Censorship and nearby countries

Research of nationwide blacklist censorship effect
on
customers Internet access in nearby countries

NETASSIST

NetAssist LLC
Ukraine, Kyiv
2016

Who we are?

- Small company from Kyiv, Ukraine (~40 people).
- Various peering connections: UA-IX, DTEL-IX, DE-CIX, PL-IX, MSK-IX. Good latency for European segment.
- We provide LIR services, ISP for home customers, Internet access for bussines. Reliable like no one other. IP Transit, L2/L3 transport VPN
- First free v6 tunnel broker in Ukraine ever!
- Develop some interesting networking software (tell you next time) http://github.com/netassist-ua

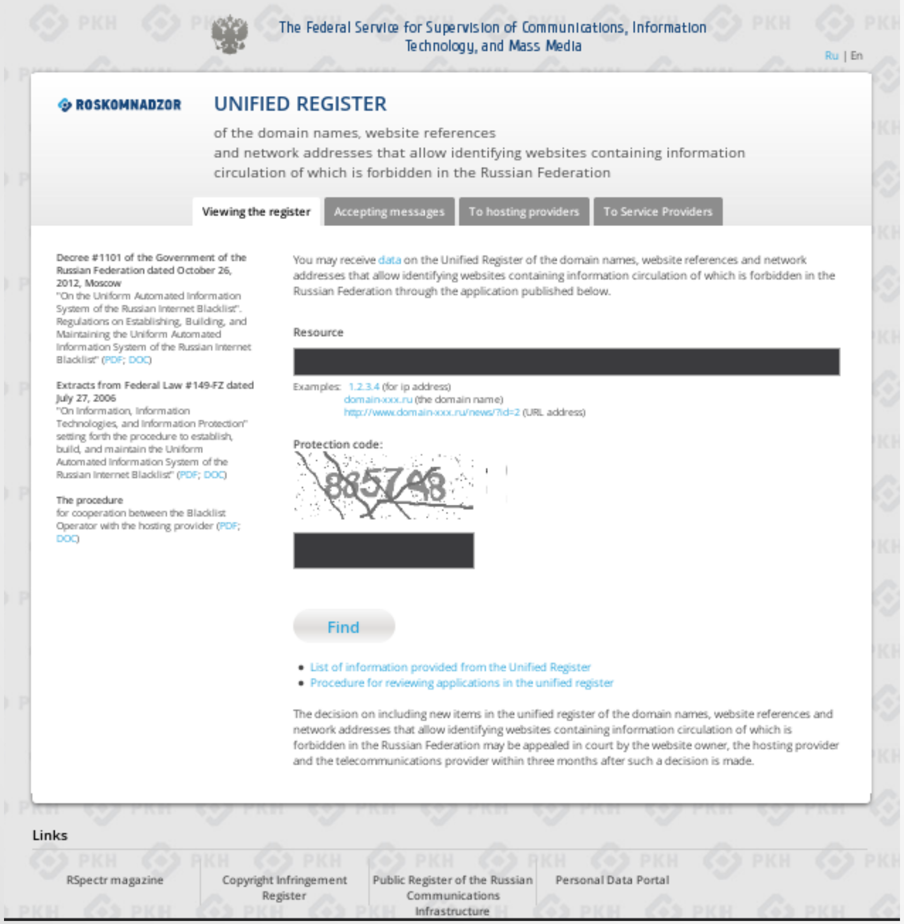
Russia

- Country with a long history
- Very big territory. Area: 17,098,242 km^2 (1st)
- Interesting for investors
- Well known for tech professional people
- A lot of really good Internet companies located there: Yandex, Rambler, VK, Mail.ru, 1C, ABBY, Ozon.ru, MTS, MGTS
- A lof ISPs, large amount of transit links
- Sad, but true. Started Internet access blacklist since 2012.

Blacklist and access filtering

- Officially designed first to protected children from «bad» information
- It blocks:
  - Online casino, gambling sites
  - Some p0rn, other sexual content
  - Suicide HOWTOs, terrorist coordination & information resources
  - Illegal drug dealing sites
  - Copyright violation sites (torrent trackers)
  - Others...
- Implemented on operators side. Every legal ISP operator SHOULD download list of blocked sites from Roskomnadzor repo

Blacklist



The Federal Service for Supervision of Communications, Information Technology, and Mass Media

Ru | En

ROSKOMNADZOR

UNIFIED REGISTER

of the domain names, website references
and network addresses that allow identifying websites containing information
circulation of which is forbidden in the Russian Federation

Decree #1101 of the Government of the Russian Federation dated October 26, 2012, Moscow
"On the Uniform Automated Information System of the Russian Internet Blacklist". Regulations on Establishing, Building, and Maintaining the Uniform Automated Information System of the Russian Internet Blacklist" (PDF; DOC)

Extracts from Federal Law #149-FZ dated July 27, 2006
"On Information, Information Technologies, and Information Protection" setting forth the procedure to establish, build, and maintain the Uniform Automated Information System of the Russian Internet Blacklist" (PDF; DOC)

The procedure
for cooperation between the Blacklist Operator with the hosting provider (PDF; DOC)

You may receive data on the Unified Register of the domain names, website references and network addresses that allow identifying websites containing information circulation of which is forbidden in the Russian Federation through the application published below.

Resource

Examples: 1.2.3.4 (for ip address)
domain-xxx.ru (the domain name)
http://www.domain-xxx.ru/news/?id=2 (URL address)

Protection code:

885748

- List of information provided from the Unified Register
- Procedure for reviewing applications in the unified register

The decision on including new items in the unified register of the domain names, website references and network addresses that allow identifying websites containing information circulation of which is forbidden in the Russian Federation may be appealed in court by the website owner, the hosting provider and the telecommunications provider within three months after such a decision is made.

Links

RSpectr magazine | Copyright Infringement Register | Public Register of the Russian Communications Infrastructure | Personal Data Portal

- Providers block resources in different ways: DNS, IP, HTTP URL
- List of blocked web-sites and IP available on http://reestr.rublacklist.net
- In most cases subject of filtering is just one page by URL
- But in some cases whole IP of server get blocked (!)

Filtering implementation

- DNS
  - Operator returns fake DNS response
  - Web-server show info page
- IP blockage
  - Operator blocks IP address or whole subnet
  - Maybe used to block some ports

- HTTP traffic URL block
  - Operator analyze URL of HTTP request
  - Returns blockage information webpage

Blockage and damage

- Blockage may lead to collateral damage
- Filtering by IP may lead to inability accessing to other sites hosted on same server
- DNS is easy but not respects URL
- URL filtering is not easy to implement in case of SSL
  - MITM is not a way to implement filtering
- Analyzing some traffic in the deep is expensive as well
- Blocking too much is not good idea

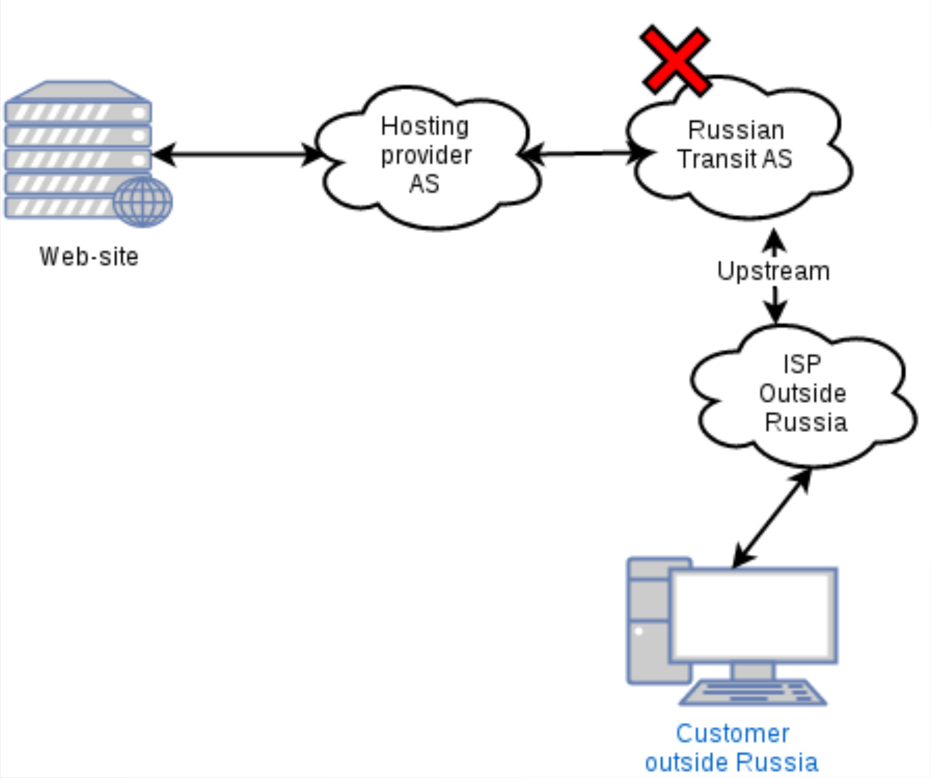
Costs

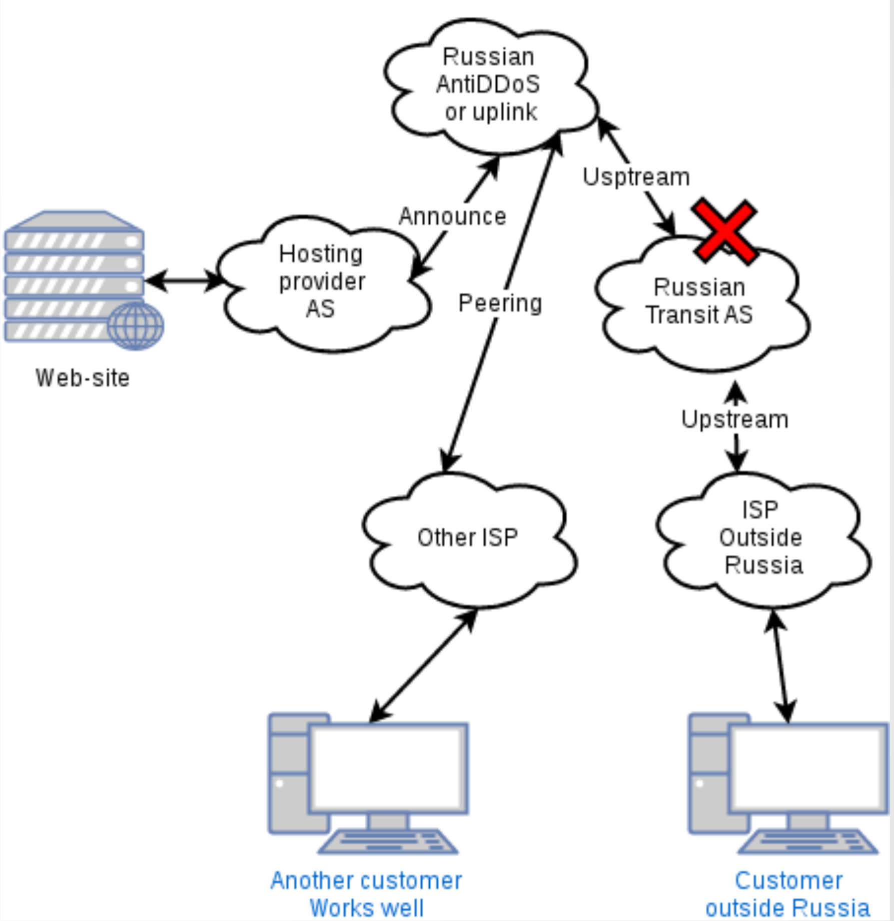
- Implementing access filtering is expensive for operator in any way
- DPI is very expensive!
- Operator have to manage large enough block list
- Many networks don’t have way to implement filtering on PE rxouters (since their network architecture or equipment performance)
- Filtering implementation is slow and steady process
- To minimize costs operators overfilter traffic. Which leads to blocking transit in some cases

Why do we care?

- A lot of transit routes run through Russian ISP's
- **Some countries** are able to use only Russian uplinks
- Sometimes operators make mistakes exporting censorship to outside world
- Creates difficulties accessing many useful but blocked Internet resources (news papers, etc)
- Exporting your own censorship is not good
- Some times it makes accidents: routing leaks and trasit traffic blockage
- Few blockage accidents were known before that lead us to start our research

Possible scenarios

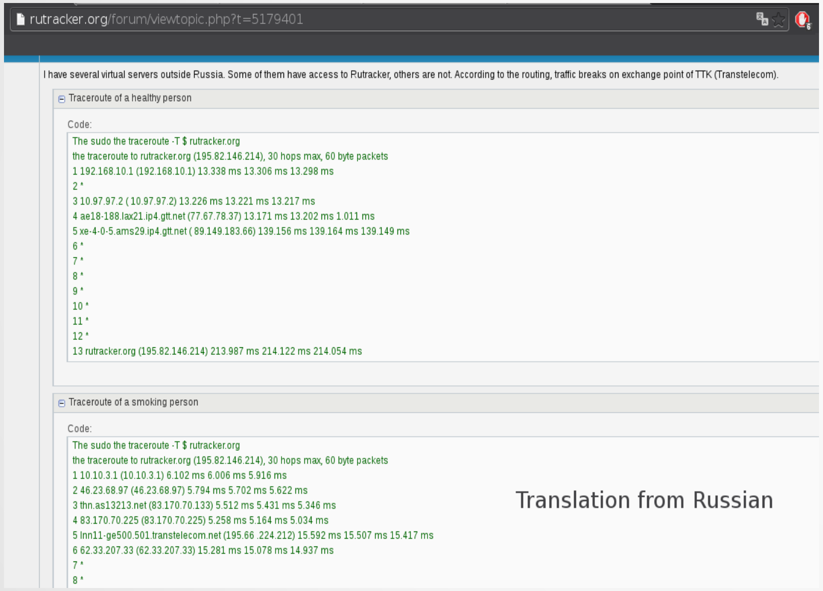




Rutracker.org (AS47105) Accident

- Torrent tracker. Yarr!!!
- Site is currently blacklisted by judgment in Russia due to copyright violations. Permanent block. Block started since January 22.
- Massive DDoS on site began in the Mid-February. Rutracker.org operators decided to filter out attack (Feb 25) by announcing routes through the DDoS filtering AS57724 (aka DDOS-Guard LTD) and AS262254 (Content delivery)
- AS57724 announced routes to their upstreams: AS9002 (ReTN) and AS20485 (Transtelecom)
- Transtelecom (TTK) filtered out transit traffic applying blacklist
- As a result rutracker.org was unavailable from some European countries

Rutracker.org accident



rutracker.org/forum/viewtopic.php?t=5179401

I have several virtual servers outside Russia. Some of them have access to Rutracker, others are not. According to the routing, traffic breaks on exchange point of TTK (Transtelecom).

⊟ Traceroute of a healthy person

Code:

```
The sudo the traceroute -T $ rutracker.org
the traceroute to rutracker.org (195.82.146.214), 30 hops max, 60 byte packets
1 192.168.10.1 (192.168.10.1) 13.338 ms 13.306 ms 13.298 ms
2 *
3 10.97.97.2 ( 10.97.97.2) 13.226 ms 13.221 ms 13.217 ms
4 ae18-188.lax21.ip4.gtt.net (77.67.78.37) 13.171 ms 13.202 ms 1.011 ms
5 xe-4-0-5.ams29.ip4.gtt.net ( 89.149.183.66) 139.156 ms 139.164 ms 139.149 ms
6 *
7 *
8 *
9 *
10 *
11 *
12 *
13 rutracker.org (195.82.146.214) 213.987 ms 214.122 ms 214.054 ms
```

⊟ Traceroute of a smoking person

Code:

```
The sudo the traceroute -T $ rutracker.org
the traceroute to rutracker.org (195.82.146.214), 30 hops max, 60 byte packets
1 10.10.3.1 (10.10.3.1) 6.102 ms 6.006 ms 5.916 ms
2 46.23.68.97 (46.23.68.97) 5.794 ms 5.702 ms 5.622 ms
3 thn.as13213.net (83.170.70.133) 5.512 ms 5.431 ms 5.346 ms
4 83.170.70.225 (83.170.70.225) 5.258 ms 5.164 ms 5.034 ms
5 lnn11-ge500.501.transtelecom.net (195.66 .224.212) 15.592 ms 15.507 ms 15.417 ms
6 62.33.207.33 (62.33.207.33) 15.281 ms 15.078 ms 14.937 ms
7 *
8 *
```

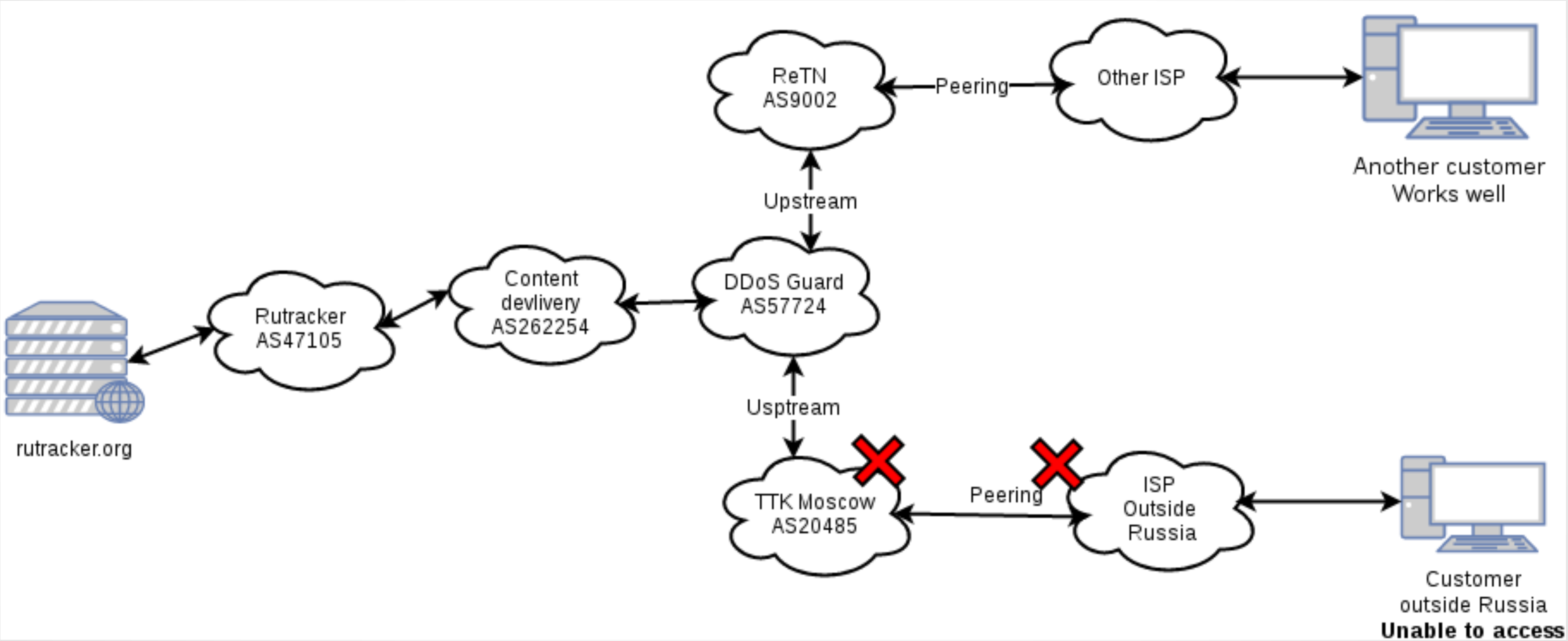
Translation from Russian

OK from NTT
Unreachable through TTK

- **Second traceroute:**

```
1 10.10.3.1 (10.10.3.1) 6.102ms 6.006ms 5.916ms

2 46.23.68.97 (46.23.68.97) 5.794ms 5.702ms
    5.622ms

3 thn.as13213.net (83.170.70.133) 5.512ms
    5.431ms 5.346ms

4 83.170.70.225 (83.170.70.225) 5.258ms 5.164ms
    5.034ms

5 lnn11-ge500.501.transtelecom.net (195.66
    224.212) 15.592ms 15.507ms 15.417ms

6 62.33.207.33 (62.33.207.33) 15.281ms 15.078ms
    14.937ms

7 *

 ...

30 * * *
```

Rutracker.org accident



Based on information provided by Rutracker.org
network operators

Rutracker.org accident

- Transtelecom fixed the problem soon after receiving complaints from customers
- Few users from **Ukraine** was complaining about receiving Russian blacklist information page (due to ISP DNS misconfiguration?)
- Displays potential problems of transit networks (filtering)
- Motivate us to make measurements and discover existing problems

Our methodology

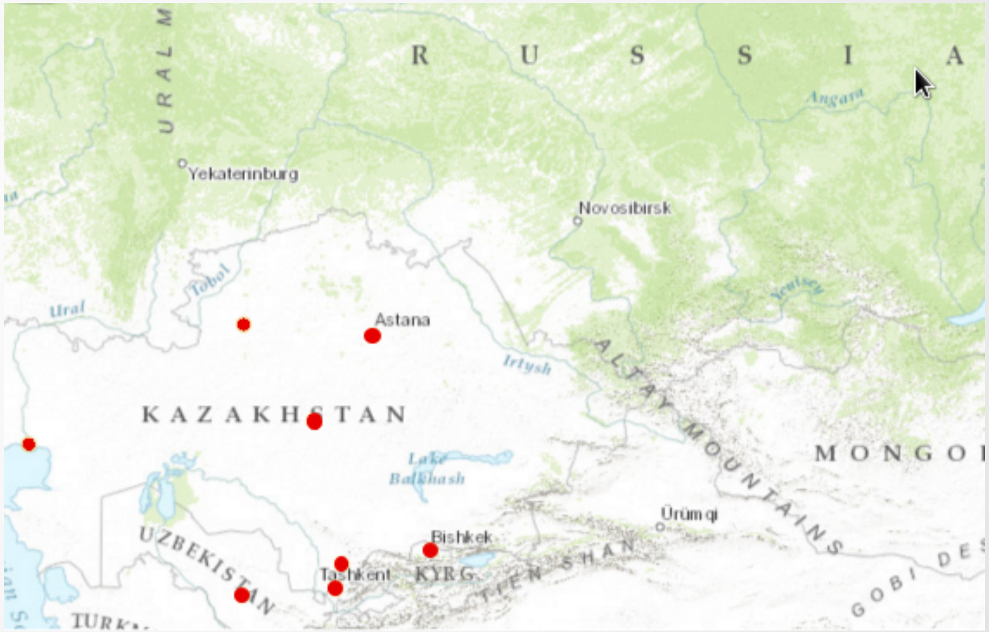
- We choose RIPE Atlas to perform measurements due to low count of Tor end nodes in problematic countries
- Test few expected-to-be-blocked sites and hosts from probes in countries near Russian border
- Test countries several times by different techniques
- Filter out nodes with connection timeout/connection failures, perform testing on such probes
- Analyze result and find out source of problems: censorship blockage/network outage/misconfiguration on probe

Our research

- We did **SSL certificate** testing to obtain first result
- During SSL test our team set **«DNS on probe»** option to detect **DNS** resolution problems to find out DNS blockage. Run test again with RIPE DNS in case of failure.
- Case to mark probe as **«failed»**:
  - SSL handshake timeout to all tested resources
  - Connection timeout to all testing resources
  - Connection reset and failures
- Perform two kinds of **traceroute** (TCP and ICMP) to find out last hop of packet.
- Review nodes «failed» nodes testing other resources like GitHub
- Eliminate misconfigured and suspicious nodes (DNS failure)

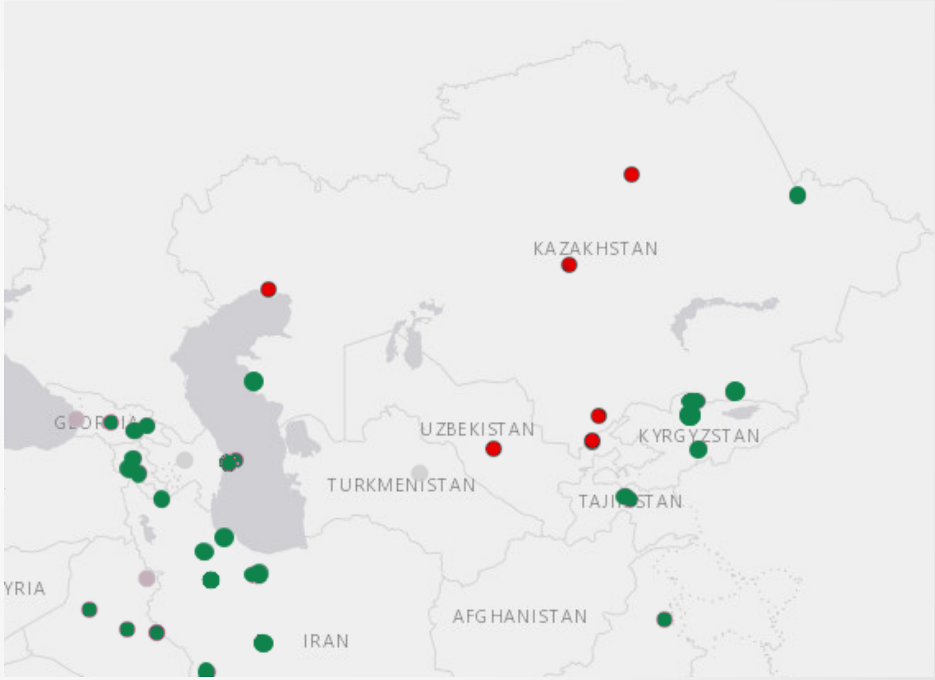
Results

- We found interesting results
- Few countries are affected by Russian censorship for sure: Kazakhstan, Uzbekistan, Kyrgyzstan
- Not entirely all probes affected in KZ an KG
- Counties like Georgia, Azerbaijan, Armenia use non-russian backbones but also might be affected by IC route selection
- European countries likely not affected
- SSL timeout, no MITM, traceroute stops somewhere in Moscow



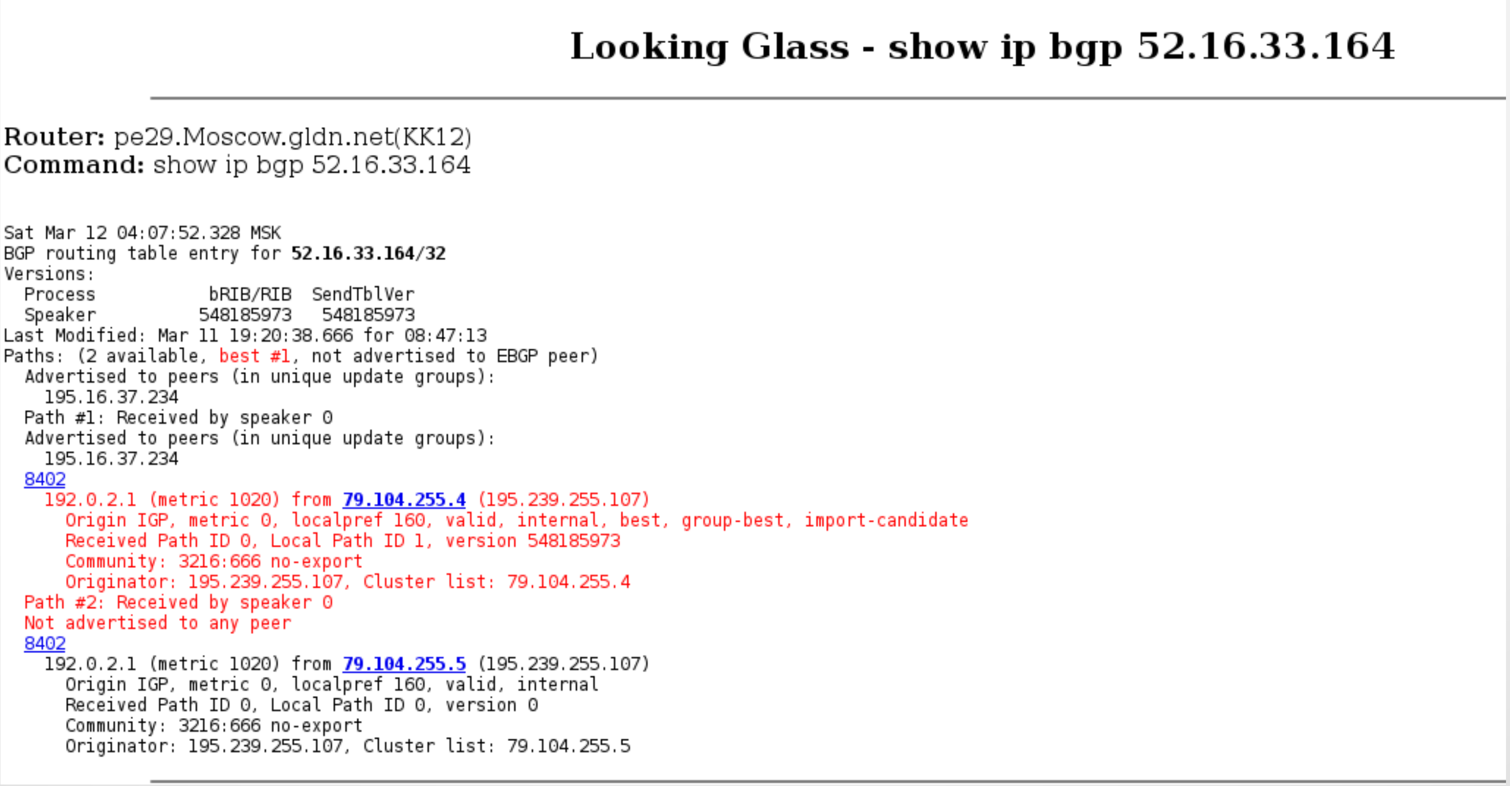
Results

- In each case of blocking - reason was Golden Telecom/Vimpelcom Russian ISP (Moscow router)
- List of affected networks
  - “KCell” JSC, KZ, AS29355
  - Nurtelecom LLC, KG, AS47237
  - Kazakhtelecom, KZ, AS9198
  - Buzton J.V., UZ, AS29385
  - Uzbektelecom, UZ, AS197486
  - “TEXNOPROSISTEM” LLC, UZ, AS34718



Source of problems

- GoldenTelecom (Vimpelcom) AS3216 blocks transit traffic
- Let's take a look on Looking Glass at Moscow RS
- We may find route nexthop to 192.0.2.1 on blocking IP



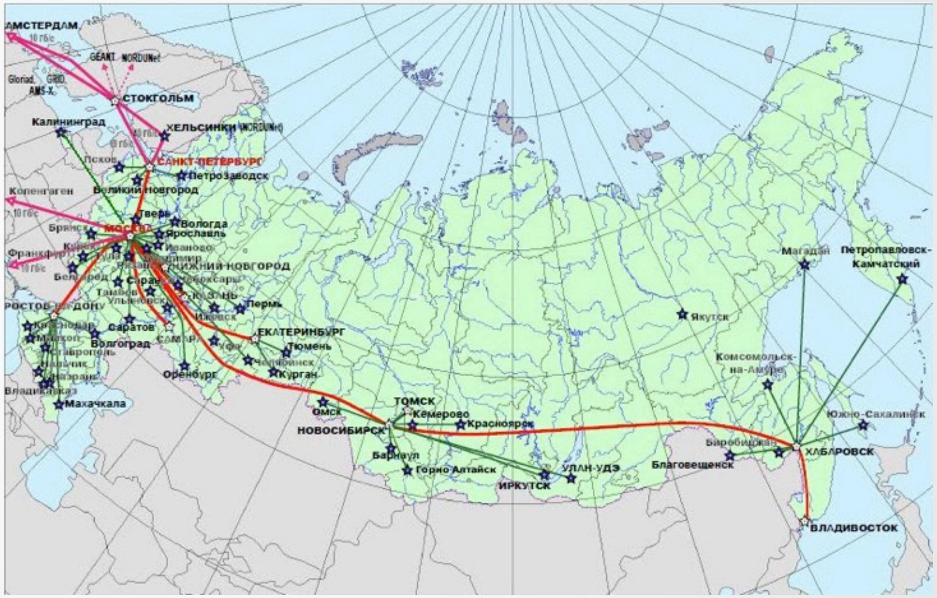
Looking Glass - show ip bgp 52.16.33.164

Router: pe29.Moscow.gldn.net(KK12)
Command: show ip bgp 52.16.33.164

```
Sat Mar 12 04:07:52.328 MSK
BGP routing table entry for 52.16.33.164/32
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker          548185973   548185973
Last Modified: Mar 11 19:20:38.666 for 08:47:13
Paths: (2 available, best #1, not advertised to EBGP peer)
  Advertised to peers (in unique update groups):
    195.16.37.234
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    195.16.37.234
  8402
    192.0.2.1 (metric 1020) from 79.104.255.4 (195.239.255.107)
      Origin IGP, metric 0, localpref 160, valid, internal, best, group-best, import-candidate
      Received Path ID 0, Local Path ID 1, version 548185973
      Community: 3216:666 no-export
      Originator: 195.239.255.107, Cluster list: 79.104.255.4
  Path #2: Received by speaker 0
  Not advertised to any peer
  8402
    192.0.2.1 (metric 1020) from 79.104.255.5 (195.239.255.107)
      Origin IGP, metric 0, localpref 160, valid, internal
      Received Path ID 0, Local Path ID 0, version 0
      Community: 3216:666 no-export
      Originator: 195.239.255.107, Cluster list: 79.104.255.5
```

Results

- Problem we confirmed is not fully shown in reports because of few factors:
  - Occasionate nature of problem
  - Unpredictability of routing changes
- There are many cases when announcing route through the Russian network lead to incorrect filtering
- Research should continue and update data from time to time
- We should monitor typical routes through transit networks



State Educational (Universities) network map in 2013

What operators should do? Conclusion

- Configure routing right way, don't route into null on intermediate routers
- AS-border and core routers is not good way to place censorship implementation. Put filtering for customers to provider edge (access)
- Transtelecom (TTK), Rostelecom already fixed problem learning lesson by hard
- Censorship is designed to limit access to the information, not to make connectivity difficult to the rest of resources
- Operator often make mistake redistributing censorship routes to outside world (like YouTube 2007 accident)

Questions?

- Our contacts:

  NetAssist LLC, AS29632

  support@netassist.ua

  http://netassist.ua

  http://github.com/netassist-ua
- Report about your access problems to our contact email
- We love to help people and assist networks