Tor censorship attempts in Russia, Iran, Turkmenistan

Roger Dingledine

December 28 2023

Outline

(1) Intro to Tor

(2) Intro to Tor and censorship resistance

(3) Russia

(4) Iran

(5) Turkmenistan

(6) Bigger context

Tor Overview

Online anonymity: open source, open network

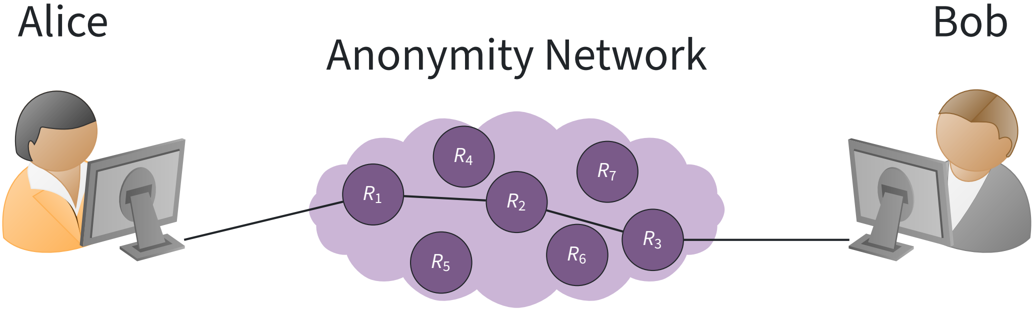
Community of devs, researchers, users, relay operators

US 501(c)(3) non-profit organization with 50ish staff

Estimated 2,000,000 to 8,000,000 daily users

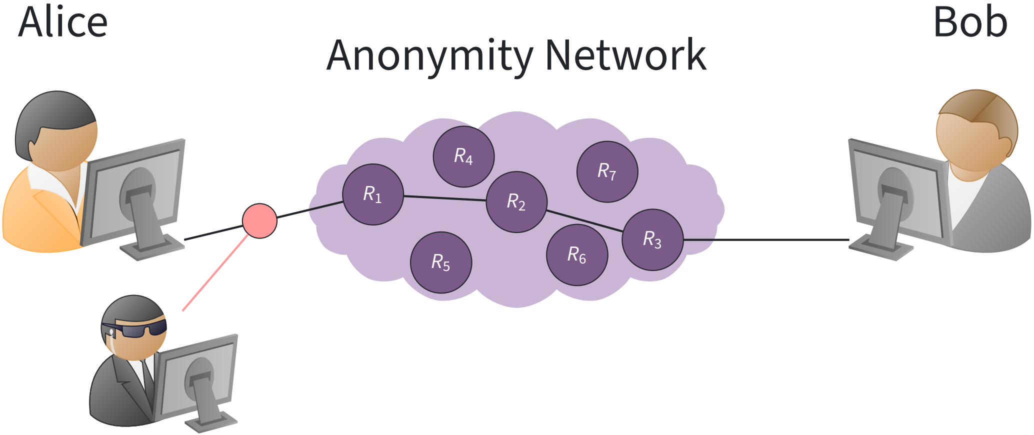
Part of larger ecosystems: internet freedom, free software, censorship resistance, anonymity research

Threat Model

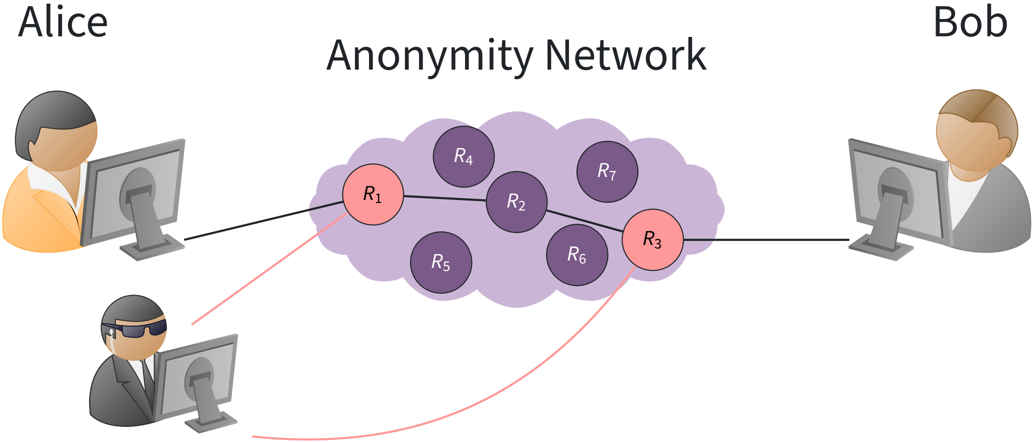


{What can the attacker do?}

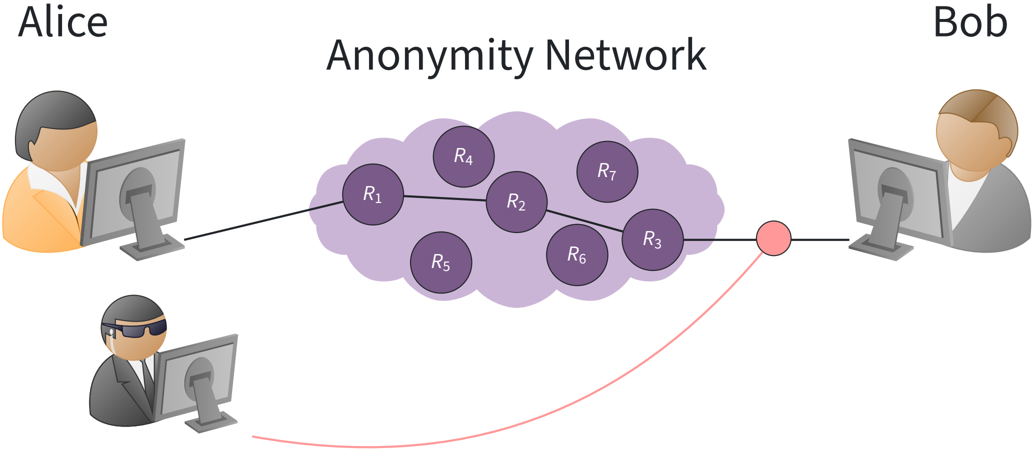
Threat Model



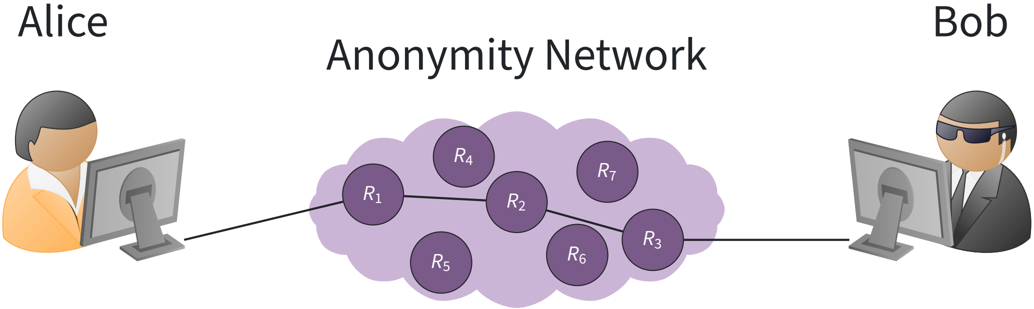
Threat Model



Threat Model



Threat Model



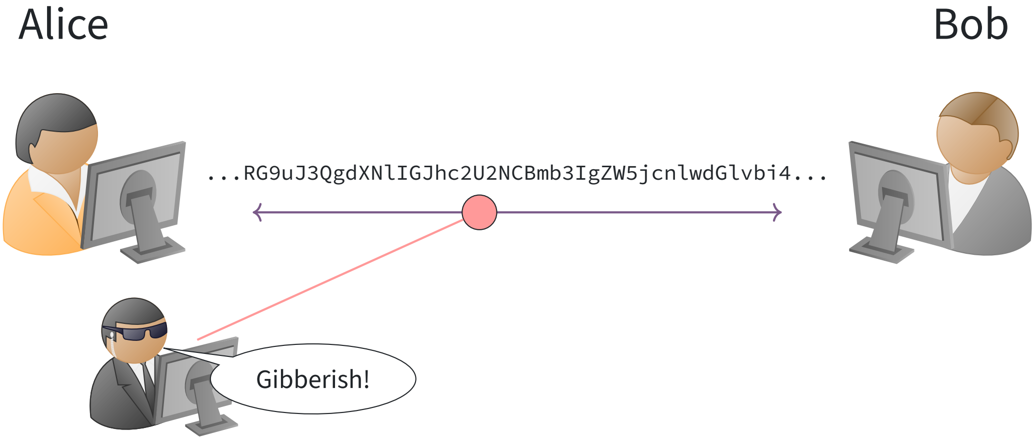
Alice

Anonymity Network

Bob

R_4 R_7 R_1 R_2 R_3 R_5 R_6

Anonymity isn’t Encryption



Encryption just protects contents.

Communications Metadata

"We Kill People Based on Metadata."

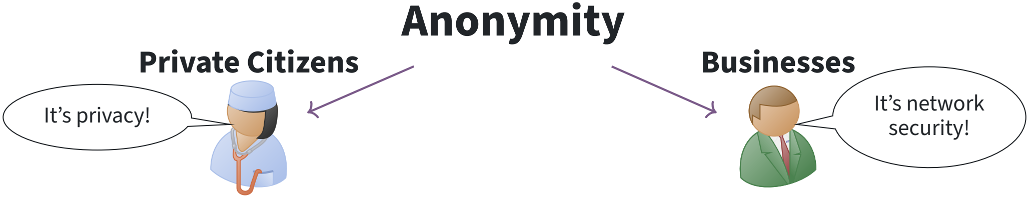
—Michael Hayden, former director, NSA

Anonymity is different for each use case

Anonymity

Private Citizens

Anonymity is different for each use case



Anonymity

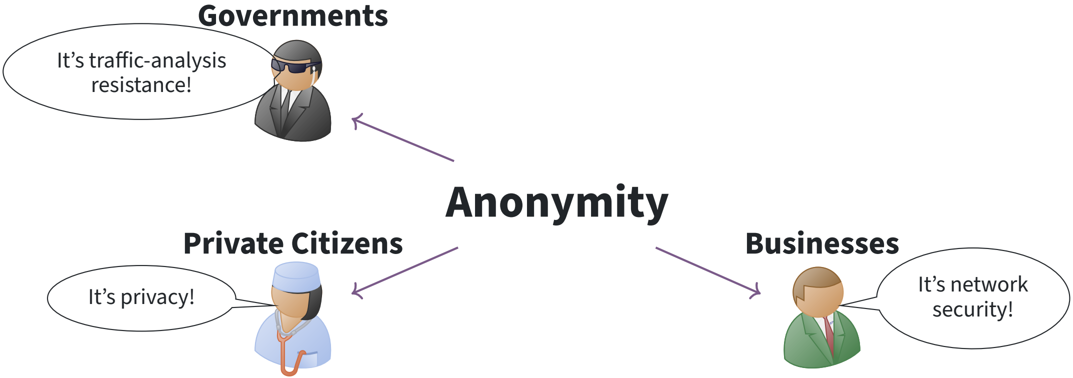
Private Citizens

It’s privacy!

Businesses

It’s network security!

Anonymity is different for each use case



Governments

It’s traffic-analysis resistance!

Anonymity

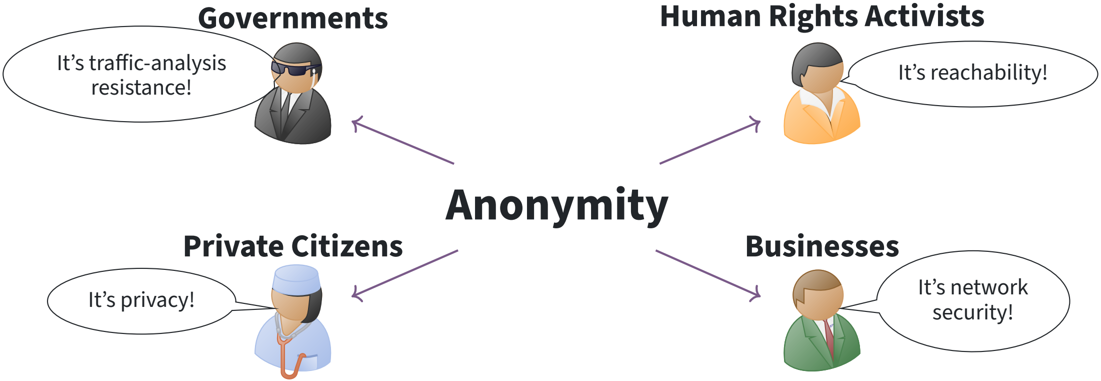
Private Citizens

It’s privacy!

Businesses

It’s network security!

Anonymity is different for each use case



Governments

It's traffic-analysis resistance!

Human Rights Activists

It's reachability!

Anonymity

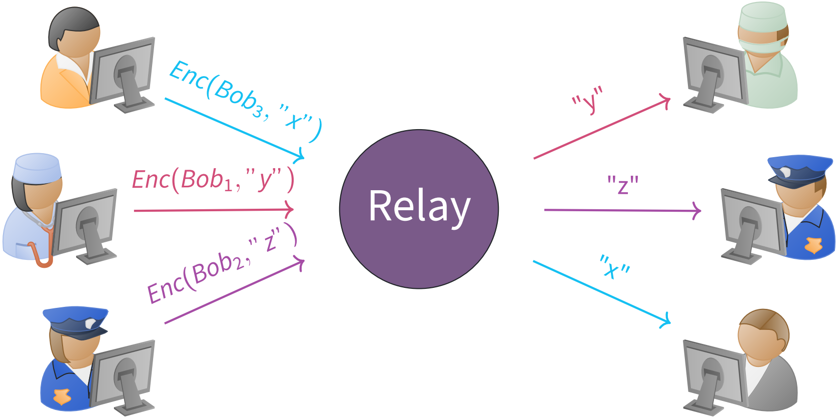
Private Citizens

It's privacy!

Businesses

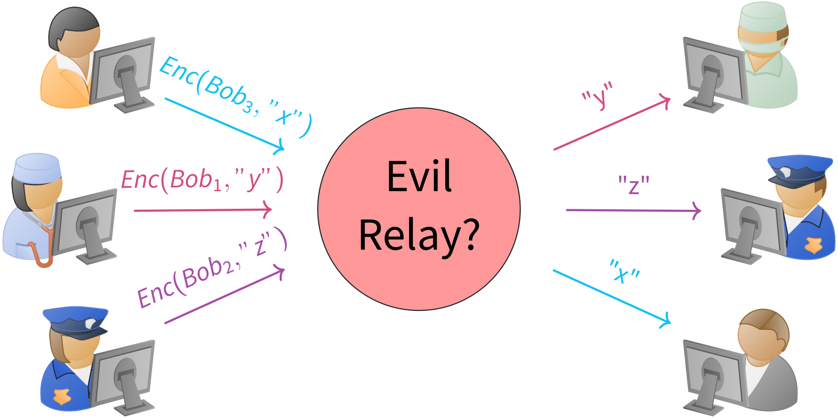
It's network security!

A Simple Design

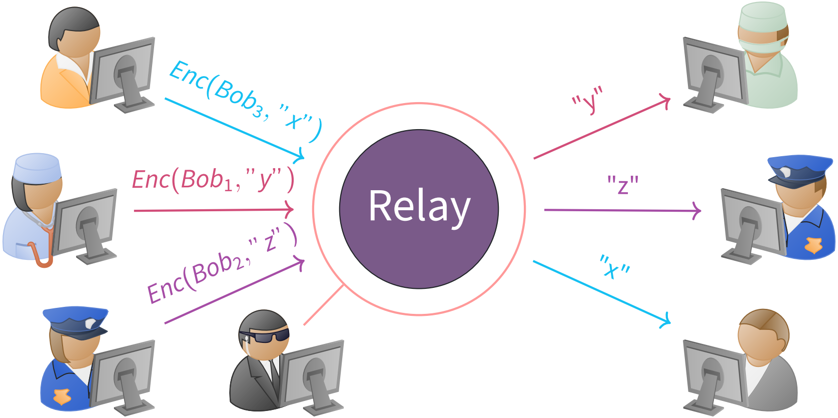


Equivalent to most commercial proxy/VPN providers.

A Simple Design

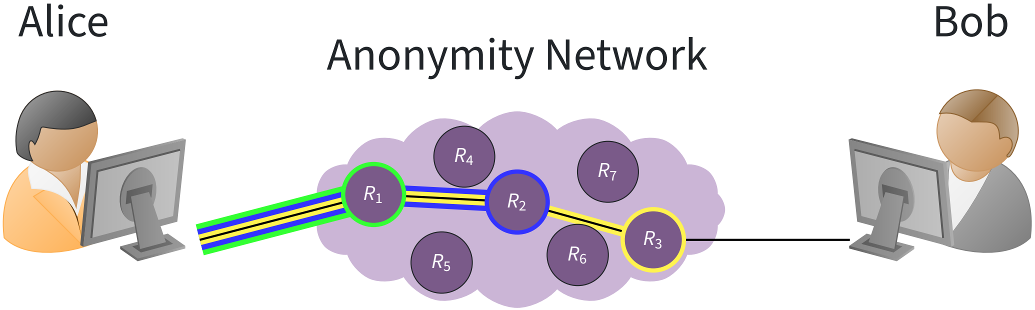


A Simple Design

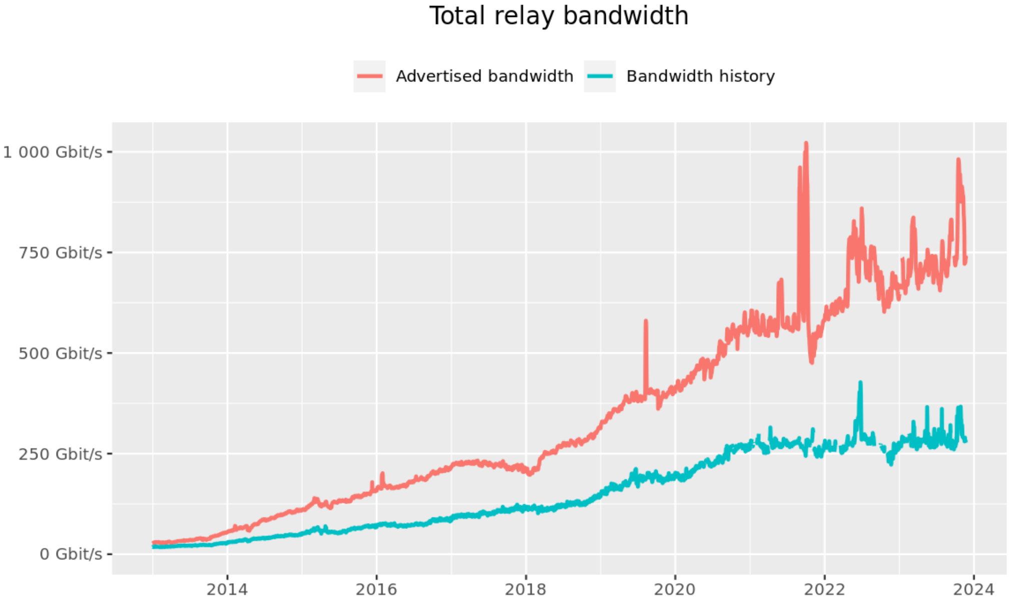


Timing analysis lets an observer match up connections.

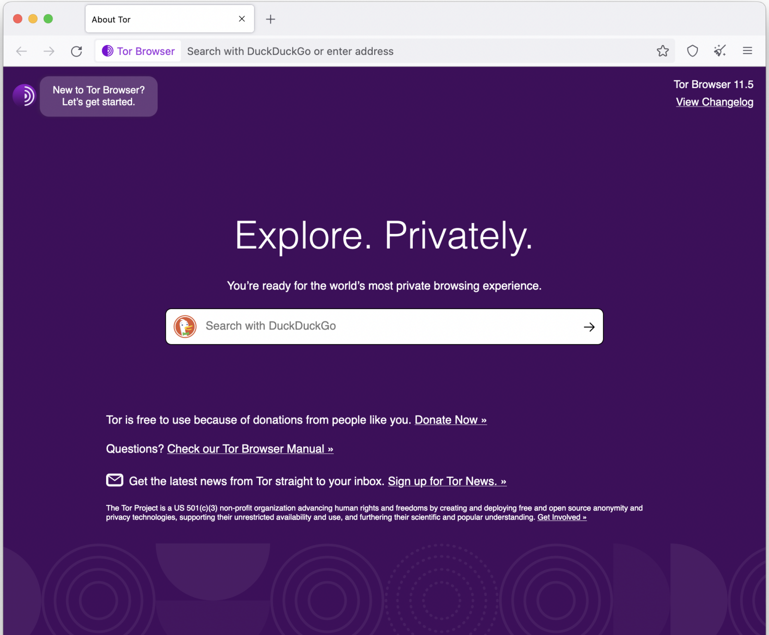
The Tor Design



Multiple relays so no single relay can link Alice to Bob.



The Tor Project - https://metrics.torproject.org/



New to Tor Browser?
Let's get started.

Tor Browser 11.5
View Changelog

Explore. Privately.

You're ready for the world's most private browsing experience.

Search with DuckDuckGo

Tor is free to use because of donations from people like you. Donate Now »

Questions? Check our Tor Browser Manual »

✉ Get the latest news from Tor straight to your inbox. Sign up for Tor News. »

The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers

Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers
- Not a contradiction: privacy is about choice!

Outline

~~(1) Intro to Tor~~

(2) Intro to Tor and censorship resistance

(3) Russia

(4) Iran

(5) Turkmenistan

(6) Bigger context

Bridges, for IP address blocking

The Tor network is made up of 8000 public relays, but the list is public and you can just fetch it and block them by IP address.

So, we have unlisted relays called “bridges” and there is a cat-and-mouse game where users try to get a bridge that the censor didn’t already find.

Pluggable transports, for DPI blocking

Protocol-level arms race too: the Tor protocol looks mostly like TLS, but only if you don't look too carefully.

Rather than perfectly mimicking Firefox+Apache, our "pluggable transports" design aims for modularity:

Tor's three-hop path provides the privacy, and you can plug in different *transports* that transform the first link's traffic into flows that your censor doesn't block.

obfs4 pluggable transport

obfs4 is still the core most successful transport.

It simply adds a new layer of encryption on top, so there are no recognizable headers or formatting at the content layer.

The idea is that automated protocol classifiers won’t have any good guesses, so censors are forced to either block all unclassified traffic or allow it all through.

Snowflake pluggable transport

Snowflake makes your traffic look like a WebRTC (zoom, jitsi, skype, signal, etc) call, and those are allowed in many parts of the world.

People can volunteer as Snowflake proxies simply by installing an extension in their browser.

The resulting volume and variety of volunteers gives us more options on how to distribute them to users.

meek pluggable transport

Domain fronting: Makes https request to a shared cloud service (azure, fastly, etc), and tunnels traffic inside it

Outer layer says the SNI (Server Name Indicator) of a popular site, but inner layer has a different Host: header

Have to pay cloud prices for the bandwidth :(, so not great for proxying full traffic flows

Matching bridges to users who need them

Divide obfs4 bridges into distribution buckets, where each bucket relies on a different scarce resource to rate-limit how many bridges the censor can get.

- https (get a few bridges based on your IPv4 /16)
- gmail (get a few bridges based on your username)
- moat (Tor Browser makes a domain-fronted connection, presents a captcha in-browser, and auto-populates your bridge settings).

Matching bridges to users who need them

and Snowflake has a similar “broker” service that matches up Snowflake users to Snowflake volunteers.

Outline

~~(1) Intro to Tor~~

~~(2) Intro to Tor and censorship resistance~~

(3) Russia

(4) Iran

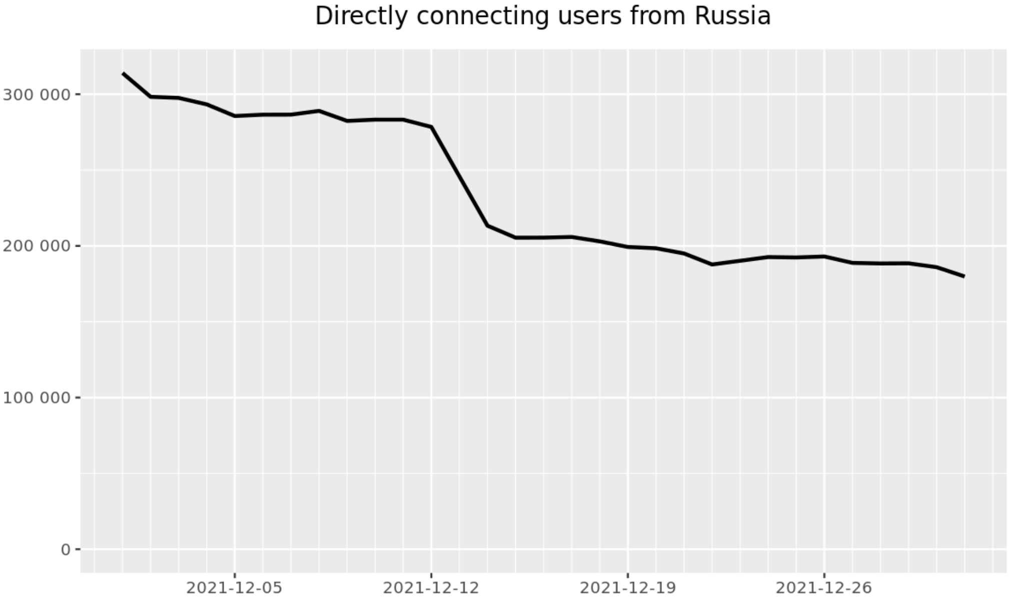
(5) Turkmenistan

(6) Bigger context

Russia, December 2021

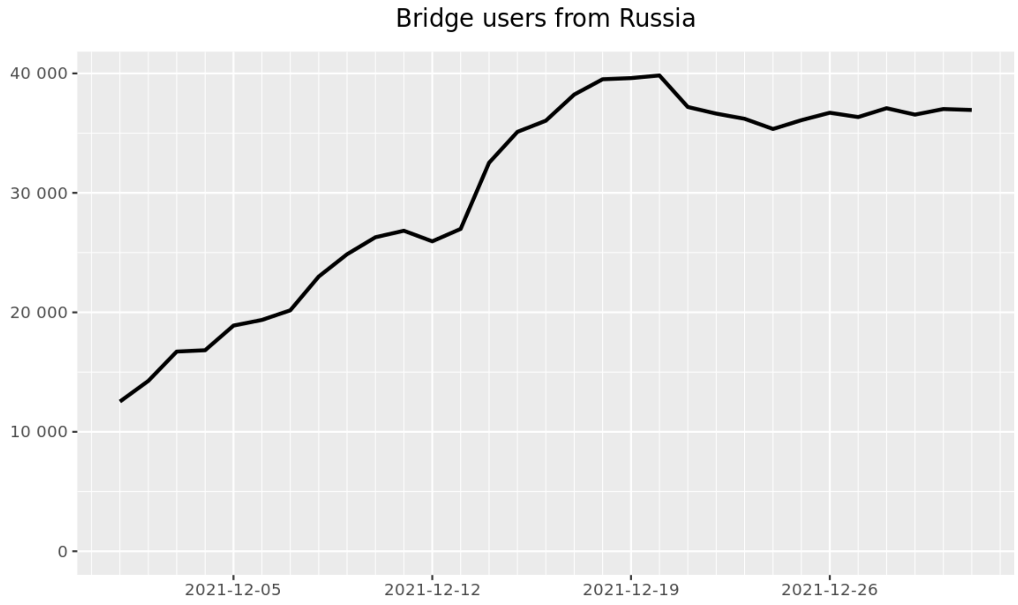
Some ISPs blocked (a) the public Tor relays, (b) meek-azure domain fronting, (c) Tor Browser’s default obfs4 bridges, (d) some moat-distributed obfs4 bridges, (e) the Snowflake protocol.

A week later we got an actual legal notice that the Tor website was evil and they were going to censor it. Then they did.

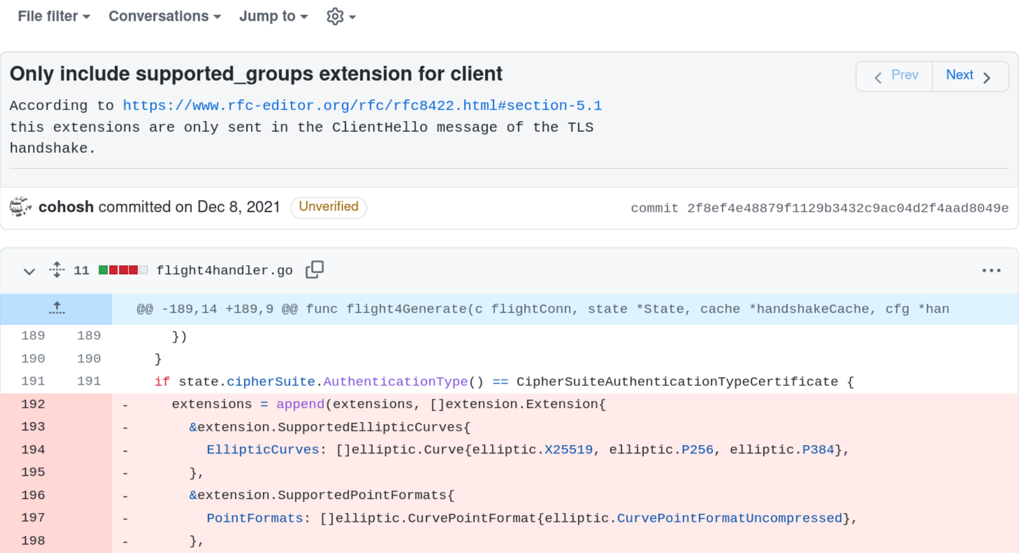


Directly connecting users from Russia

The Tor Project - https://metrics.torproject.org/



The Tor Project - https://metrics.torproject.org/

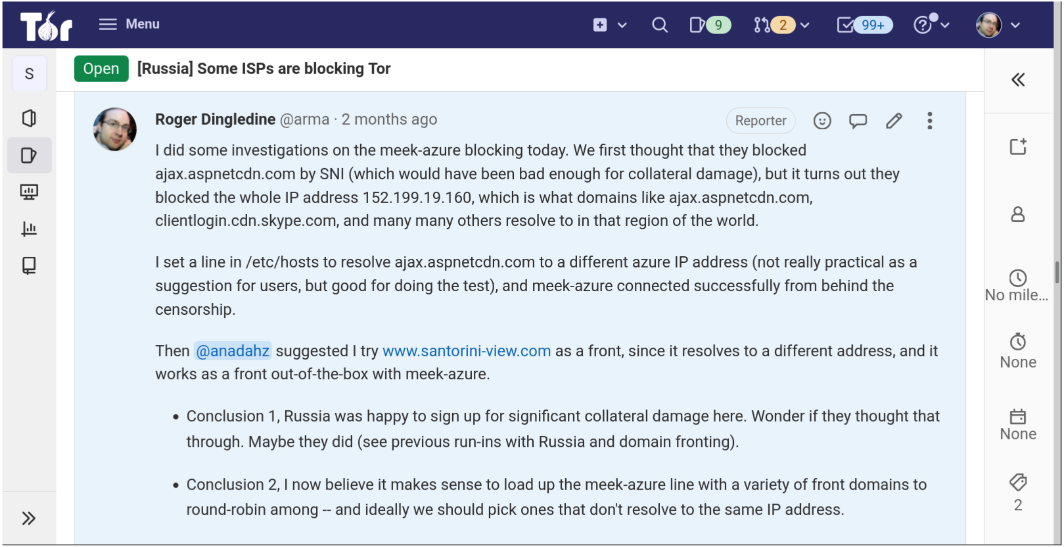


Only include supported_groups extension for client

```
According to https://www.rfc-editor.org/rfc/rfc8422.html#section-5.1
this extensions are only sent in the ClientHello message of the TLS
handshake.
```

cohosh committed on Dec 8, 2021 `commit 2f8ef4e48879f1129b3432c9ac04d2f4aad8049e`

```
@@ -189,14 +189,9 @@ func flight4Generate(c flightConn, state *State, cache *handshakeCache, cfg *han
        })
      }
      if state.cipherSuite.AuthenticationType() == CipherSuiteAuthenticationTypeCertificate {
-        extensions = append(extensions, []extension.Extension{
-          &extension.SupportedEllipticCurves{
-            EllipticCurves: []elliptic.Curve{elliptic.X25519, elliptic.P256, elliptic.P384},
-          },
-          &extension.SupportedPointFormats{
-            PointFormats: []elliptic.CurvePointFormat{elliptic.CurvePointFormatUncompressed},
-          },
```



[Russia] Some ISPs are blocking Tor

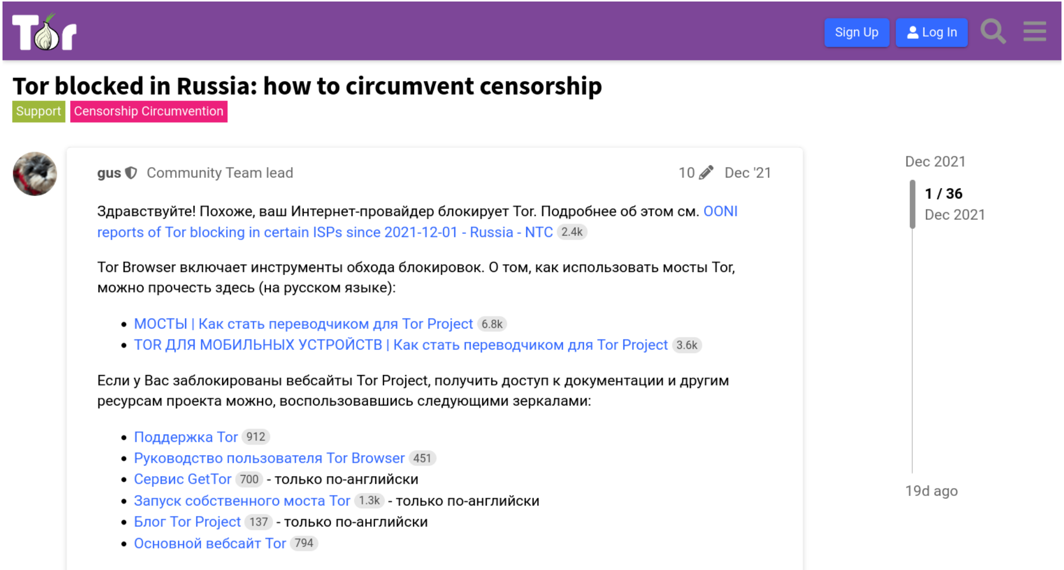
Roger Dingledine @arma · 2 months ago

I did some investigations on the meek-azure blocking today. We first thought that they blocked ajax.aspnetcdn.com by SNI (which would have been bad enough for collateral damage), but it turns out they blocked the whole IP address 152.199.19.160, which is what domains like ajax.aspnetcdn.com, clientlogin.cdn.skype.com, and many many others resolve to in that region of the world.

I set a line in /etc/hosts to resolve ajax.aspnetcdn.com to a different azure IP address (not really practical as a suggestion for users, but good for doing the test), and meek-azure connected successfully from behind the censorship.

Then @anadahz suggested I try www.santorini-view.com as a front, since it resolves to a different address, and it works as a front out-of-the-box with meek-azure.

- Conclusion 1, Russia was happy to sign up for significant collateral damage here. Wonder if they thought that through. Maybe they did (see previous run-ins with Russia and domain fronting).
- Conclusion 2, I now believe it makes sense to load up the meek-azure line with a variety of front domains to round-robin among -- and ideally we should pick ones that don't resolve to the same IP address.



Tor blocked in Russia: how to circumvent censorship

Support Censorship Circumvention

gus Community Team lead 10 Dec '21

Здравствуйте! Похоже, ваш Интернет-провайдер блокирует Tor. Подробнее об этом см. OONI reports of Tor blocking in certain ISPs since 2021-12-01 - Russia - NTC 2.4k

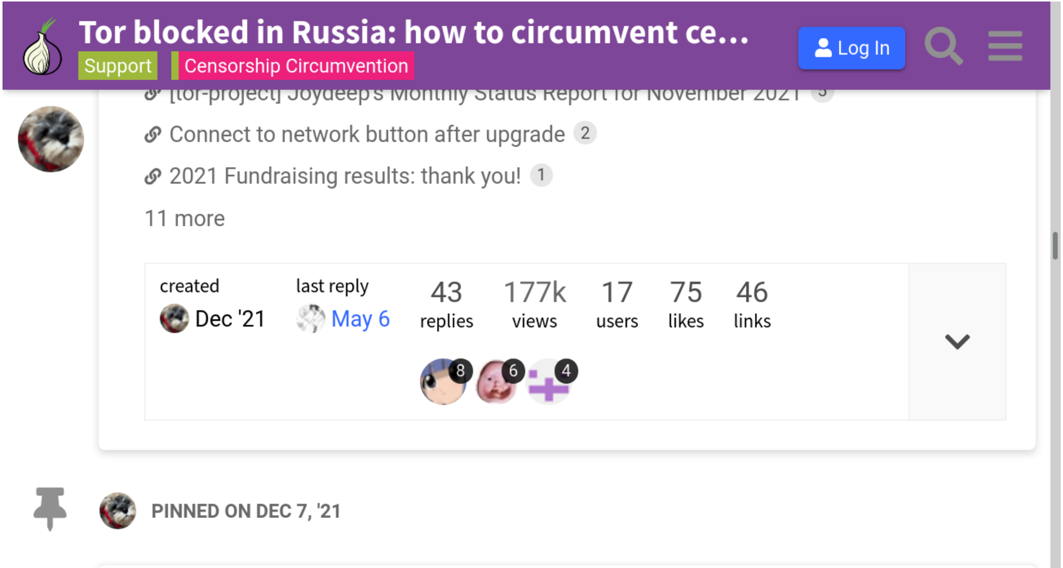
Tor Browser включает инструменты обхода блокировок. О том, как использовать мосты Tor, можно прочесть здесь (на русском языке):

- МОСТЫ | Как стать переводчиком для Tor Project 6.8k
- TOR ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ | Как стать переводчиком для Tor Project 3.6k

Если у Вас заблокированы вебсайты Tor Project, получить доступ к документации и другим ресурсам проекта можно, воспользовавшись следующими зеркалами:

- Поддержка Tor 912
- Руководство пользователя Tor Browser 451
- Сервис GetTor 700 - только по-английски
- Запуск собственного моста Tor 1.3k - только по-английски
- Блог Tor Project 137 - только по-английски
- Основной вебсайт Tor 794

177k views!



Tor blocked in Russia: how to circumvent ce...

Support | Censorship Circumvention

Log In

[tor-project] Joydeep's Monthly Status Report for November 2021 5

Connect to network button after upgrade 2

2021 Fundraising results: thank you! 1

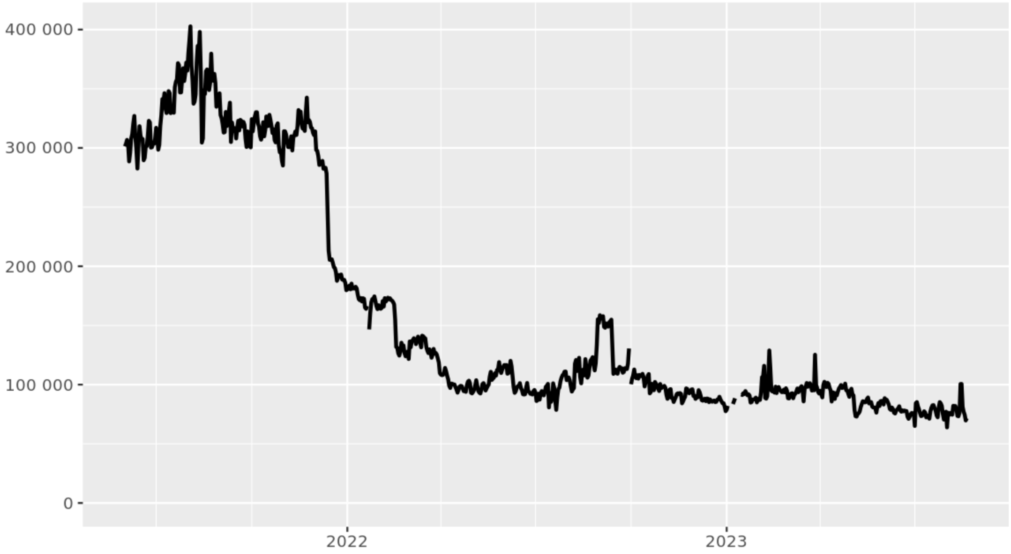
11 more

created	last reply	43	177k	17	75	46
Dec '21	May 6	replies	views	users	likes	links

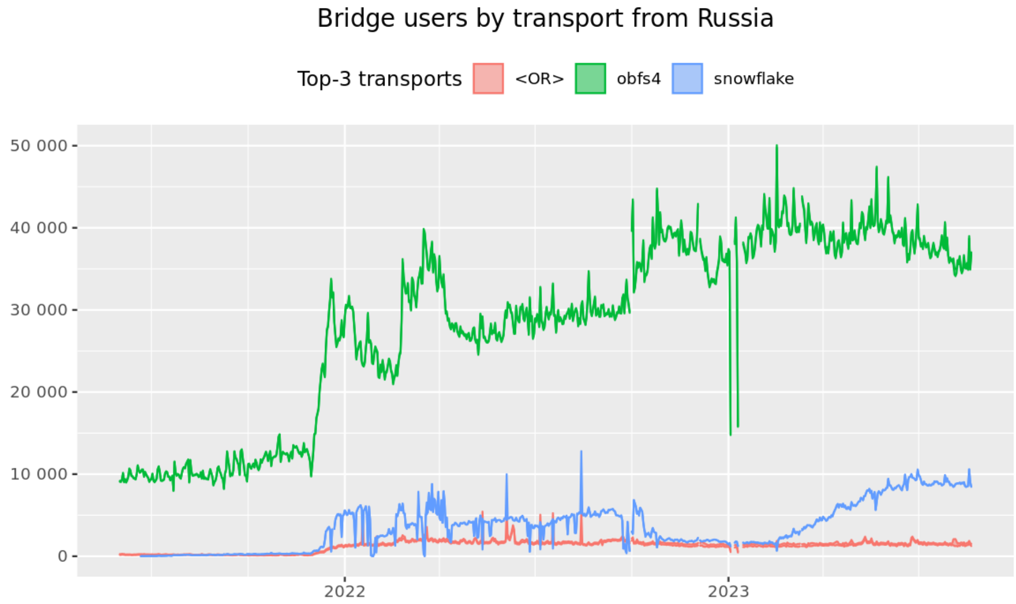
8 6 4

PINNED ON DEC 7, '21

Directly connecting users from Russia

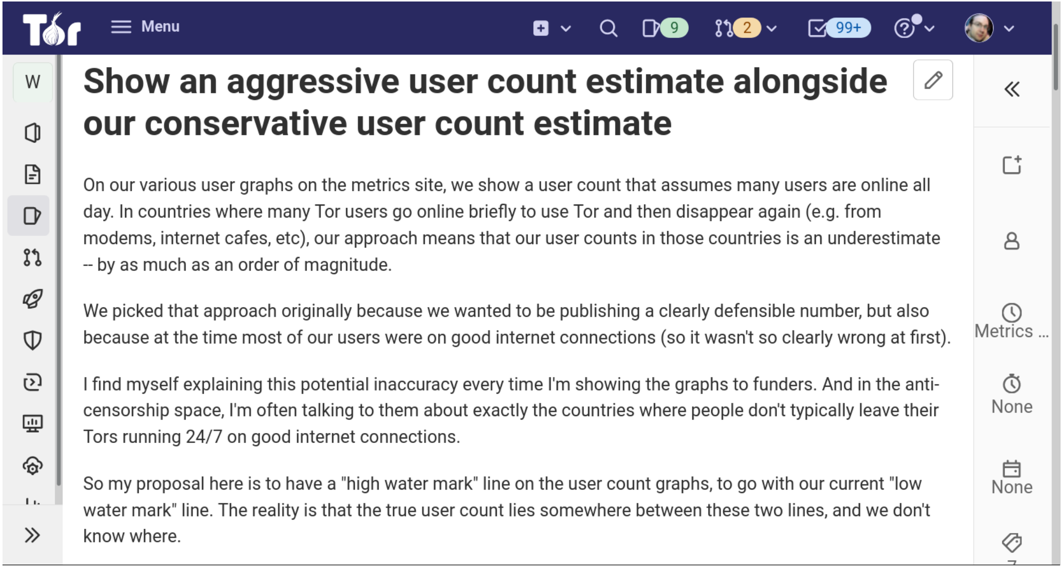


The Tor Project - https://metrics.torproject.org/



Bridge users by transport from Russia

The Tor Project - https://metrics.torproject.org/



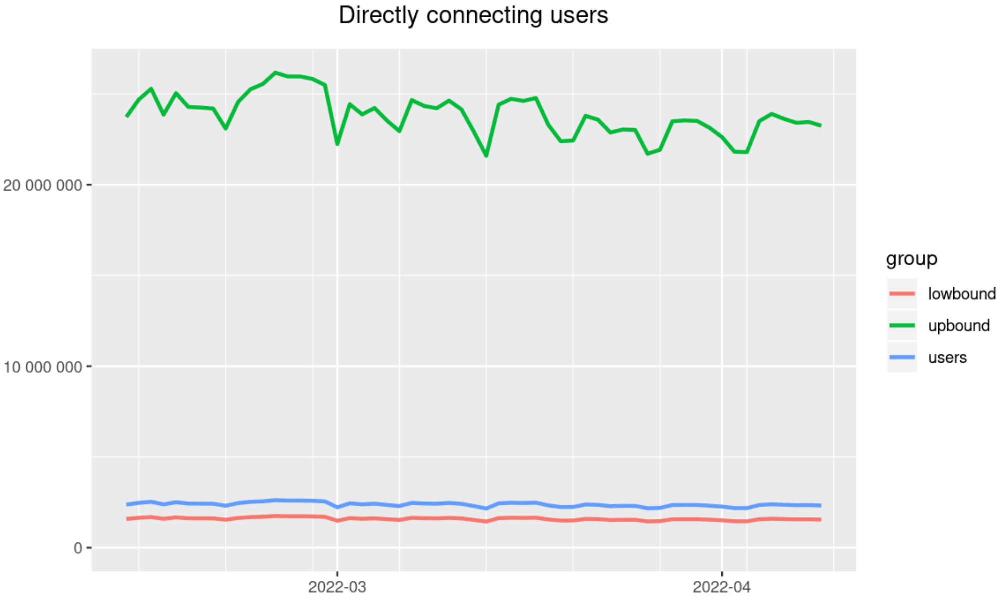
Show an aggressive user count estimate alongside our conservative user count estimate

On our various user graphs on the metrics site, we show a user count that assumes many users are online all day. In countries where many Tor users go online briefly to use Tor and then disappear again (e.g. from modems, internet cafes, etc), our approach means that our user counts in those countries is an underestimate -- by as much as an order of magnitude.

We picked that approach originally because we wanted to be publishing a clearly defensible number, but also because at the time most of our users were on good internet connections (so it wasn't so clearly wrong at first).

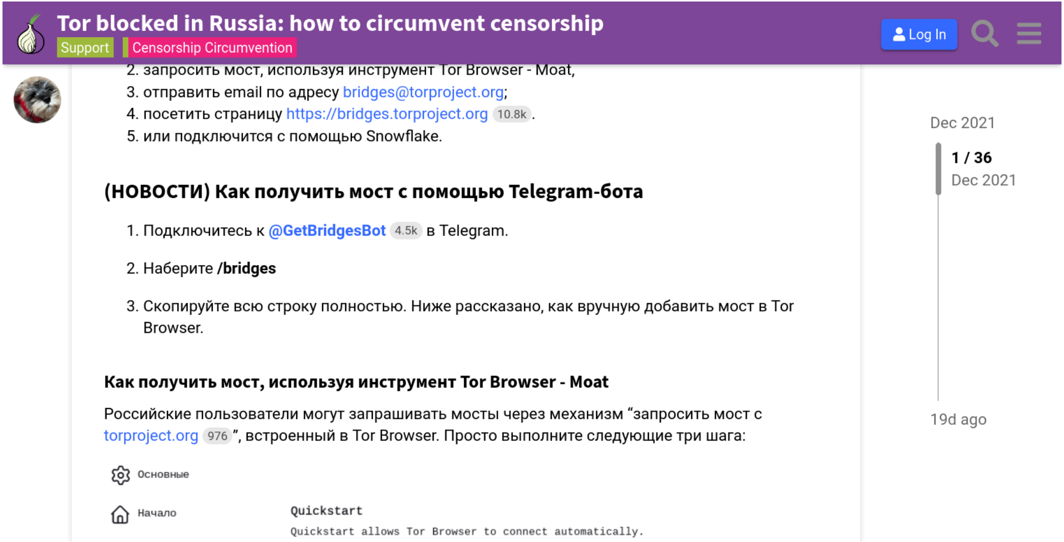
I find myself explaining this potential inaccuracy every time I'm showing the graphs to funders. And in the anti-censorship space, I'm often talking to them about exactly the countries where people don't typically leave their Tors running 24/7 on good internet connections.

So my proposal here is to have a "high water mark" line on the user count graphs, to go with our current "low water mark" line. The reality is that the true user count lies somewhere between these two lines, and we don't know where.



The Tor Project - https://metrics.torproject.org/

Telegram-based bridge distribution



Tor blocked in Russia: how to circumvent censorship

2. запросить мост, используя инструмент Tor Browser - Moat,
3. отправить email по адресу bridges@torproject.org;
4. посетить страницу https://bridges.torproject.org 10.8k.
5. или подключится с помощью Snowflake.

(НОВОСТИ) Как получить мост с помощью Telegram-бота

1. Подключитесь к **@GetBridgesBot** 4.5k в Telegram.

2. Наберите **/bridges**

3. Скопируйте всю строку полностью. Ниже рассказано, как вручную добавить мост в Tor Browser.

Как получить мост, используя инструмент Tor Browser - Moat

Российские пользователи могут запрашивать мосты через механизм “запросить мост с torproject.org 976”, встроенный в Tor Browser. Просто выполните следующие три шага:

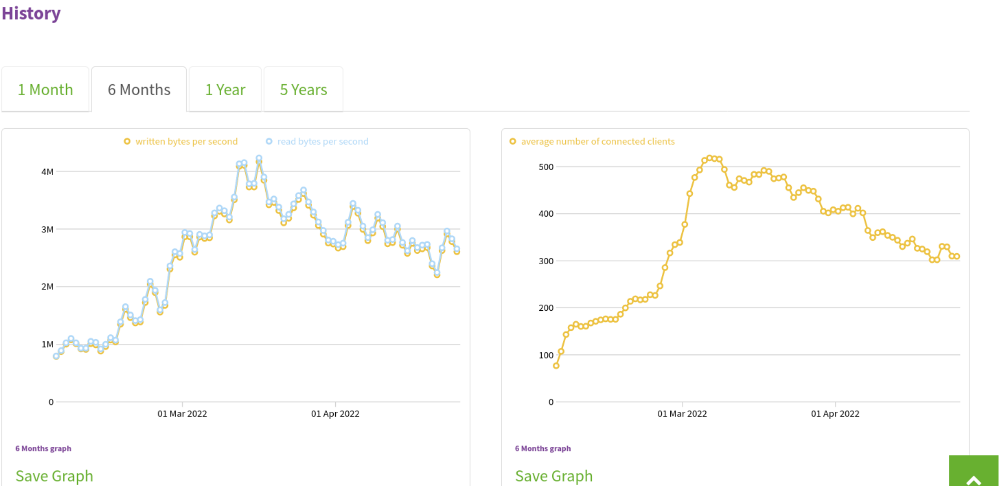
Quickstart

Quickstart allows Tor Browser to connect automatically.

Insider information

<redacted>

A popular telegram-distributed obfs4 bridge

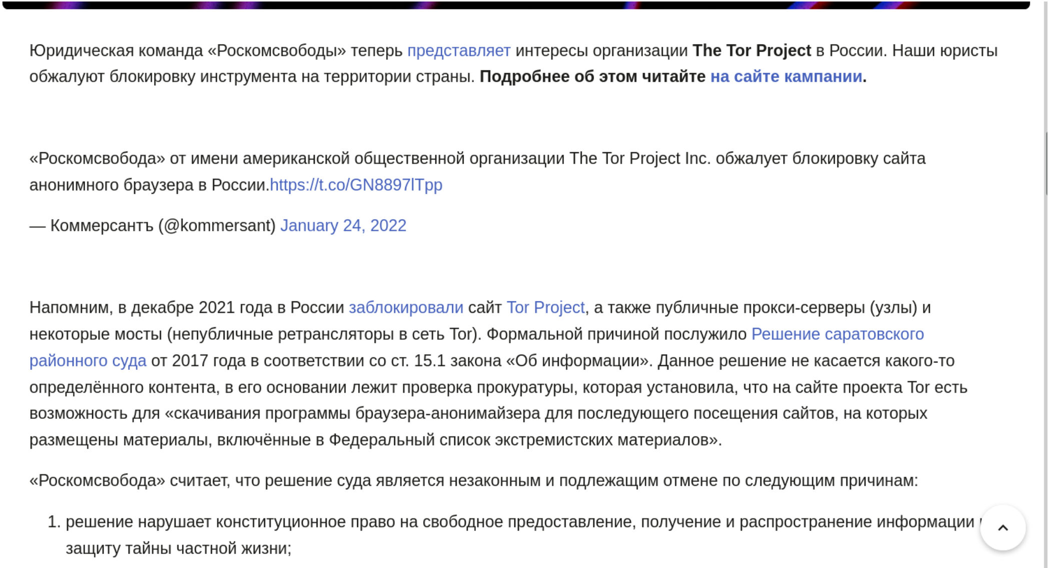


History

6 Months graph

6 Months graph

Challenging the censorship legally



Юридическая команда «Роскомсвободы» теперь представляет интересы организации **The Tor Project** в России. Наши юристы обжалуют блокировку инструмента на территории страны. **Подробнее об этом читайте на сайте кампании.**

«Роскомсвобода» от имени американской общественной организации The Tor Project Inc. обжалует блокировку сайта анонимного браузера в России.https://t.co/GN8897lTpp

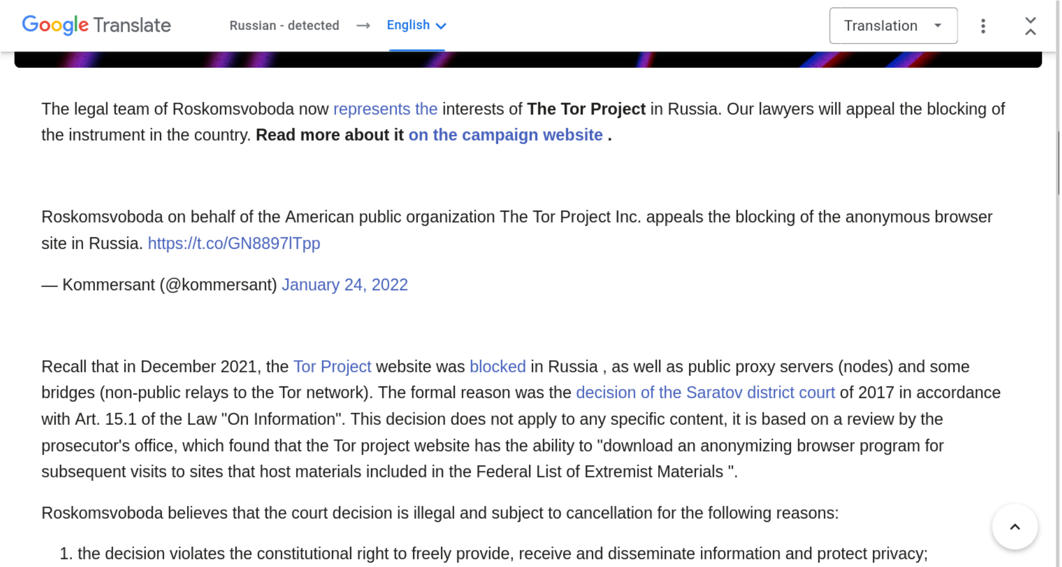
— Коммерсантъ (@kommersant) January 24, 2022

Напомним, в декабре 2021 года в России заблокировали сайт Tor Project, а также публичные прокси-серверы (узлы) и некоторые мосты (непубличные ретрансляторы в сеть Tor). Формальной причиной послужило Решение саратовского районного суда от 2017 года в соответствии со ст. 15.1 закона «Об информации». Данное решение не касается какого-то определённого контента, в его основании лежит проверка прокуратуры, которая установила, что на сайте проекта Tor есть возможность для «скачивания программы браузера-анонимайзера для последующего посещения сайтов, на которых размещены материалы, включённые в Федеральный список экстремистских материалов».

«Роскомсвобода» считает, что решение суда является незаконным и подлежащим отмене по следующим причинам:

1. решение нарушает конституционное право на свободное предоставление, получение и распространение информации и защиту тайны частной жизни;

Challenging the censorship legally



The legal team of Roskomsvoboda now represents the interests of **The Tor Project** in Russia. Our lawyers will appeal the blocking of the instrument in the country. **Read more about it on the campaign website .**

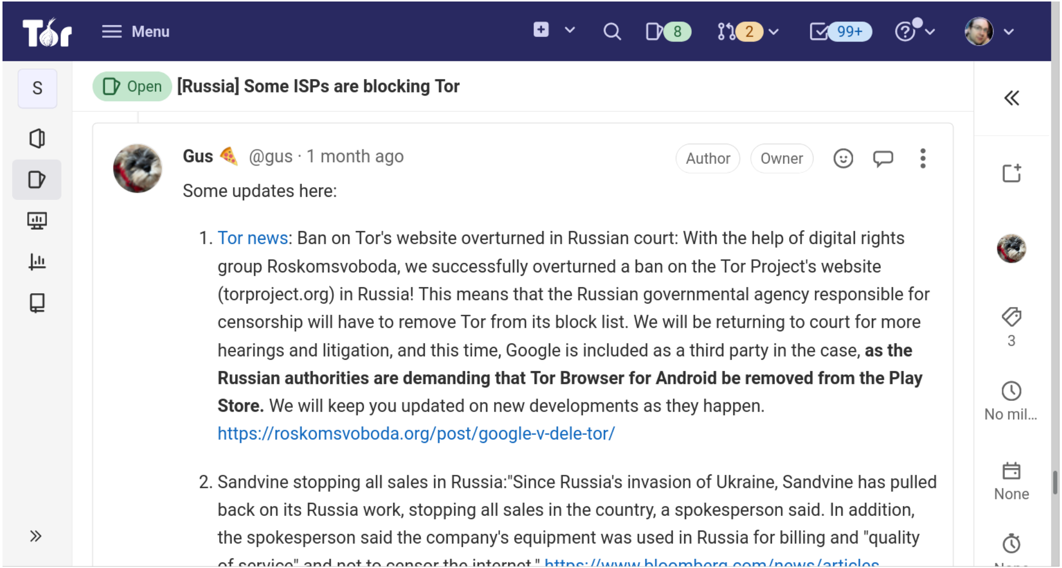
Roskomsvoboda on behalf of the American public organization The Tor Project Inc. appeals the blocking of the anonymous browser site in Russia. https://t.co/GN8897ITpp

— Kommersant (@kommersant) January 24, 2022

Recall that in December 2021, the Tor Project website was blocked in Russia , as well as public proxy servers (nodes) and some bridges (non-public relays to the Tor network). The formal reason was the decision of the Saratov district court of 2017 in accordance with Art. 15.1 of the Law "On Information". This decision does not apply to any specific content, it is based on a review by the prosecutor's office, which found that the Tor project website has the ability to "download an anonymizing browser program for subsequent visits to sites that host materials included in the Federal List of Extremist Materials ".

Roskomsvoboda believes that the court decision is illegal and subject to cancellation for the following reasons:

1. the decision violates the constitutional right to freely provide, receive and disseminate information and protect privacy;



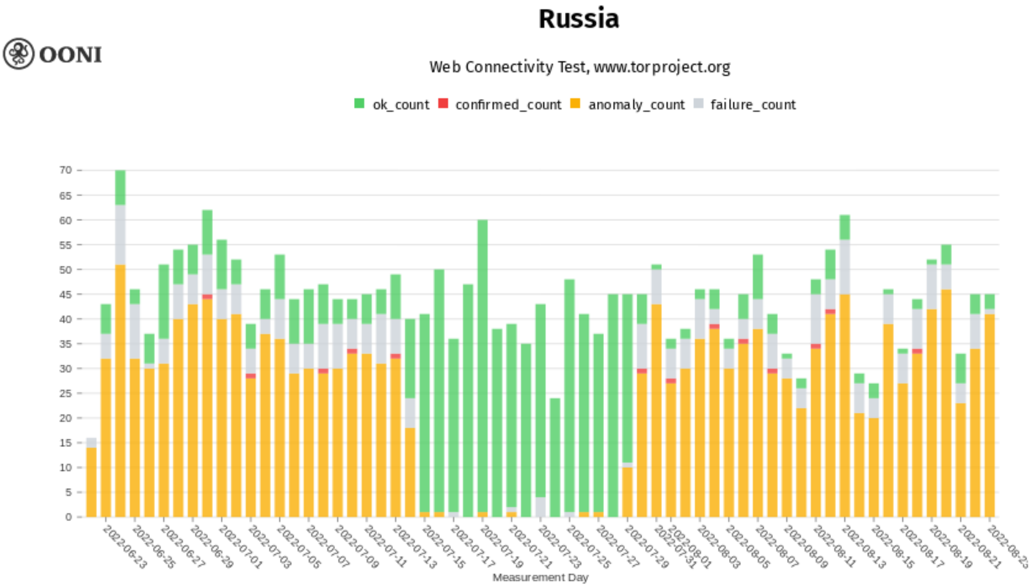
Open [Russia] Some ISPs are blocking Tor

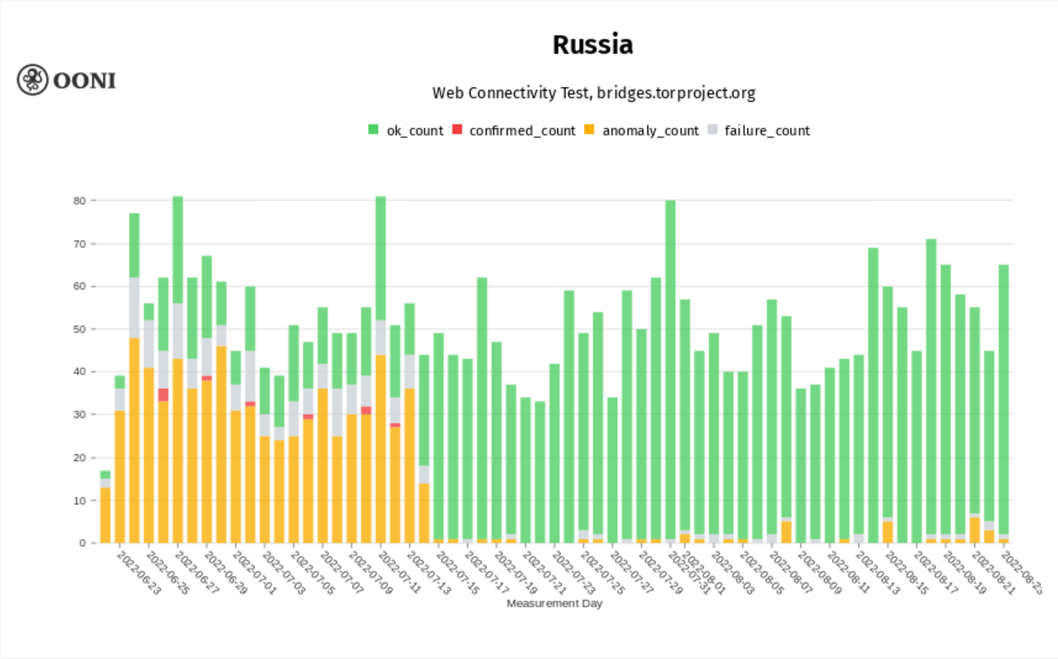
Gus 🍕 @gus · 1 month ago

Some updates here:

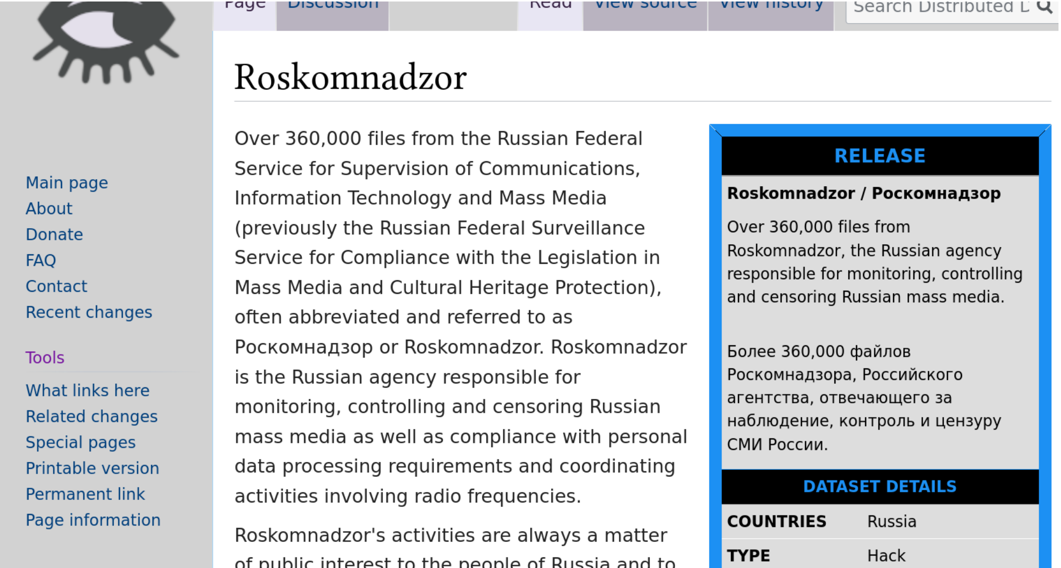
1. Tor news: Ban on Tor's website overturned in Russian court: With the help of digital rights group Roskomsvoboda, we successfully overturned a ban on the Tor Project's website (torproject.org) in Russia! This means that the Russian governmental agency responsible for censorship will have to remove Tor from its block list. We will be returning to court for more hearings and litigation, and this time, Google is included as a third party in the case, **as the Russian authorities are demanding that Tor Browser for Android be removed from the Play Store.** We will keep you updated on new developments as they happen. https://roskomsvoboda.org/post/google-v-dele-tor/

2. Sandvine stopping all sales in Russia:"Since Russia's invasion of Ukraine, Sandvine has pulled back on its Russia work, stopping all sales in the country, a spokesperson said. In addition, the spokesperson said the company's equipment was used in Russia for billing and "quality of service" and not to censor the internet." https://www.bloomberg.com/news/articles


OONI
Russia
Web Connectivity Test, www.torproject.org
ok_count
confirmed_count
anomaly_count
failure_count
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
2022-06-23
2022-06-25
2022-06-27
2022-06-29
2022-07-01
2022-07-03
2022-07-05
2022-07-07
2022-07-09
2022-07-11
2022-07-13
2022-07-15
2022-07-17
2022-07-19
2022-07-21
2022-07-23
2022-07-25
2022-07-27
2022-07-29
2022-07-31
2022-08-01
2022-08-03
2022-08-05
2022-08-07
2022-08-09
2022-08-11
2022-08-13
2022-08-15
2022-08-17
2022-08-19
2022-08-21
2022-08-2
Measurement Day


OONI
Russia
Web Connectivity Test, bridges.torproject.org
🟩 ok_count
🟥 confirmed_count
🟧 anomaly_count
⬜ failure_count
80
70
60
50
40
30
20
10
0
2022-06-23
2022-06-25
2022-06-27
2022-06-29
2022-07-01
2022-07-03
2022-07-05
2022-07-07
2022-07-09
2022-07-11
2022-07-13
2022-07-15
2022-07-17
2022-07-19
2022-07-21
2022-07-23
2022-07-25
2022-07-27
2022-07-29
2022-07-31
2022-08-01
2022-08-03
2022-08-05
2022-08-07
2022-08-09
2022-08-11
2022-08-13
2022-08-15
2022-08-17
2022-08-19
2022-08-21
2022-08-2
Measurement Day

Censorship authority dox (via DDoSecrets)



Roskomnadzor

Over 360,000 files from the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (previously the Russian Federal Surveillance Service for Compliance with the Legislation in Mass Media and Cultural Heritage Protection), often abbreviated and referred to as Роскомнадзор or Roskomnadzor. Roskomnadzor is the Russian agency responsible for monitoring, controlling and censoring Russian mass media as well as compliance with personal data processing requirements and coordinating activities involving radio frequencies.

Roskomnadzor's activities are always a matter of public interest to the people of Russia and to

RELEASE

Roskomnadzor / Роскомнадзор

Over 360,000 files from Roskomnadzor, the Russian agency responsible for monitoring, controlling and censoring Russian mass media.

Более 360,000 файлов Роскомнадзора, Российского агентства, отвечающего за наблюдение, контроль и цензуру СМИ России.

DATASET DETAILS

COUNTRIES	Russia
TYPE	Hack

Russia censorship into 2023

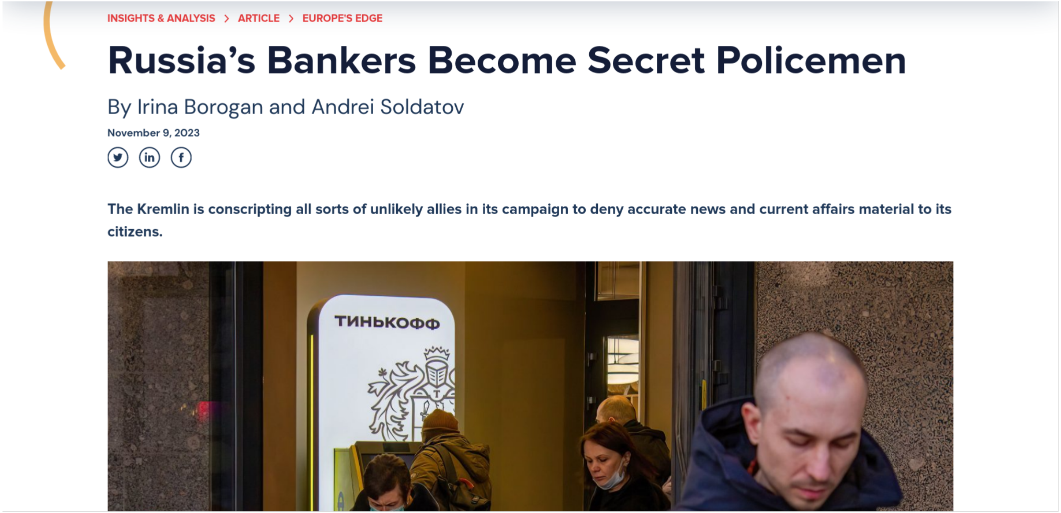
Russia inconsistently crawling all three legacy categories of obfs4 bridges (moat, https, email)

But still not instantaneous: new bridges last days to weeks

Other obfs4 bridges still work fine

Snowflake and meek continue to work, but are slower

Punishing credit card VPN payments



INSIGHTS & ANALYSIS > ARTICLE > EUROPE'S EDGE

Russia’s Bankers Become Secret Policemen

By Irina Borogan and Andrei Soldatov

November 9, 2023

The Kremlin is conscripting all sorts of unlikely allies in its campaign to deny accurate news and current affairs material to its citizens.

Outline

~~(1) Intro to Tor~~

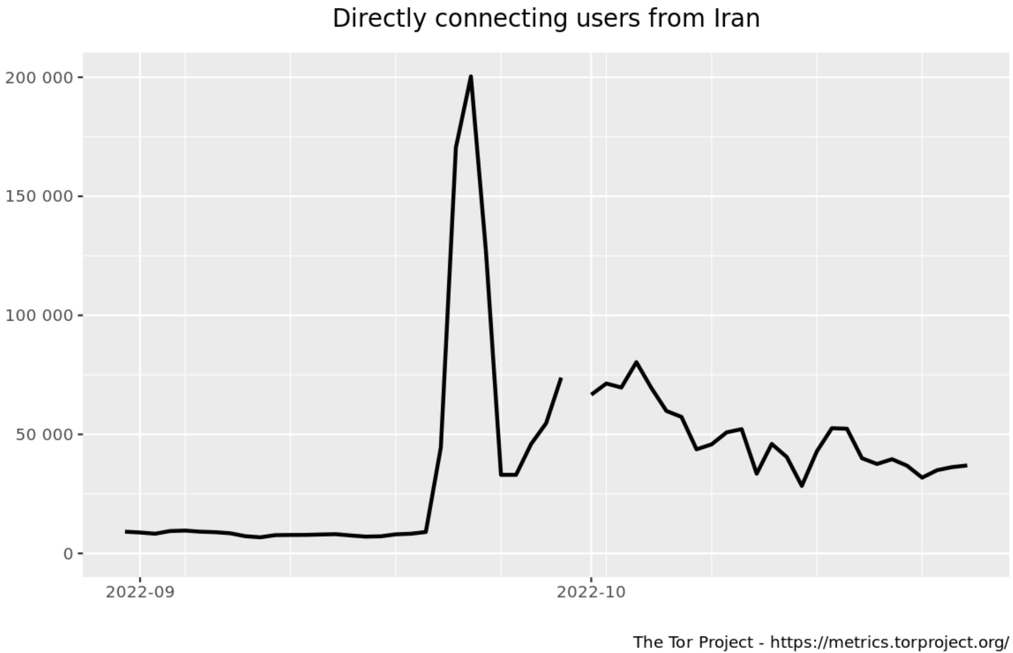
~~(2) Intro to Tor and censorship resistance~~

~~(3) Russia~~

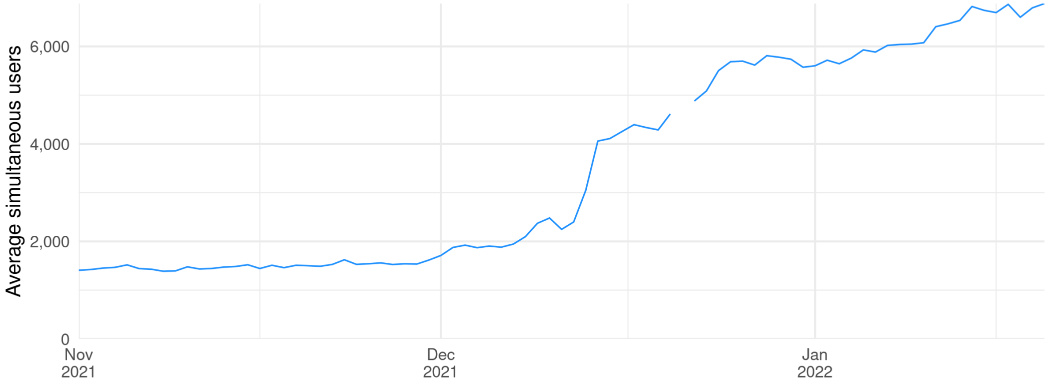
(4) Iran

(5) Turkmenistan

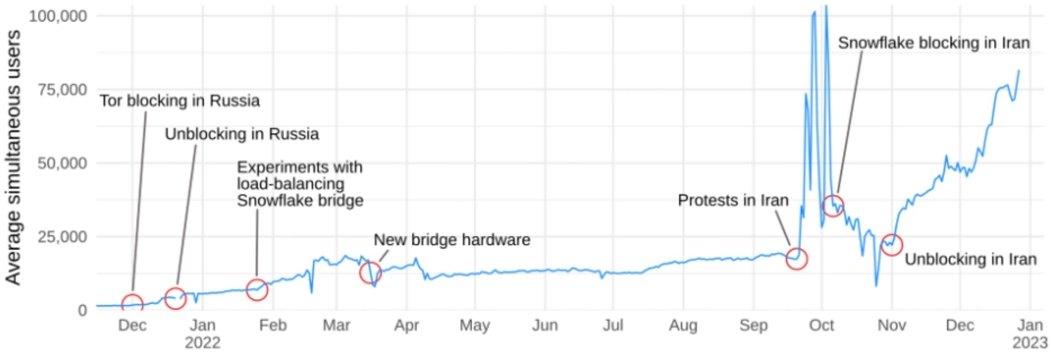
(6) Bigger context

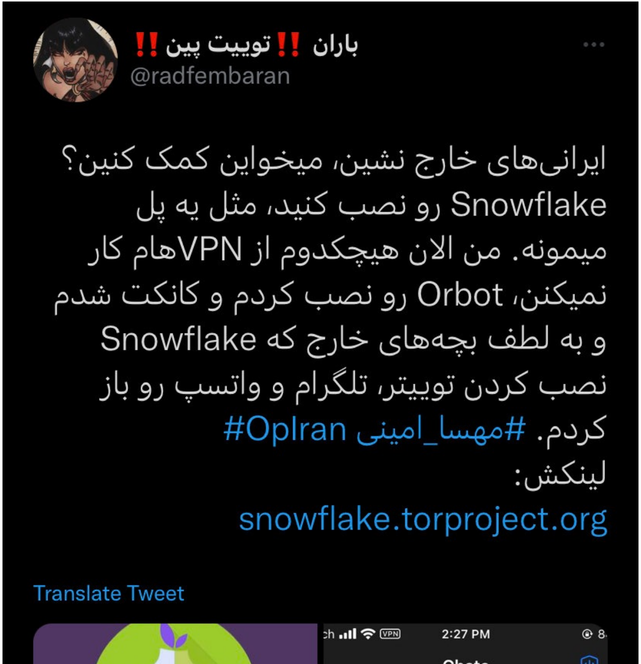

Directly connecting users from Iran
200 000
150 000
100 000
50 000
0
2022-09
2022-10
The Tor Project - https://metrics.torproject.org/

Snowflake users under Russia censorship



Daily Snowflake users in 2022

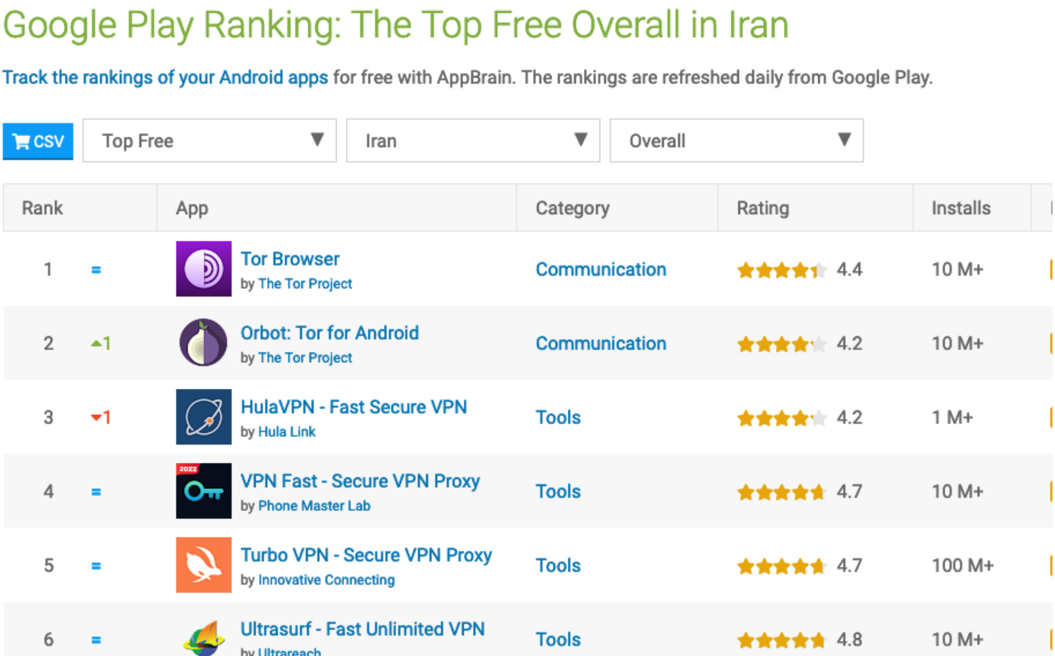




باران ‼ توییت پین ‼
@radfembaran

ایرانی‌های خارج نشین، میخواین کمک کنین؟
Snowflake رو نصب کنید، مثل یه پل
میمونه. من الان هیچکدوم از VPNهام کار
نمیکنن، Orbot رو نصب کردم و کانکت شدم
و به لطف بچه‌های خارج که Snowflake
نصب کردن توییتر، تلگرام و واتسپ رو باز
کردم. #مهسا_امینی #OpIran
لینکش:
snowflake.torproject.org

Translate Tweet

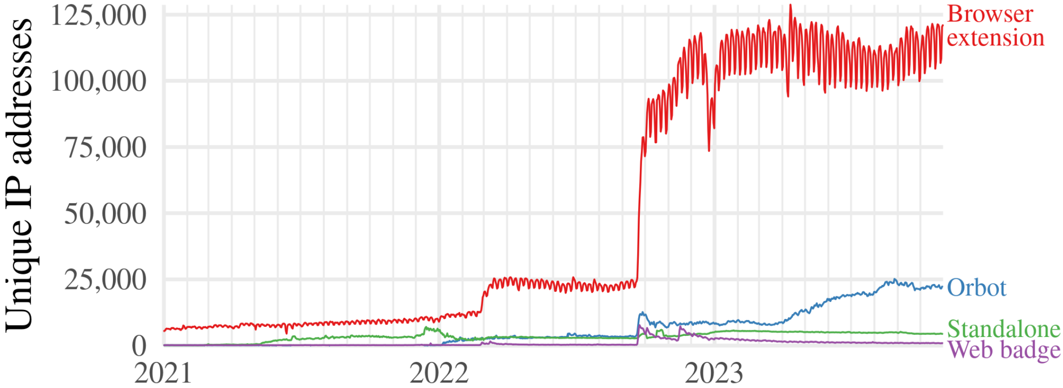


Google Play Ranking: The Top Free Overall in Iran

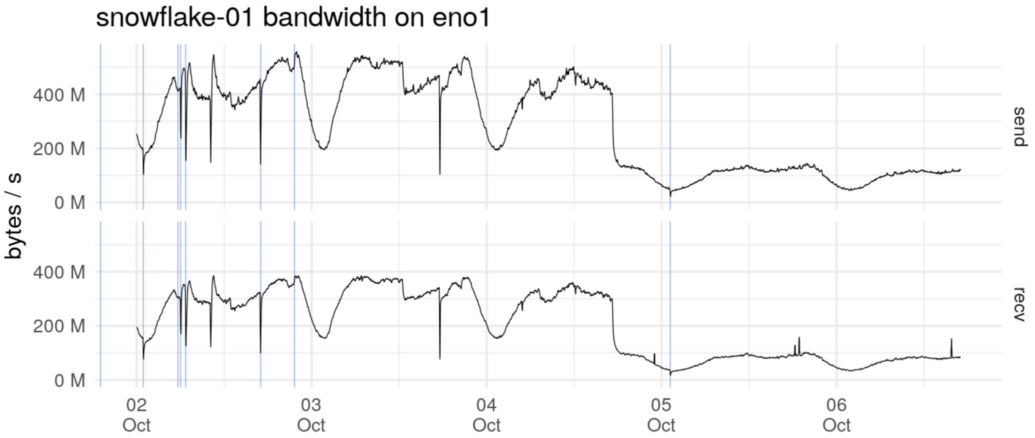
Track the rankings of your Android apps for free with AppBrain. The rankings are refreshed daily from Google Play.

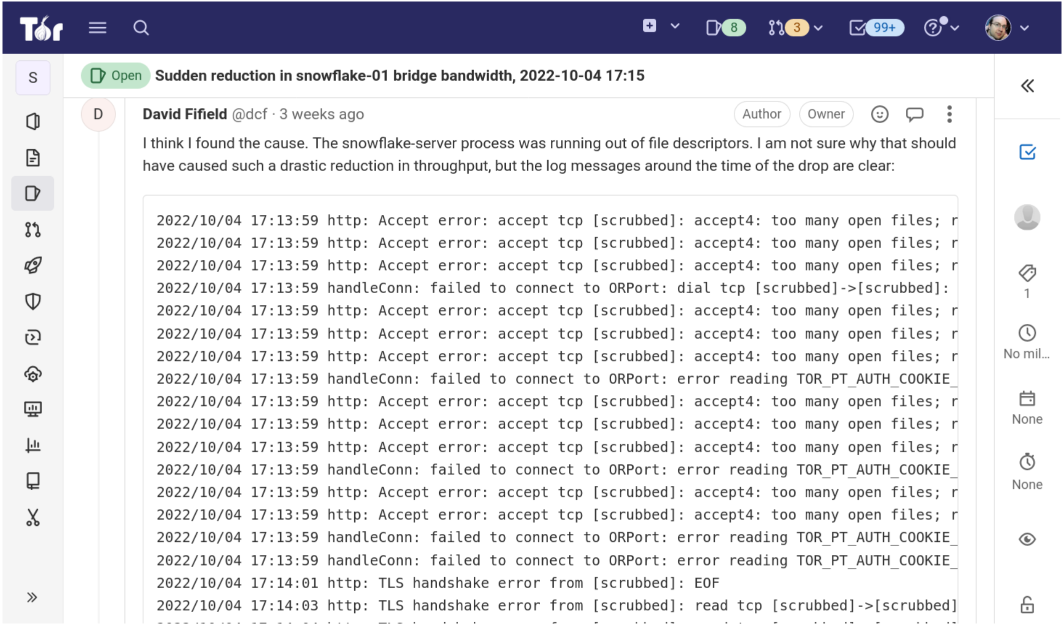
Rank	App	Category	Rating	Installs
1 =	Tor Browser by The Tor Project	Communication	4.4	10 M+
2 ▲1	Orbot: Tor for Android by The Tor Project	Communication	4.2	10 M+
3 ▼1	HulaVPN - Fast Secure VPN by Hula Link	Tools	4.2	1 M+
4 =	VPN Fast - Secure VPN Proxy by Phone Master Lab	Tools	4.7	10 M+
5 =	Turbo VPN - Secure VPN Proxy by Innovative Connecting	Tools	4.7	100 M+
6 =	Ultrasurf - Fast Unlimited VPN by Ultrareach	Tools	4.8	10 M+

Snowflake volunteers



Snowflake activity reported by back-end server



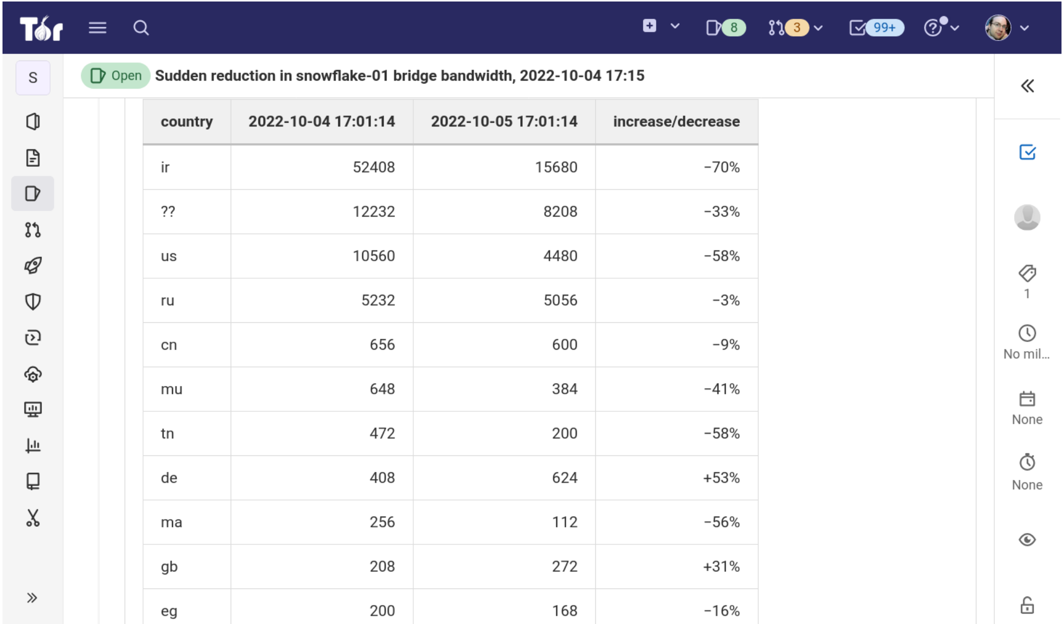


Sudden reduction in snowflake-01 bridge bandwidth, 2022-10-04 17:15

David Fifield @dcf · 3 weeks ago

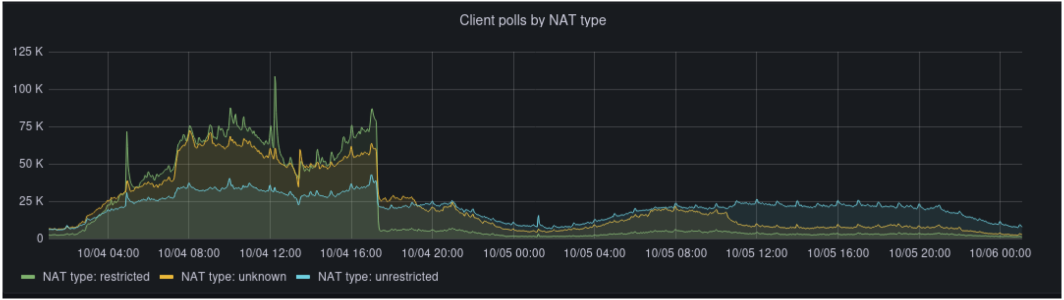
I think I found the cause. The snowflake-server process was running out of file descriptors. I am not sure why that should have caused such a drastic reduction in throughput, but the log messages around the time of the drop are clear:

```
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 handleConn: failed to connect to ORPort: dial tcp [scrubbed]->[scrubbed]:
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 handleConn: failed to connect to ORPort: error reading TOR_PT_AUTH_COOKIE_
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 handleConn: failed to connect to ORPort: error reading TOR_PT_AUTH_COOKIE_
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 http: Accept error: accept tcp [scrubbed]: accept4: too many open files; r
2022/10/04 17:13:59 handleConn: failed to connect to ORPort: error reading TOR_PT_AUTH_COOKIE_
2022/10/04 17:13:59 handleConn: failed to connect to ORPort: error reading TOR_PT_AUTH_COOKIE_
2022/10/04 17:14:01 http: TLS handshake error from [scrubbed]: EOF
2022/10/04 17:14:03 http: TLS handshake error from [scrubbed]: read tcp [scrubbed]->[scrubbed]
```

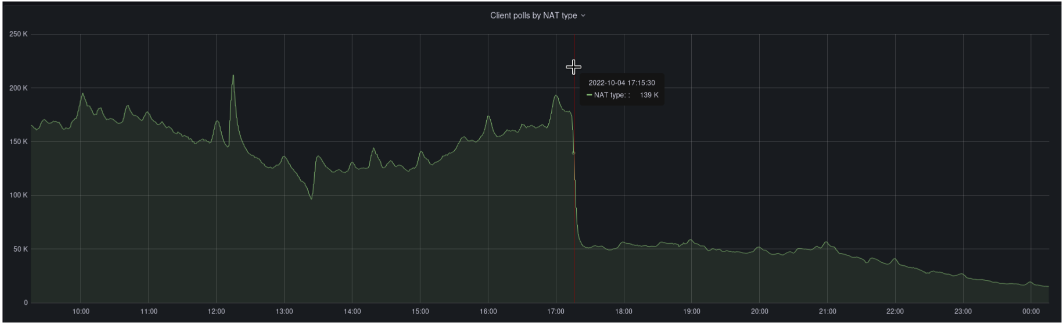


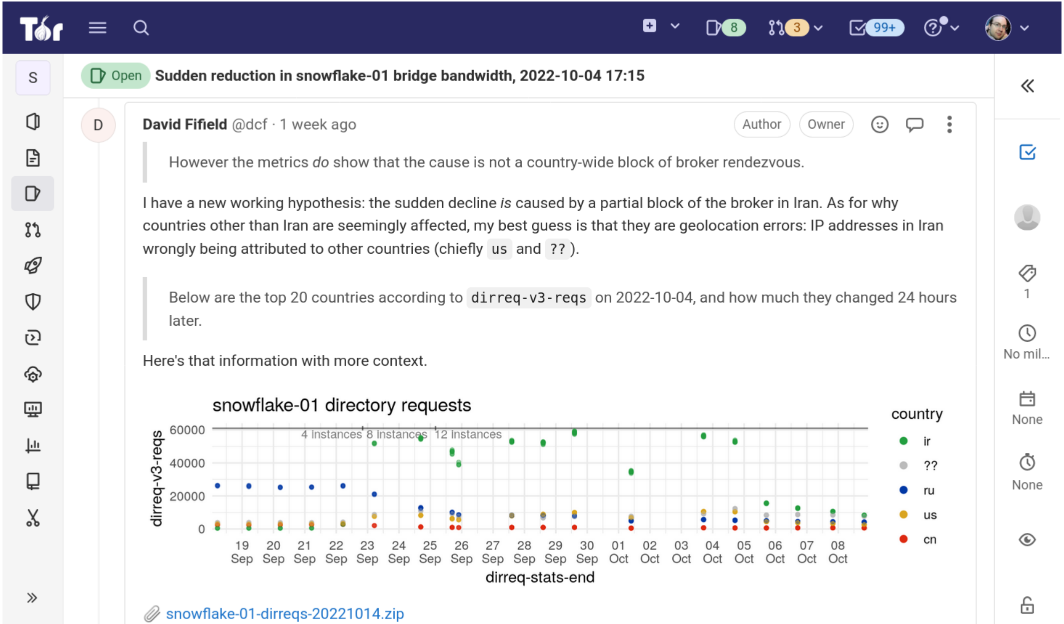
Open Sudden reduction in snowflake-01 bridge bandwidth, 2022-10-04 17:15

country	2022-10-04 17:01:14	2022-10-05 17:01:14	increase/decrease
ir	52408	15680	−70%
??	12232	8208	−33%
us	10560	4480	−58%
ru	5232	5056	−3%
cn	656	600	−9%
mu	648	384	−41%
tn	472	200	−58%
de	408	624	+53%
ma	256	112	−56%
gb	208	272	+31%
eg	200	168	−16%


Client polls by NAT type
125 K
100 K
75 K
50 K
25 K
0
10/04 04:00
10/04 08:00
10/04 12:00
10/04 16:00
10/04 20:00
10/05 00:00
10/05 04:00
10/05 08:00
10/05 12:00
10/05 16:00
10/05 20:00
10/06 00:00
NAT type: restricted
NAT type: unknown
NAT type: unrestricted

number of clients contacting the Snowflake broker





Open **Sudden reduction in snowflake-01 bridge bandwidth, 2022-10-04 17:15**

David Fifield @dcf · 1 week ago

Author Owner

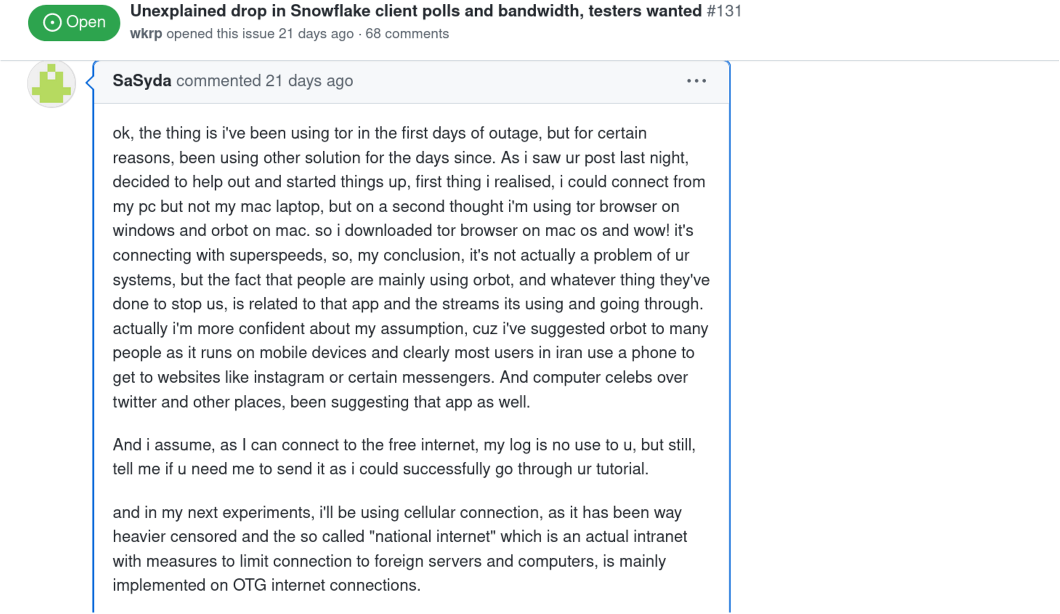
> However the metrics *do* show that the cause is not a country-wide block of broker rendezvous.

I have a new working hypothesis: the sudden decline *is* caused by a partial block of the broker in Iran. As for why countries other than Iran are seemingly affected, my best guess is that they are geolocation errors: IP addresses in Iran wrongly being attributed to other countries (chiefly `us` and `??`).

> Below are the top 20 countries according to `dirreq-v3-reqs` on 2022-10-04, and how much they changed 24 hours later.

Here's that information with more context.

snowflake-01-dirreqs-20221014.zip



Unexplained drop in Snowflake client polls and bandwidth, testers wanted #131

wkrp opened this issue 21 days ago · 68 comments

SaSyda commented 21 days ago

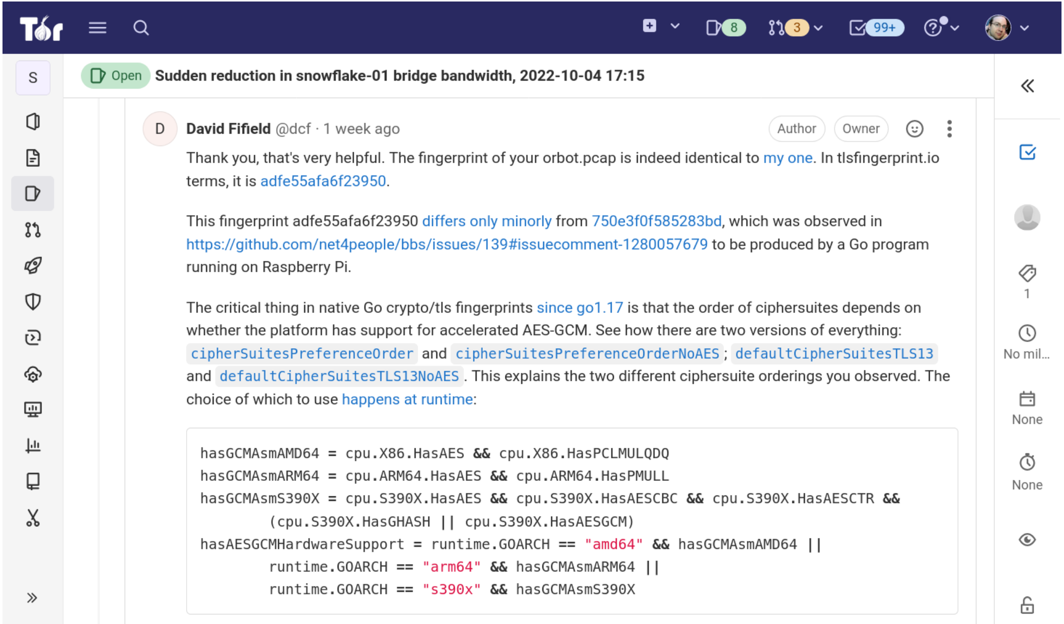
ok, the thing is i've been using tor in the first days of outage, but for certain reasons, been using other solution for the days since. As i saw ur post last night, decided to help out and started things up, first thing i realised, i could connect from my pc but not my mac laptop, but on a second thought i'm using tor browser on windows and orbot on mac. so i downloaded tor browser on mac os and wow! it's connecting with superspeeds, so, my conclusion, it's not actually a problem of ur systems, but the fact that people are mainly using orbot, and whatever thing they've done to stop us, is related to that app and the streams its using and going through. actually i'm more confident about my assumption, cuz i've suggested orbot to many people as it runs on mobile devices and clearly most users in iran use a phone to get to websites like instagram or certain messengers. And computer celebs over twitter and other places, been suggesting that app as well.

And i assume, as I can connect to the free internet, my log is no use to u, but still, tell me if u need me to send it as i could successfully go through ur tutorial.

and in my next experiments, i'll be using cellular connection, as it has been way heavier censored and the so called "national internet" which is an actual intranet with measures to limit connection to foreign servers and computers, is mainly implemented on OTG internet connections.

Reachability testing from inside Iran

	Works?
Tor Browser Linux	yes
Tor Browser Android	yes
Orbot	yes
Orbot	no



Sudden reduction in snowflake-01 bridge bandwidth, 2022-10-04 17:15

D **David Fifield** @dcf · 1 week ago

Thank you, that's very helpful. The fingerprint of your orbot.pcap is indeed identical to my one. In tlsfingerprint.io terms, it is adfe55afa6f23950.

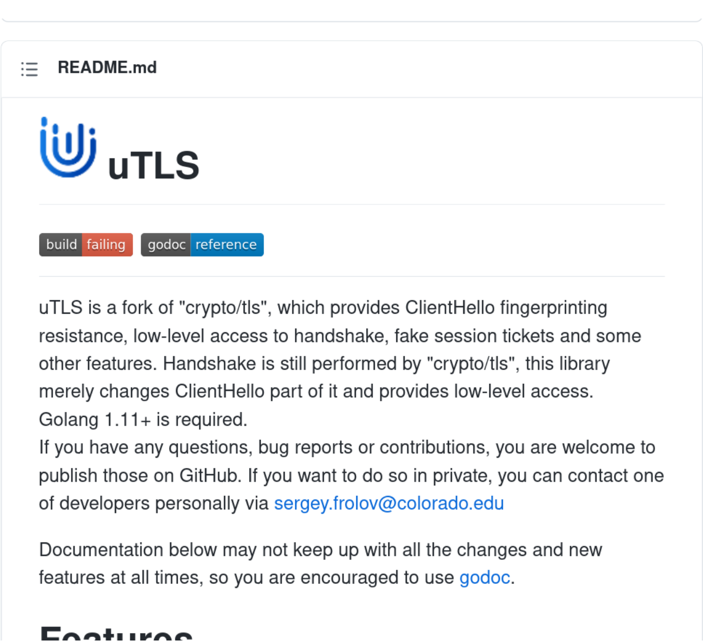
This fingerprint adfe55afa6f23950 differs only minorly from 750e3f0f585283bd, which was observed in https://github.com/net4people/bbs/issues/139#issuecomment-1280057679 to be produced by a Go program running on Raspberry Pi.

The critical thing in native Go crypto/tls fingerprints since go1.17 is that the order of ciphersuites depends on whether the platform has support for accelerated AES-GCM. See how there are two versions of everything: `cipherSuitesPreferenceOrder` and `cipherSuitesPreferenceOrderNoAES`; `defaultCipherSuitesTLS13` and `defaultCipherSuitesTLS13NoAES`. This explains the two different ciphersuite orderings you observed. The choice of which to use happens at runtime:

```
hasGCMAsmAMD64 = cpu.X86.HasAES && cpu.X86.HasPCLMULQDQ
hasGCMAsmARM64 = cpu.ARM64.HasAES && cpu.ARM64.HasPMULL
hasGCMAsmS390X = cpu.S390X.HasAES && cpu.S390X.HasAESCBC && cpu.S390X.HasAESCTR &&
        (cpu.S390X.HasGHASH || cpu.S390X.HasAESGCM)
hasAESGCMHardwareSupport = runtime.GOARCH == "amd64" && hasGCMAsmAMD64 ||
        runtime.GOARCH == "arm64" && hasGCMAsmARM64 ||
        runtime.GOARCH == "s390x" && hasGCMAsmS390X
```

Reachability testing from inside Iran

	Works?	
Tor Browser Linux	yes	⇐ go 1.17, AES-GCM
Tor Browser Android	yes	⇐ go 1.18, AES-GCM
Tor Browser Android	yes	⇐ go 1.18, no AES-GCM
Orbot	yes	⇐ go 1.17, AES-GCM
Orbot	no	⇐ go 1.17, no AES-GCM

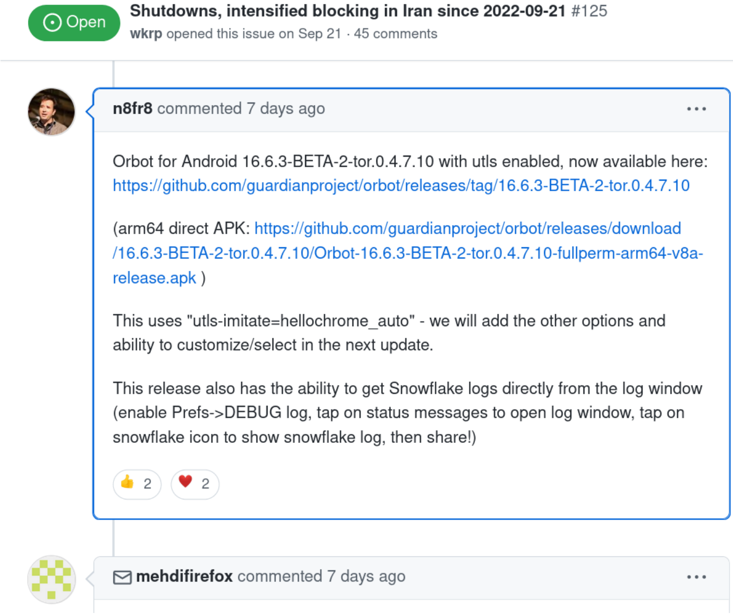


uTLS

uTLS is a fork of "crypto/tls", which provides ClientHello fingerprinting resistance, low-level access to handshake, fake session tickets and some other features. Handshake is still performed by "crypto/tls", this library merely changes ClientHello part of it and provides low-level access.
Golang 1.11+ is required.
If you have any questions, bug reports or contributions, you are welcome to publish those on GitHub. If you want to do so in private, you can contact one of developers personally via sergey.frolov@colorado.edu

Documentation below may not keep up with all the changes and new features at all times, so you are encouraged to use godoc.

Features



Shutdowns, intensified blocking in Iran since 2022-09-21 #125

wkrp opened this issue on Sep 21 · 45 comments

n8fr8 commented 7 days ago

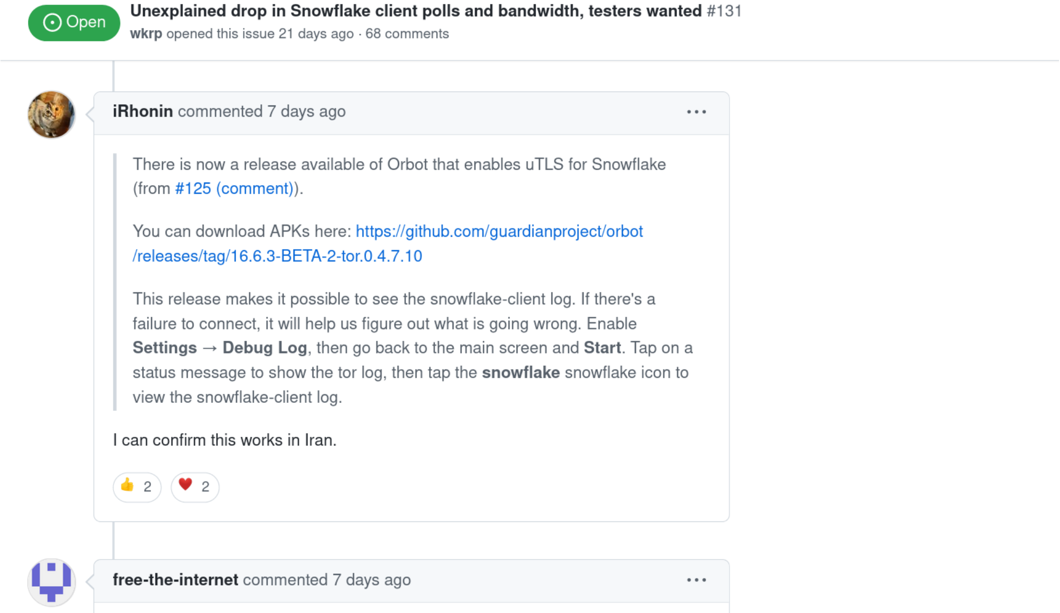
Orbot for Android 16.6.3-BETA-2-tor.0.4.7.10 with utls enabled, now available here: https://github.com/guardianproject/orbot/releases/tag/16.6.3-BETA-2-tor.0.4.7.10

(arm64 direct APK: https://github.com/guardianproject/orbot/releases/download/16.6.3-BETA-2-tor.0.4.7.10/Orbot-16.6.3-BETA-2-tor.0.4.7.10-fullperm-arm64-v8a-release.apk)

This uses "utls-imitate=hellochrome_auto" - we will add the other options and ability to customize/select in the next update.

This release also has the ability to get Snowflake logs directly from the log window (enable Prefs->DEBUG log, tap on status messages to open log window, tap on snowflake icon to show snowflake log, then share!)

mehdifirefox commented 7 days ago



○ Open **Unexplained drop in Snowflake client polls and bandwidth, testers wanted** #131

wkrp opened this issue 21 days ago · 68 comments

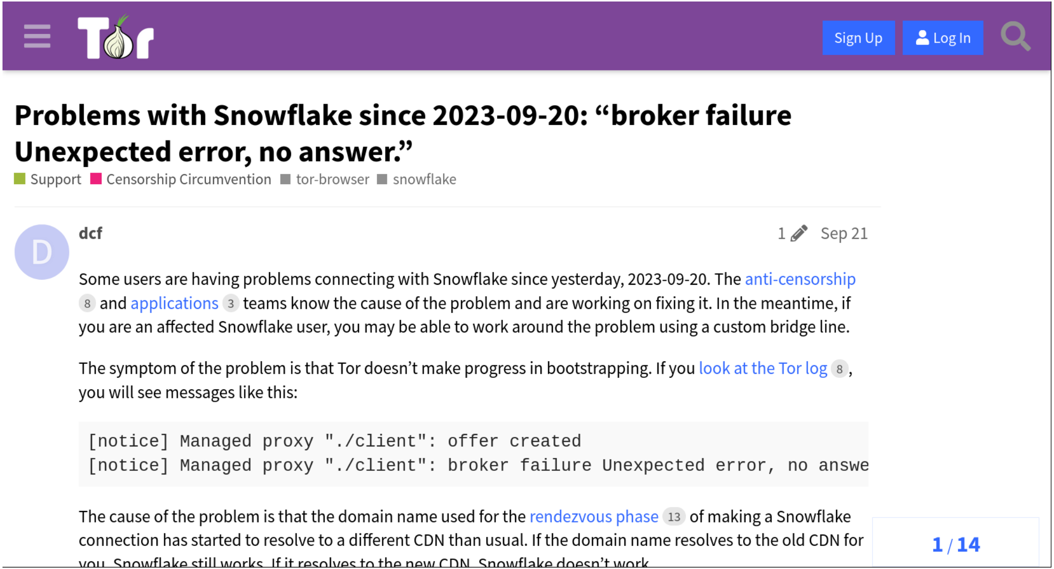
iRhonin commented 7 days ago ···

> There is now a release available of Orbot that enables uTLS for Snowflake (from #125 (comment)).
>
> You can download APKs here: https://github.com/guardianproject/orbot/releases/tag/16.6.3-BETA-2-tor.0.4.7.10
>
> This release makes it possible to see the snowflake-client log. If there's a failure to connect, it will help us figure out what is going wrong. Enable **Settings → Debug Log**, then go back to the main screen and **Start**. Tap on a status message to show the tor log, then tap the **snowflake** snowflake icon to view the snowflake-client log.

I can confirm this works in Iran.

👍 2 ❤️ 2

free-the-internet commented 7 days ago ···



Problems with Snowflake since 2023-09-20: “broker failure Unexpected error, no answer.”

🟩 Support 🟥 Censorship Circumvention ■ tor-browser ■ snowflake

dcf 1 ✎ Sep 21

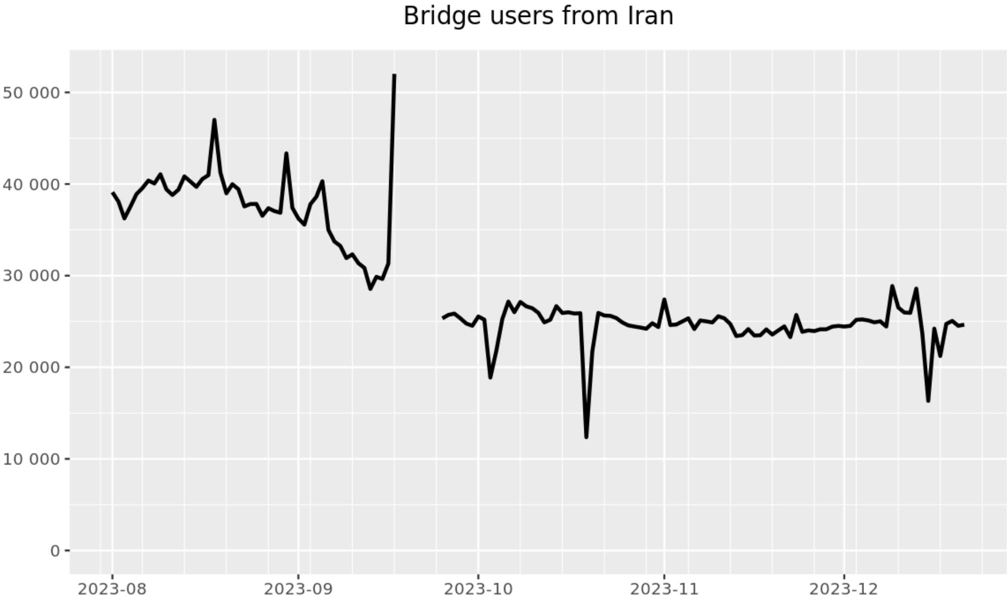
Some users are having problems connecting with Snowflake since yesterday, 2023-09-20. The anti-censorship 8 and applications 3 teams know the cause of the problem and are working on fixing it. In the meantime, if you are an affected Snowflake user, you may be able to work around the problem using a custom bridge line.

The symptom of the problem is that Tor doesn’t make progress in bootstrapping. If you look at the Tor log 8, you will see messages like this:

```
[notice] Managed proxy "./client": offer created
[notice] Managed proxy "./client": broker failure Unexpected error, no answe
```

The cause of the problem is that the domain name used for the rendezvous phase 13 of making a Snowflake connection has started to resolve to a different CDN than usual. If the domain name resolves to the old CDN for you, Snowflake still works. If it resolves to the new CDN, Snowflake doesn’t work

1 / 14



The Tor Project - https://metrics.torproject.org/

Down the road of the arms race (1/2)

Consider *user impact* from the censorship arms race.

Yes, we have steps to counter each step the censor takes. But as we move down that path, users have a higher burden to achieve a working connection.

Down the road of the arms race (2/2)

We see this user drop-off effect already, where the number of Tor users who switched over to bridges is impressive, but it’s definitely not all of them.

We need to find ways to reduce that burden, and/or slow down the arms race, else the censor wins because the average user won’t care enough to bother.

Outline

~~(1) Intro to Tor~~

~~(2) Intro to Tor and censorship resistance~~

~~(3) Russia~~

~~(4) Iran~~

(5) Turkmenistan

(6) Bigger context

Blocking in Turkmenistan

They block most cloud networks by IP address (!) so many circumvention components, such as Hetzner/OVH/Digital Ocean obfs4 bridges, are not reachable.

They filter most destination ports internet-wide, including default ports of Snowflake’s STUN servers.

Circumvention in Turkmenistan

We’ve been running a set of private port 8080 obfs4 bridges on residential addresses, reliably serving a community of human rights defenders.

meek-azure (domain fronting) often works, but doesn’t scale.

We set up a STUN server on port 8080 on a residential address, and it worked. Next stumbling block: volunteers are on censored addresses.

Turkmenistan censorship ministry

Happy to accept high collateral damage from blocking

So if you can pay to get ‘real’ internet, you will

We can’t solve this policy issue with technical tricks

Compare to recent bandwidth overload trend in China

Outline

~~(1) Intro to Tor~~

~~(2) Intro to Tor and censorship resistance~~

~~(3) Russia~~

~~(4) Iran~~

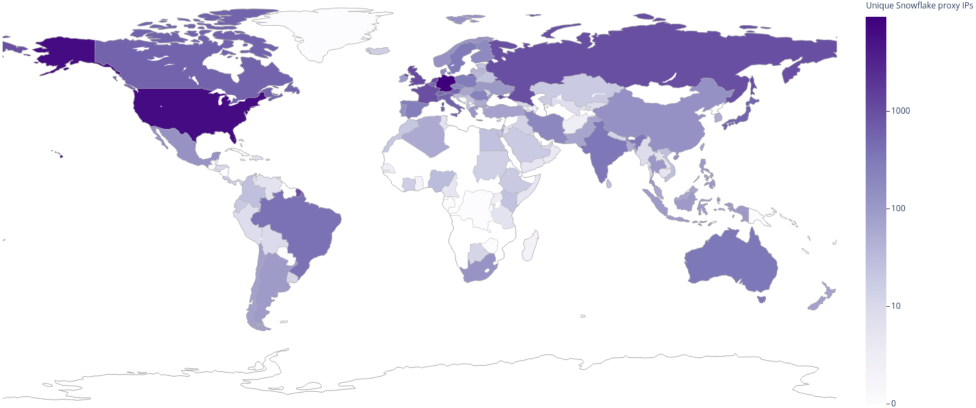
~~(5) Turkmenistan~~

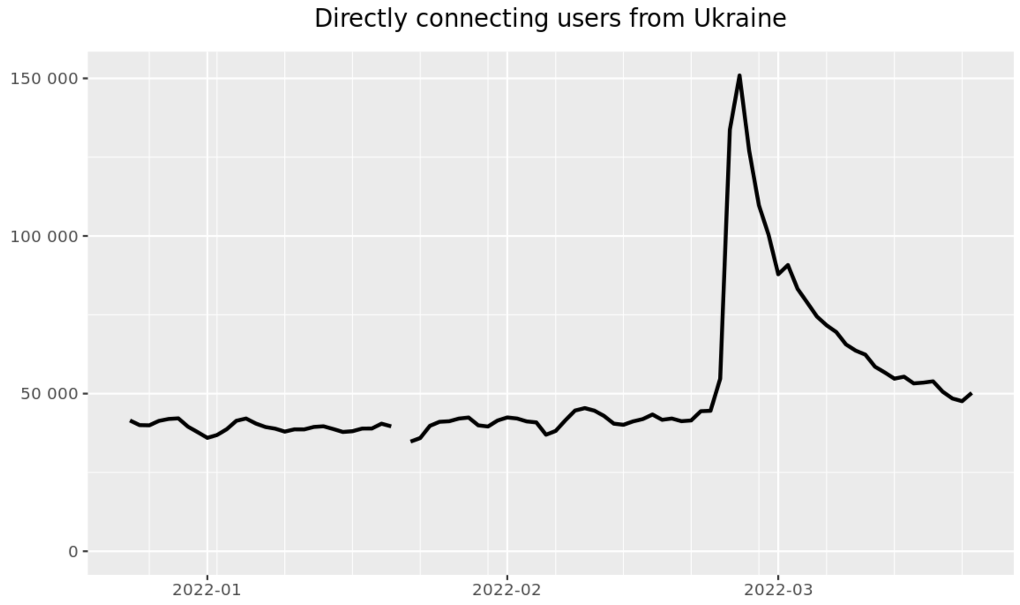
(6) Bigger context

Other surprises

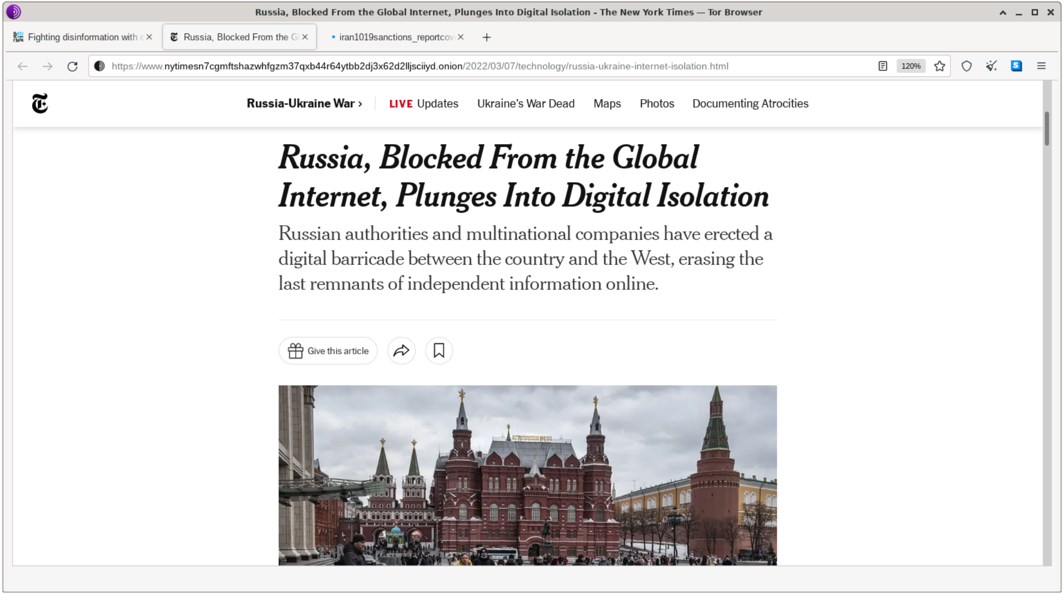
- rt.com censored from many Tor exits, because Europe (i.e. France, part of Germany, maybe more now?) pledged to censor it.
- Actually, many Tor exits can’t reach sites in Russia now, because the blocking is bidirectional?
- New groups of Russian and Ukrainian exit relays, “hmm”

Distribution of Snowflake proxies July 20 2022





The Tor Project - https://metrics.torproject.org/



Russia, Blocked From the Global Internet, Plunges Into Digital Isolation - The New York Times — Tor Browser

https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion/2022/03/07/technology/russia-ukraine-internet-isolation.html

Russia, Blocked From the Global Internet, Plunges Into Digital Isolation

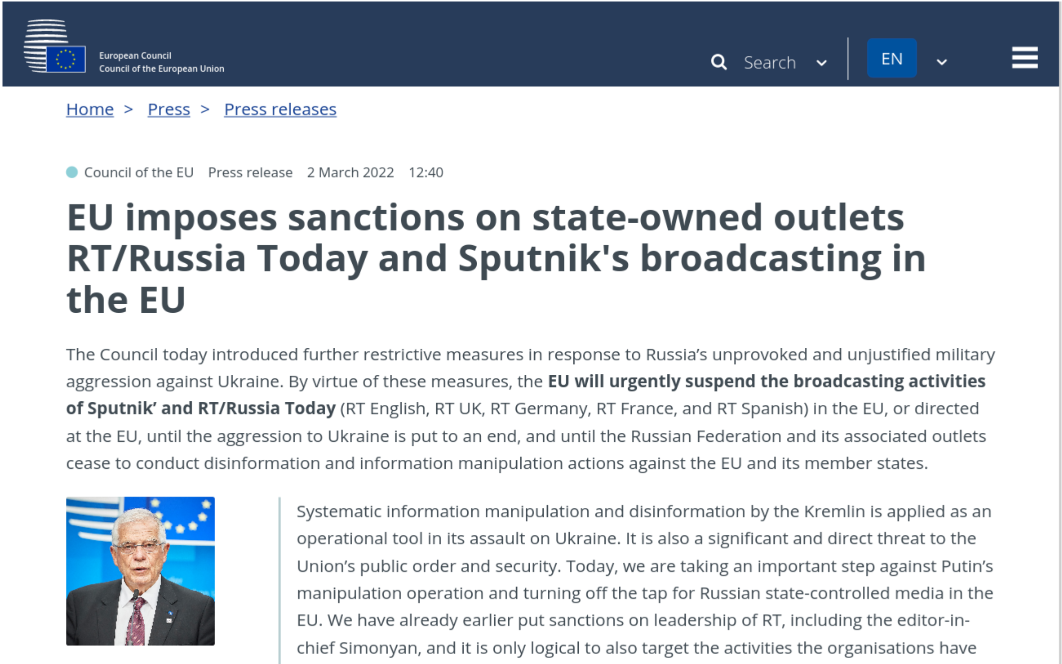
Russian authorities and multinational companies have erected a digital barricade between the country and the West, erasing the last remnants of independent information online.

First, a rant about sanctions

Especially about hurting internet connectivity for people in Russia as a way to punish their government.

Compare to the effects of Trump’s “maximum pressure” sanctions against Iran.

We will see the same outcome in Russia.



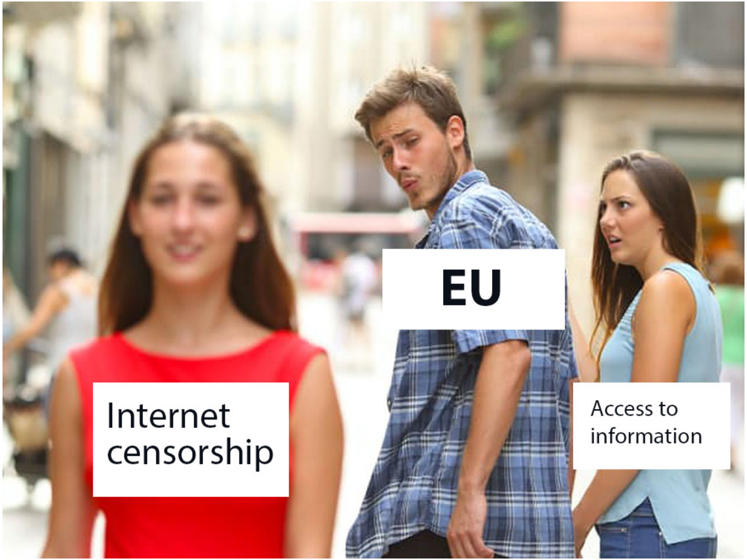
Home > Press > Press releases

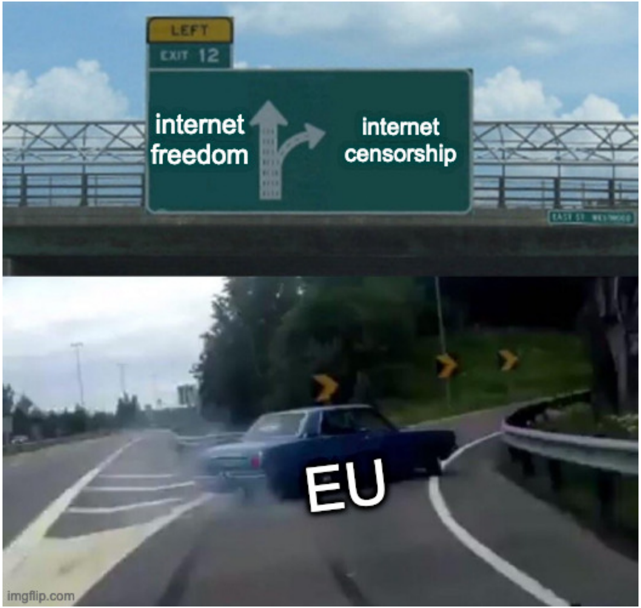
Council of the EU Press release 2 March 2022 12:40

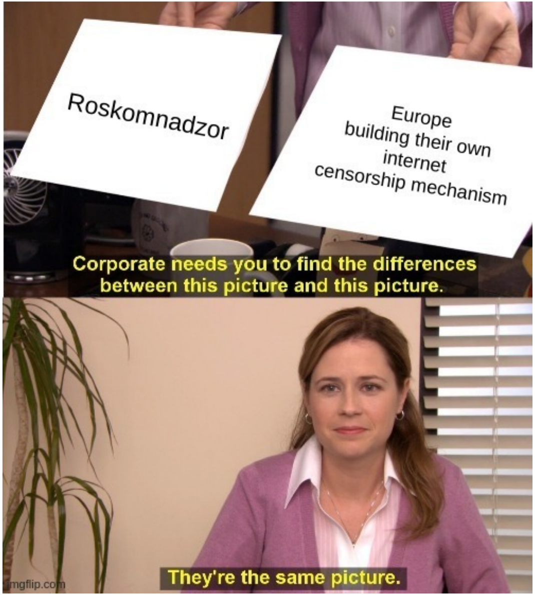
EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU

The Council today introduced further restrictive measures in response to Russia's unprovoked and unjustified military aggression against Ukraine. By virtue of these measures, the **EU will urgently suspend the broadcasting activities of Sputnik' and RT/Russia Today** (RT English, RT UK, RT Germany, RT France, and RT Spanish) in the EU, or directed at the EU, until the aggression to Ukraine is put to an end, and until the Russian Federation and its associated outlets cease to conduct disinformation and information manipulation actions against the EU and its member states.

> Systematic information manipulation and disinformation by the Kremlin is applied as an operational tool in its assault on Ukraine. It is also a significant and direct threat to the Union's public order and security. Today, we are taking an important step against Putin's manipulation operation and turning off the tap for Russian state-controlled media in the EU. We have already earlier put sanctions on leadership of RT, including the editor-in-chief Simonyan, and it is only logical to also target the activities the organisations have


Internet censorship
EU
Access to information


LEFT
EXIT 12
internet freedom
internet censorship
EU
imgflip.com


Roskomnadzor
Europe building their own internet censorship mechanism
Corporate needs you to find the differences between this picture and this picture.
They're the same picture.
imgflip.com

WTF Europe?? Why u like censoring so much??

Internet censorship: early warning system

Notice that our Russia Tor blocking story started at the beginning of December 2021.

From the rest of the world’s perspective, the Russia story started in February 2022.

So (a) yeah they knew this was coming, and (b) internet censorship often serves as an early warning system for upcoming political events.

Calls to action

Please run bridges!

Please run snowflakes!

Please run relays!

...How do we fix policy in these countries?

Please participate in anti-censorship research!
https://foci.community/ attached to
https://petsymposium.org (in Bristol in July).

Calls to action

(Run bridges, snowflakes, relays! Fix policy! Research!)

Day 3 Tor spaces:
- general meetup (Saal E 16:00-18:00)
- relay operators meetup and Q&A (Saal D 20:30-22:00)
- torservers.net meetup (Saal D 00:00-01:30)