

Race-addition update

Roger Dingledine, Cecylia Bocovich

August 9, 2021

The Tor Project



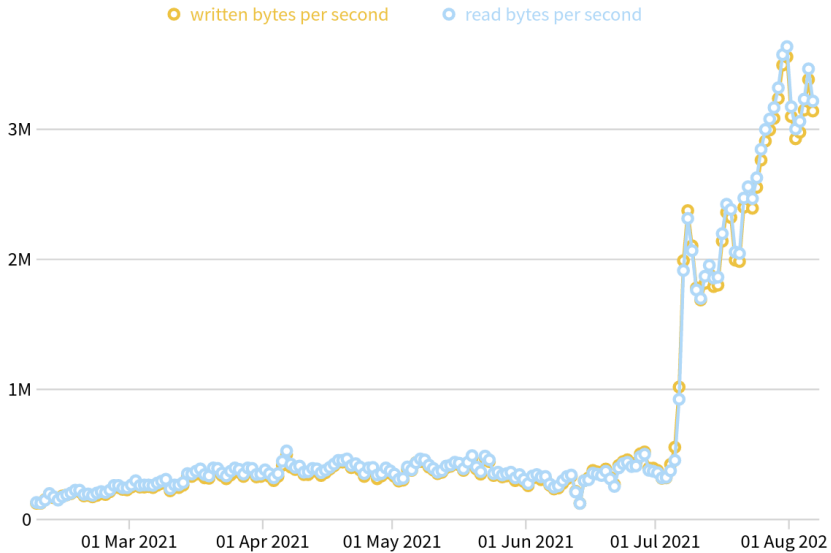
Outline

- (0) Meanwhile
- (1) OONI context
- (2) Tor censorship assessment roadmap
- (3) Tor Browser integration
- (4) Bridge distribution
- (5) Discussion

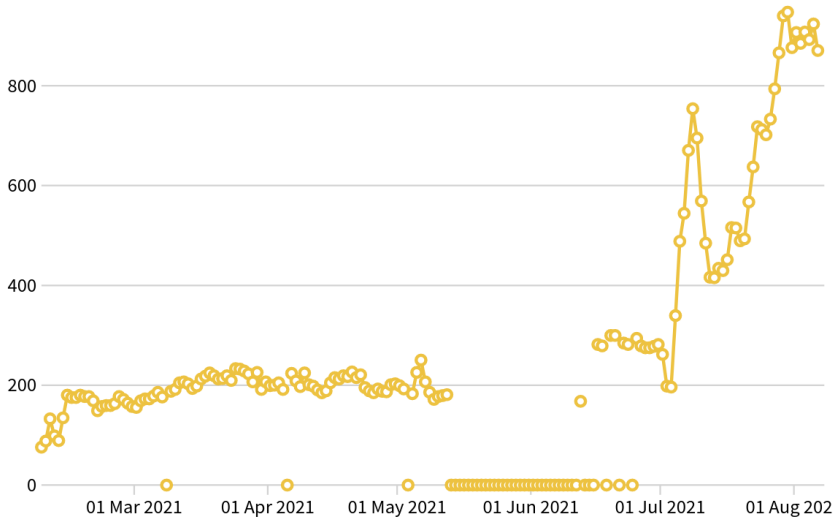
Meanwhile

Snowflake finally in Tor Browser stable!

- Windows/Linux/OSX (July 6)
- Android (July 20)



○ average number of connected clients



6 Months graph

Save Graph



Meanwhile

Philipp's replacement, Meskio, ramping up.

- Focusing on bridgedb (rdsys) and gettor.

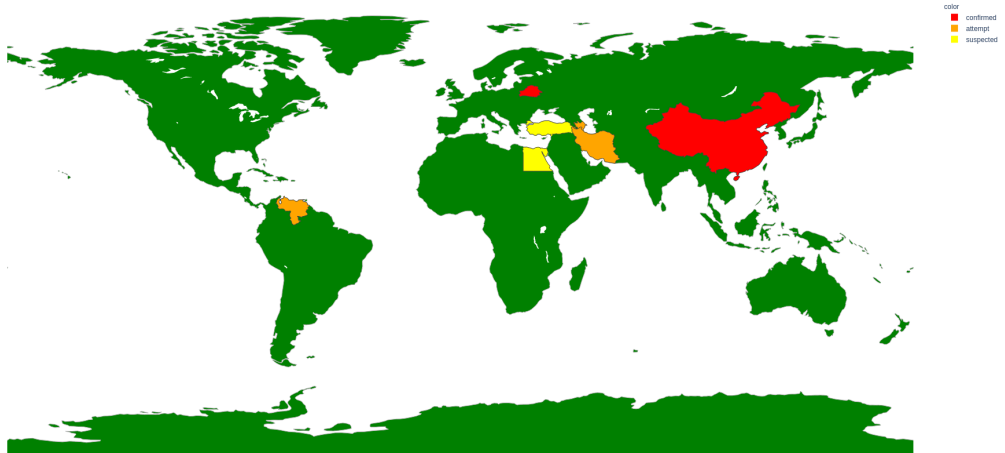
Meanwhile

New DRL-China project started a few days ago!

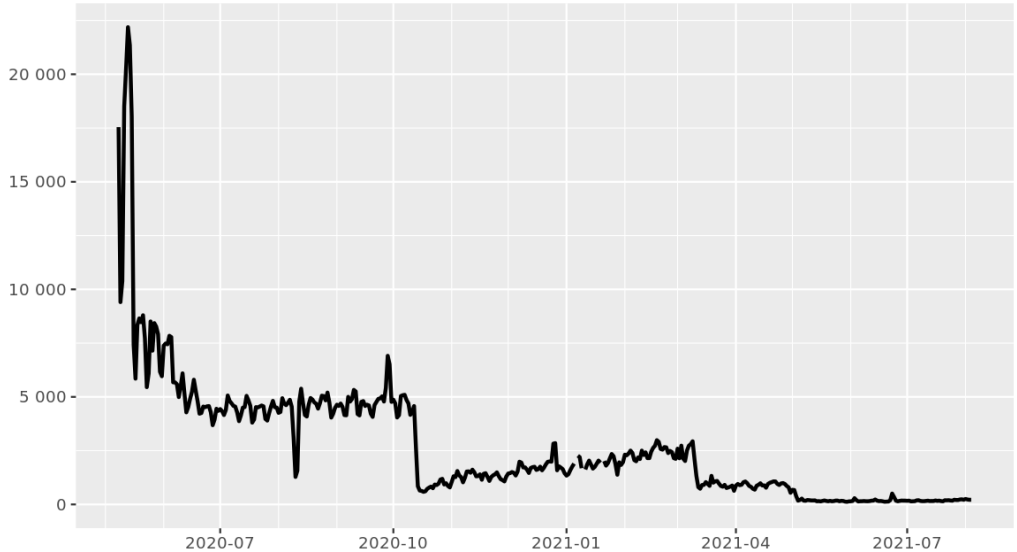
- Onionshare usability plus 'Tor launcher' style PT selection.
- CalyxOS integration.
- Pluggable transports library for Android / iOS
- Snowflake deployment and experience.
- And upcoming new dev/community person too.

Confirmed/attempted/suspected censorship

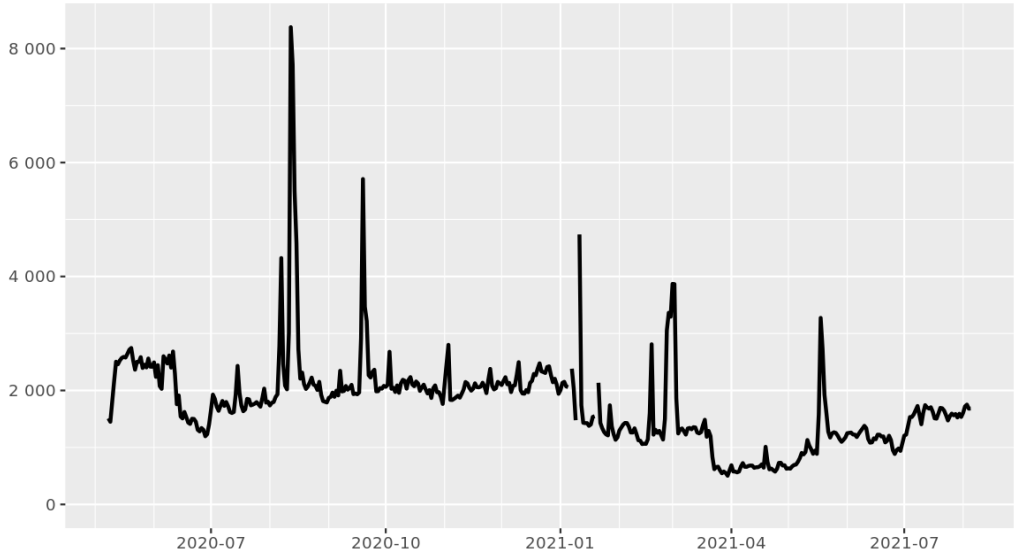
Detected blocking of vanilla Tor



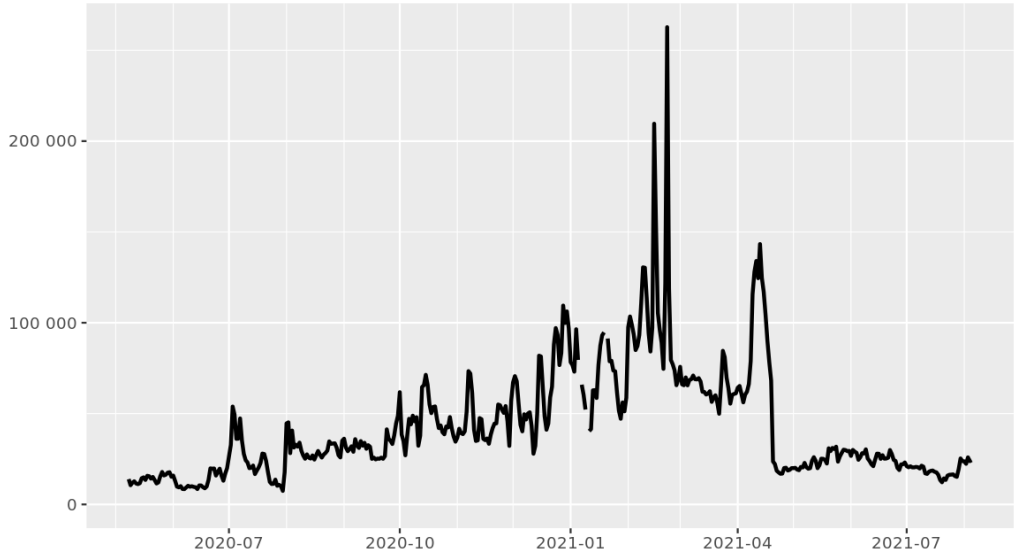
Directly connecting users from Belarus



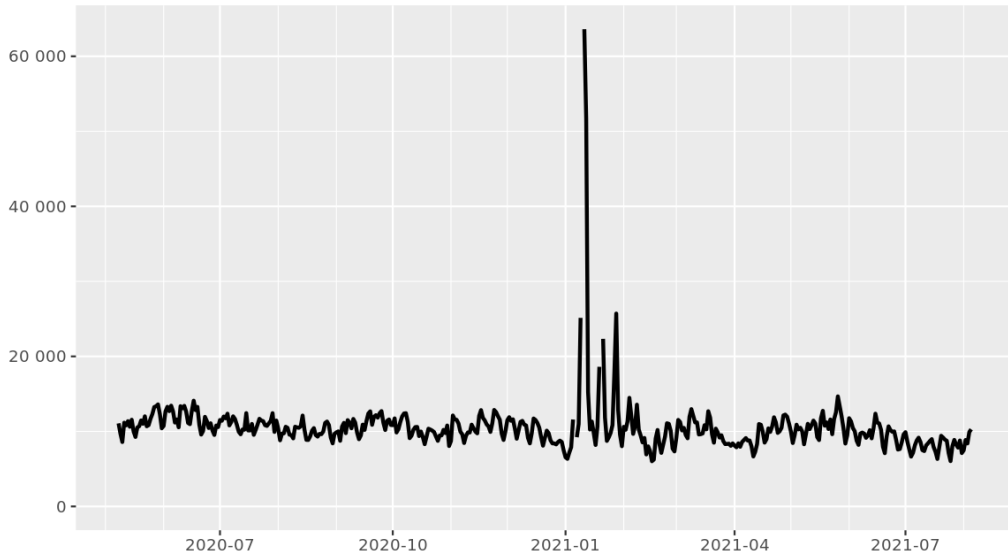
Directly connecting users from China



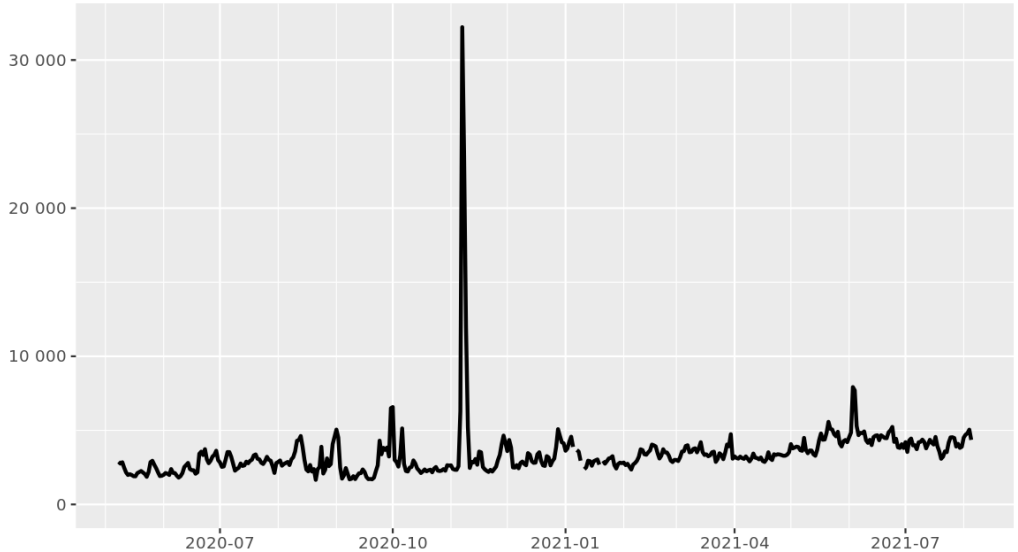
Directly connecting users from Turkey



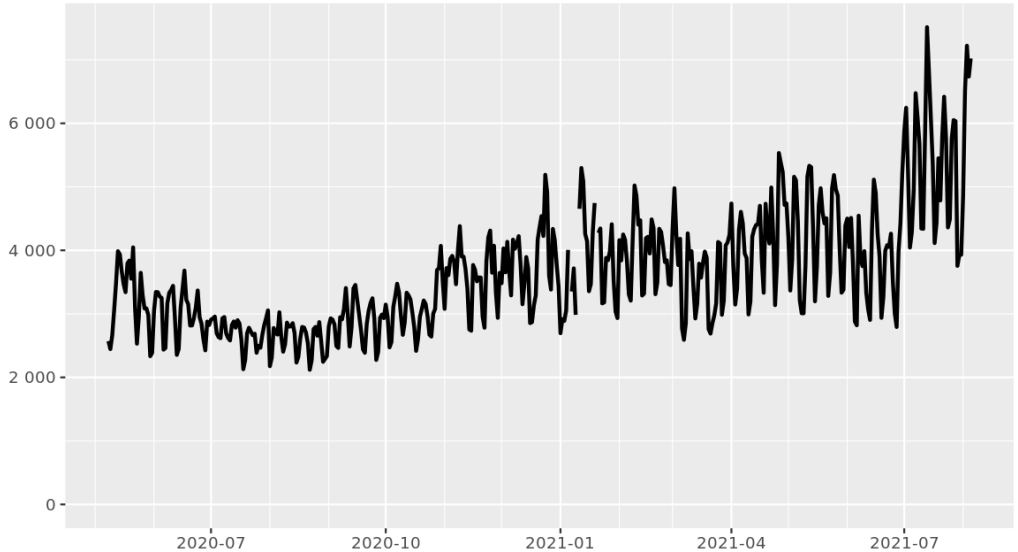
Directly connecting users from Venezuela



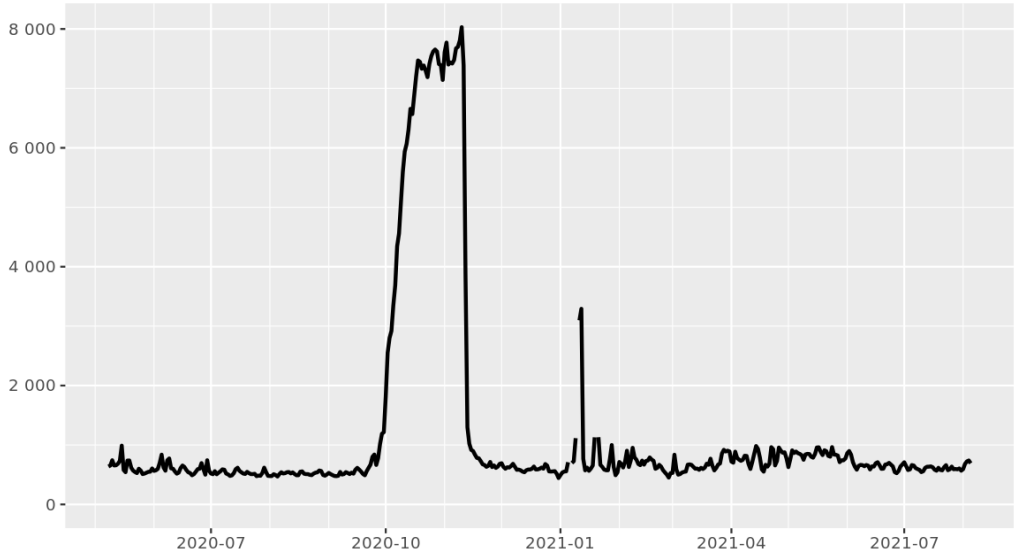
Directly connecting users from Egypt



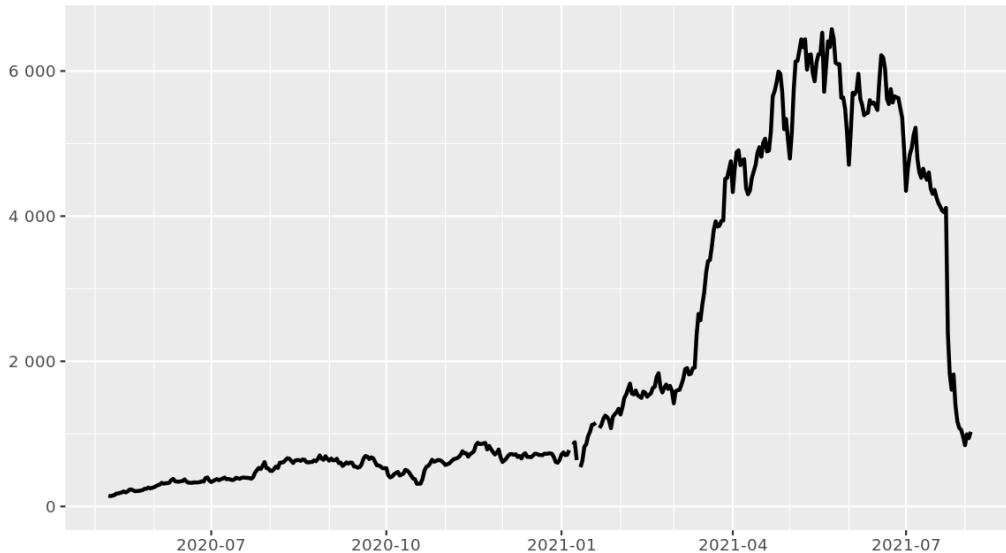
Directly connecting users from Kazakhstan



Directly connecting users from Azerbaijan



Directly connecting users from Turkmenistan



OONI Context

We've helped OONI to accurately describe the Tor conclusions (“blocks Tor” -> “attempts to block Tor”).

<https://ooni.org/post/2021-azerbaijan/>

OONI's deployed Tor test has two components:

- TLS handshake with Tor dir auths (but, is it Tor's TLS?)
- obfs4 handshake with default (i.e. pre-configured in Tor Browser) obfs4 bridges

Can't use OONI data to conclude about whether Tor actually works.

Statement of Work, Area One

“better understand the blocking that we see in practice, and produce a map of the circumvention methods that are known to work in each country. [. . .] collecting external probes and usage metrics of a base core of popular techniques [. . .] investigate anecdotal blocking reports to try to understand whether they’re a false positive and pin down the point of failure in each case”

Tor censorship assessment roadmap (1/7)

Start archiving the data we've got.

- ✓ We've been running our Snowflake+obfs4 reachability assessment tool at the China VPS.
<https://gitlab.torproject.org/cohosh/probetest>
- ✓ Start archiving the data we get out of it, so we have an ongoing data set.
- ✓ To start, just rsync it to some outside computer.
- ☐ Talk to the sysadmin team and the metrics team to figure out a better place to keep it.

Tor censorship assessment roadmap (2/7)

Deploy this tool in a few more places (and archive its output).

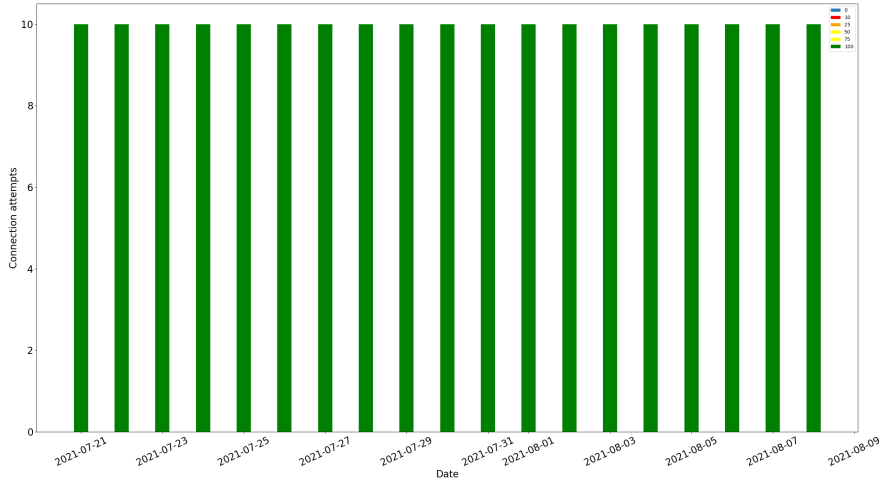
- ✓ The Turkey VPS that we used for Raven evaluation.
- ✓ Someplace-in-Canada so we can have a “control”.

Tor censorship assessment roadmap (3/7)

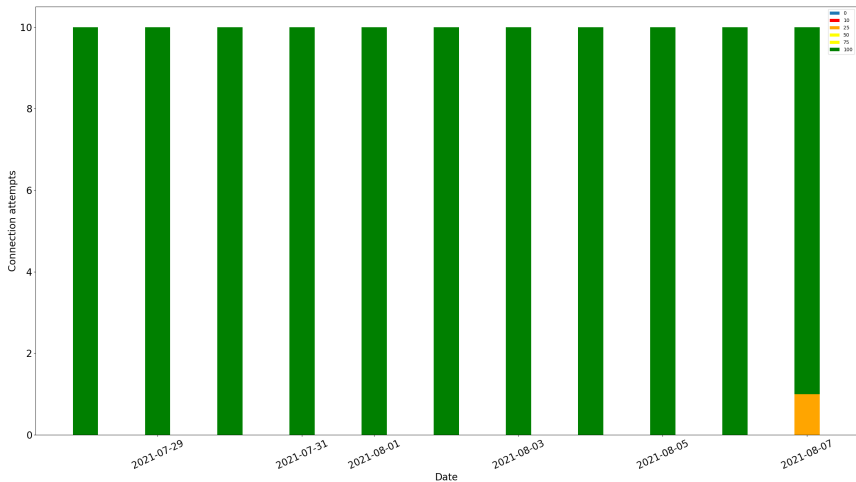
Streamline the deployment, so re-deploying it when we lose a VPS is easy, and also so adding more countries is easy.

- ✓ Make a docker image that runs the tools and outputs logs.
<https://github.com/cohosh/bridgetest/>
- ☐ Maybe we want a fallback “unpacker” script for destinations that don’t play well with docker?
- ☐ Have a plan for how we’ll keep installs up-to-date.

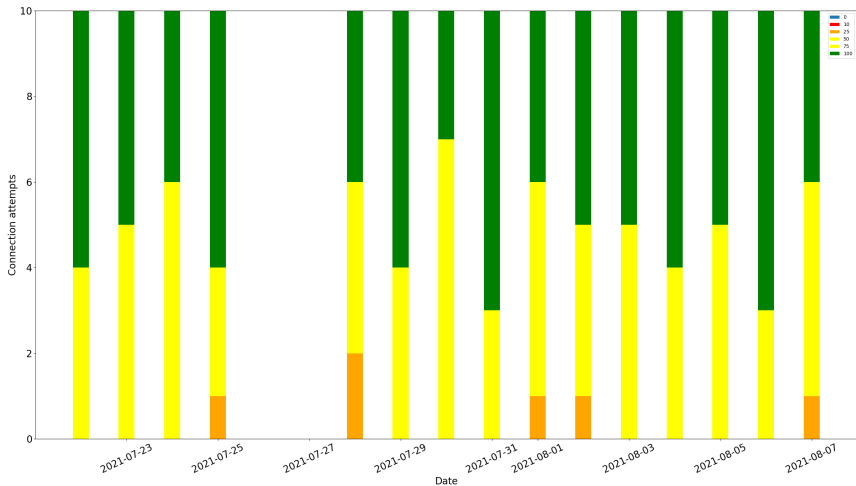
Snowflake in Canada



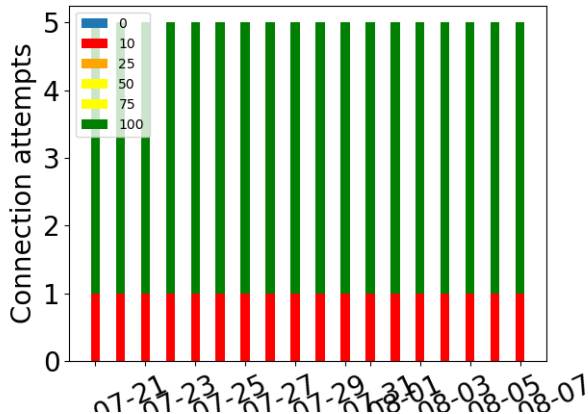
Snowflake in Turkey



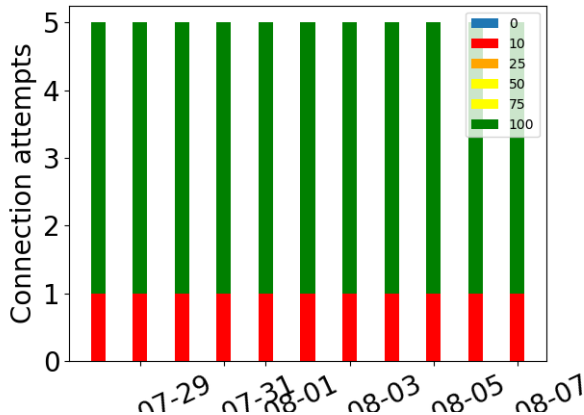
Snowflake in China



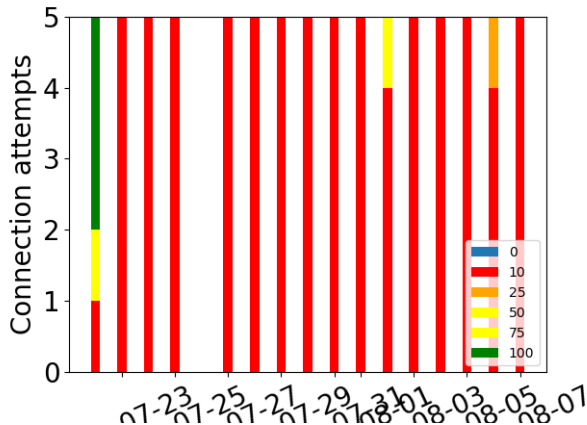
obfs4-moat in Canada



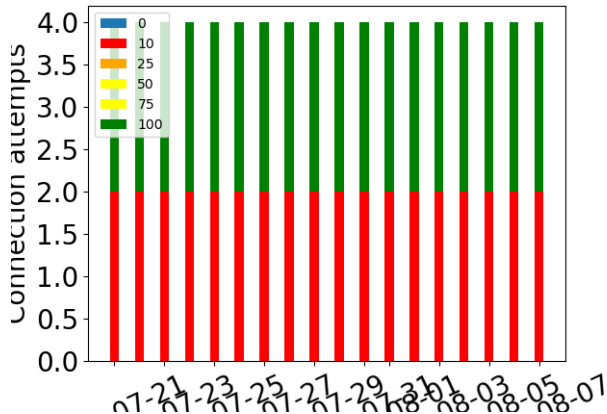
obfs4-moat in Turkey



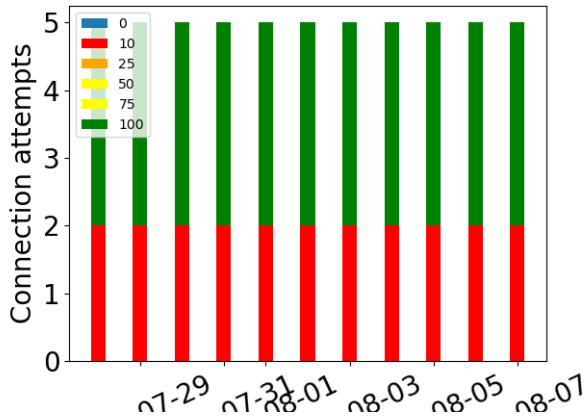
obfs4-moat in China



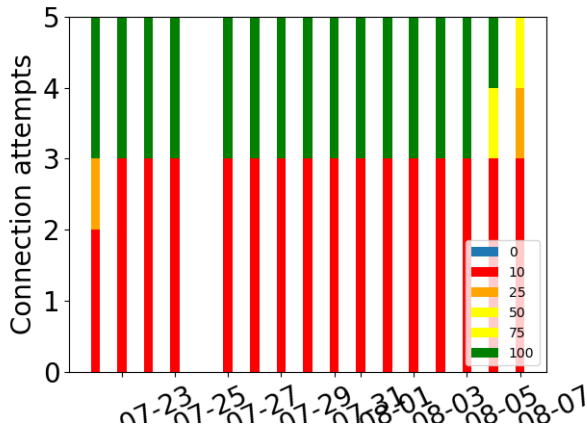
obfs4-email in Canada



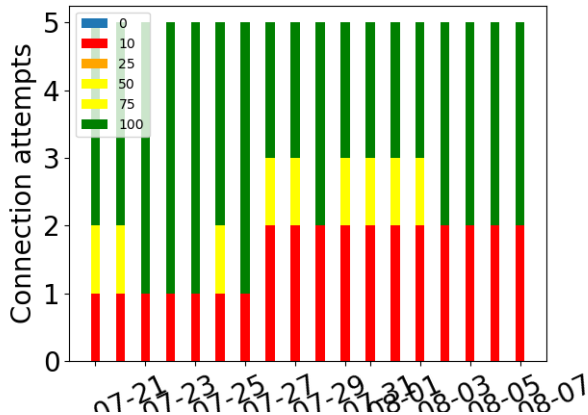
obfs4-email in Turkey



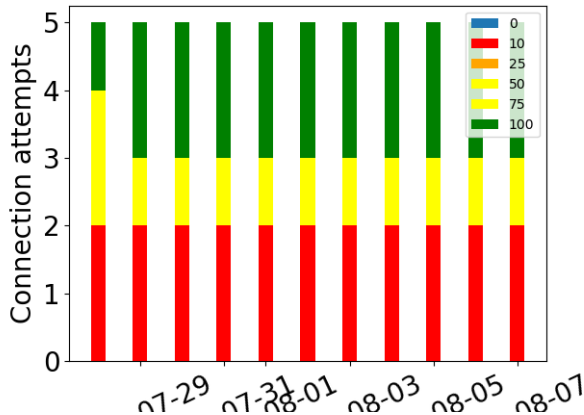
obfs4-email in China



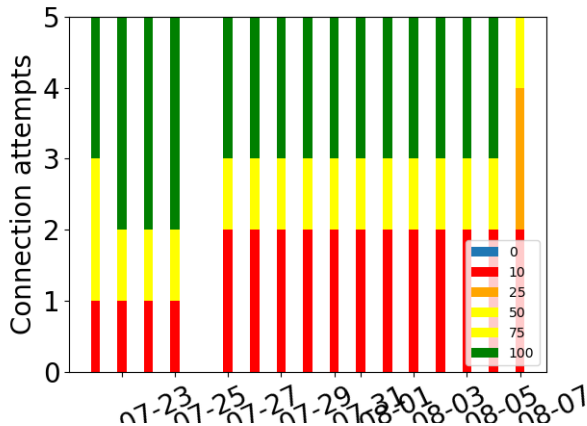
obfs4-https in Canada



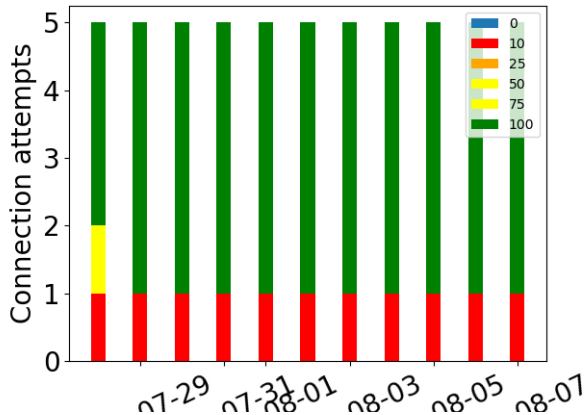
obfs4-https in Turkey



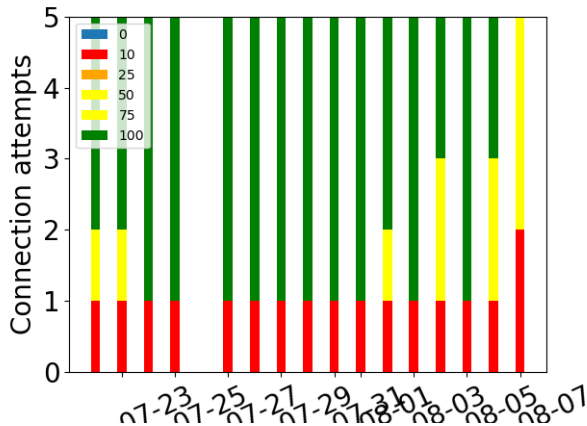
obfs4-https in China



obfs4-private in Turkey



obfs4-private in China



Tor censorship assessment roadmap (4/7)

Add more tools to the suite of assessment tools we run.

- ☐ emma does TCP tests for directory authorities, meek, and key websites like Tor's download site and BridgeDB.
- ☐ marco does SSL handshakes with all the relays in a consensus.
- ☐ We should also do a full vanilla Tor bootstrap attempt test.
- ☐ I'd like to test for active probing too—maybe the repeated-game marco is enough for that?

Automate them in each location, and collect and archive their output too.

Tor censorship assessment roadmap (5/7)

Make (some parts of) our archived data sets public.

- ☐ Sanitize them so for example they don't include the IP address of our VPS, which would compromise our continued ability to do measurements.
- ☐ Publish whatever we can, and over time try to shrink the part that we can't.

Preliminary data format:

<https://gitlab.torproject.org/cohosh/probetest#data-format>

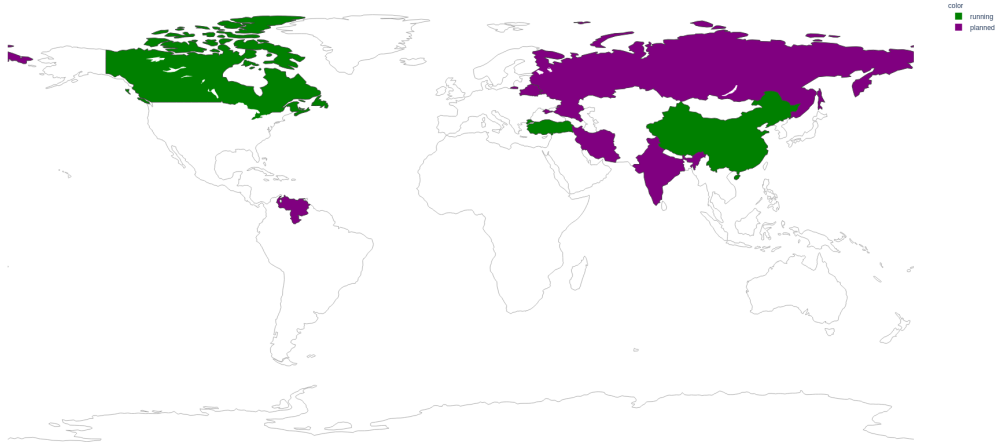
Tor censorship assessment roadmap (6/7)

Expand the set of vantage points beyond the ones we run ourselves.

- ☐ Core community members running vantage points in their censored environments—India, Venezuela, etc.
- ☐ Set up automated monitoring *of the vantage points* so we can be quick to learn when they go offline or when our test automation breaks.
- ☐ Eventually publish sanitized versions of the community data sets, but maybe keep them private to start.

Current/future probe locations

Distribution of Tor circumvention probes



Tor censorship assessment roadmap (7/7)

Make sure we're doing the right tests, with a useful output format.

- ☐ The two critical questions in each location are:
 - “does Tor with this config work on this network?”
 - “**why** does Tor with this config not work on this network?”
- ☐ Some tests assess **components** of Tor bootstrapping, which focuses on the second question; we also need full beginning-to-end bootstrap tests.
- ☐ We should adapt our data format to be convenient for others, e.g. by matching OONI's data format.

Tor censorship assessment meta-topics (1/5)

Not all tests are appropriate for all countries.

- Running marco on the China VPS will attract attention eventually.
- Active censorship triggered by one test could impact the outcome of another test (e.g. in China if they drop all your packets for five minutes after you do something naughty).
- In those cases we need to orchestrate the **timing** of tests, and have config settings so it's easy to disable or modify some tests per location.

Tor censorship assessment meta-topics (2/5)

Censorship can vary inside each country.

- Focus on automation first: get a scalable test suite up and collecting data—mainly engineering and logistics work.
- For the specific China and Turkey VPSs that we have, I think we're doing quite well.
- *Every* location we run this test suite will be different. There is no “best” place in any country: each place that we pick will give us a different vantage point, and each place will give us authentic feedback about how Tor works on that network.

Tor censorship assessment meta-topics (3/5)

As new blocking events happen, we will use our data sets and our scanners to help understand what happened.

- We will likely end up thinking of and running new tests during each blocking event.
- Each post-mortem event analysis should feed back to improving future tests in all locations.

Tor censorship assessment meta-topics (4/5)

Use cycles to better instrument Tor and the pluggable transports.

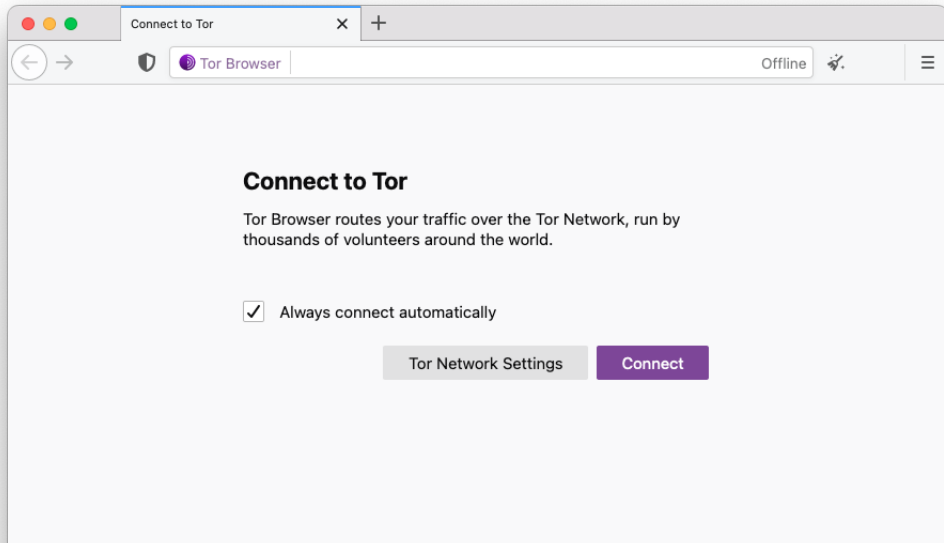
- While we're trying to answer the “why does it not work” question, we should actively look for missing features in the Tor client and the pluggable transports.
- The endgame is for the core tools themselves to self-assess the reasons for failure—which scales better because other tools (and users!) can benefit too.

Tor censorship assessment meta-topics (5/5)

People will naturally ask “why not OONI?”

- #1: We want to test more things, spend more time per test, and require larger components than OONI is willing to include.
- #2: Open research problem: how to test sensitive destinations in the OONI model?
- #3: Think of this as a development testbed for OONI tests. We should actively look for tests and subtests to shift to OONI, to get better coverage and to reduce our own complexity.
- #4: If OONI is a test output format, and we write our test outputs in that format...

New config flow for Tor Browser startup



json to list what locales need what PTs



Menu



Sign in

```
74     "by": {  
75       "infrastructure": {  
76         "website": false,  
77         "bridgedb_www": false,  
78         "bridgedb_moat": true  
79       },  
80       "relays": false,  
81       "dirauths": false,  
82       "bridges": {  
83         "default": false,  
84         "published_vanilla": true,  
85         "unpublished_vanilla": true,  
86         "published_obfs4": true,  
87         "unpublished_obfs4": true,  
88         "meek": true  
89       }  
90     }  
91   }
```

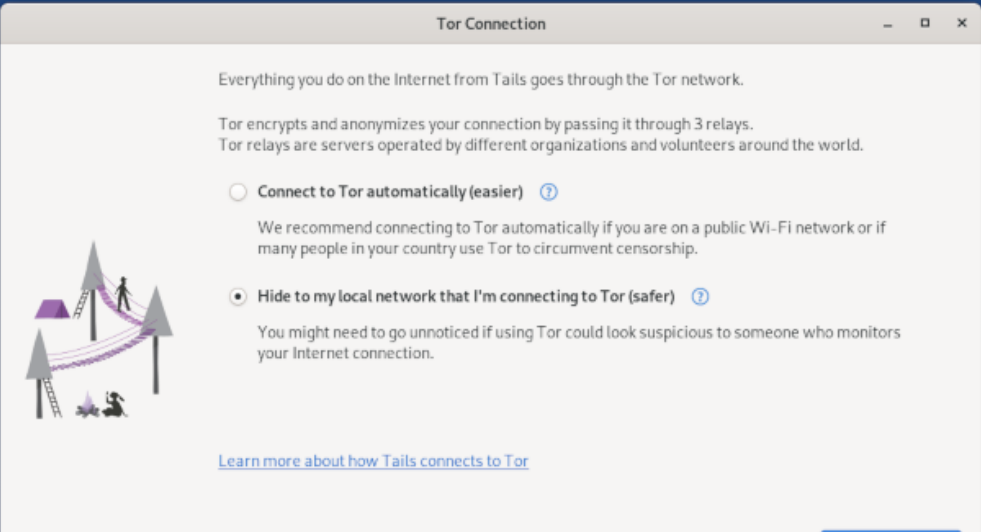
Tor Browser integration

The goal is for “always connect automatically” to do the right thing based on your locale.

Upcoming Tor Browser UX flow questions:

- How to know what locale we're in?
- Also tied into: are pluggable transports for being invisible or for getting around censorship?

Compare to the approach Tails is taking



The screenshot shows a window titled "Tor Connection" with standard window controls. The text inside explains that internet activity from Tails is routed through the Tor network, which encrypts and anonymizes connections by passing them through three relays. Two radio buttons are present: "Connect to Tor automatically (easier)" and "Hide to my local network that I'm connecting to Tor (safer)". The second option is selected. A blue link at the bottom says "Learn more about how Tails connects to Tor". On the left, there is a stylized illustration of a person climbing a ladder to a tent in a forest, with a campfire and another person sitting nearby.

Tor Connection

Everything you do on the Internet from Tails goes through the Tor network.

Tor encrypts and anonymizes your connection by passing it through 3 relays.
Tor relays are servers operated by different organizations and volunteers around the world.

☐ **Connect to Tor automatically (easier)** ?

We recommend connecting to Tor automatically if you are on a public Wi-Fi network or if many people in your country use Tor to circumvent censorship.

☒ **Hide to my local network that I'm connecting to Tor (safer)** ?

You might need to go unnoticed if using Tor could look suspicious to someone who monitors your Internet connection.

[Learn more about how Tails connects to Tor](#)



Statement of Work, Area Two

“design more robust defenses against proxy enumeration based on recent research on reputation systems for proxy distribution. [. . .] write up a clear design for the “Salmon” bridge distribution framework, including identifying missing pieces from the original paper and proposing concrete plans for them. [. . .] focus on getting the design worked out and understand exactly what external components are still missing.”

Bridge Distribution updates

Domain fronting still going: Azure -> Fastly.

AMP cache rendezvous implementation
(though only Google hosts a big AMP cache).

Talking to Ian Goldberg's research group about a Salmon variant.

Salmon open problems: How to do initial Sybil resistance? How to re-allocate users after a failed bridge?

Talking to Conjure team about an obfs4 integration.

Tor censorship assessment roadmap (recap)

- Start archiving the data we've got.
- Deploy this tool in a few more places (and archive its output).
- Streamline the deployment, so re-deploying it when we lose a VPS is easy, and also so adding more countries is easy.
- Add more tools to the suite of assessment tools we run.
- Make (some parts of) our archived data sets public.
- Expand the set of vantage points beyond the ones we run ourselves.
- Make sure we're doing the right tests, with a useful output format.