Проруха на СОРМ
лесные были и небылицы

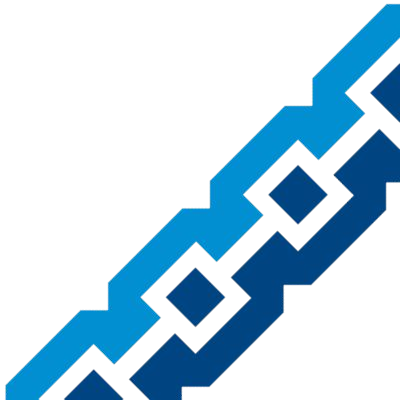
Леонид Евдокимов
Chaos Constructions
Санкт-Петербург, 25 августа 2019
darkk.net.ru/2019/cc

$ whoami

ex-Yandex: SWE, SRE

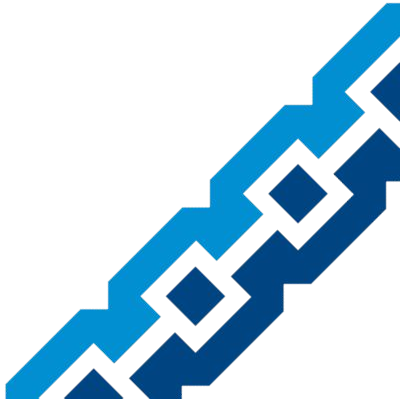
ex-OONI, The Tor Project: Data Analyst

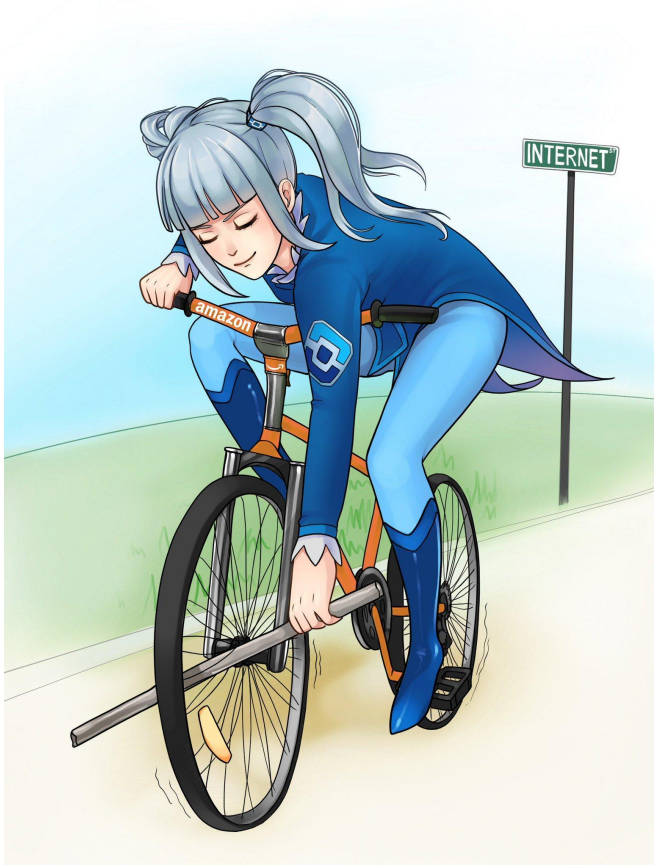
Клуб “Эшер-II”: почётный клоун



y.com/d/?resource=pubJS14��,PÏanalysis2.chartboosts.com/appfloo
r/selfpush/gameframe/www/wwwroot/gateway.php?act=203&data=%5B%7
B%22p%22:%22com.tap.fruitherolegend%22,%22g%22:%5B%22c2088f32635
aafa933009740961da2cc914f5e51%22,877,879,6,0,107,1814819,0,0,5,
5,0,6,0,0,0,0,0,0,0,5,107,0,0%5D,%22h%22:%5B%22qnubT6f0MVc7hutXu
1SQkA==%22,%22j7vFAyLvR7CNVi4mWktgrQ==%22,%22Sn+0RMB6loXpPlzofBi
4ew==%22,%22YQ9RzAMxDMZ7bo9yHaAzRg==%22,%22C%5C/4NoKvpRQSOEM+AiF
mAOA==%22%5D,%22f%22:%5B877,107,5,1,1,0,1814819,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0%5D%7D%5D&test=1�2���)GPY�50.7.168.
146/content/stream/serials/chernobelaya_lyubov/7f_cherno.belaya.
lubov.s01.e22.2018.l1.webrip720p.a1.02.04.18_8344/hls/segment15
3.tsd3�-��d�?��2���N5�Z���Z
arslan8724:a4:3c:a8:31:65
ppp456�?���d�,�S�2����

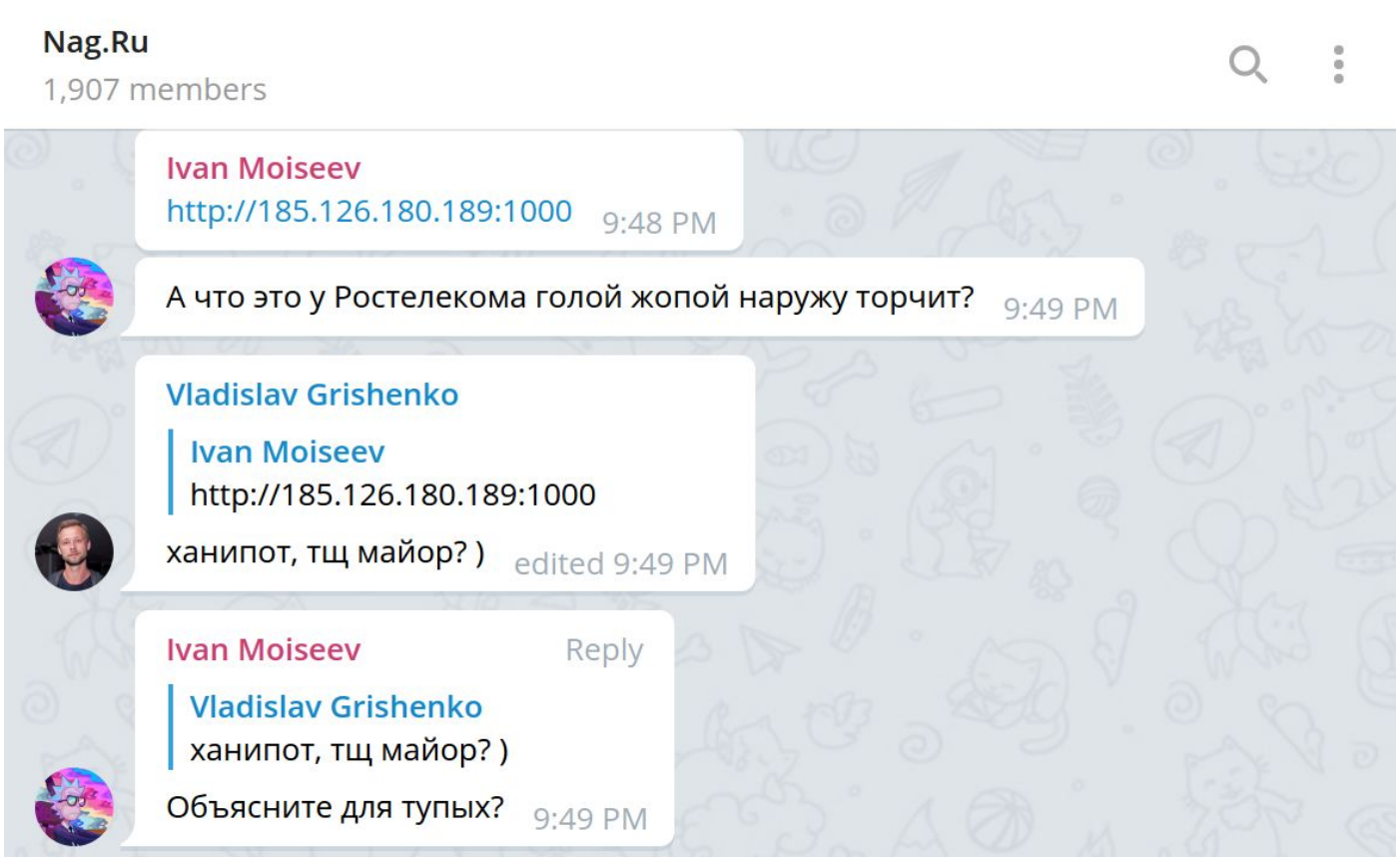
Опять Telegram





Роскомнадзор-тян пытается заблокировать 14 миллионов IP адресов сетей Amazon EC2, на мощностях которого работает каждый второй сервис в интернете.

– @aquam1ne



28 апреля, @nag_public

```
========== НАЧАЛО КОМБИНИРОВАННОГО ТЕСТИРОВАНИЯ СНИФФЕРА ==========
+====================================
 SNIFFER STATS
+====================================
    ================================================
    Статистика кучи:
    Управляемая память: 0 всего, 0 свободно, 0 занято
    Блоков выделено:    573
    Байт выделено:      5370806272
    Блоков освобождено: 2825
    Байт освобождено:   13543407616
    Число арен:         80
    ================================================
    ================================================
    Используемые модули захвата:
    Имя модуля: mc0_data0
    191,925 Мбит/сек, 30911 пак/с, RX байт/пакетов: 344287241181741/429870149898, skipped:
0, dropped: 0
    Имя модуля: mc0_pb_data0
    0  бит/сек, 0 пак/с, RX байт/пакетов: 0/0, skipped: 0, dropped: 0
    ================================================
    ================================================
    Используемые интерфейсы получения данных от ПУ:
```

30 апреля,
ОЗИ

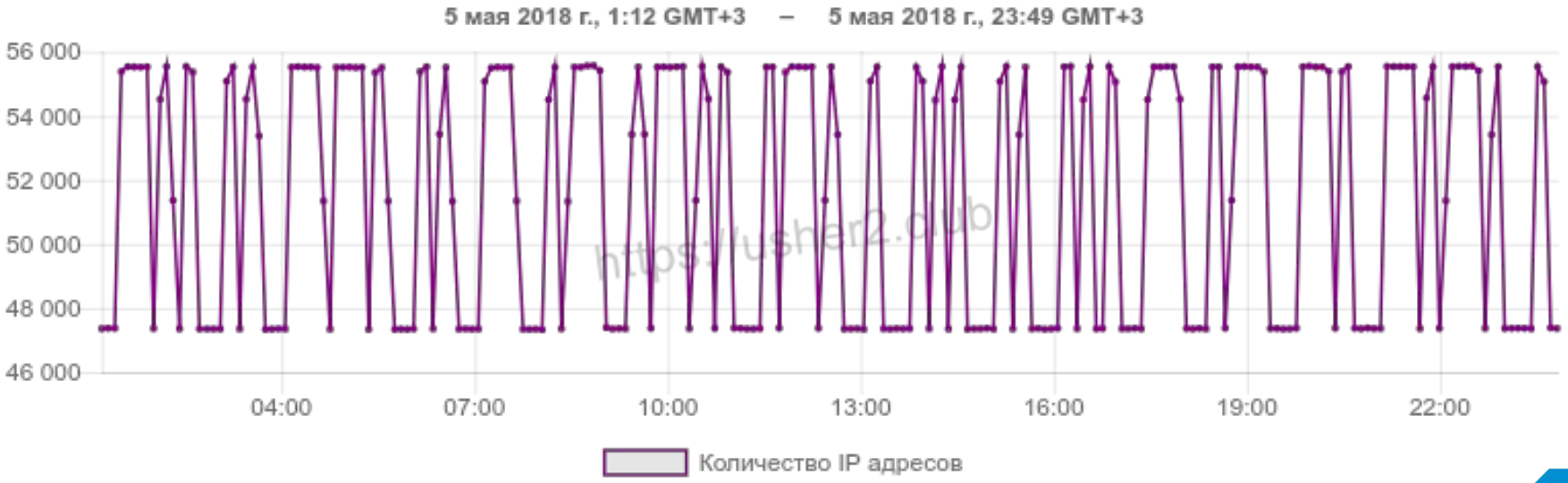
```
sip: трафик: 320  бит/сек ( 226669143 ), макс 5,416 К, ctx: 0 созд./сек (0)
skinny: трафик: 0  бит/сек ( 47782 ), макс 144  , ctx: 0 созд./сек (0)
skype: трафик: 0  бит/сек ( 17700 ), макс 8  , ctx: 0 созд./сек (0)
smtp: трафик: 149,496 Кбит/сек ( 37940640343 ), макс 17,115 М, ctx: 0 созд./сек (0)
ssh: трафик: 0  бит/сек ( 0 ), макс 0  , ctx: 0 созд./сек (0)
ssl: трафик: 0  бит/сек ( 0 ), макс 0  , ctx: 0 созд./сек (0)
ssl_taster: трафик: 0  бит/сек ( 0 ), макс 0  , ctx: 0 созд./сек (0)
tacacs: трафик: 0  бит/сек ( 0 ), макс 0  , ctx: 0 созд./сек (0)
telegram: трафик: 0  бит/сек ( 0 ), макс 0  , ctx: 0 созд./сек (0)
tor: трафик: 0  бит/сек ( 888147822 ), макс 331,952 К, ctx: 0 созд./сек (0)
viber: трафик: 0  бит/сек ( 0 ), макс 0  , ctx: 0 созд./сек (0)
whatsapp: трафик: 0  бит/сек ( 0 ), макс 0  , ctx: 0 созд./сек (0)
xmpp: трафик: 312  бит/сек ( 1387287949 ), макс 20,184 К, ctx: 0 созд./сек (13)
yahoo: трафик: 0  бит/сек ( 0 ), макс 0  , ctx: 0 созд./сек (0)
zello: трафик: 0  бит/сек ( 0 ), макс 0  , ctx: 0 созд./сек (0)
zello_tcp: трафик: 0  бит/сек ( 13789385 ), макс 13,096 К, ctx: 0 созд./сек (0)
================================================

========================= L7_import UDP =========
Циклов декодирования: 737/с
Последний декодер:

dns: трафик: 695,136 Кбит/сек ( 1293208861367 ), макс 263,378 М, ctx: 0 созд./сек (0)
```

30 апреля, ОЗИ

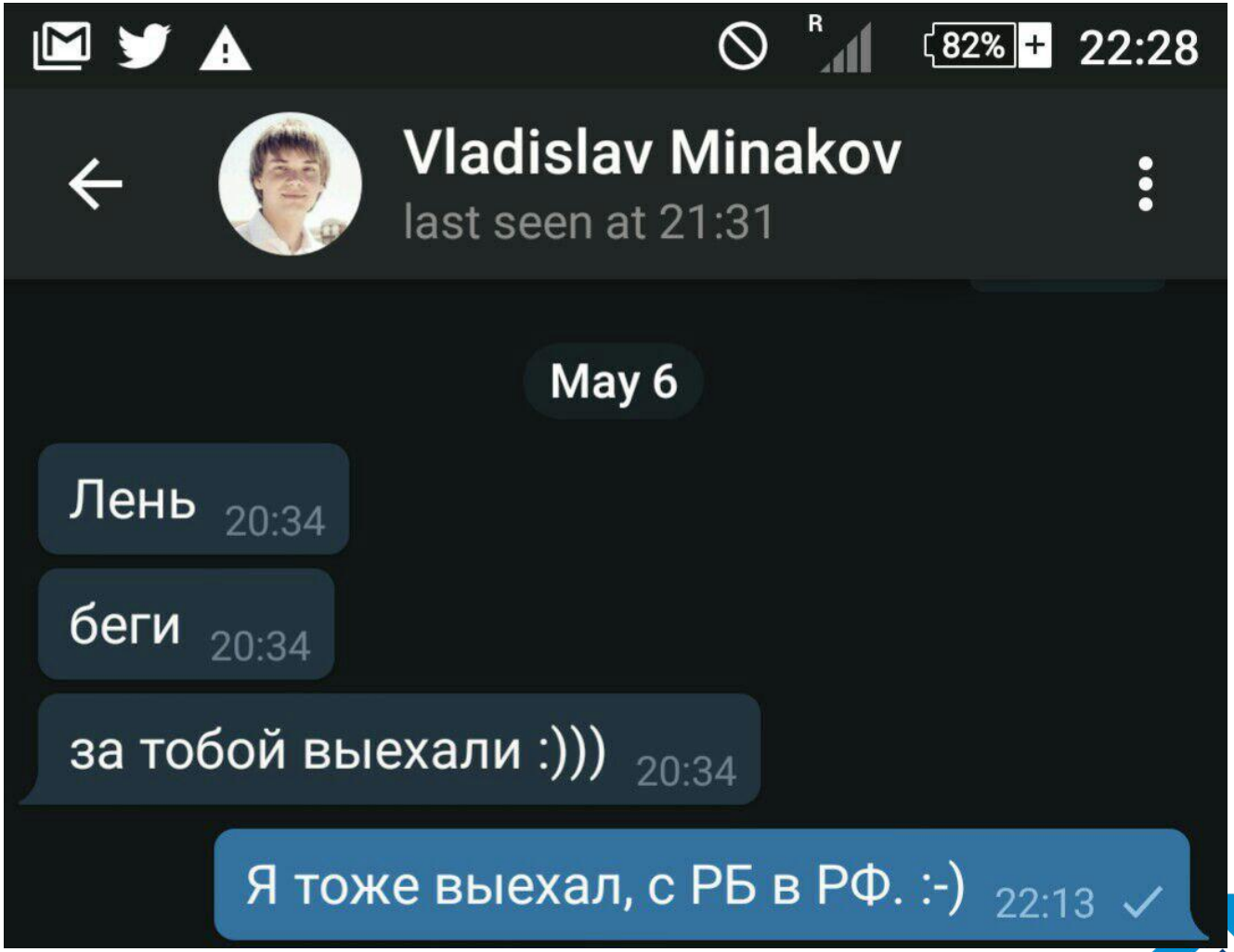

4 мая, Польша

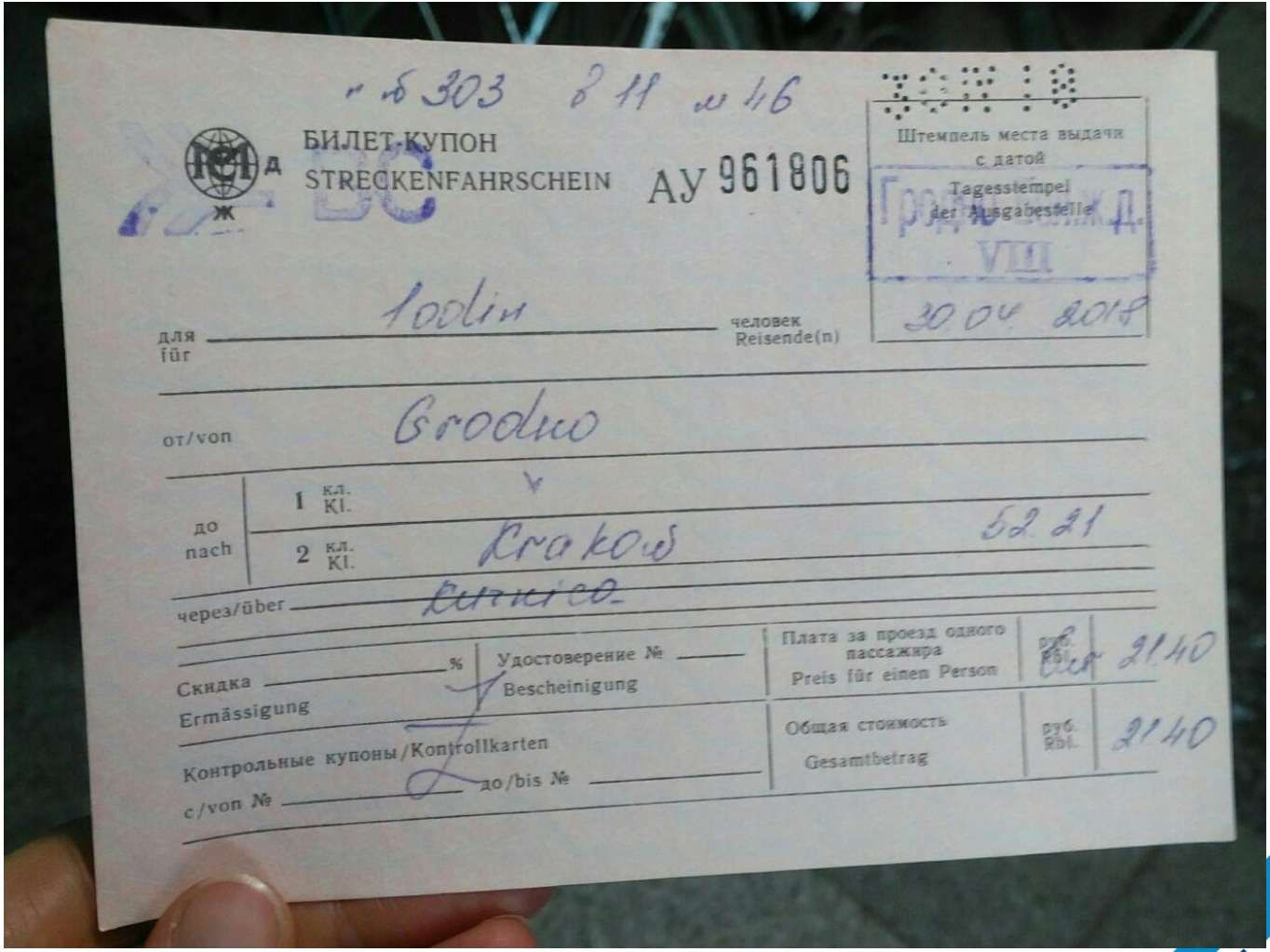
5 мая, Польша

Попов воскрес!



D I G I T A L R E S I S T A N C E


82%
22:28
Vladislav Minakov
last seen at 21:31
May 6
Лень 20:34
беги 20:34
за тобой выехали :))) 20:34
Я тоже выехал, с РБ в РФ. :-) 22:13



г. б 303 2 11 ш 46

ГЦ Д Ж

БИЛЕТ-КУПОН
STRECKENFAHRSCHEIN

АУ 961806

Штемпель места выдачи с датой
Tagesstempel der Ausgabestelle

Гродно ж.д.
VIII
30.04.2018

для / für 1 odin человек / Reisende(n)

от/von Grodno

до / nach
1 кл. / Kl.
2 кл. / Kl. Krakow 52.21

через/über Brest

Скидка / Ermässigung ____ %

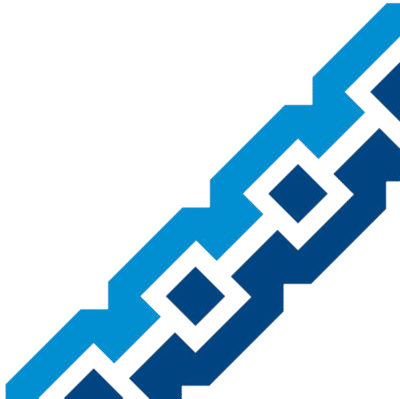
Удостоверение № / Bescheinigung

Плата за проезд одного пассажира / Preis für einen Person
руб. / Rbl. Сбор 21.40

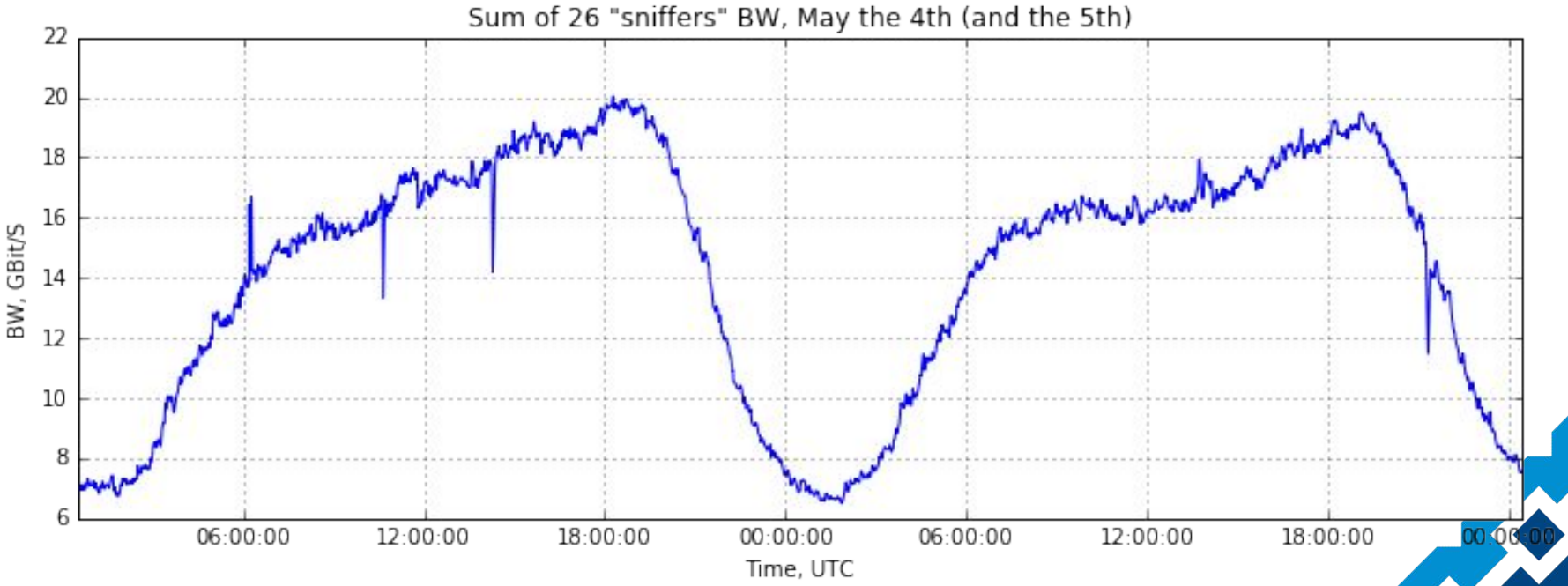
Контрольные купоны / Kontrollkarten
с/von № ____ до/bis № ____

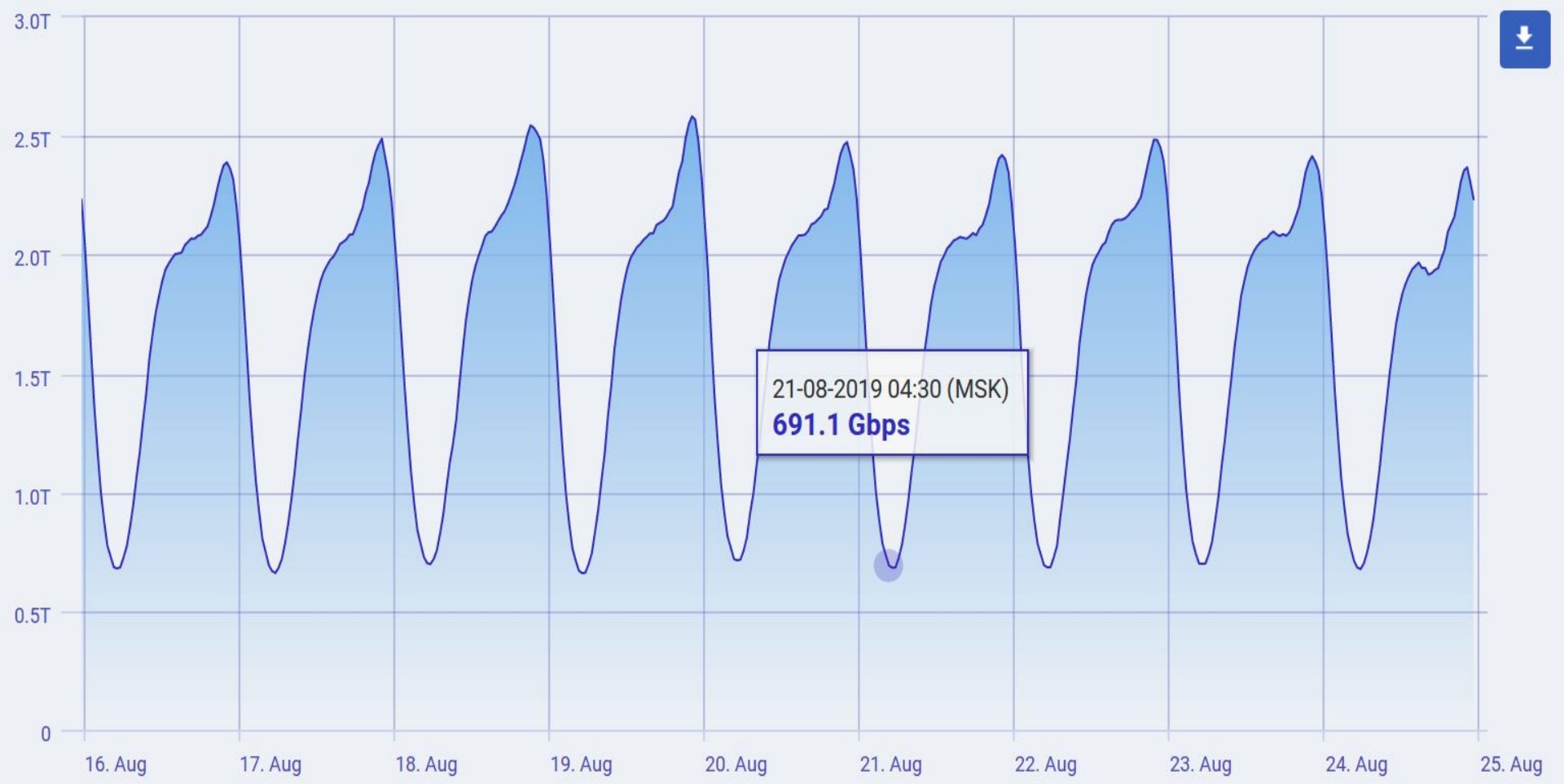
Общая стоимость / Gesamtbetrag
руб. / Rbl. 21.40

СОРМ: Цифры



SORM: this incident was reported





AVG: 1 683.6 Gbps
MAX: 2 583.1 Gbps

Updated at 24-08-2019 23:00:00 MSK

Это стандартная коробочка от МФИ-Софт. Когда мы покупали такую, нам никто не говорил о такой "особенности". Теоретически она вообще не должна в Интернет смотреть, но вот присматривать-то за ней вендор должен - вот и просит сделать интерфейс для удалённого доступа к ней. Ну и высунуть наружу кишки от неё - в порядке вещей. ;(Один оператор повесит acl, а другой понадеется что вендор с головой дружит. Логическая цепочка ведь "ФСБ - безопасность". 9:12 PM

В принципе, это ещё безобидная статистика... 9:13 PM

кто знает что там ещё припасено... 9:13 PM

ftp://*.#.%.^/pub/Sorm/repo/...

<summary>Interception network traffic utilite for DECODER</summary>
<checksum ...>983c...22ee</checksum>
<rpm:license>Proprietary</rpm:license>
<rpm:vendor>**MFI Soft**</rpm:vendor>

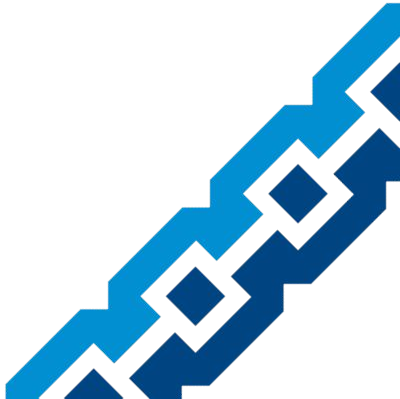
А ещё...

Samba 4.1.1 (RCE CVE-2015-0240 и др.)

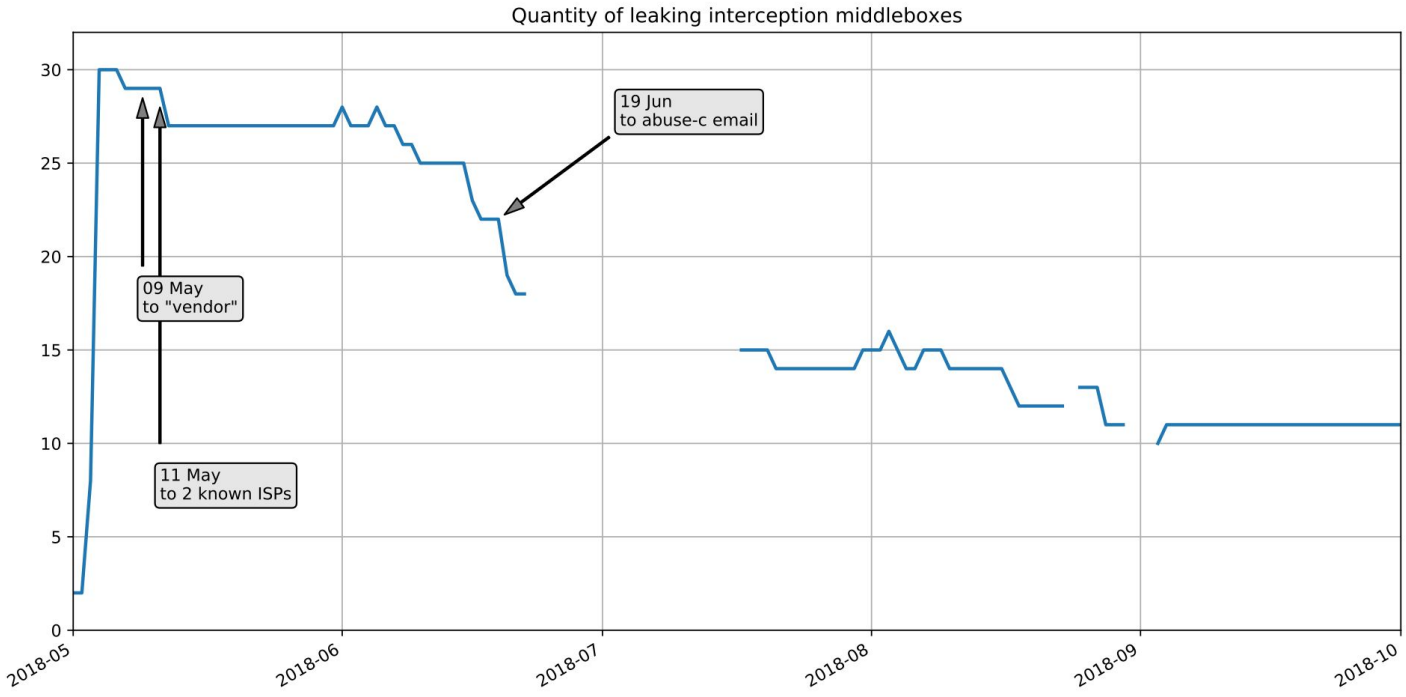
PostgreSQL

Elasticsearch 1.7.5

NFS, etc.



Таймлайн


Quantity of leaking interception middleboxes
30
25
20
15
10
5
0
19 Jun
to abuse-c email
09 May
to "vendor"
11 May
to 2 known ISPs
2018-05
2018-06
2018-07
2018-08
2018-09
2018-10

> в любом случае, спасибо. Клиент уже отреагировал, вроде.

Видимо, ACL был "правильным", т.к. 1 июня, кажется, оно обратно вернулось в строй.
Прошу прощения за беспокойство ¯_(ツ)_/¯ edited 5:47 PM ✓✓

Кхм... Спасибо, сейчас стукну кого-то по башке. 5:48 PM

Мне даже не понятно — надо ли. Может, так и задумано.
В любом случае — хорошего ENOG :) 5:48 PM ✓✓

не должно такого быть. 5:49 PM

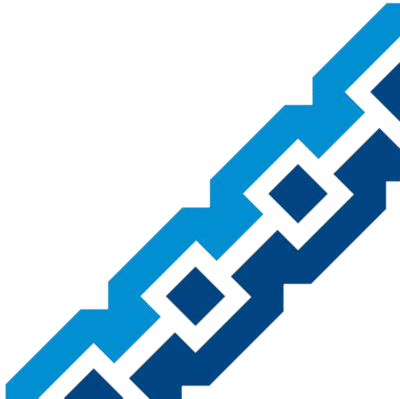
мне тут сказали что мфи'шники просили для тестов открыть. 5:51 PM

Ну я говорю — так, видимо, и задумано :) 5:51 PM ✓✓

потом уберётся 5:51 PM

Но это жесть, я согласен 5:51 PM

СОРМ: Буквы



Где съёмник?

IP ⇉ AS ⇉ Бизнес

IP ⇉ MaxMind ⇉ Город

IP ⇉ RIPE Atlas Ping RTT ⇉ OpenIPMap

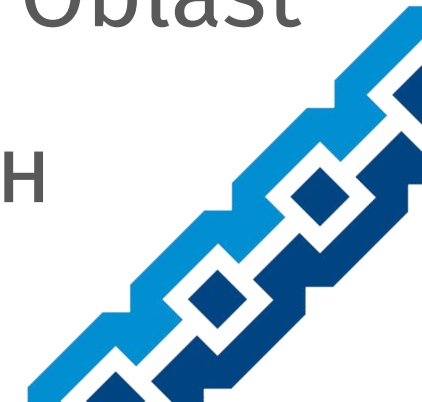
Где съёмник?

109.237.224.27 ⇉ ООО Квант, Зарайск

… ⇉ AS50449 ⇉ LLC Kvant Zaraysk

… ⇉ MaxMind ⇉ Zaraysk, Moscow Oblast

… ⇉ Ping 1ms ⇉ Зарайский район



Leonid Evdokimov @mathemonkey · Feb 23

Ужасный, конечно, контекст для вопроса получатеся, но, надеюсь, очевидно, что я не издеваюсь.
Пользуясь случаем, я хотел бы уточнить. Нормально ли что, например, вот этот инстанс без авторизации статистику отдаёт:
http://178.34.177.174:1000/ ?

1 1

Artem Shpynov @ashpynov · Feb 23

ну судя по статистике.. это какойто корпоративный съемник а фсб тут не причем. Там под наблюдением только 9 логинов.. маловато для кровавой руки режима. не находите?

1

Leonid Evdokimov @mathemonkey · Feb 23

Replying to @ashpynov @AndyPetrov0 @leonidvolkov

Я про то, что таких съемников не один (в т.ч. с чем-то подобным кликстриму на :8800, с открытым эластиком и т.п.).
Сервисы без аутентификации -- это как-то диковато для допустимой конфигурации LI, нет?
Или я всё неверно понял и зря беспокоюсь?

1 1

Artem Shpynov @ashpynov · Feb 23

это не LI это у какой то компании корпоративная ИБ жопой наружу торчит

1

Leonid Evdokimov @mathemonkey · Feb 23

Ну ок... когда гадал на PTR, кликстримах, объёмах трафика и ответах abuse@, я сделал предположение что местами LI такие разгильдяи конфигурируют! :-) Хорошо, если не так.
Да и в любом случае, по письмам на abuse@ позакрывали ~⅔ из тех, на которые я (довольно случайно) наткнулся.

1

Artem Shpynov @ashpynov · Feb 23

На LI изолированный контур и часто черное волокно. и если канал оператор жопой в инет выставит там ему такой пздец прилетит. не не от того что ваш трафик засветят. а от того что закон об орм нарушат..

1

y.com/d/?resource=pubJS14��,�PÏanalysis2.chartboosts.com/appfloo
r/selfpush/gameframe/www/wwwroot/gateway.php?act=203&data=%5B%7
B%22p%22:%22com.tap.fruitherolegend%22,%22g%22:%5B%22c2088f32635
aafa933009740961da2cc914f5e51%22,877,879,6,0,107,1814819,0,0,5,
5,0,6,0,0,0,0,0,0,0,5,107,0,0%5D,%22h%22:%5B%22qnubT6f0MVc7hutXu
1SQkA==%22,%22j7vFAyLvR7CNVi4mWktgrQ==%22,%22Sn+0RMB6loXpPlzofBi
4ew==%22,%22YQ9RzAMxDMZ7bo9yHaAzRg==%22,%22C%5C/4NoKvpRQSOEM+AiF
mAOA==%22%5D,%22f%22:%5B877,107,5,1,1,0,1814819,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0%5D%7D%5D&test=1�2���)GPY�50.7.168.
146/content/stream/serials/chernobelaya_lyubov/7f_cherno.belaya.
lubov.s01.e22.2018.l1.webrip720p.a1.02.04.18_8344/hls/segment15
3.tsd3�-��d�?��2���N5�Z���Z
arslan8724:a4:3c:a8:31:65
ppp456�?���d�,�S�2����

Чей трафик?

Погода и реклама ⇉ GPS, MAC, IMEI

MAC-адреса Wi-Fi ⇉ Координаты

ICQ, email, телефоны ⇉ Код города, сообщества, объявления

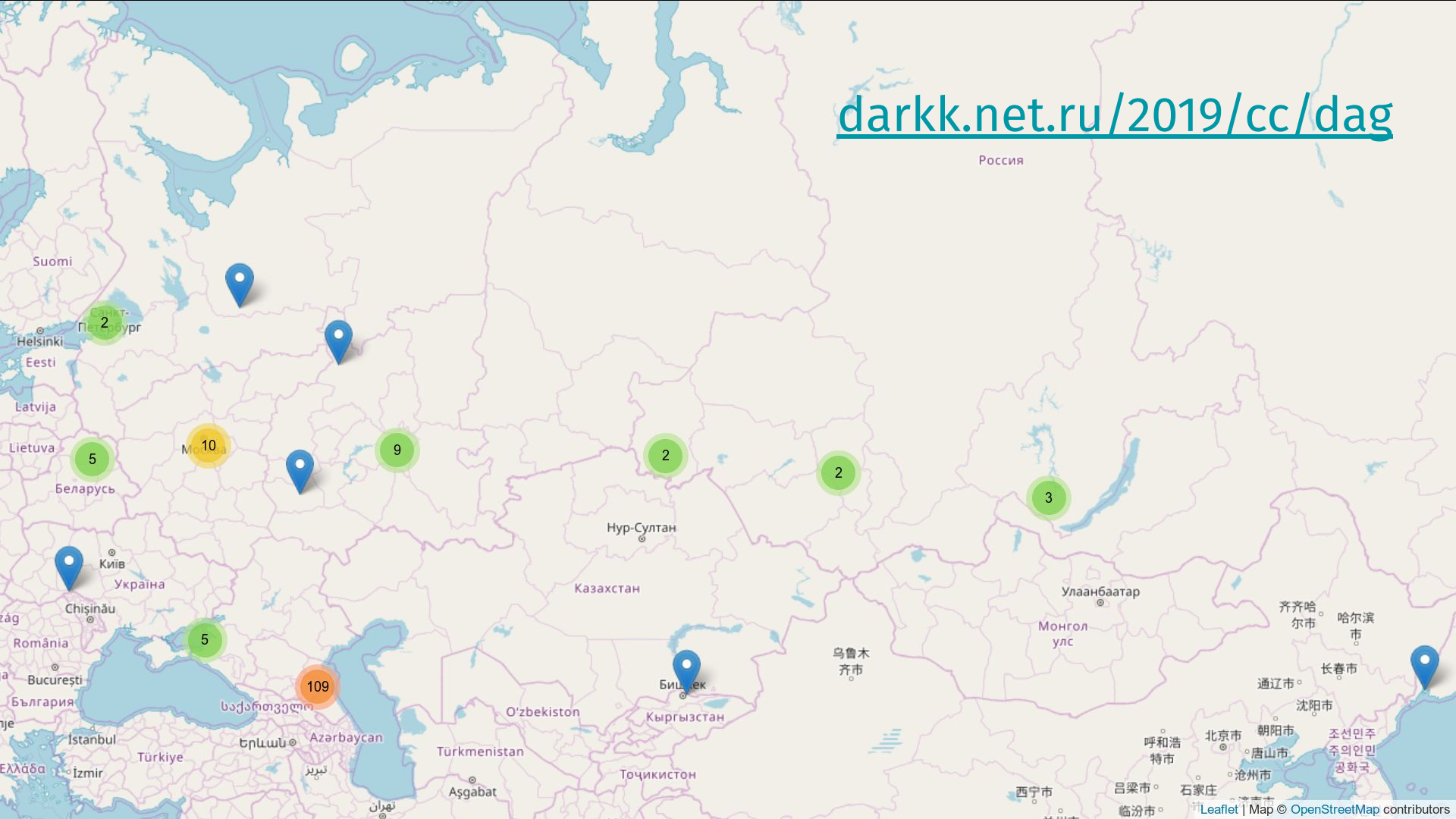
185.126.180.189

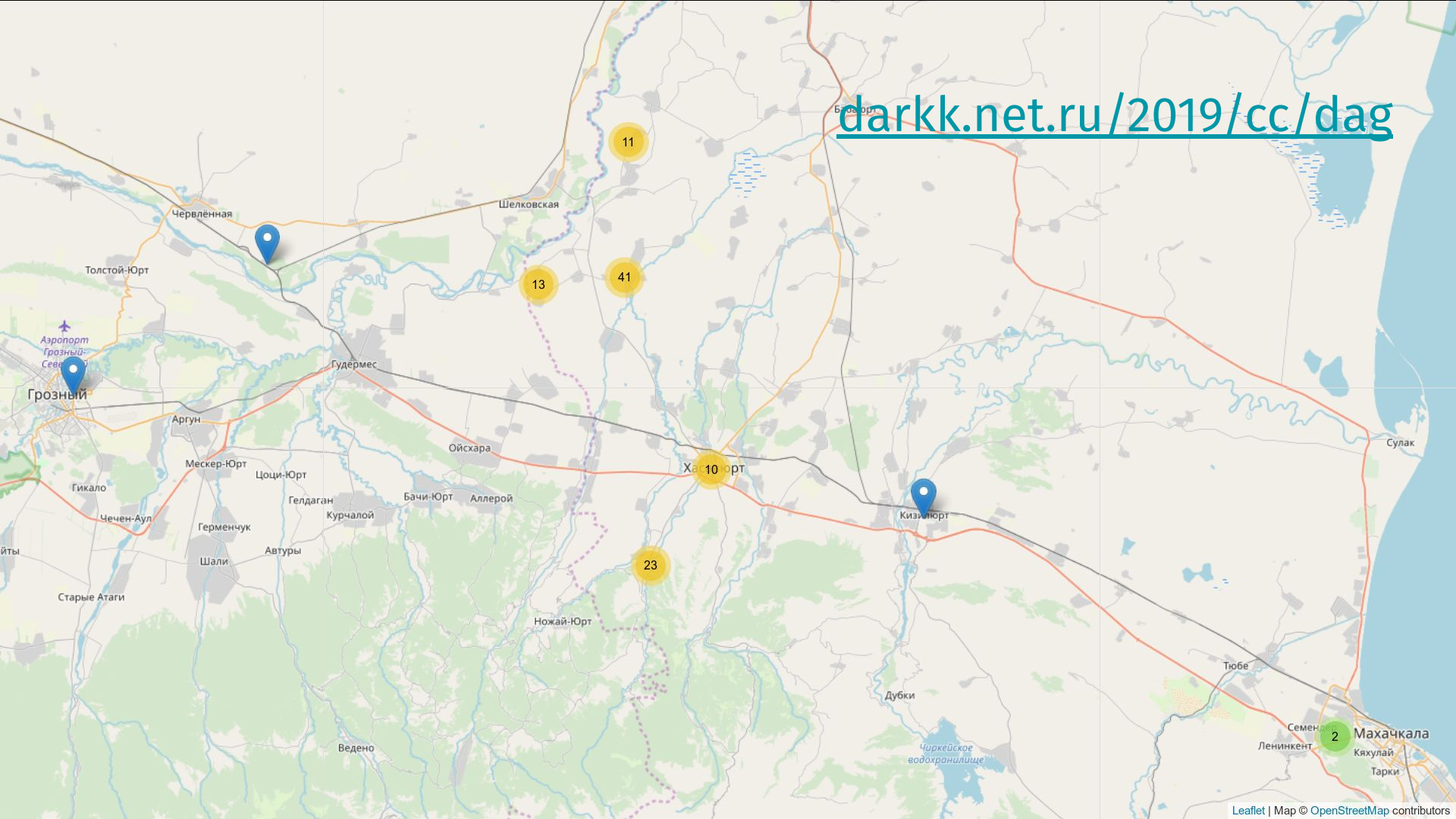
Shodan & MaxMind ⇉ Хасавюрт

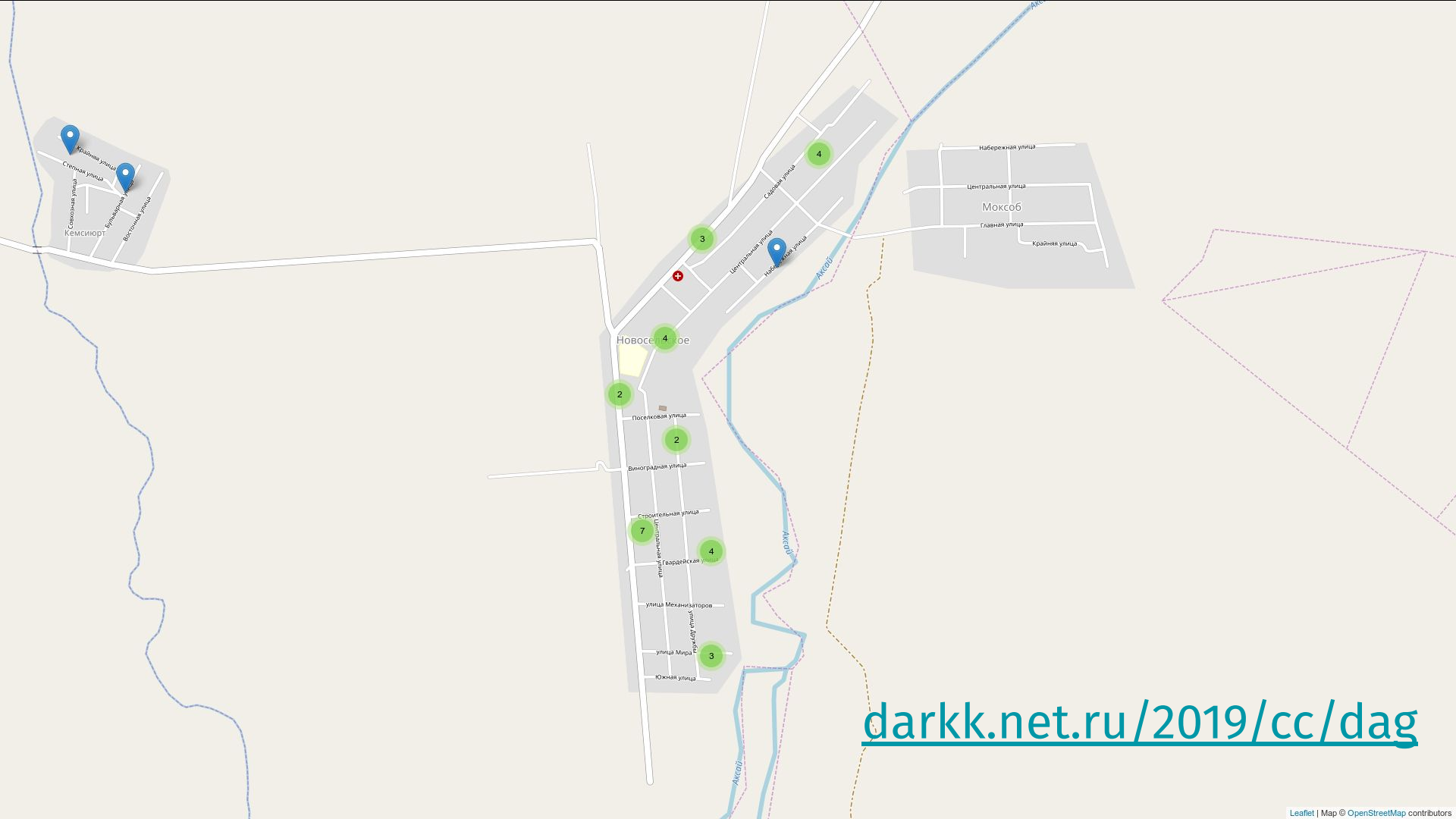
56 телефонов ⇉ Авито ⇉

7 из Хасавюрта, 2 из Махачкалы

314 MAC клиентов ⇉ 153 геоточки


darkk.net.ru/2019/cc/dag
Россия
Suomi
Helsinki
Eesti
Latvija
Lietuva
Беларусь
Київ
Україна
Chișinău
România
București
България
İstanbul
Türkiye
İzmir
Ελλάδα
საქართველო
Երևան
Azərbaycan
تبریز
تهران
Türkmenistan
Aşgabat
O'zbekiston
Қазахстан
Нур-Султан
Кыргызстан
Тоҷикистон
乌鲁木齐市
Улаанбаатар
Монгол улс
齐齐哈尔市
哈尔滨市
长春市
通辽市
沈阳市
朝阳市
北京市
唐山市
沧州市
呼和浩特市
吕梁市
石家庄
西宁市
临汾市
조선민주주의인민공화국
2
5
10
9
2
2
3
5
109
Leaflet | Map © OpenStreetMap contributors


darkk.net.ru/2019/cc/dag
11
13
41
10
23
2
Червлённая
Шелковская
Толстой-Юрт
Аэропорт Грозный-Север
Грозный
Гудермес
Аргун
Ойсхара
Мескер-Юрт
Цоци-Юрт
Гикало
Гелдаган
Бачи-Юрт
Аллерой
Чечен-Аул
Курчалой
Герменчук
Автуры
Шали
Старые Атаги
Ножай-Юрт
Ведено
Кизилюрт
Сулак
Тюбе
Дубки
Семендер
Ленинкент
Махачкала
Кяхулай
Тарки
Чиркейское водохранилище
Leaflet | Map © OpenStreetMap contributors


Крайняя улица
Степная улица
Совхозная улица
Бульварная улица
Восточная улица
Кемсиюрт
Набережная улица
Центральная улица
Моксоб
Главная улица
Крайняя улица
Сквозная улица
Центральная улица
Набережная улица
Аксай
Новосе кое
Поселковая улица
Виноградная улица
Строительная улица
Центральная улица
Гвардейская
улица Механизаторов
улица Дружбы
улица Мира
Южная улица
4
3
4
2
2
7
4
3
darkk.net.ru/2019/cc/dag
Leaflet | Map © OpenStreetMap contributors

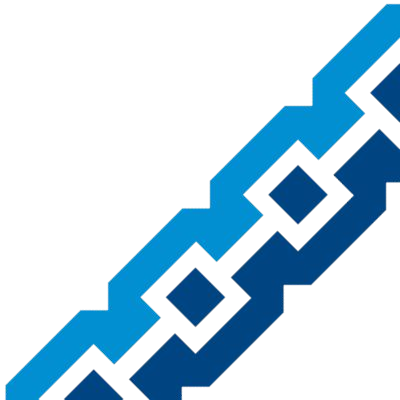
109.95.160.166, будто бы Москва

20 ICQ, “кучка” email, 261 IMEI

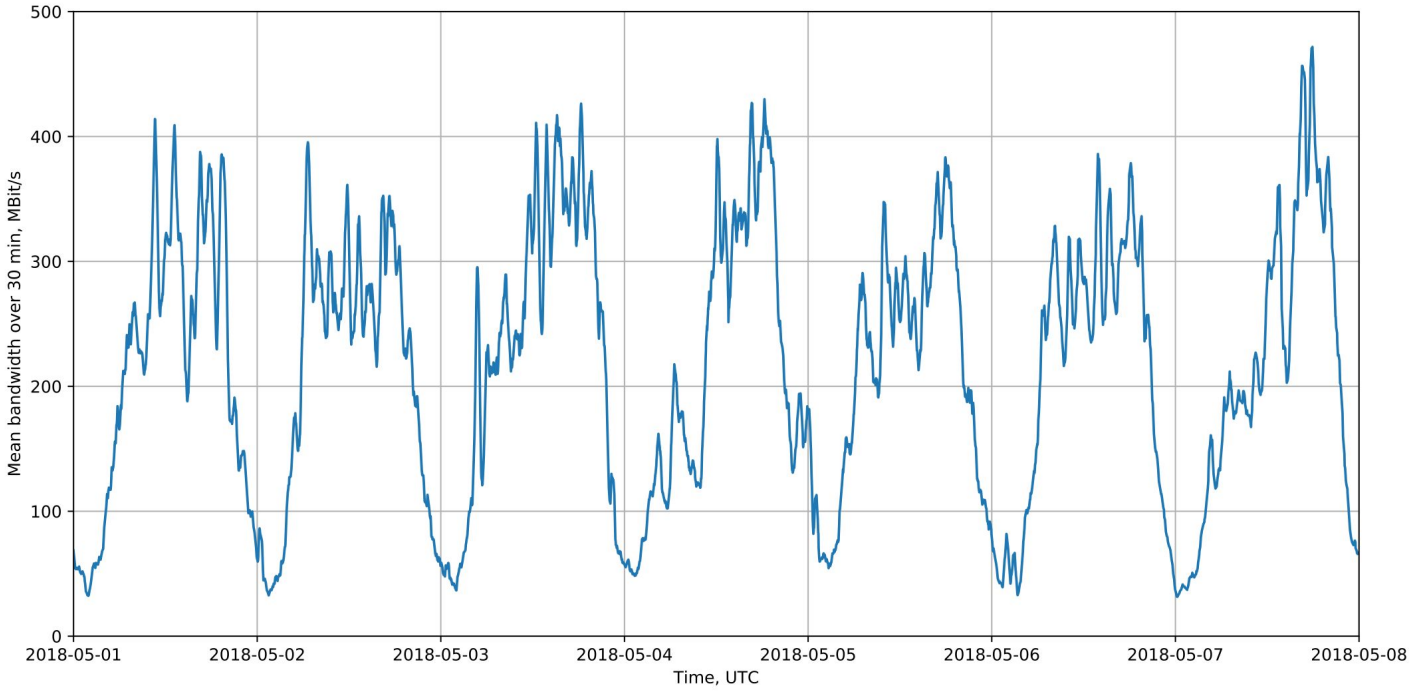
315 номеров телефонов

4’587 Wi-Fi из 20’137 поисков

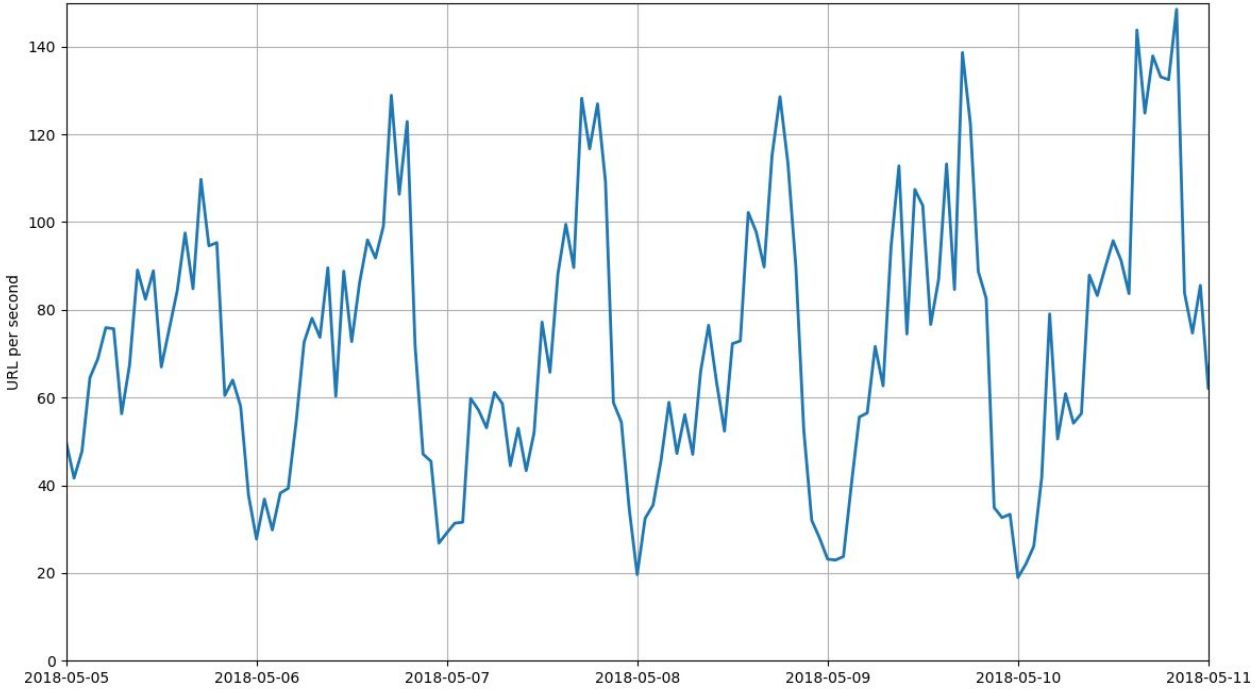
345’337 геоточек с дублями



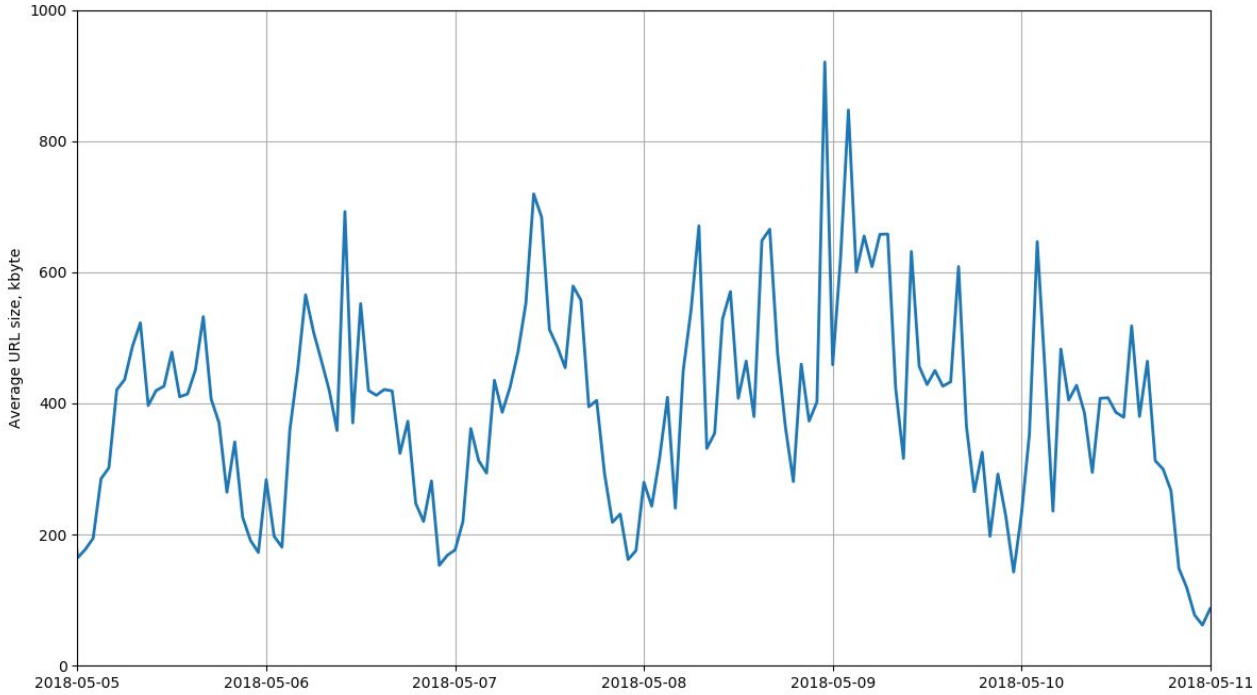
Трафик: 250 мегабит



Трафик: 80 URL / s



Трафик: web asset size



Clickstream. Избранное

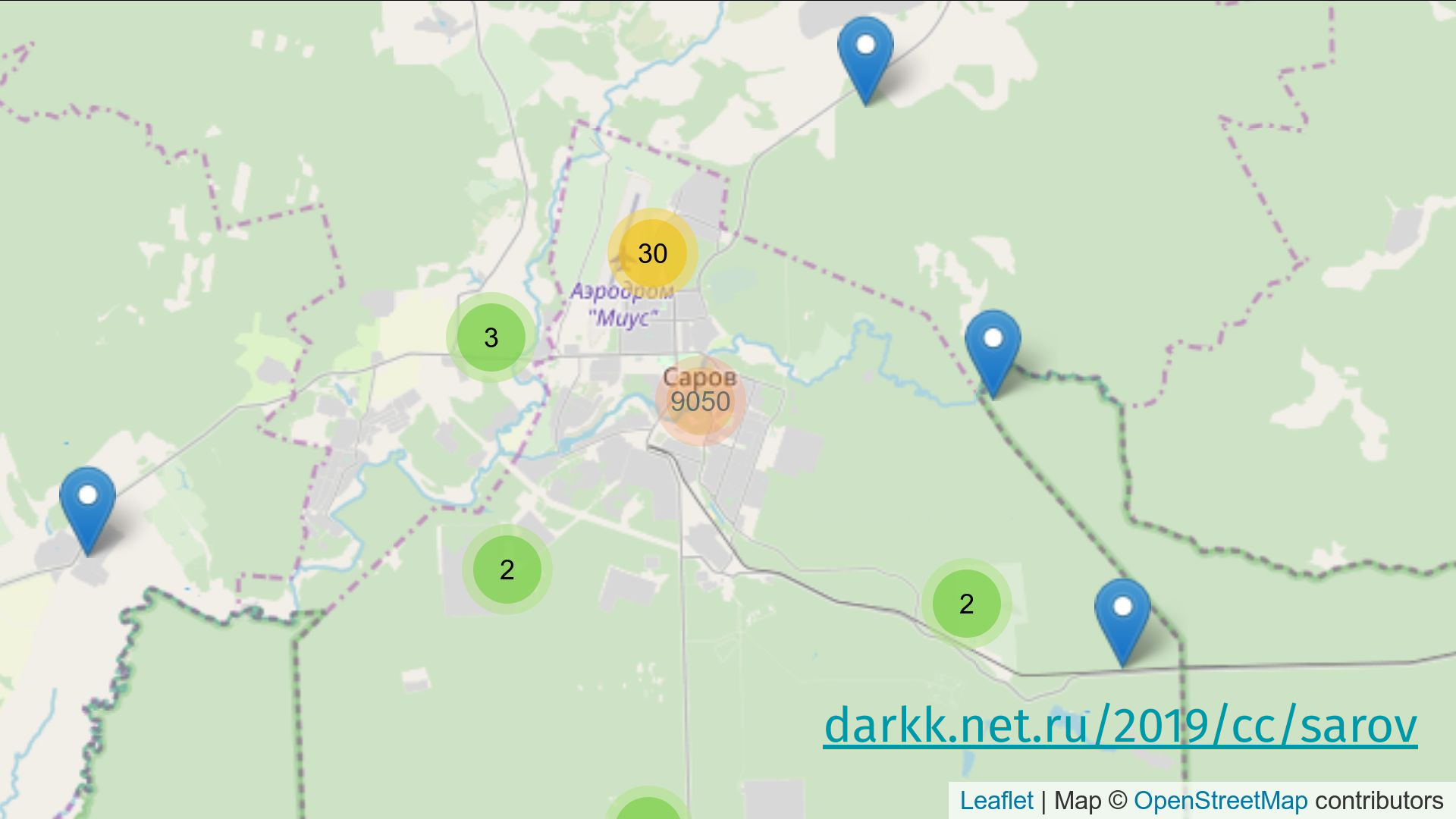
5.227.163.45 : **5060** ⇇ 195.140.215.9 : 18824

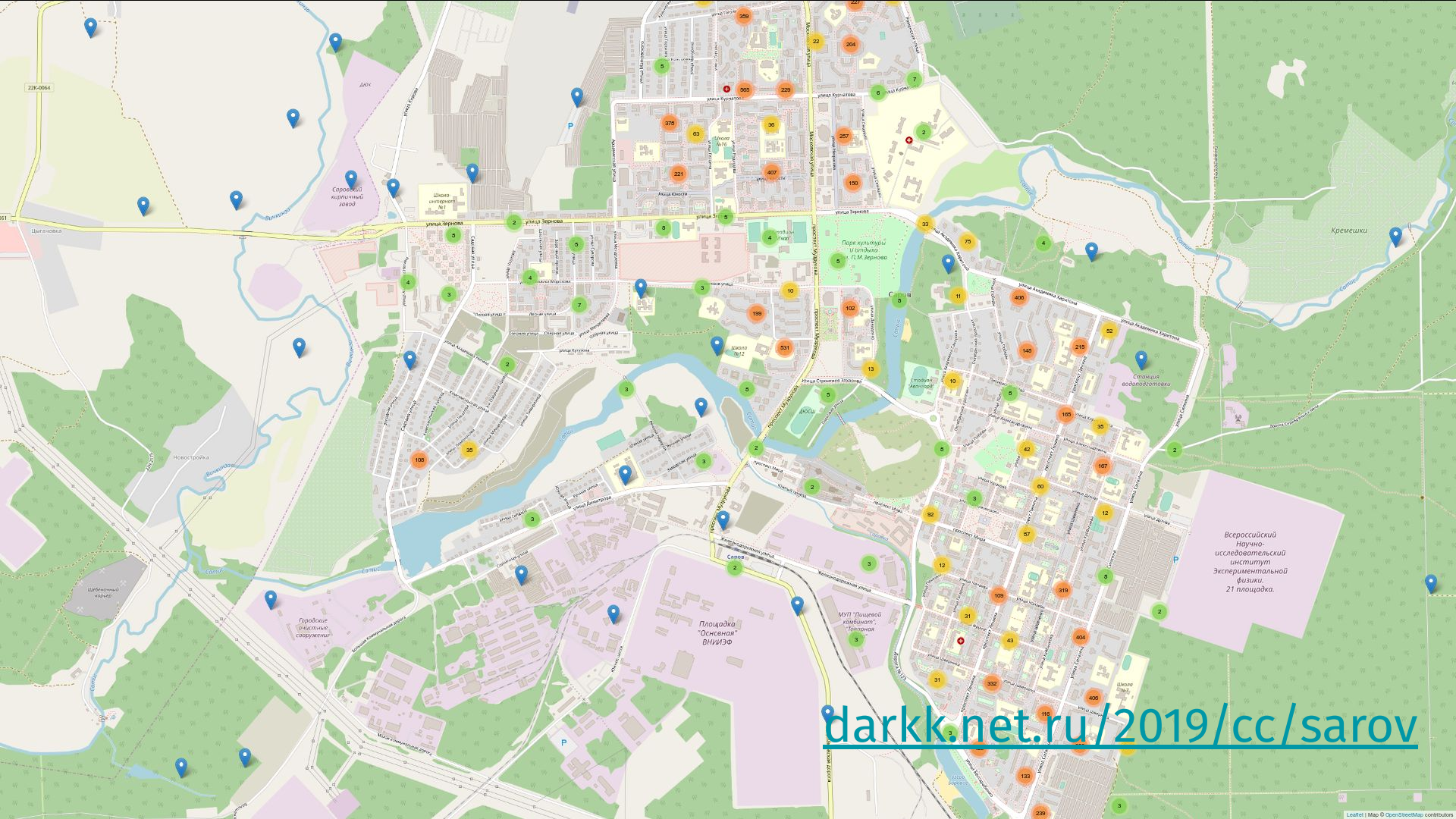
sip:**' OR '1'='1' --**@5.227.163.45:5060

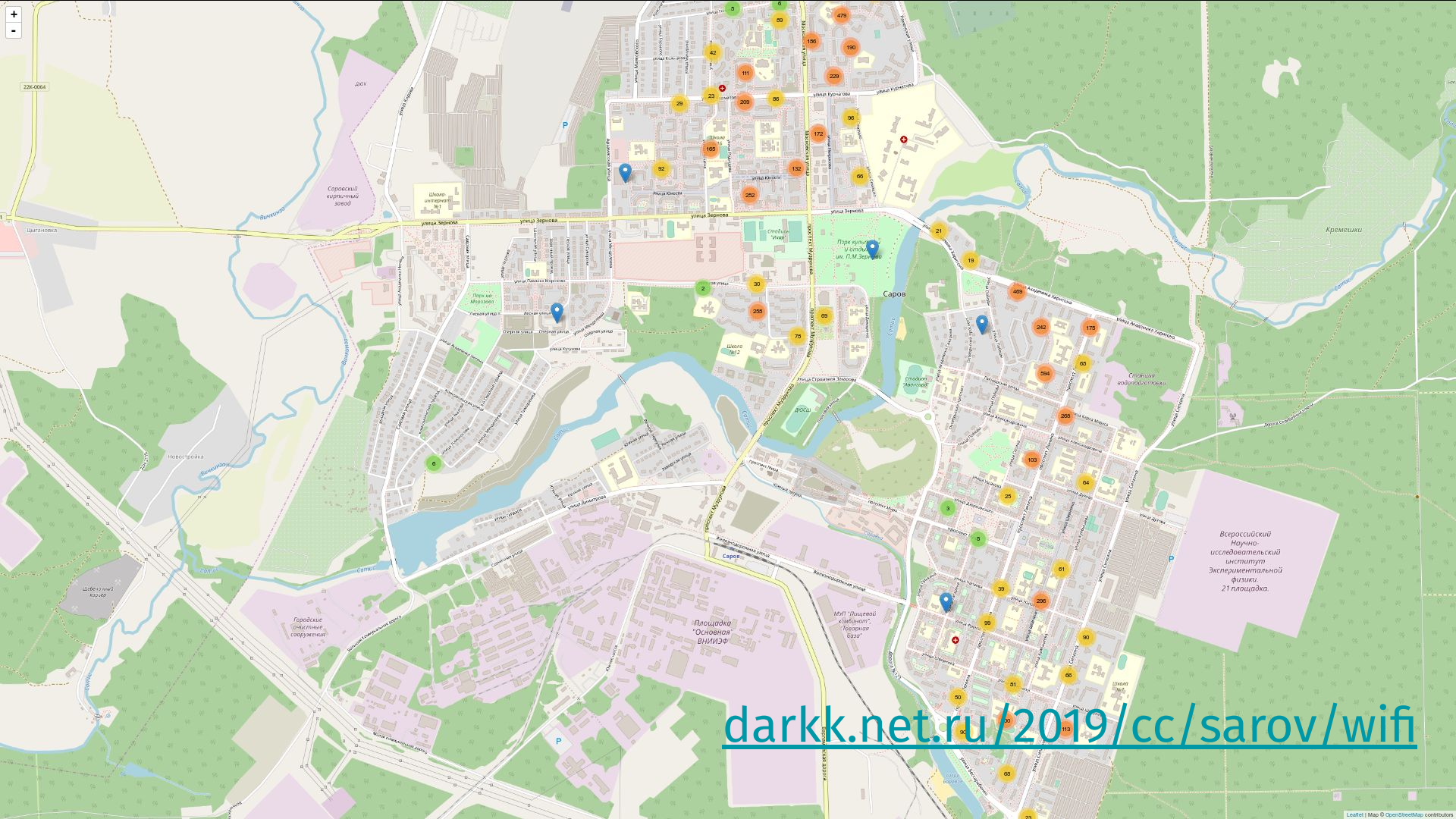
5.227.160.130 : 33206 ⇉ 178.237.19.21 : **443**

Филиал №2 библиотека Пушкина

ICQ 697278360


30
3
Аэродром
"Мичс"
Саров
9050
2
2
darkk.net.ru/2019/cc/sarov
Leaflet | Map © OpenStreetMap contributors


darkk.net.ru/2019/cc/sarov



darkk.net.ru/2019/cc/sarov/wifi

...кучка email

90% – SPAM + течёт только Subject

...@sbbank.ru – СаровБизнесБанк

...@tersy.ru – промавтоматика

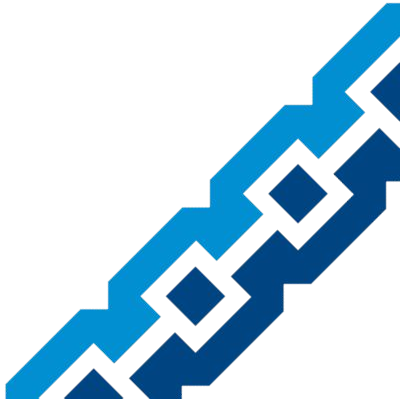
...@elmipro.ru – для РФЯЦ-ВНИИЭФ

...@sarovlabs.com – R&D

Clickstream. Избранное

5.227.160.201:50086 ⇉ 145.220.21.40:63173

ftp://**anonymous**@145.220.21.40
/pub/vim/pc/gvim80-586.exe



400 Bad Request

The plain HTTP request was sent to HTTPS port

---

nginx

Clickstream. Избранное

5.227.160.130 : 45624 ⇉ 178.237.20.54 : **443**

api.icq.net**/expressions/get?t=6548...**

5.227.162.222 : 49242 ⇉ 85.17.24.66 : **443**

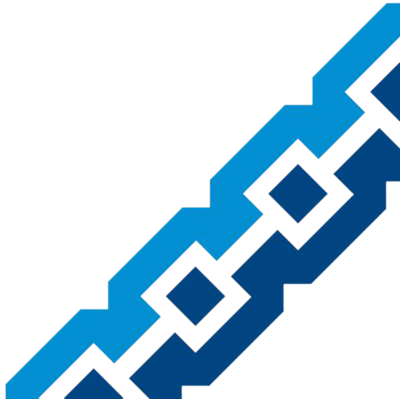
nl.hideproxy.me**/includes/process.p...**

https 443/tcp

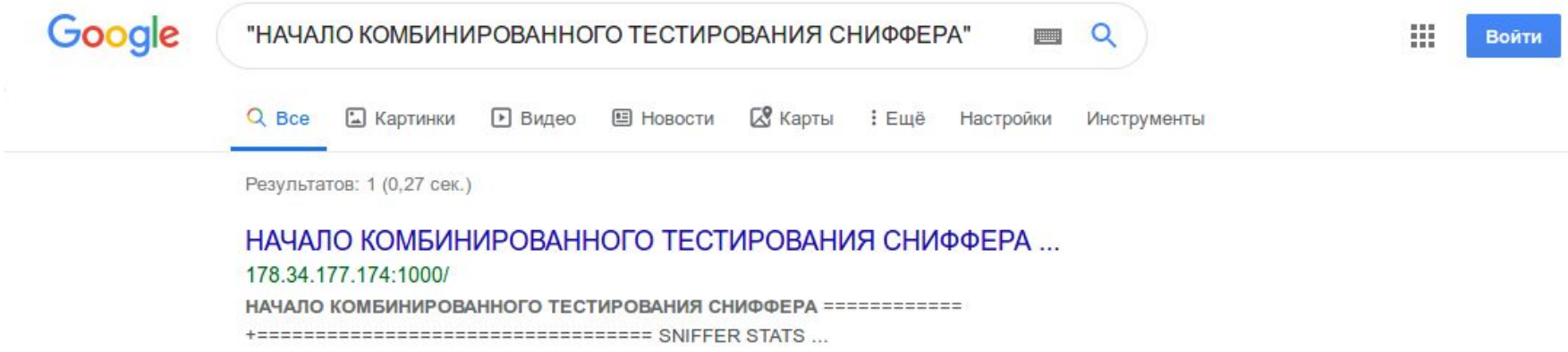
- mra1.mail.ru
  - ⚠️ img.imgsmail.ru, mra.mail.ru
  - ⚠️ api.icq.net

.....

- ⚠️ nl.hideproxy.me ?!



Прошёл год...


Google
"НАЧАЛО КОМБИНИРОВАННОГО ТЕСТИРОВАНИЯ СНИФФЕРА"
Войти
Все
Картинки
Видео
Новости
Карты
Ещё
Настройки
Инструменты
Результатов: 1 (0,27 сек.)
НАЧАЛО КОМБИНИРОВАННОГО ТЕСТИРОВАНИЯ СНИФФЕРА ...
178.34.177.174:1000/
НАЧАЛО КОМБИНИРОВАННОГО ТЕСТИРОВАНИЯ СНИФФЕРА ==========
+================================== SNIFFER STATS ...

Прошло полтора...

176.115.152.127

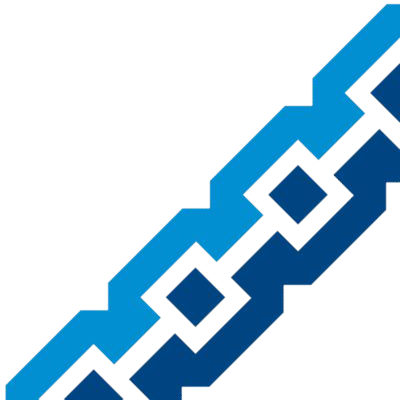
109.237.224.27

77.220.208.250

194.190.16.18

93.157.171.2

62.182.48.4

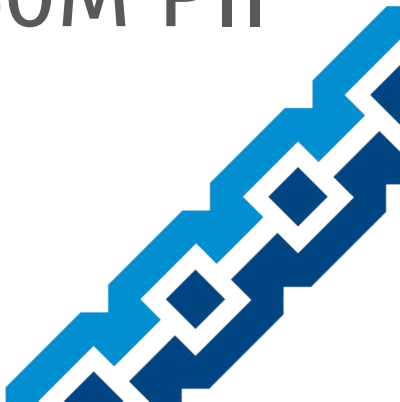


Криворукие внедряторы?

Memcached ~ 1.3 Tbit/s DDoS

MongoDB ~ утечка скорой помощи

Elasticsearch ~ утечка Exactis, 340M PII



Что делать?

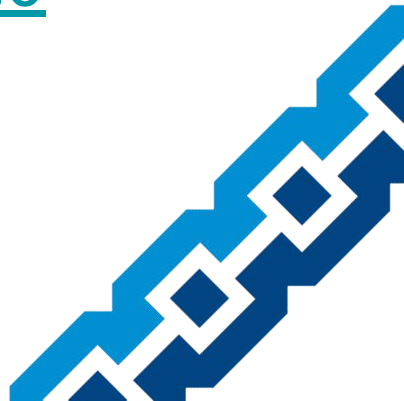
Q&A про DPI – 15:00, зал A (HackZone)

Донаты!

- Неугомонному Филу: usher2.club
- РКС: donate.roskomsvoboda.org
- ОЗИ: signal.fund

Спасибо!
Вопросы?

darkk.net.ru/2019/cc



Товарищ, знай! Пройдёт она

И демократия, и гласность.

И вот тогда госбезопасность

Припомнит наши имена!