Система DNS: Противодействие противоправной активности в Рунете

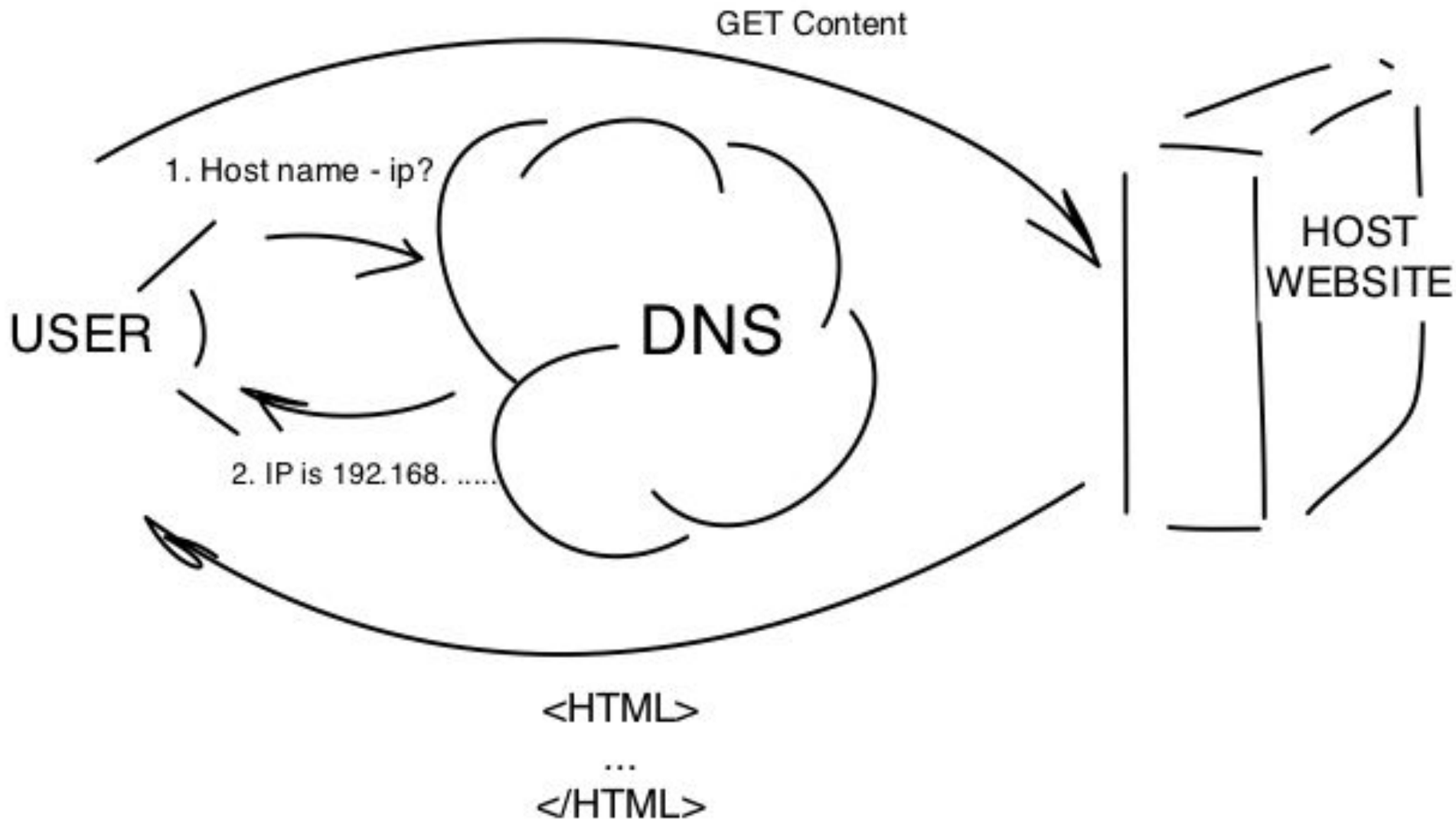
Шаг первый: Угрозы
Шаг второй: Классификатор

Павел Храмцов (p.khramtsov@faitid.org)

Основные угрозы

- Вывести из строя DNS (ТЦИ)
- Подменить соответствие в DNS (DNS-провайдеры)
- Использовать DNS в качестве средства доставки «плохого» контента (провайдеры и DNS-сервисы)
- Построить обузоустойчивый хостинг или регистратора доменов (Хостинг-провайдеры и регистраторы)

Ключевой элемент инфраструктуры

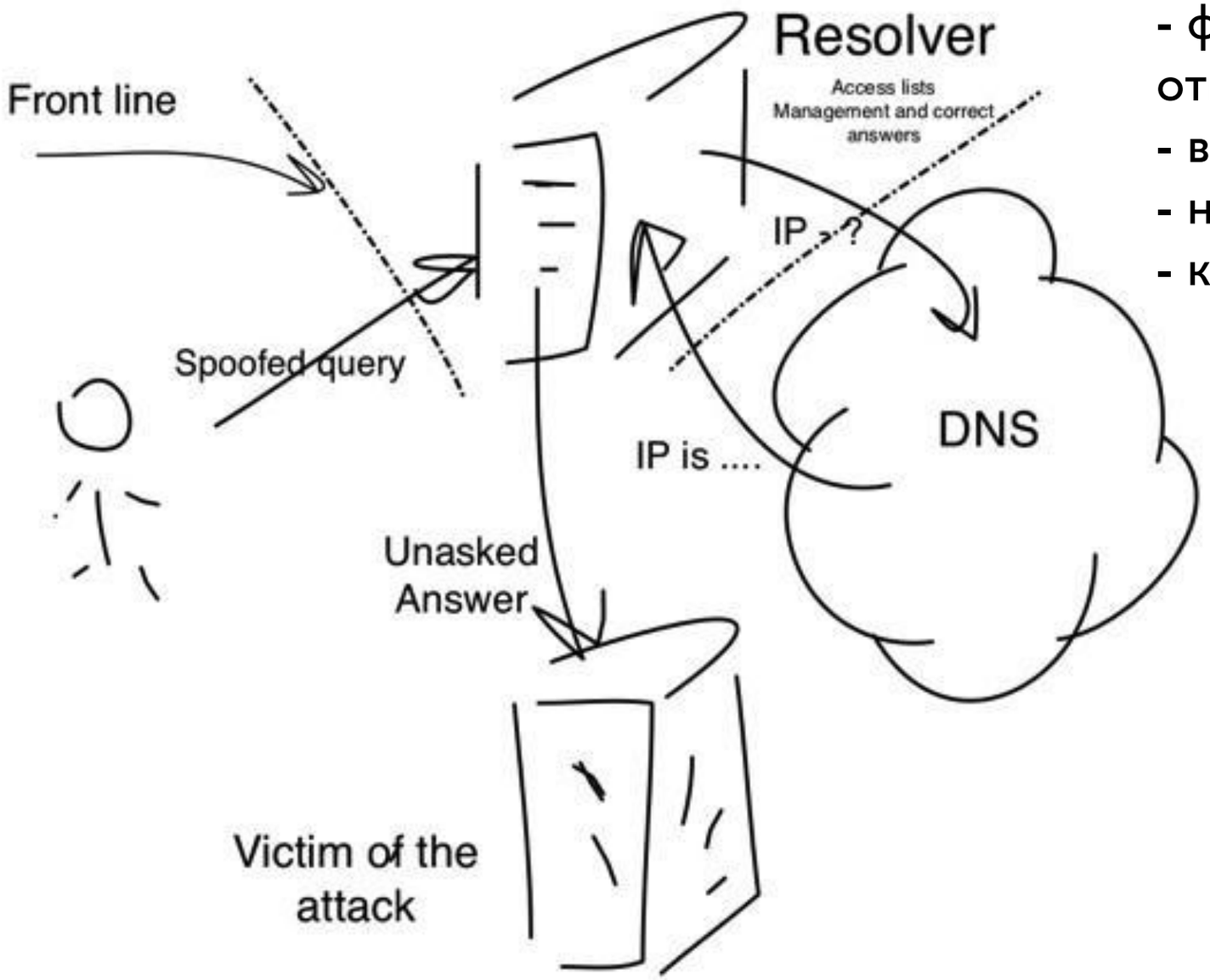


DDoS DNS

- Цель: затруднить возможность получения IP-адресов

12 февраля 2012 о подготовке к такой атаке сообщила команда Anonimous, потом правда от этого объявления они открестились.

DNS amplification



Суть борьбы:
- фильтровать на входе resolver-а по IP-отправителя;
- входная фильтрация;
- непубличные resolver-ы;
- корректная обработка запросов;

DNS amplification

- Согласно VeriSign на корневых серверах за месяц отметилось примерно 10 млн. резолверов

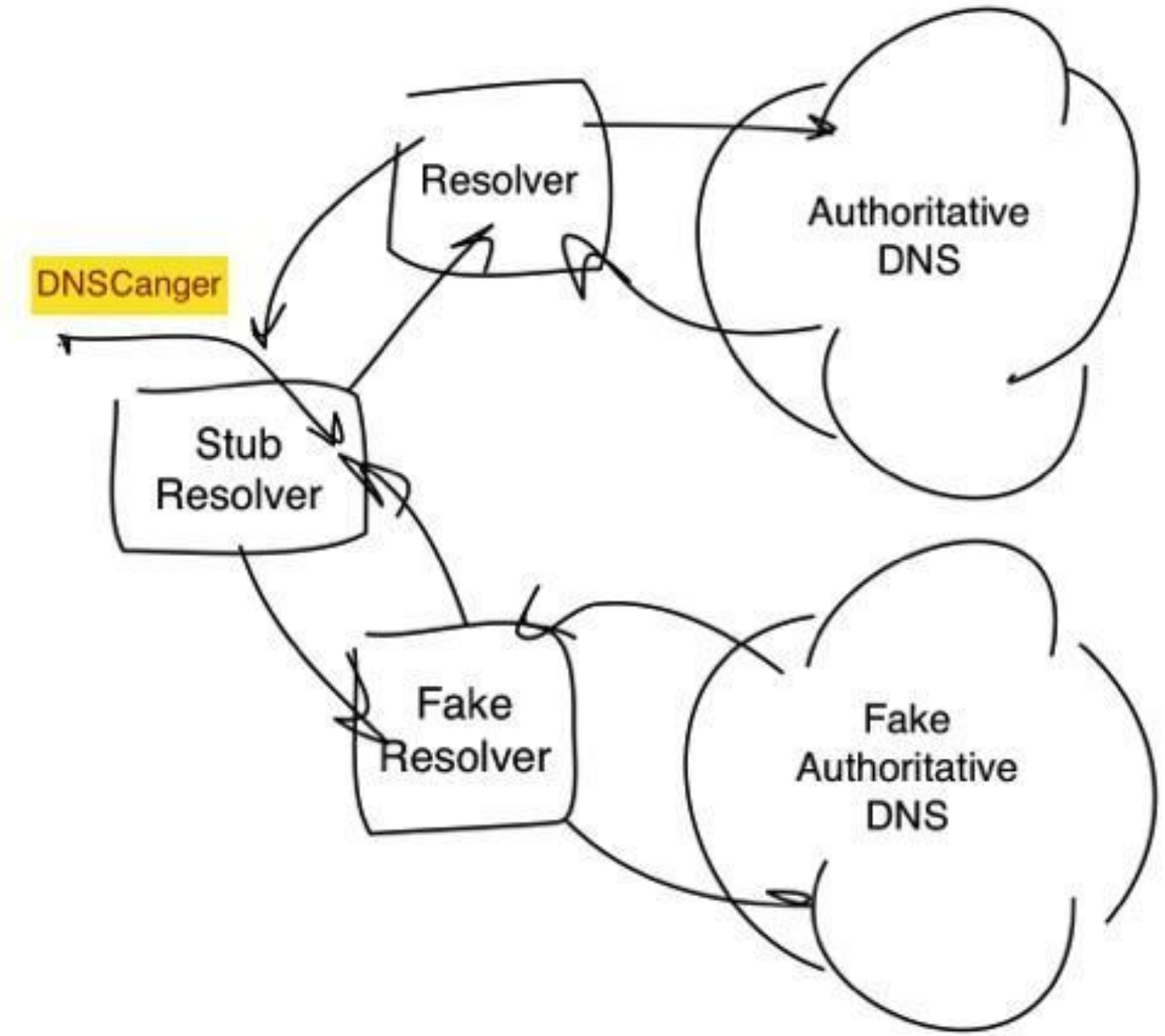
- Согласно данным ТЦИ на авторитативных серверах RU за сутки отмечается в среднем 1,5 млн. резолверов со всего мира

- 1/4 отвечает на spoof-пакеты

- 1/8 - открытые резолверы

- Power dns resolver - 100 тыс ответов в секунду, у bind производительность в 4-5 раз меньше.

DNSChanger



4 млн зараженных компьютеров;
регистратор EstDomains - Rove Digital;
2 года расследований ФБР;
Привлечение лидеров рынка;
8 месяцев «лечения».

DNS - серверы

85.255.112.0 through 85.255.127.255

67.210.0.0 through 67.210.15.255

93.188.160.0 through 93.188.167.255

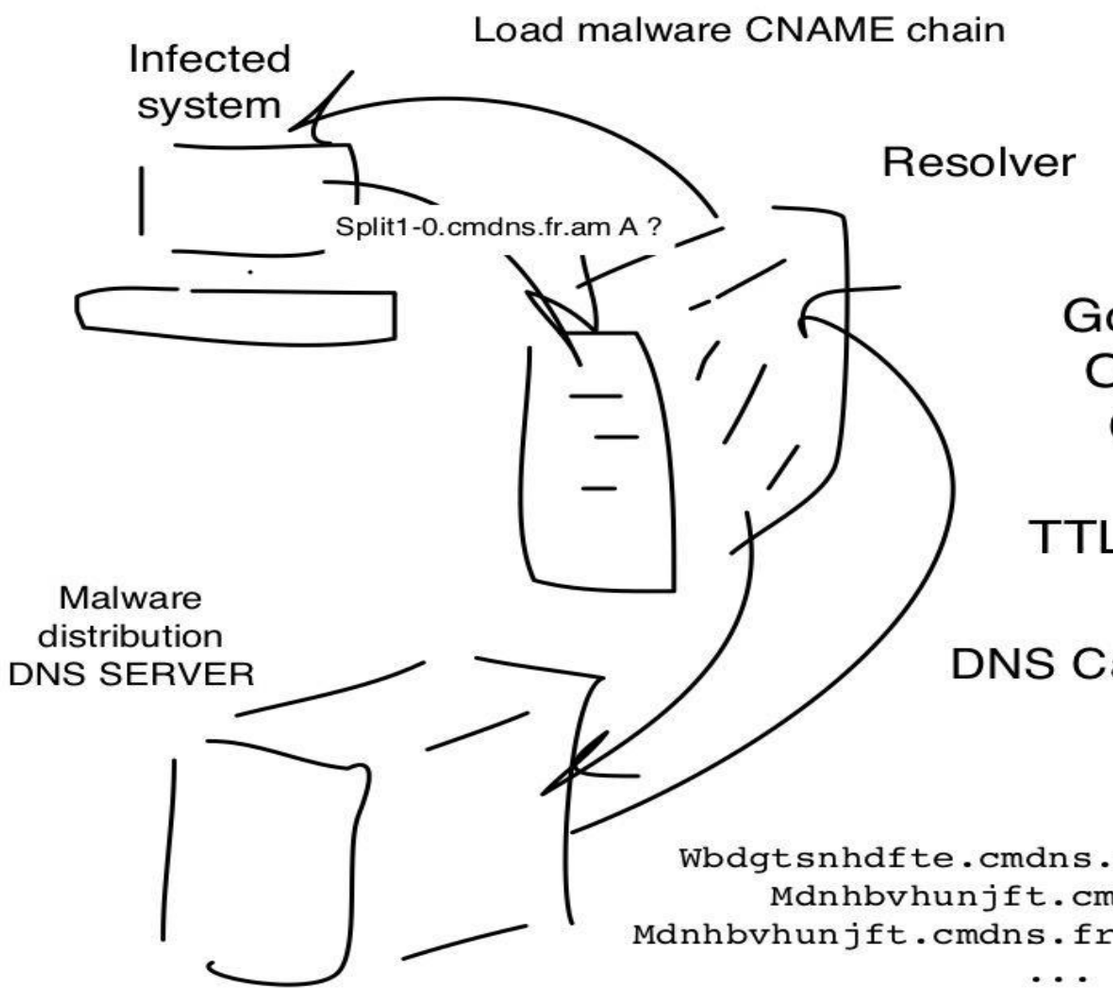
77.67.83.0 through 77.67.83.255

213.109.64.0 through 213.109.79.255

64.28.176.0 through 64.28.191.255

Что можно хранить в файле зоны?

Carlos Díaz Hidalgo
Francisco J.Gomez Rodrigues
"Malware Cloud Distribution"




```
Wbdgtsnhdfte.cmdns.fr.am IN CNAME
    Mdnhbvhunjft.cmdns.fr.am.
Mdnhbvhunjft.cmdns.fr.am IN CNAME ...
...
```

И весь этот спам (2010)

Начиная с февраля 2010 года интернет-домен .ru находится на первом месте по количеству зарегистрированного на нем нежелательного контента (спама), обогнав такие домены, как .com, .net, .cn и .info.

Среди стран, где физически расположены серверы, с которых отправляется спам, **Россия занимает 4 позицию с 5,3% от общего объема нежелательной почты.** Первые три места достались США (9.7% спама), Бразилии (8.4%) и Индии (8.1%).

При **этом более 60%** зарегистрированных в Китае спамерских URL-адресов **имеют домен .ru**. Таким образом, согласно исследованию, типичное спам-сообщение рассылается с компьютера, физически расположенного в США, Индии или Бразилии, **но имеет URL на домене .ru**, а его хостинг находится в Китае.»

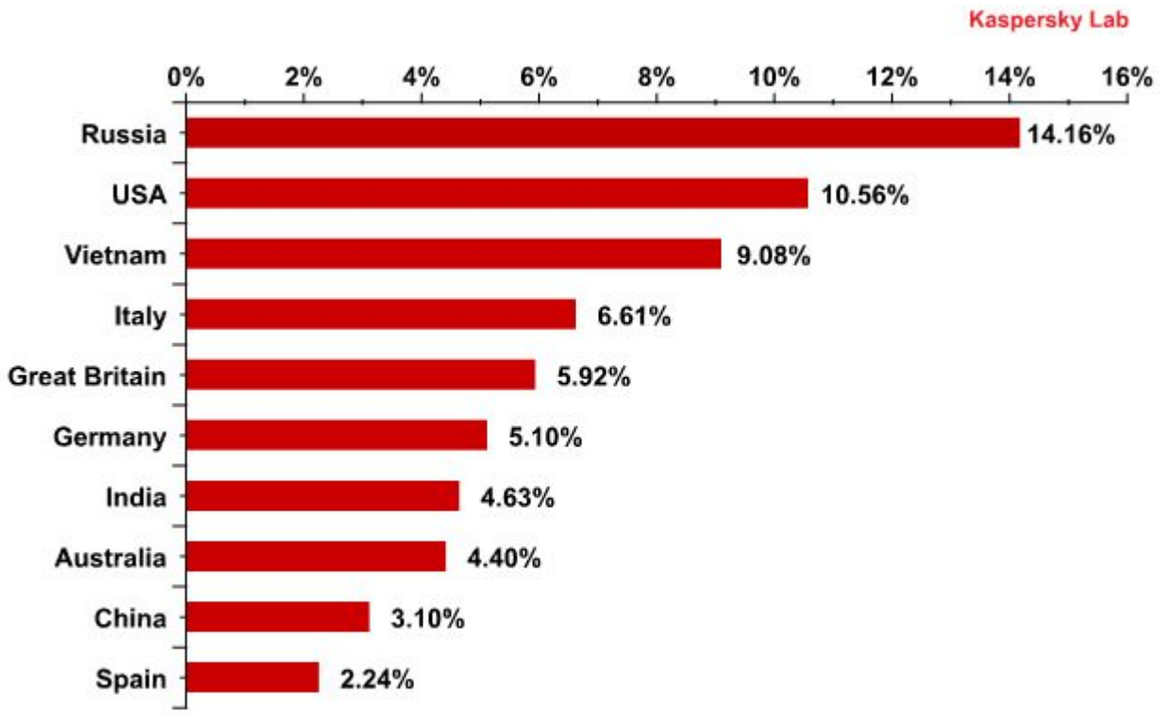
2010 Mid-Year Trend and Risk Report

треть всех доменов, зарегистрированных под спам в мире были зарегистрированы в зоне .RU. Почти все эти домены были зарегистрированы через двух **российских регистраторов NAUNET и REGRU**.

«Russian Pro-Spam Registrars», M86 Security Lab, 09,2010

И весь этот спам (2011)

Russia and the USA maintained their status as the countries where malware was detected most frequently in mail traffic. Russia was the overall leader, with the amount of blocked emails with malicious attachments decreasing slightly.



Spam report: June 2011. Kaspersky Lab

«the top five countries sending spam include India, Russia, Brazil, South Korea and Indonesia.».

2011 Mid-Year Trend and Risk Report

Россия занимает первое место в мире по уровню спама (82,2%)

Intelegence Report , Symantec, May 2011

Cooperation from ICANN and Top Level Domains. Members of the Working Group were especially pleased with the cooperation and coordination of ICANN and the ccTLDs in the33process. They view ICANN and ccTLD cooperation as a precedent that will help future efforts and discourage malware authors from believing they can easily exploit that portion of the DNS system. Several said they want this emphasized publicly to reinforce that message and thank those organizations for the job they did.

Conficker Working Group: Lessons Learned. June 2010 (Published January 2011)

И весь этот спам (2012)

«Согласно статистике ZeuS Tracker по состоянию на 1 февраля, число активных центров управления ZeuS в Сети приближается к 200. Больше половины из них находятся на территории США, вдвое меньше — в России. *Из регистраторов хуже всех ситуация у российских «Наунет СП» (94 домена, ассоциированных с ZeuS) и REG.RU (78)*, из AS-провайдеров — у азербайджанской ADaNET (15 C&C серверов) и американской GNAXNET (12)»

«Зевс нашел тихую гавань», Kaspersky Lab, (2 февраля 2012)

“Spamhaus also recommends that networks use our Don't Route Or Peer list to drop all traffic originating from or destined for NAUNET's IP address space. This will help protect end users from the activities of the cybercriminals to whom NAUNET persists in providing services.”

Russian registrar NAUNET knowingly harbours Cybercriminals. Spamhous, 22.03.2012

Microsoft против Джон Доу 1-39

AGAVA-REG-RIPN	1
NAUNET-REG-FID	90
R01-REG-RIPN	4
REGGI-REG-RIPN	1
REGISTRATOR-REG-RIPN	5
REGRU-REG-RIPN	107
REGTIME-REG-RIPN	25
RU-CENTER-REG-RIPN	39

Всего на анкетах, которым принадлежат эти домены, ~21000 доменов

Работа по новым правилам

Когда администратор не виноват (не контролирует контент)

- Парковка
- Блоки коммерческой рекламы
- Дефекты ПО хостинг-провайдера

Классификатор целей использования доменов

- Account
- Имя домена
- Вредоносная активность
- Взломанный хостинг
- Fast-Flux
- Экспертная оценка

Вредоносная активность

- Malware
    - Количество зарегистрированных в БД фактов размещения malware на данном домене
    - Тип(ы) Malware если возможно определить — в случае если мы располагаем такой информацией.
    - First seen / Время начала активности (время первого зарегистрированного в БД размещения malware на данном домене)
    - Last Seen / Время последней активности (последние данные о размещении malware по данному домену)
    - Уровень доверия (0-10) — в зависимости от достоверности источников и частоты жалоб (по фактам размещения malware) на данный домен присваивается число.
- Phishing
- Botnet

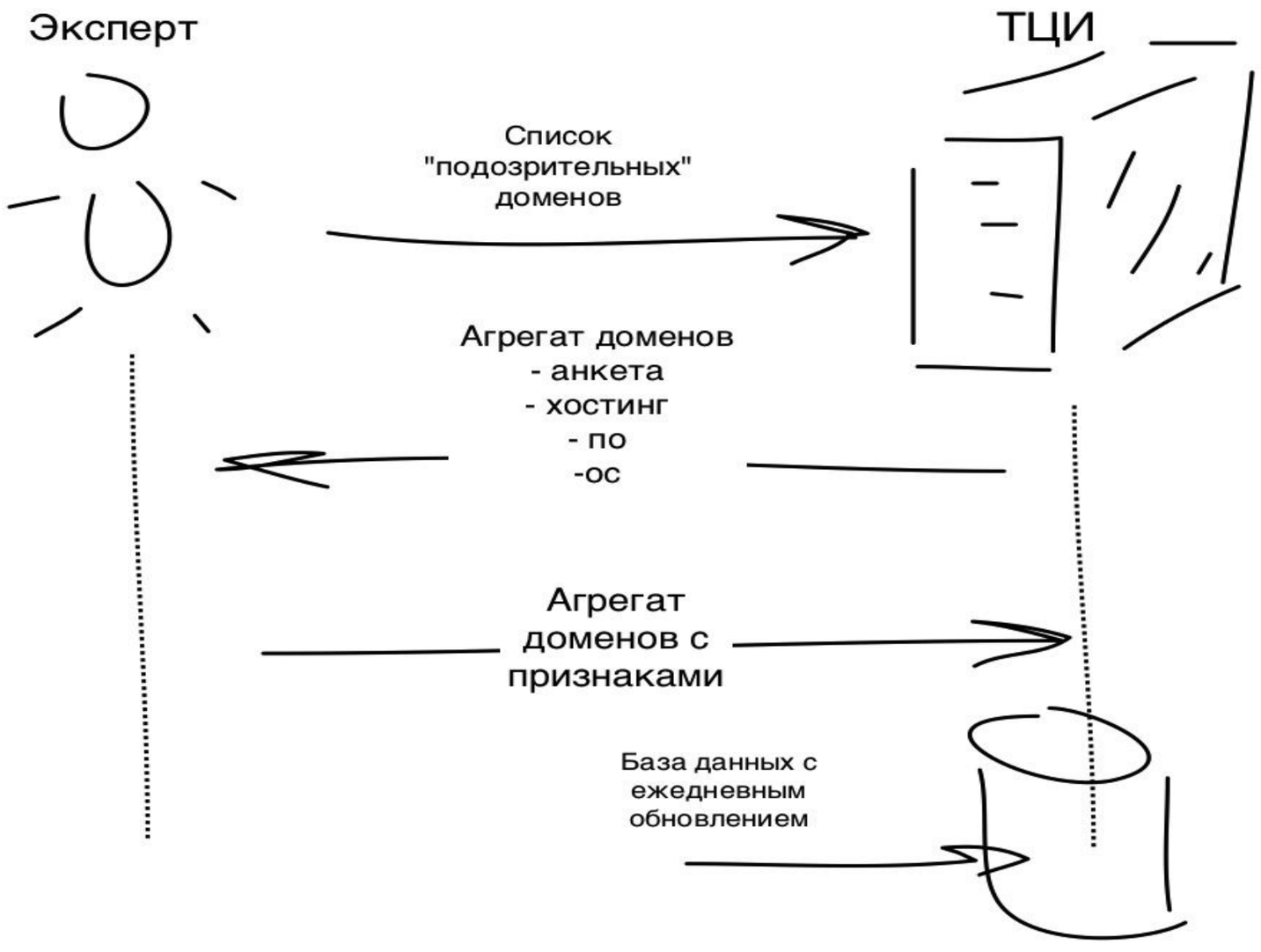
Вредоносная активность

- Malware
- Phishing
    - Количество зарегестрированных в БД фактов размещения phishing на данном домене
    - Phishing Target(s) (Ebay, Paypal, Яндекс Деньги etc..) если возможно определить
    - First seen (по аналогии с malware)
    - Last Seen
    - Уровень доверия (0-10)
- Botnet

Вредоносная активность

- Malware
- Phishing
- Botnet
  - Количество зарегестрированных в БД фактов размещения элементов управления ботнетами
  - Botnet type (Zeus, Spyeye etc..) если возможно определить
  - Уровень доверия (0-10)

Порядок накопления информации и ее использования



1. Предупреждение администратора о наличии проблем по аналогии с поисковыми системами
2. Предупреждение Хостинг-провайдеров о наличии проблем
3. Предупреждение регистраторов о наличии проблем
4. Подготовка информации для администрации КЦ и ТЦИ
5. Взаимодействие с коллегами и «братьями по оружию»

Что может получиться

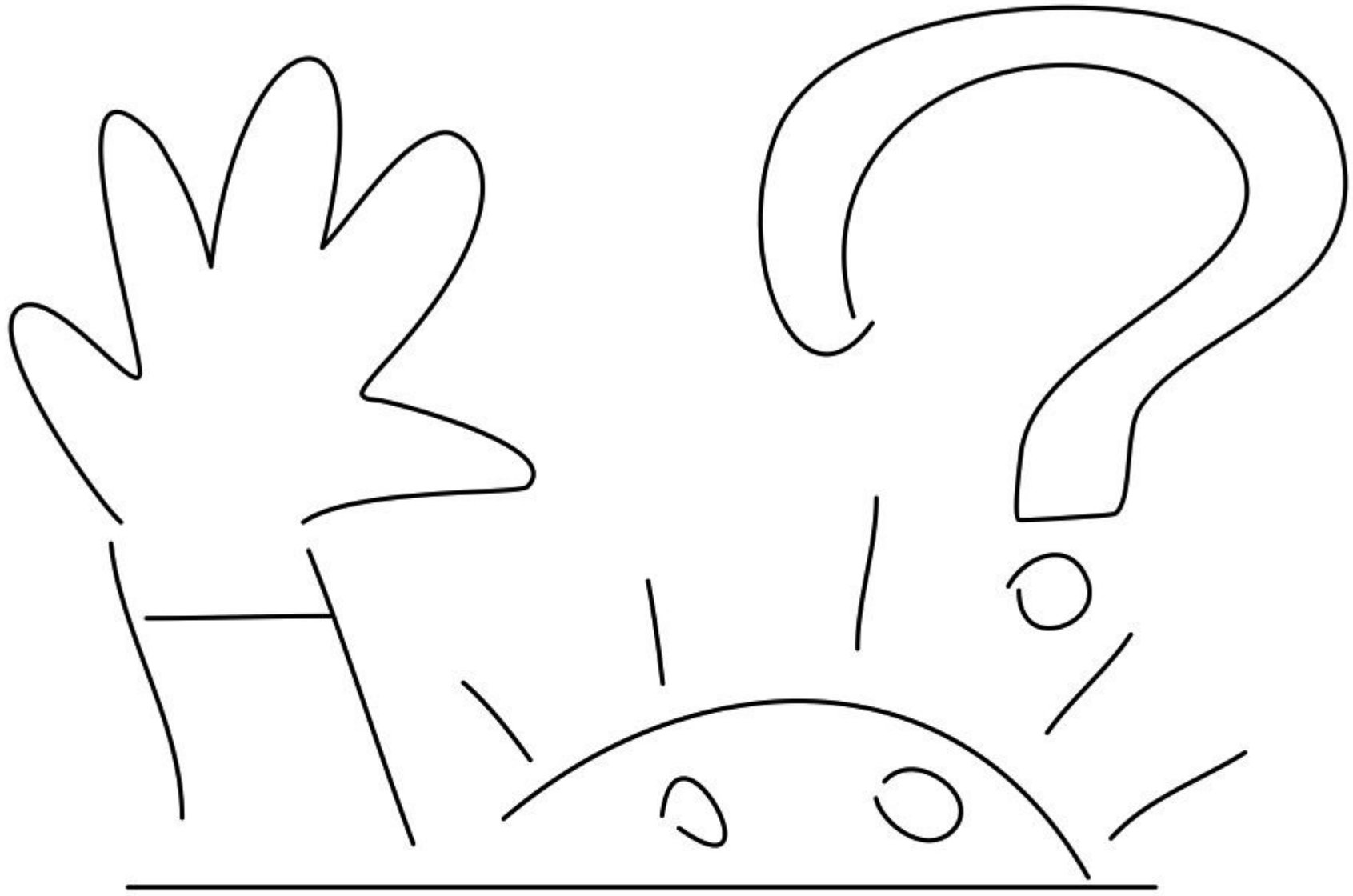
0bc6652ff9740520d881c93cf6b8799b	NAUNET-REG-RIPN	9	56
917a9b9c9e188e1558391eb5affdc125	NAUNET-REG-RIPN	158	170
4bfb6cefe8a603081168b38017ff000e	R01-REG-RIPN	373	6
456e830a10f9b1a99eab41a9f48cb5f4	R01-REG-RIPN	524	136
ce76fd52928d523d8d21a8e411b0ba81	REGRU-REG-RIPN	2	2
c7556a0ea7b1c75c6fc5e0b93a340aaa	REGRU-REG-RIPN	10	18
654bea4c3d0d74bf532634563b4488a8	REGRU-REG-RIPN	11	72
d9e7f1fd3f30c53a3154e934bfbde0fd	REGRU-REG-RIPN	27	12
058fbfc98638b324d6e8d582e1431285	REGRU-REG-RIPN	28	4
e96bb0fda446f0f696062861e588c543	REGRU-REG-RIPN	130	50
2b870324c21be6679773ccf77fbed1d2	REGRU-REG-RIPN	260	232
d4491dfd1bf9c9e0e207923ef88ab858	REGRU-REG-RIPN	310	10
49748d8a5cbd622ca74ad0c51e8fd268	REGRU-REG-RIPN	338	392
6ba2f1af9542ccf4ca92c488f615763e	REGRU-REG-RIPN	552	1305
d8d689813feabf49a0a55ecf2e652687	REGRU-REG-RIPN	588	96
26638c291b37079df0d5cc9bb16fceab	REGRU-REG-RIPN	592	48
3d0d5407b77ad303fe0489033eec96bc	REGRU-REG-RIPN	4506	1098
83595a2345dd16e40f5e3f0f2c68b6ab	REGRU-REG-RIPN	8232	1512
a83fc781c767ca42192b119da03116b8	REGRU-REG-RIPN	11363	9328
84a44aa8a0e93fc013d78c2c5ccbe438	REGRU-REG-RIPN	18164	266
2a5e5a32a21166a24f58ce41ce7afa08	REGTIME-REG-RIPN	4	10

В дополнение к существующему бану было проверено и добавлено 13400 доменов

А всего в бане 46181 домен

Резюме

- Быть изгоями плохо
- Нужно реально понимать «картину мира»
- Нужно интегрироваться в общую систему мероприятий по безопасности DNS
- Нужно и демонстрировать и реально участвовать в общем деле



Вопросы

p.khramtsov@faitid.org