



Domain aftermarket and DNS

Pavel Khramtsov, MSK-IX
p.khramtsov@msk-ix.ru

TLDCON-2016
Tbilisi

Domain aftermarket and DNS

Expire contracts

Expire domain p

Auction

Parking

Написать письмо владельцу

32.SPB.RU

ДОМЕН ПРОДАЕТСЯ!

ИМЯ

EMAIL

СООБЩЕНИЕ

ОТПРАВИТЬ

Показать меню

© Домен припаркован с помощью сервиса [DomainParking.ru](#)

Показать меню

© Региональный Сетевой Информационный Центр (RU-CENTER)

Domain Aftermarket DNS features

Domain name resolving:

- a lot of name per server,
- wildcard support,
- skip recursion.

Domain name support:

- a lot of changes per day ($\sim n \cdot 1000$ domains per day);
- small zones.

As a result: Separated DNS-servers

Domain Aftermarket: Threats

Domain name resolving reliability:

- DNS-amplification attack;
- Domain Generation Algorithm attack;
- «Diving»;
- Flood.

Domains Reincarnation :

- SEO;
- “Bad” Domains.

As a result: Separated DNS-servers

.TR under fire (DNS amplification)

Start point: 14 December

Duration: 3 weeks.

Characteristics:

- 185000 q/s per server
- 220 Gbs per channel.

Type: DNS-amplification DDoS (from 10 150 times).

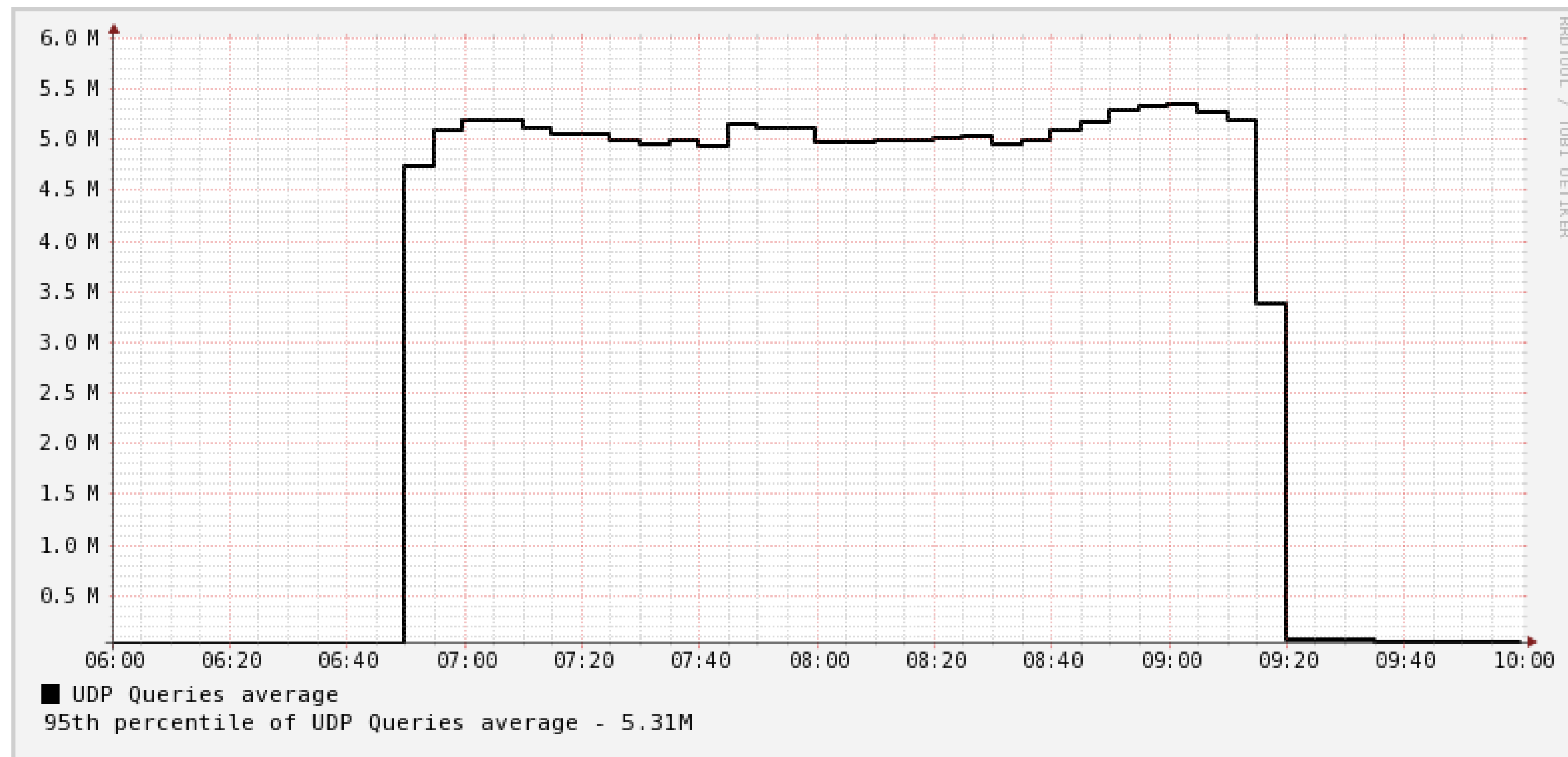
Why: open resolvers, 25% inside .TR.

Target:

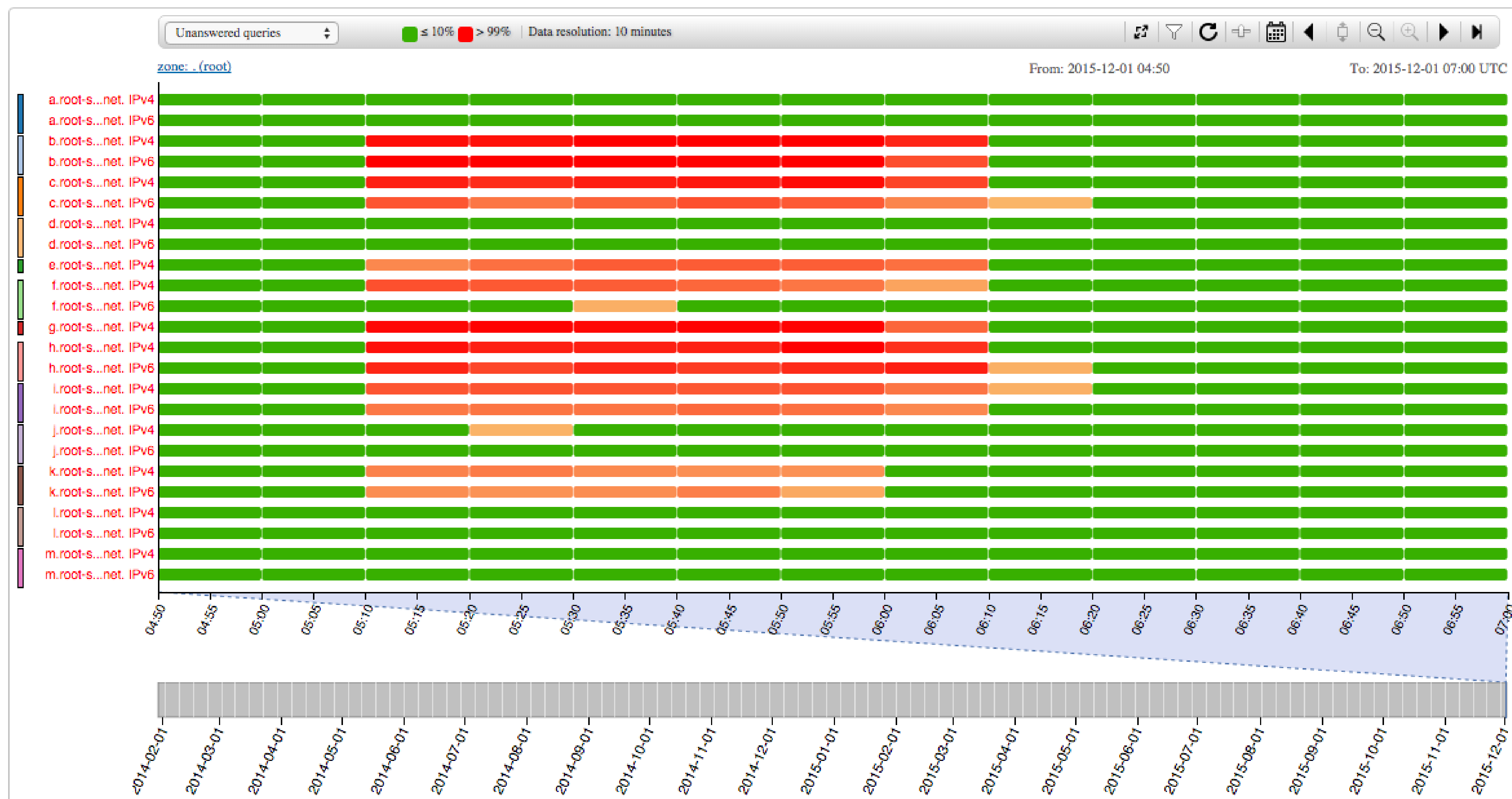
- .TR;
- .TR registry.

Атака на Root (30 November 2015)

- A-Root - 5.2 mlnq/s



Атака на Root (30 November 2015)(RIPE Atlas)



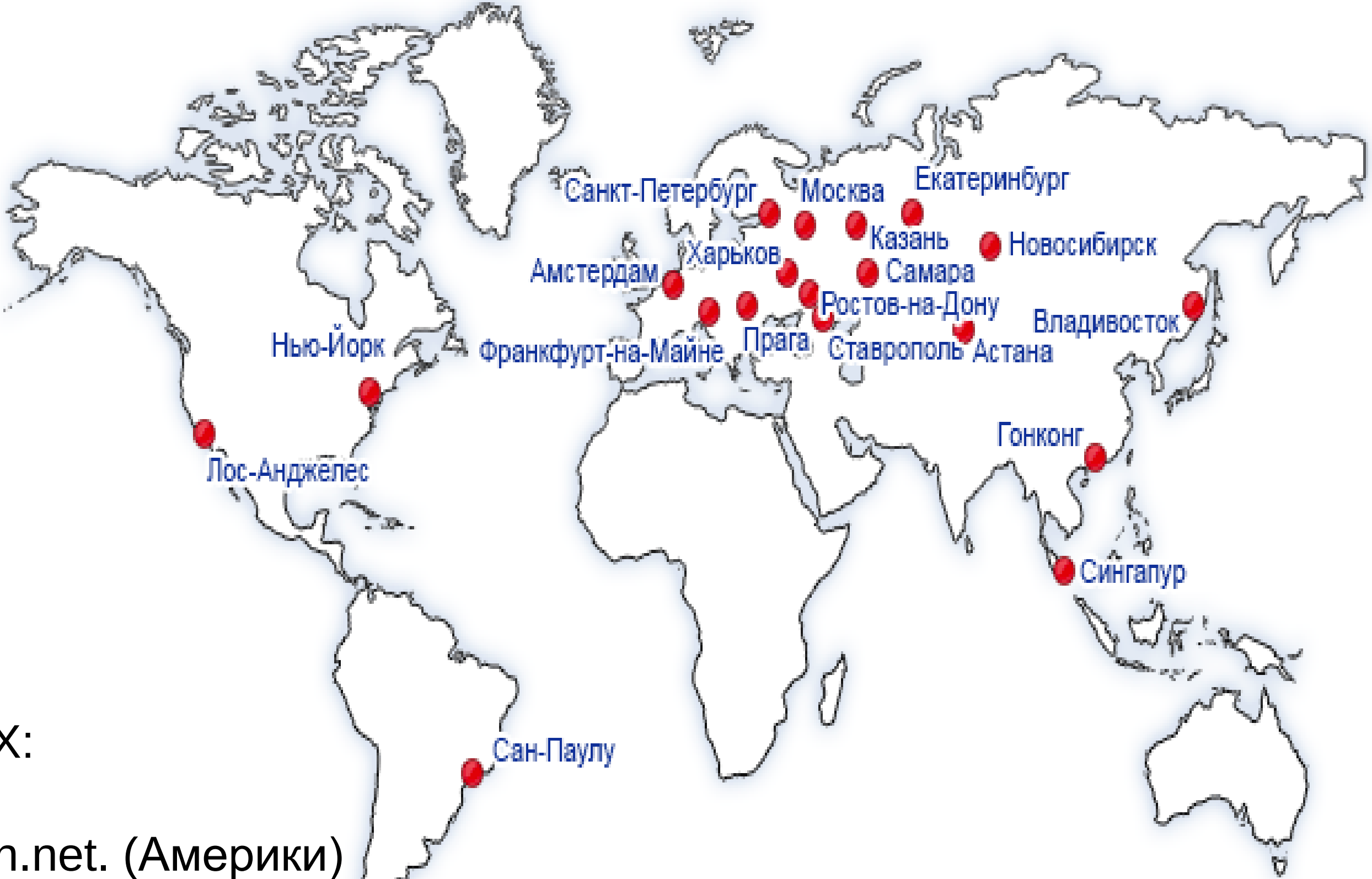
MSK-IX DNS-HOSTING

Russian Nodes:

- 1.Moscow
- 2.St Petersburg
- 3.Ekaterenburg
- 4.Novosibirsk
- 5.Kazan
- 6.Samara
- 7.Vladivostok
- 8.Rostov-Don
- 9.Stavropol

Nodes Outside Russia:

- 1.New York
- 2.Los Angeles
- 3.São Paulo
- 4.Hong Kong
- 5.Singapore
- 6.Praha
- 7.Amsterdam
- 8.Frankfurt
- 9.Astana
- 10.Kharkov



Серверы имеют IPv4/IPv6
адреса в AS-ах: 42385,
43832.

DNS-geo-anycast-cloud MSK-IX:

```
ru. 345600 IN NS f.dns.ripn.net. (Америки)
ru. 345600 IN NS b.dns.ripn.net. (Россия)
ru. 345600 IN NS e.dns.ripn.net. (Европа)
ru. 345600 IN NS d.dns.ripn.net. (Азия)
ru. 345600 IN NS a.dns.ripn.net. (Москва+Питер)
```


DNS Stats & Netosc

56/2219
Expire
Domains

across-in-monday.ru 1000
allandscape.ru 1000
already-mental.ru 1000
apartrocky.ru 1000

MacBook-Air-tanariff-2:~ paul\$ dig @d.dns.riprn.net kxkgdsep.ru ns

```
;; <<>> DiG 9.8.3-P1 <<>> @d.dns.riprn.net kxkgdsep.ru ns
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, stat
;; flags: qr rd; QUERY: 1, ANSWER:
;; WARNING: recursion requested but

;; QUESTION SECTION:
;kxkgdsep.ru.                IN

;; AUTHORITY SECTION:
kxkgdsep.ru.                345600  IN
kxkgdsep.ru.                345600  IN
kxkgdsep.ru.                345600  IN

;; Query time: 224 msec
;; SERVER: 194.190.124.17#53(194.19
;; WHEN: Tue Sep  6 00:23:29 2016
;; MSG SIZE  rcvd: 117
```

MacBook-Air-tanariff-2:~ paul\$ dig

```
;; <<>> DiG 9.8.3-P1 <<>> @ns2.freed
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, stat
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;kxkgdsep.ru.                IN      NS

;; Query time: 204 msec
;; SERVER: 108.59.2.228#53(108.59.2.228)
;; WHEN: Tue Sep  6 00:24:15 2016
;; MSG SIZE  rcvd: 29
```

Verify domains:

Netoscope.ru;
Whois;
Dig.

Before registration!

https://partnerion.ru/contact_admin.html
created: 2015.12.12
paid-till: 2016.12.12
free-date: 2017.01.12
source: TCI

Last updated on 2016.09.05 23:46:32 MSK

код;

Проверить

В домене neznana.ru
участниками проекта
зафиксированы типы
зловредов:

- спам

Сообщить о зловреде!

Resume

- DNS architecture for domain aftermarket has some features
- DNS amplification attacks and DGA attacks are still popular
- Aftermarket DNS service is in the Group of risk.
- Aftermarket DNS service should be supported by anycast infrastructure.
- Professionals are ready to help you (msk-ix.ru) ☺!
- Test any expired domain or domain for sale on the Netoscope.ru

Вопросы?

