Russia vs. Telegram
technical notes on the battle

Leonid Evdokimov
35c3, Leipzig, 29 Dec 2018
darkk.net.ru/35c3

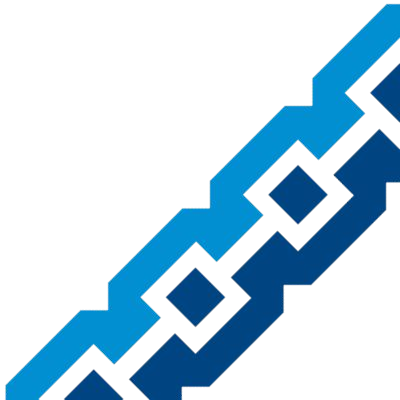
$ whoami

Internet measurement fanatic

NOT a Telegram team member

One of the millions of Telegram users

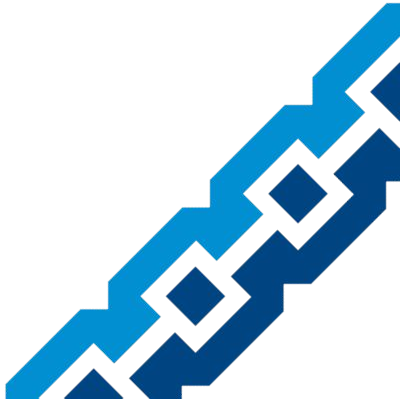
Brief history



Pre-blocklist era

2007 May 23: court order for 4 (four) ISP to block access to “extremist” websites

2007 Jul 14: the 1st issue of the “Federal List of Extremist Materials” by Ministry of Justice

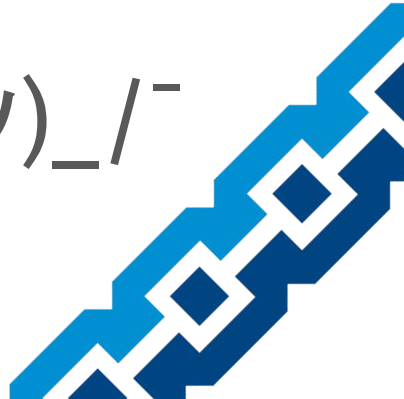


Librarian’s resistance

2011 Feb: www.zhurnal.lib.ru is banned

Maksim Moshkow “transfers” domain to the Ministry of Justice (via DNS “A” RR)

Some ISPs block minjust.ru ¯_(ツ)_/¯

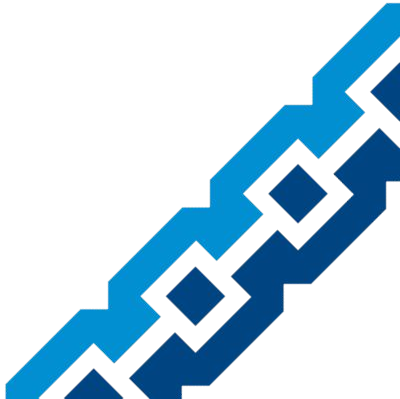


Blocklist awakens

2012 Jul 10: Wikipedia strikes, Yandex & VK protest

2012 Jul 11: the internet restriction bill accepted by Duma (Parliament)

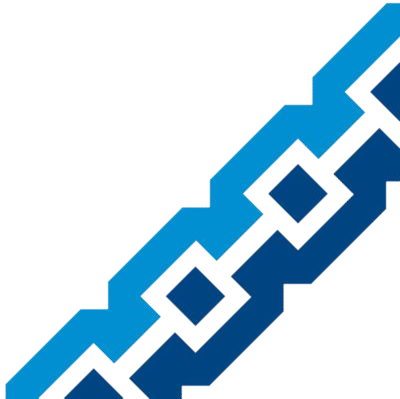
2012 Jul 28: the bill signed



What's the blocklist like today?

XML file, signed by CN=Roskomnadzor with GOST, fetched by ISPs via SOAP, updated at least hourly.

ISPs ***control*** filtering equipment. Roskomnadzor ***monitors*** it.



Blocklist 2012 awards

8 Nov: Absurdopedia (Uncyclopedia)

11 Nov: Lurkmore memepedia, lib.rus.ec

17 Nov: Github repo with blocklist leak

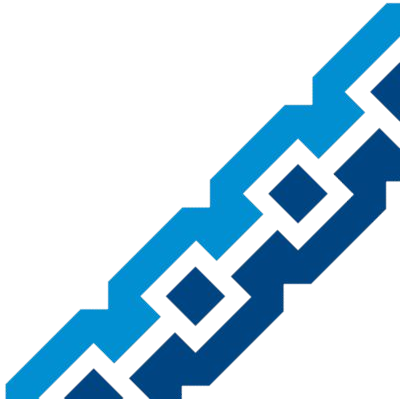
18 Nov: Google's https://....gstatic.com

Blacklisted resources in pre-Telegram era

Web Archive, GitHub, Google, LinkedIn, Pornhub, Reddit, VK, Wikipedia…

Comodo CA CRL & OCSP responders

127.0.0.1 (sic!)



“Revisor” — Roskomnadzor’s monitoring system

The law does not matter. The fine does.

2016 Jan: OpenWRT-based TP-Link MR3020, that was talking with C&C via https API without `ca-certificates` and via ssh without `known_hosts`

Внимание!

Эта страница НЕ ИМЕЕТ ОТНОШЕНИЯ к провайдеру, через которого осуществляется проверка факта открытия веб-сайтов Ревизором.

Подробную информацию читайте по ссылке: https://habrahabr.ru/post/282087/

ValdikSS

“Revisor” — complying with blackbox

No codified monitoring rules, just FAQ

Some ISPs reverse-engineer it

Some ISPs comply at best-effort

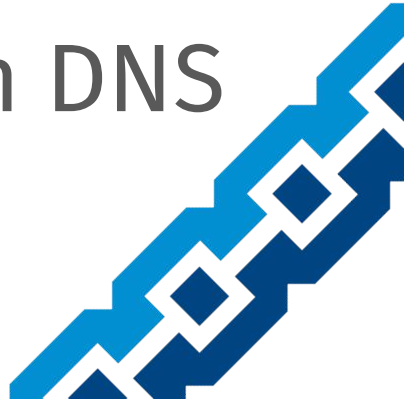
Some ISPs place it into a “sandbox”

Logo of Revisor-devoted Telegram chat @i_love_auditor

“Revisor” & DNS

ISPs are forced to comply with the black-box monitoring system

Stale IPs in `dump.xml`, “Revisor” using DNS… ⇒ ISPs feed A & AAAA from DNS ***directly*** to filters



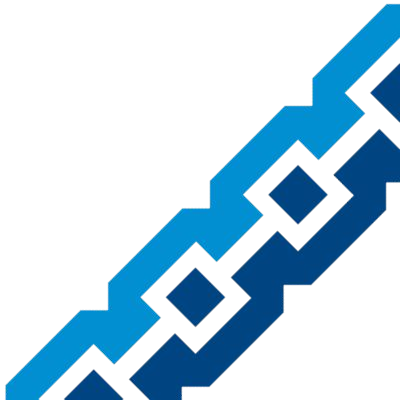
“Revisor”-provoked so called “DNS-attacks”

2017 May 15: block IP from DNS? Bo-om!

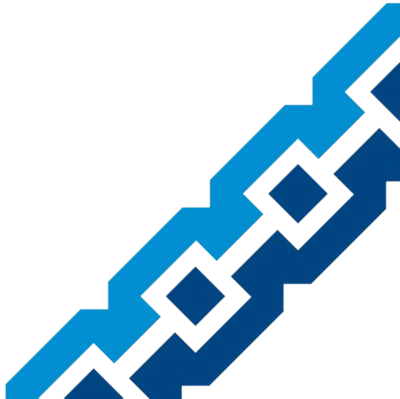
Adding /32 from DNS to routing table?

2017 Jun 7: drop IX peers!

2018 Mar 14: routers go on strike!



Telegram:
Policeman Enters The Game



Telegram? Why?

2017 Apr 7: St.Petersburg bombing

2017 Jun 26, FSB: “terrorists used TG”
RKN promises to block, counts days.

2017 Jun 28: Telegram added to the “Information Distributors Registry”

Telegram non-compliance

2017 Dec: Roskomsvoboda starts legal campaign Telegram vs. FSB

2018 Mar 20: court orders Telegram to pass encryption keys to FSB

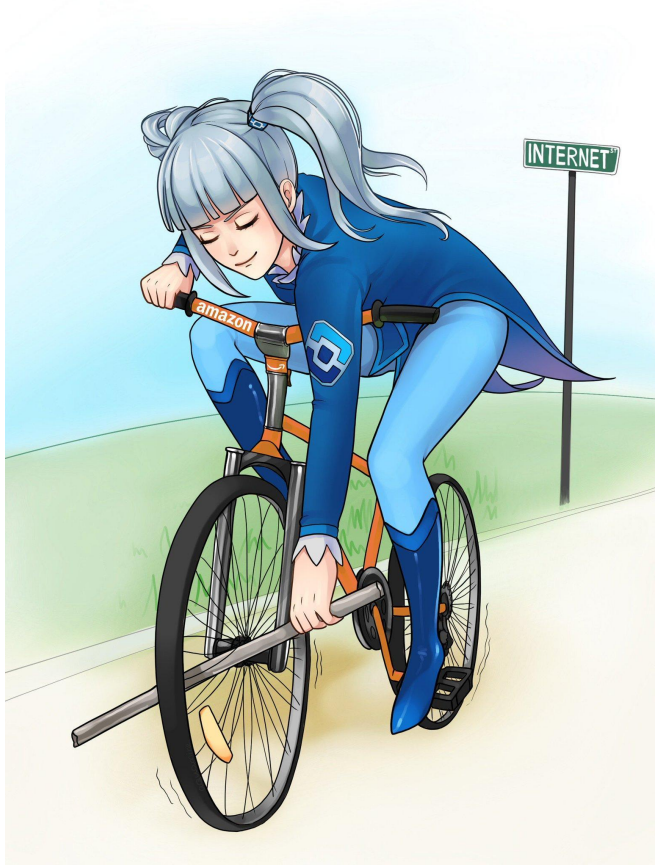
2018 Apr 16: RKN attempts to block

Civil cyber-war: leak of BGP-Blackholing letter

Mar 23: Mikhael Klimarev publishes leak

RKN plans ban of 15M IPs: 36 subnets of Amazon, SoftLayer, ... to block Zello.

Keywords: Null0, BGP, redistribute.



RKN-tan tries to block 14 million IP addresses of Amazon hosting half of Internet

– @aquam1ne

Civil cyber-war: April, 16th, TZ=MSK

11:39 RKN bans TG's ~/19, no effect

17:58 bans Amazon's ~/13, TG works

18:33 adds missing TG's /24 ¯_(ツ)_/¯

20:21 Google's /12, Amazon's /15...

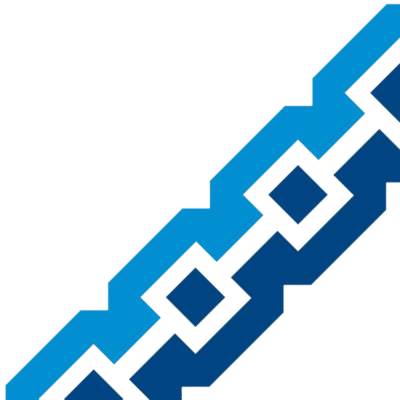
1.8 M IPs banned, Telegram is ~fine

Civil cyber-war: that escalated quickly

Apr 16: ~ 1.8 M banned IPs

Apr 17: ~ 16 M

Apr 22: ~ 19 M, *local* peak



Civil cyber-war: IP space sanity checks? Ha!

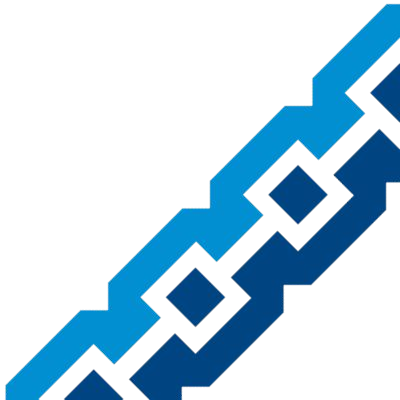
Overlapping subnets in blocklist:

52.0/11 ∩ 52.28/15

34.192/10 ∩ 34.240/13

52.192/11 ∩ 52.208/13

...



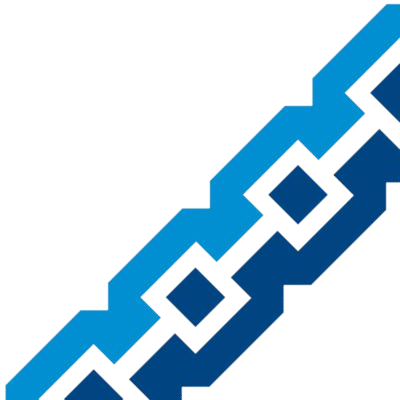
Civil cyber-war: URL sanity checks? Ha!

Malformed URL in blocklist:

<![CDATA[http:// 46.101.189.65]]>

^ whitespace

Guess, what filter do?



Civil cyber-war: major services by mistake? Ha!

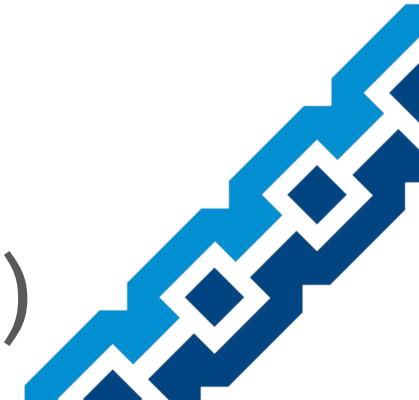
RKN: significant ones are not affected

Affected: ~34 k .ru, .рф, .su services

Affected: vk.com (87.240.129.133)

Affected: Yandex.Metrica (213.180.193.119)

Affected: Yandex ads (77.88.21.90)



Civil cyber-war: fakenews? Sure!

RKN: “Google Play, Google Drive and google.ru IPs were not banned”

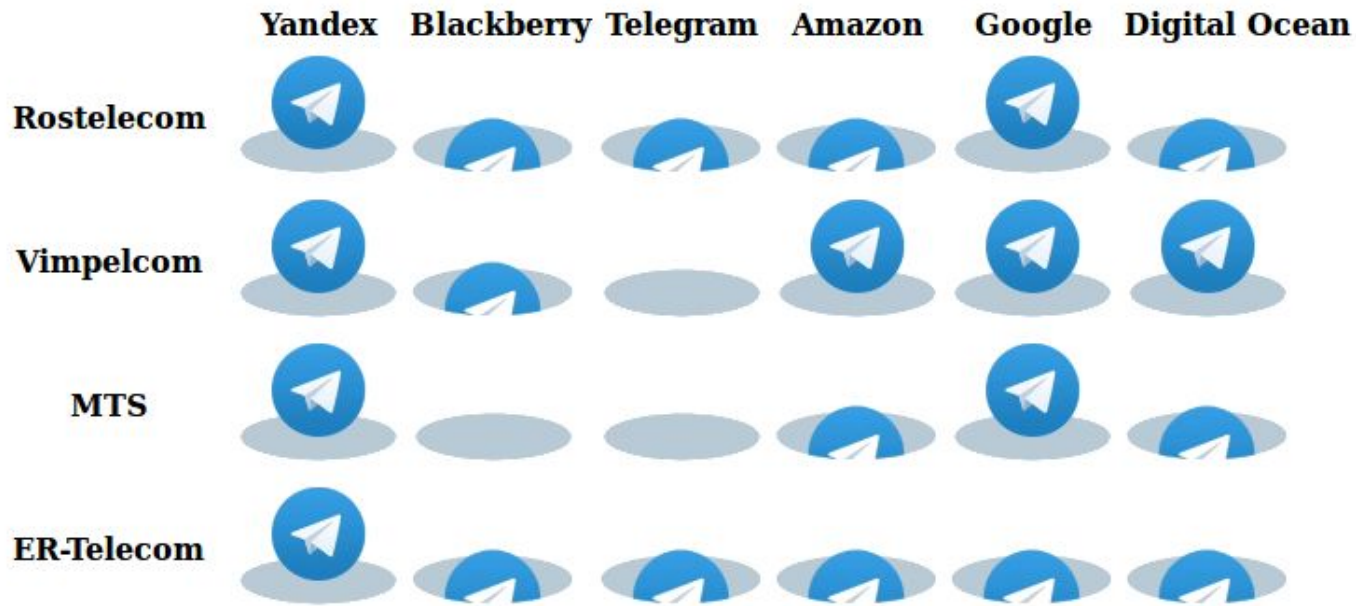
Data: dozens IPs of load balancers discovered via EDNS Client Subnet are actually blocklisted

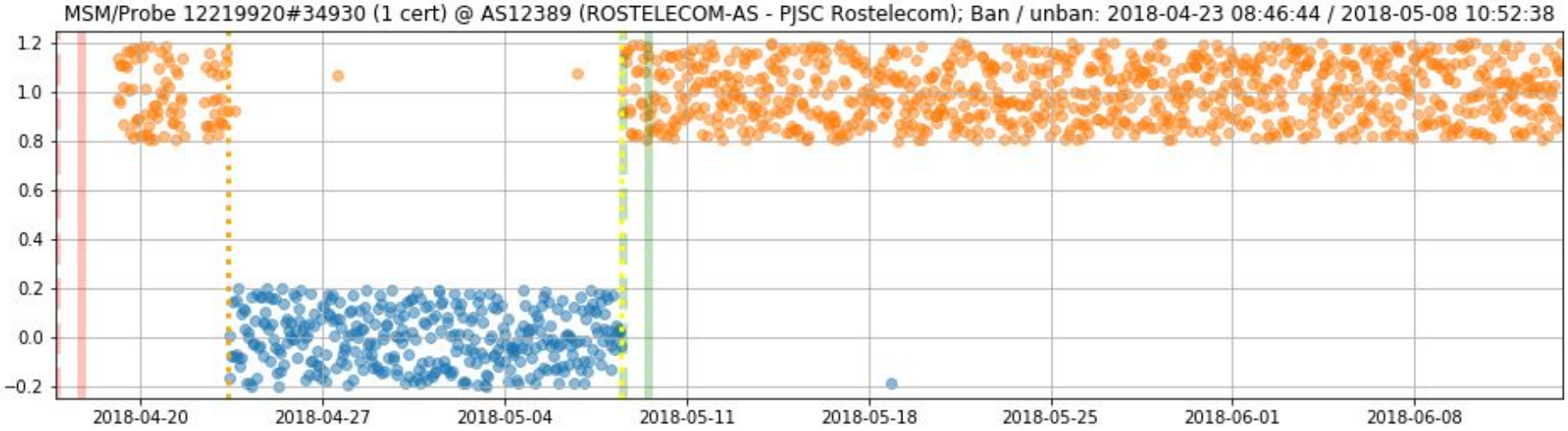
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	IPv4
www.google.com, №0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	418
google.com, №1	0	100	96	61	86	76	82	89	76	95	0	0	0	0	0	0	0	0	0	509
play.google.com, №2	0	94	100	60	84	75	81	87	75	94	0	0	0	0	0	0	0	0	0	520
www.youtube.com, №3	0	47	48	100	45	41	48	45	49	47	0	0	0	0	0	0	0	0	0	659
docs.google.com, №4	0	85	85	57	100	82	73	79	73	85	0	0	0	0	0	0	0	0	0	514
drive.google.com, №5	0	82	83	58	90	100	74	80	76	82	0	0	0	0	0	0	0	0	0	468
connectivitycheck.android.com, №6	0	94	95	71	85	78	100	90	79	94	0	0	0	0	0	0	0	0	0	444
clients3.google.com, №7	0	95	96	62	86	79	84	100	80	96	0	0	0	0	0	0	0	0	0	474
s.ytimg.com, №8	0	84	85	70	82	78	77	83	100	85	0	0	0	0	0	0	0	0	0	458
www.google-analytics.com, №9	0	95	96	61	86	75	82	89	76	100	0	0	0	0	0	0	0	0	0	510
stats.g.doubleclick.net, №10	0	0	0	0	0	0	0	0	0	0	100	40	0	0	0	0	0	0	0	308
googleads.g.doubleclick.net, №11	0	0	0	0	0	0	0	0	0	0	33	100	0	0	0	0	0	0	0	375
www.googletagmanager.com, №12	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	0	250
fonts.googleapis.com, №13	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0	0	0	0	235
fonts.gstatic.com, №14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	86	92	0	0	275
www.google.ru, №15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	91	100	92	0	0	261
google.ru, №16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	88	84	100	0	0	287
mail.google.com, №17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	91	362
gmail.com, №18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	94	100	351

G.DNS

Civil cyber-war: ISP non-compliance

А примерно так ISP (не) блокируют облака:





Delayed compliance example, RIPE Atlas data

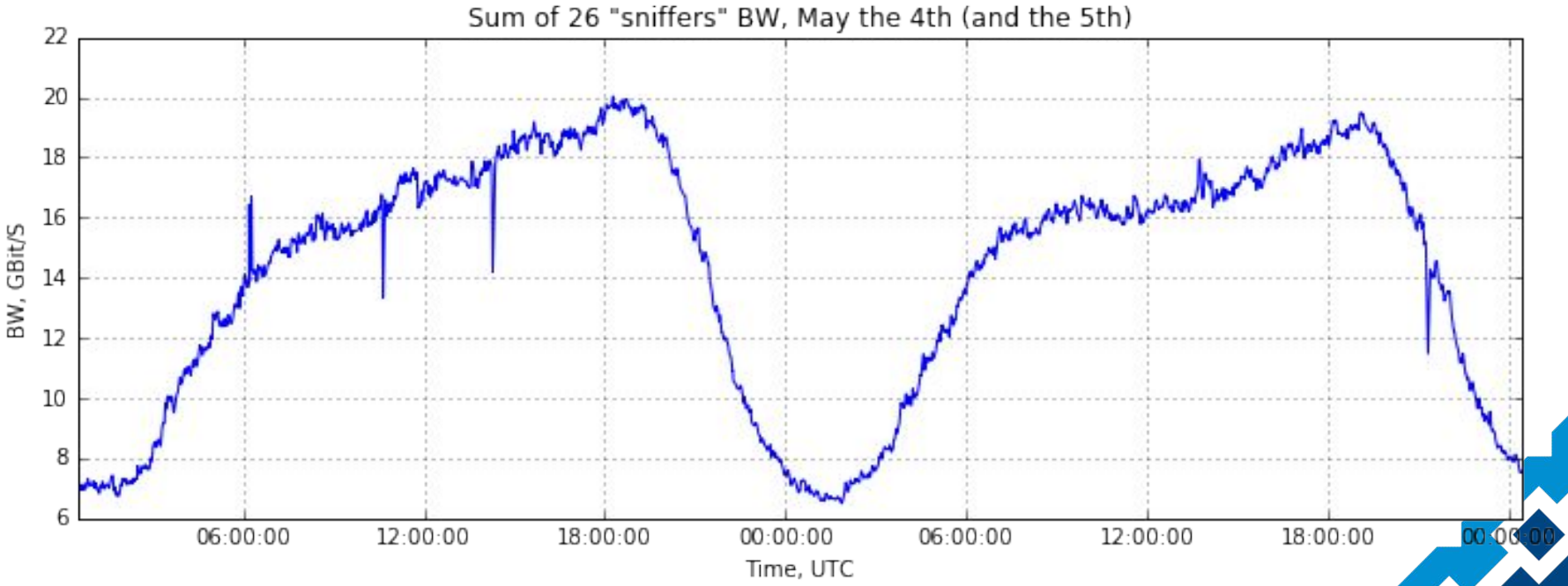
Civil cyber-war: lawful interception?

Sniffers used to hunt proxies?

28 Apr: public “tip”, 30 Apr: private tip

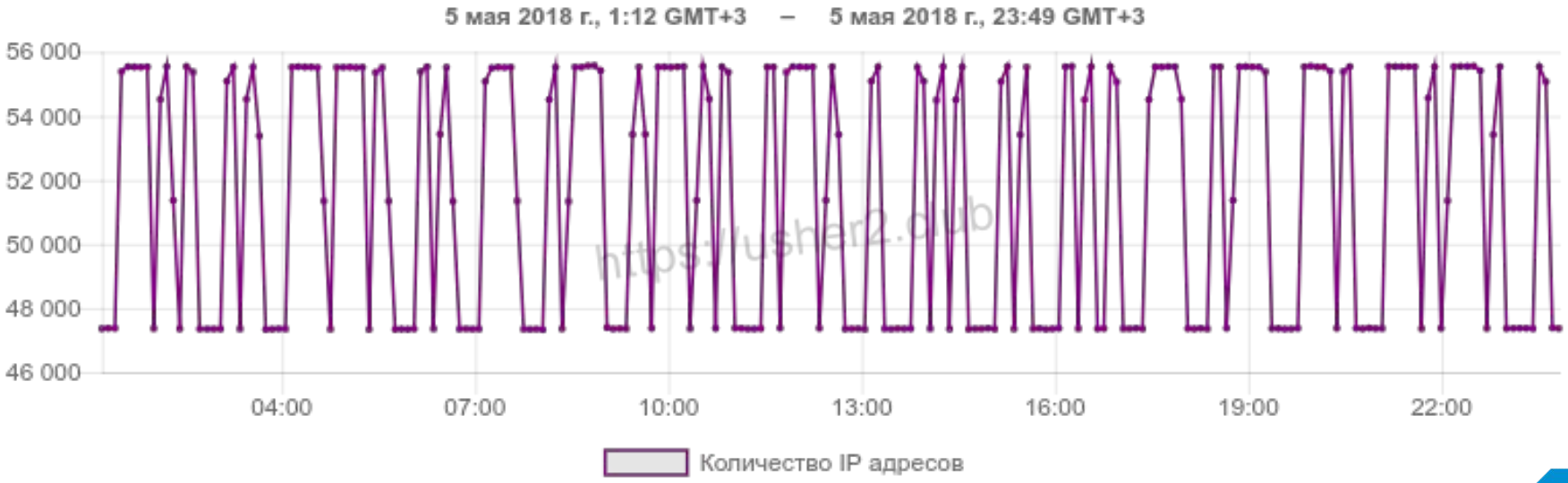
Unsecured SORMs, pumping 20 Gbit/s, leaking rpm repo, clickstream and PII?!

SORM: this incident was reported



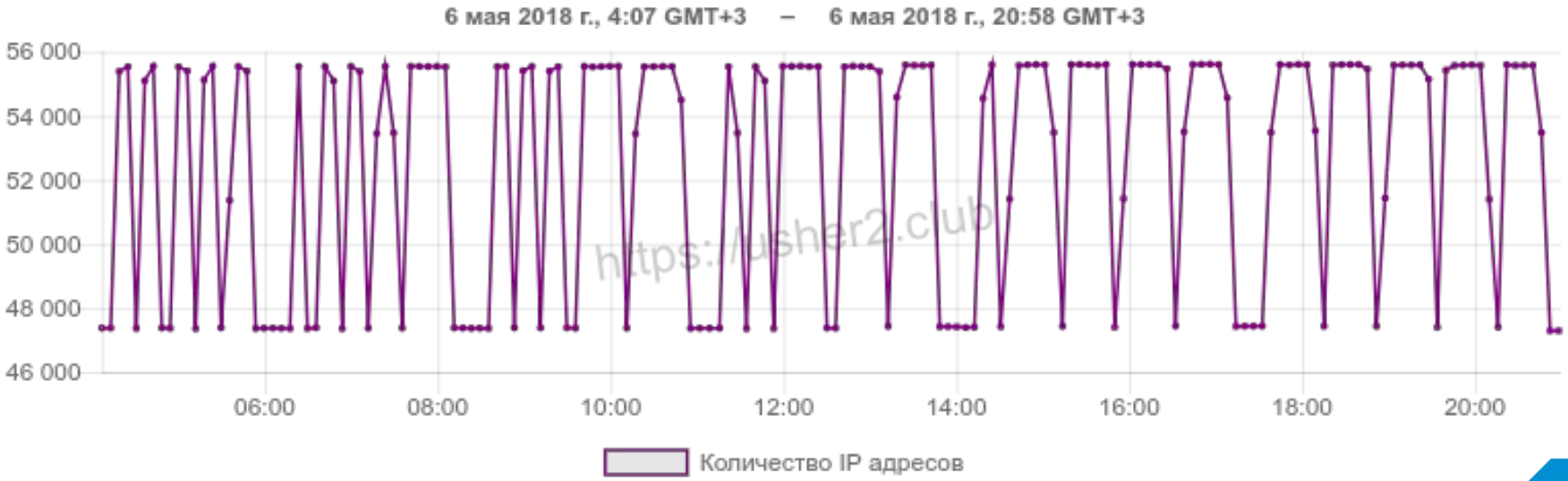
Protest meetings because of app ban!

Civil cyber-war: Morse prank



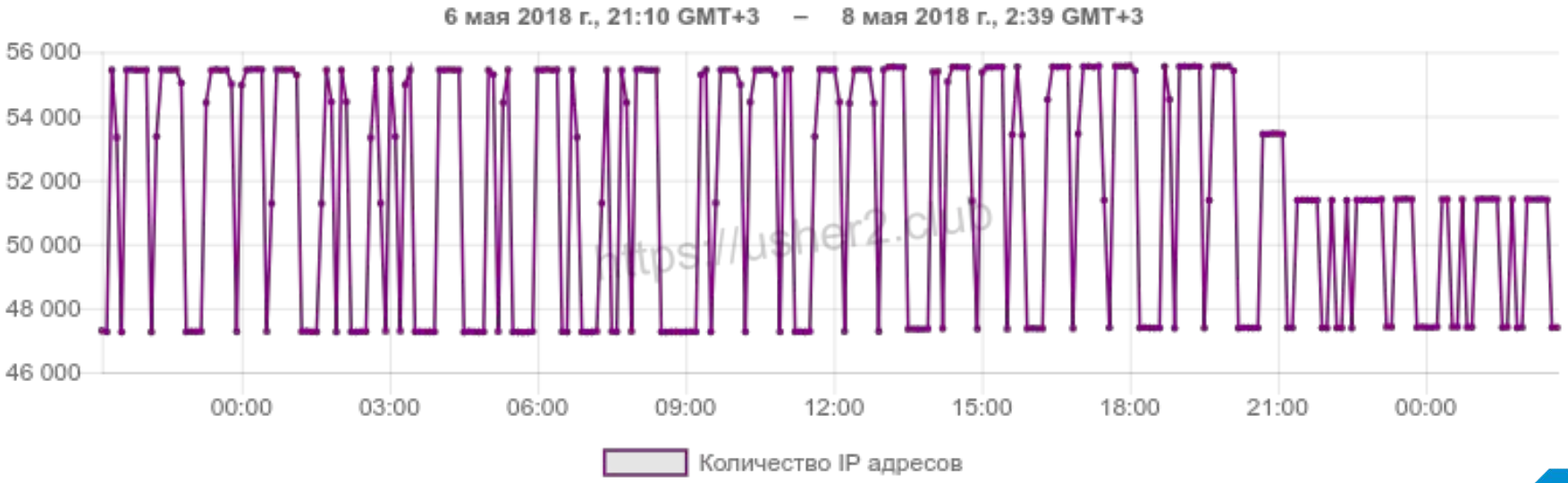
D I G I T A L R E S I S T A N C E

Civil cyber-war: Morse prank



Countdown (cheap drama)

Civil cyber-war: Morse prank



“Truly, Popov!” – Radio Day greeting

Civil cyber-war: prank-effects

Nice amplitude fade-out (thanks, RKN!)

“&.” TLD flash-blocking

15 M → 11 M banned IPs

Expired domains blocklist cleanup

Civil cyber-war: partial rollback

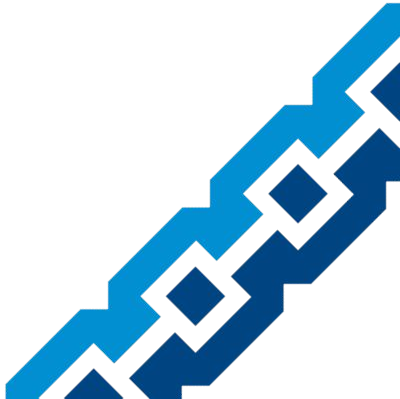
28 Apr: 19 M → 15 M (protest)

8 May: 15 M → 11 M (prank?)

8 Jun: 11 M → 3.7 M (?)

7 Jul: Open Letter on collateral damage had no effect, still ~3.7 M

PCAP or it didn’t happen



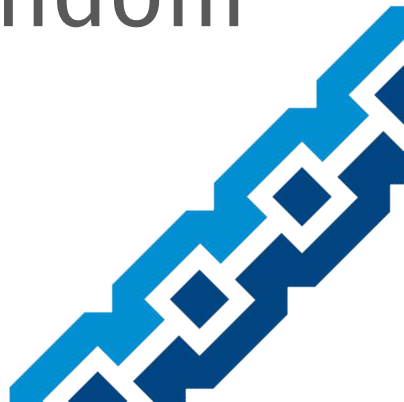
Selective protocol throttling

TG speaks Socks5, MTProto, MTproto-dd

~7500 kbps: Socks5, HTTP xor RC4

~22 kbps: MTProto, obfs4, `nc urandom`

Camouflage matters!



Proxy-hunting: MTProto

`pkt.len`-based hunting was noticed

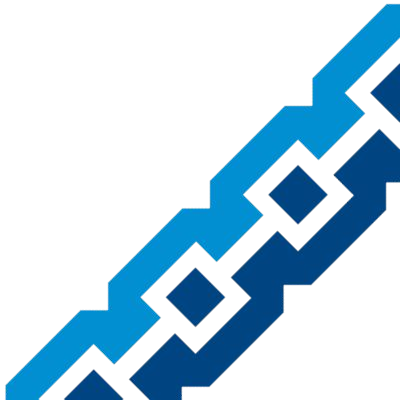
Rostelecom was part of the experiment

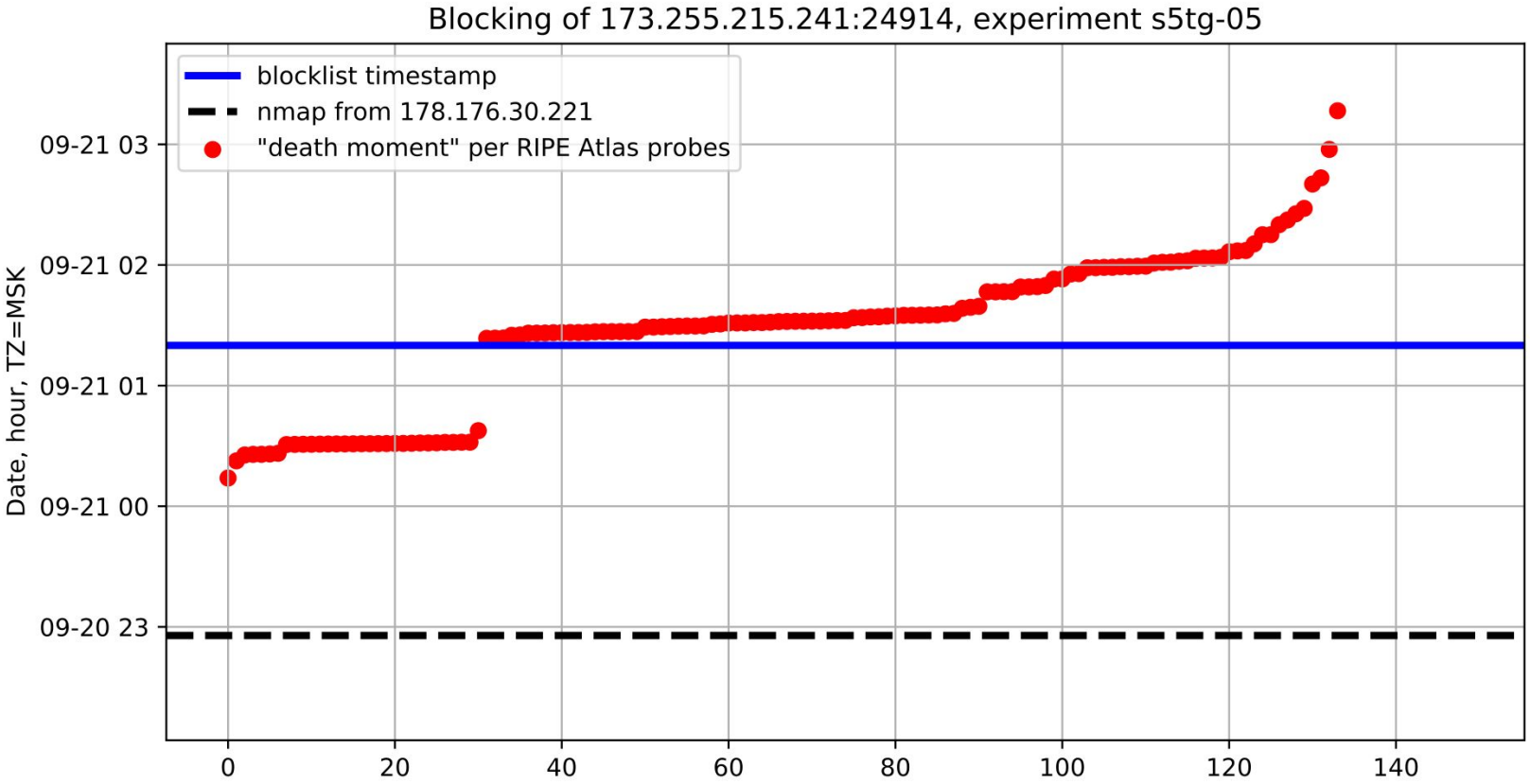
Any IP:Port may be killed by “knocking”

Reuters: “alike experiment happened”

Proxy-hunting: Socks5 in Moscow subway

1. One uses Socks5 in subway
2. Nmap scans IP:Port
3. Socks5-scanner tries connect(TG)
4. IP unreachable via ***some*** ISPs
5. IP officially blocklisted




Blocking of 173.255.215.241:24914, experiment s5tg-05
blocklist timestamp
nmap from 178.176.30.221
"death moment" per RIPE Atlas probes
Date, hour, TZ=MSK
09-21 03
09-21 02
09-21 01
09-21 00
09-20 23
0
20
40
60
80
100
120
140

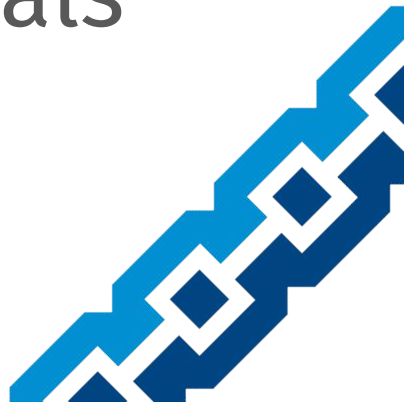
Secret blocklist private to some ISPs?

*> 4. IP unreachable via **some** ISPs*

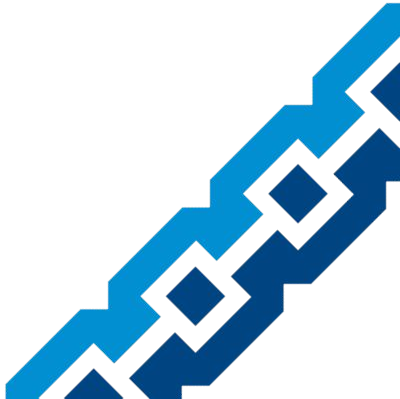
Some other blacklists exist... regional?...

...***at least*** List of Extremist Materials

Block-race is still observed



And then things got worse



Roskomnadzor: The Phantom Menace

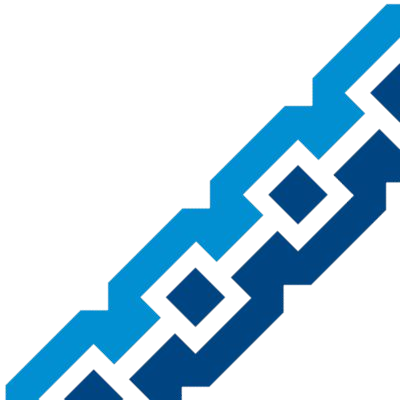
RKN deploys “anti-threat” equipment

That also acts as filter

RKN ***directly*** controls IP routing & DNS

Registry of “good” Internet Exchanges

so it goes



Thanks to!

Philipp Kulin, ValdikSS, Mikhael Klimarev, Dmitry Nazarov, Alex Rudenko, Dmitry Belyavskiy, Wartan Hachaturow, Dmitry Moskin, Dmitry Morozovsky, Simone Basso, Maria Xynou, Moritz Bartl, zapret-info, SPb CTF, Roskomsvoboda, Digital Resistance Measurement Squadron, “the one who is to blame”, “Revisor” fans, NAG, RIPE Atlas, …

Thanks RKN & Durov for fun!

Questions?

usher2.club

darkk.net.ru/35c3