и инфраструктуры Интернета

Возможные применения исследования FAITID

Малый срез – исследование регистратурой трафика не ко всем не делегированным доменам, а только к доменам, подлежащим удалению. (бывает до 10тыс. в день в .RU).

- Перед удалением домена временно устанавливать делегирование на сайт регистратуры.
- Исследовать http-трафик к доменам, подлежащим удалению.
- Организовать для пользователей экспертную систему, дающую оценку каждому освобождающемуся домену на предмет наличия в том или ином объёме паразитного трафика и трафика пользователей к бывшему сайту в этом домене.
- Домены с особым трафиком можно временно изымать из оборота и редуцировать трафик к этим доменам.

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

За рамками темы

- Получение для СБ информации о компьютерах, задействованных в сетевых атаках.
- Домен WPAD.TLD – должен принадлежать регистратуре.

FAITID

Фонд содействия развитию технологий
и инфраструктуры Интернета

Спасибо за внимание!