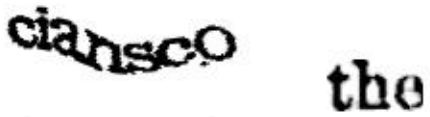
Pluggable transport work

- Flashproxy can do IPv6.
  - Upcoming Flashproxy Tor Browser Bundle (TBB) Windows package
- Obfsproxy packages:
  - debs and bridge-side docs
  - (and obfsproxy in our ec2 images)
  - Client-side Obfsproxy TBBs
- New library: pyptlib, obfs3 spec

https://bridges.torproject.org/

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

To receive your bridge relays, please prove you are human



Type the two words

I am human

Another way to find public bridge addresses is to send mail to bridges@torproject.org with the line "get bridges" by itself in the body of the mail. However, so we can make it harder for an attacker to learn lots of bridge addresses, you must send this request from an email address at one of the following domains:

- gmail.com
- yahoo.com

Looking for IPv6 bridges?

Looking for obfsproxy bridges?

Specify transport by name:

Submit Query

Performance/simulations

- Shadow bugfixes (see Storm talk)
- We have a µTP-based transport branch (we're debugging it)
- New “channel” and “circuit mux” abstractions in the Tor code
- Found a design flaw in n23: it lacks stream flow control

Recent Tor design proposals

- 202: Tagging resistance
- 205: Remove global DNS cache on client
- 206: Ship with more directory mirrors
- 207: Directory guards
- 208: Exiting to IPv6 destinations
- 216: ntor (a new circuit handshake)
- 217: Extended ORPort authentication

New Tor research papers

- “Changing of the Guards” (WPES 2012)
- “Torchestra” (WPES 2012)
- “CensorSpoofer” (CCS 2012)
- “Real-time Traffic Classification” (CCS 2012)

Looking forward to Year 3

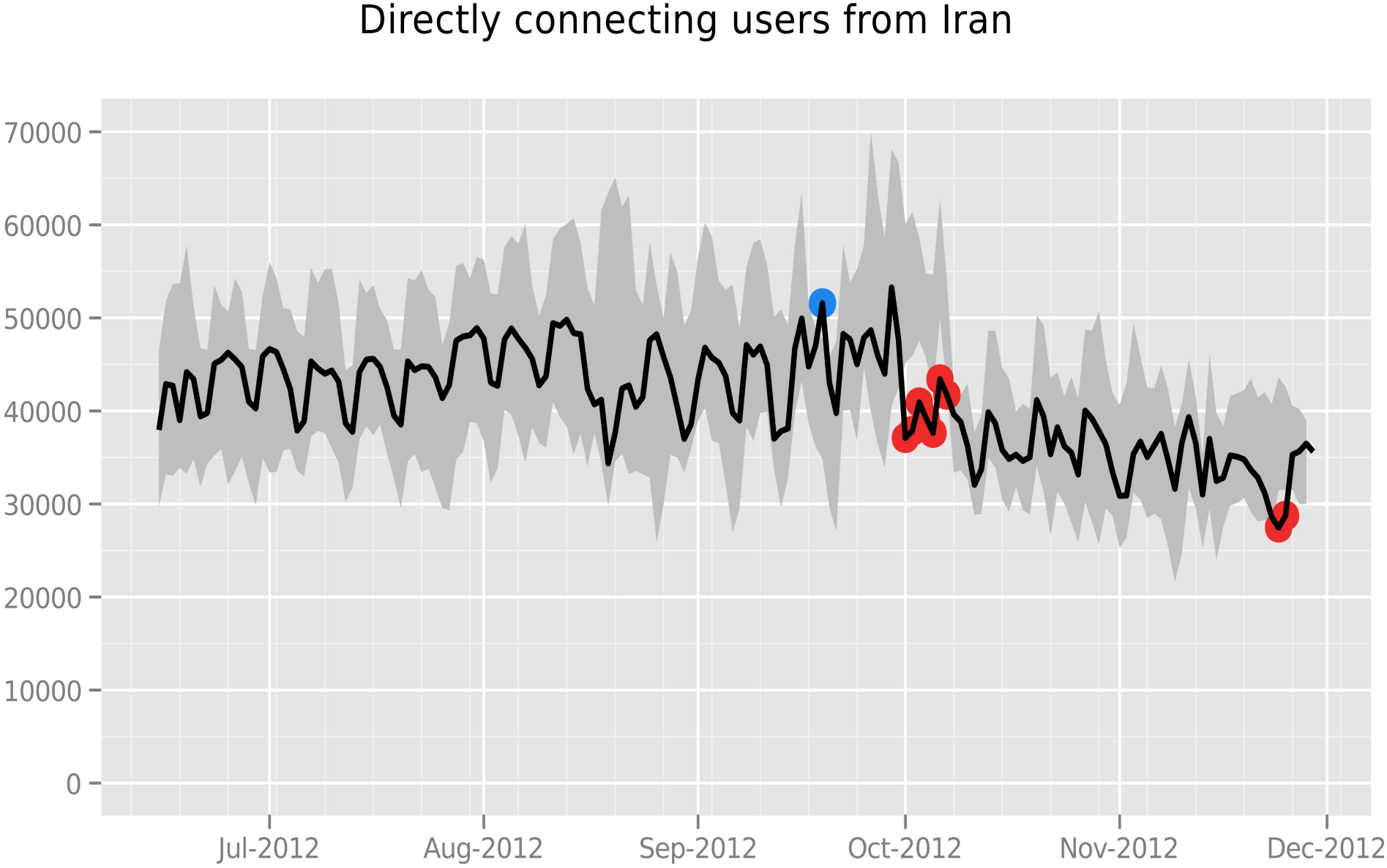
- VoIP:
  - Push-to-talk VoIP-alike over TCP
  - Skype itself over TCP
- Simulated Tor networks:
  - What is realistic traffic load?
  - Automated regression test harness
  - TestingTorNetwork config changes

Looking forward to Year 3

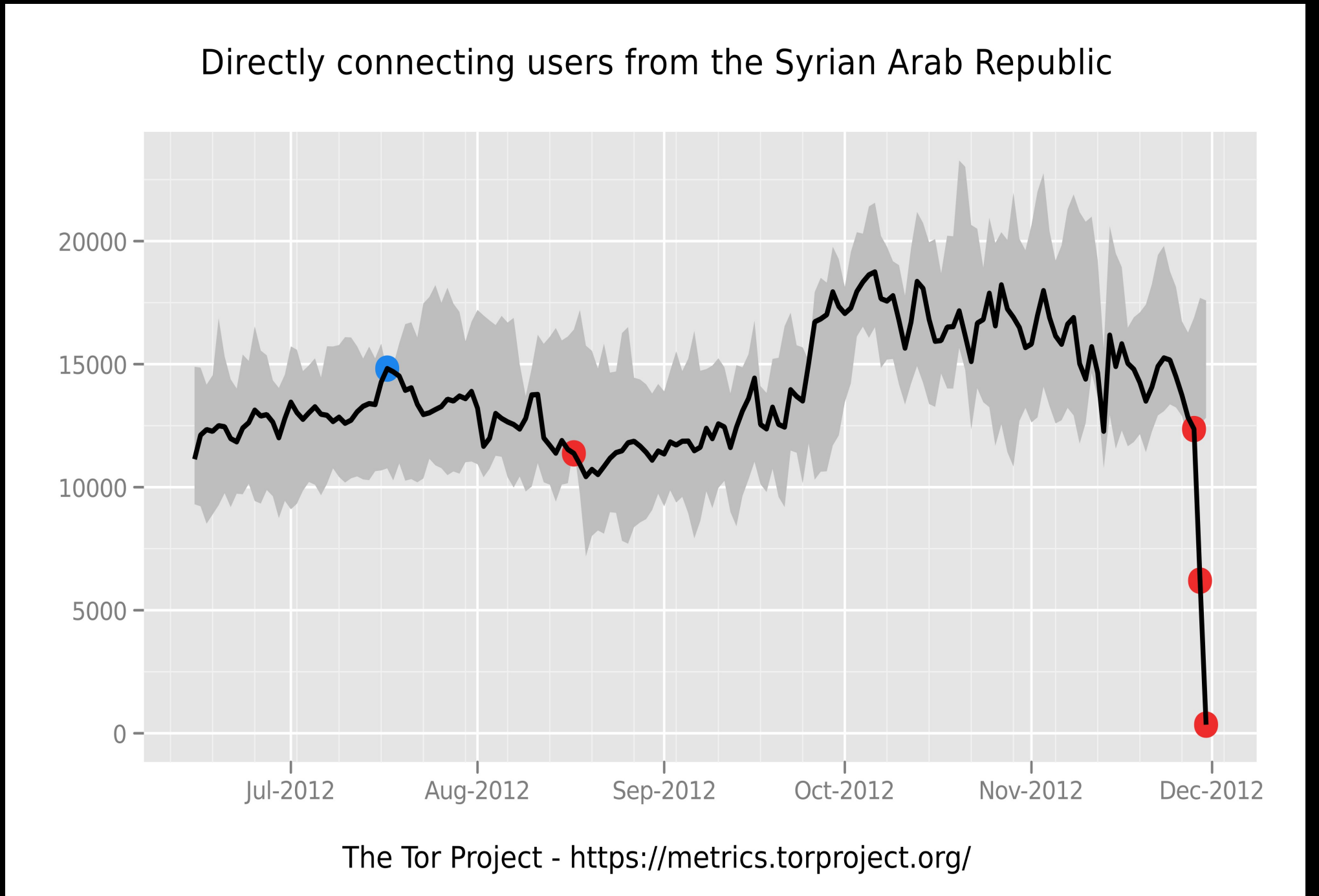
- Performance:
  - Alternate scheduling algorithms
  - Throttling at guards
  - Drop slow relays
  - Redesign n23, do new experiments
  - Have a working μTP-based transport

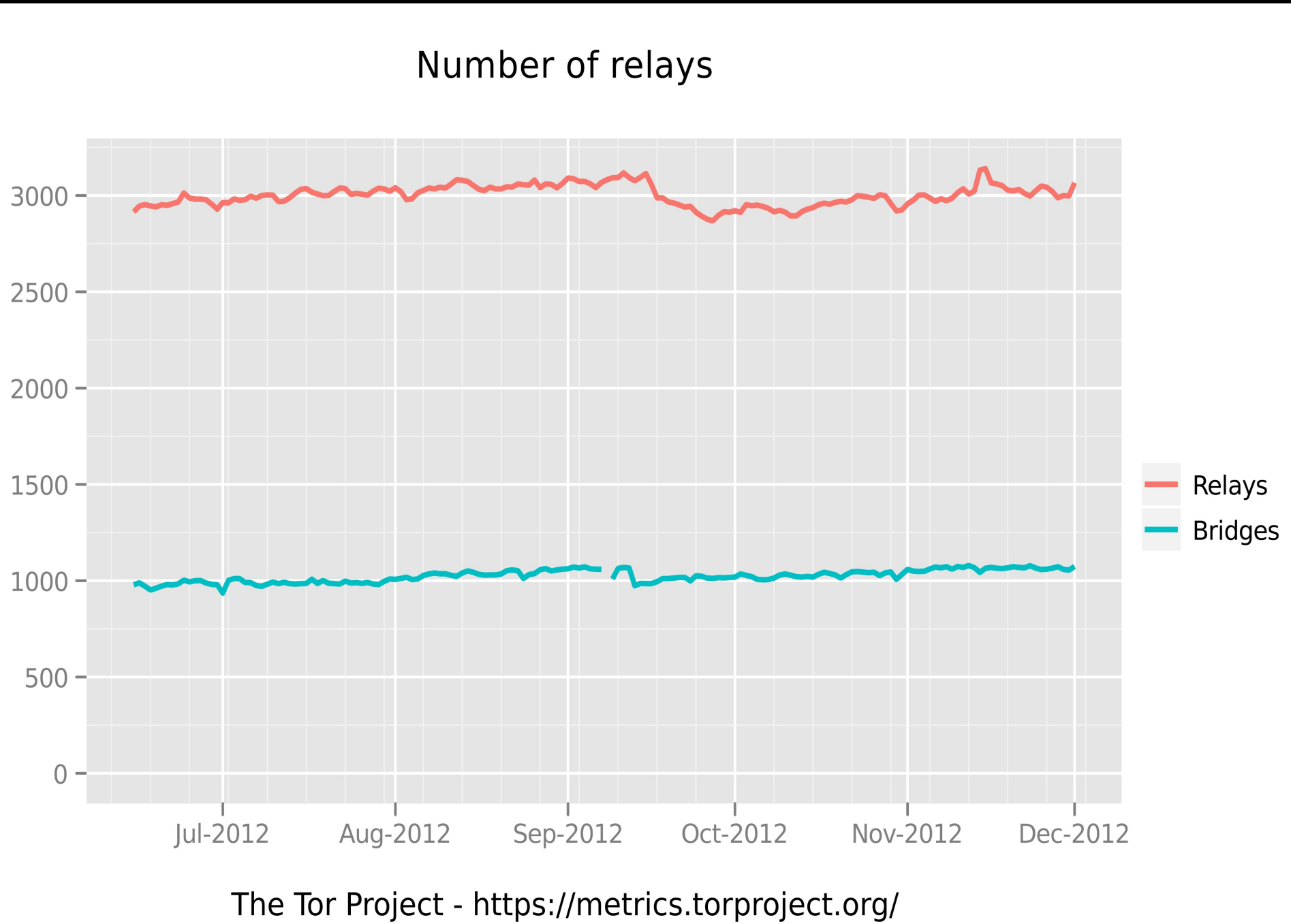
Looking forward to Year 3

- Layered pluggable transports
  - Combine obfsproxy + chopper + flashproxy
- Want to get a UDP pluggable transport going

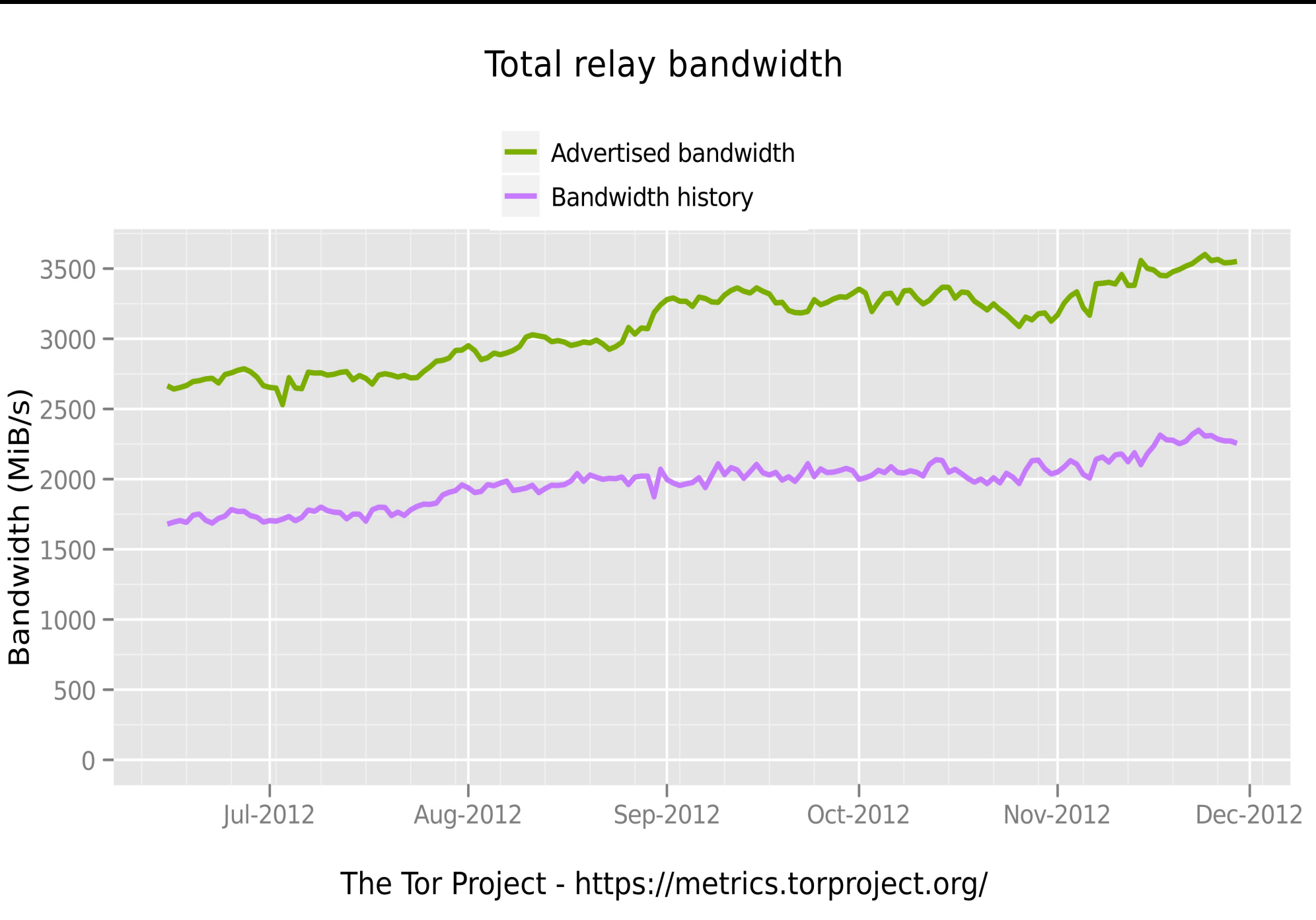


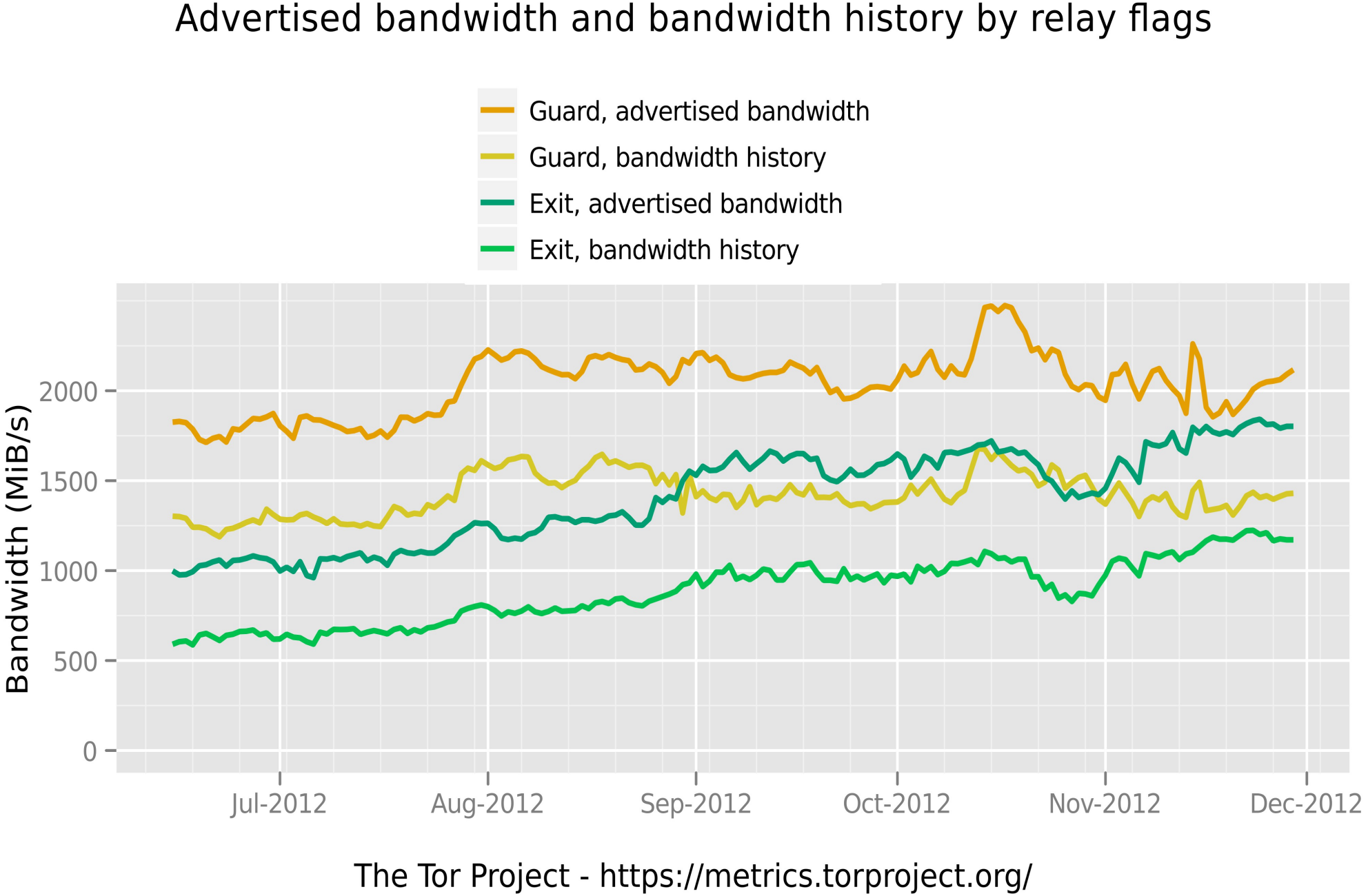
The Tor Project - https://metrics.torproject.org/

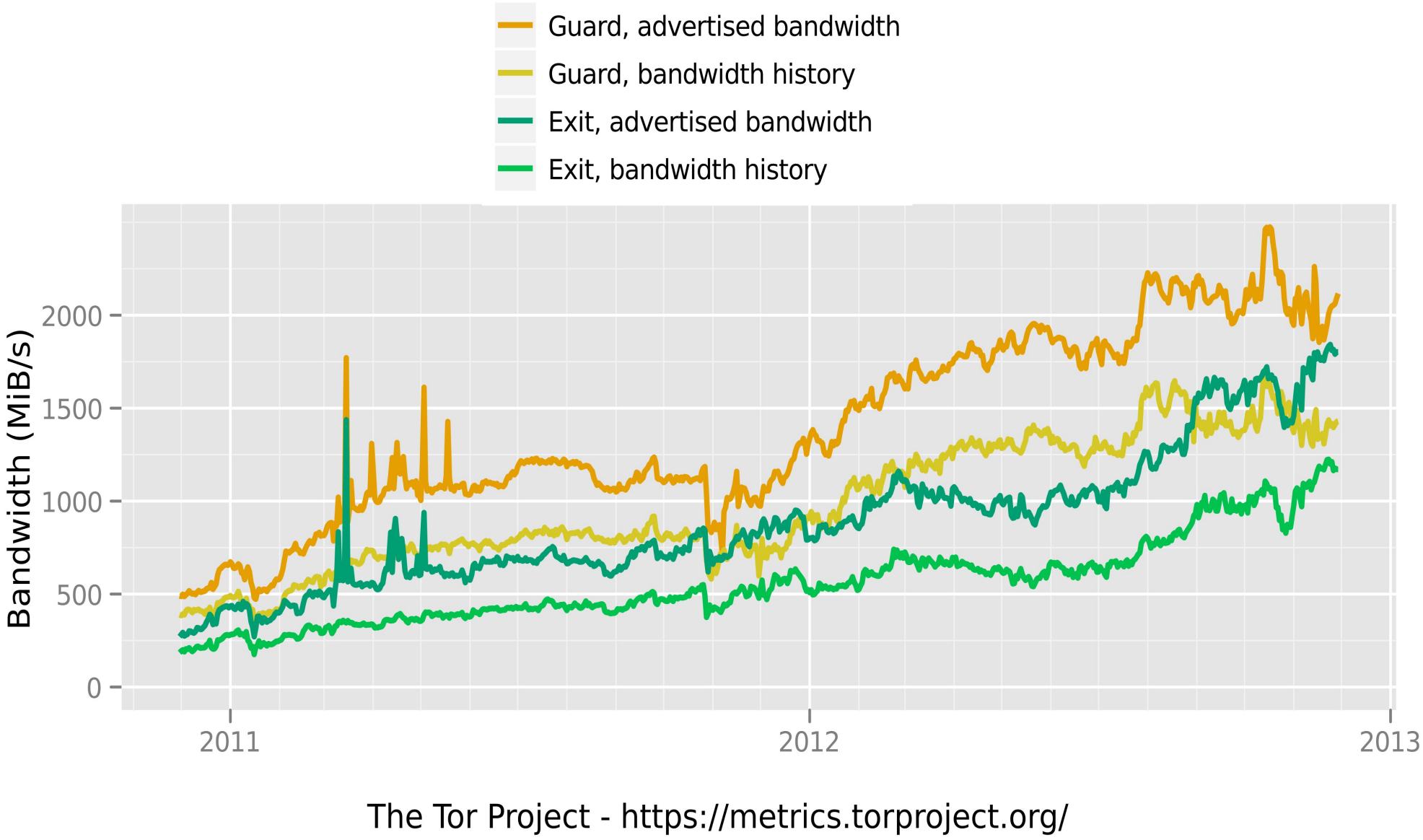

Directly connecting users from the Syrian Arab Republic
20000
15000
10000
5000
0
Jul-2012
Aug-2012
Sep-2012
Oct-2012
Nov-2012
Dec-2012
The Tor Project - https://metrics.torproject.org/

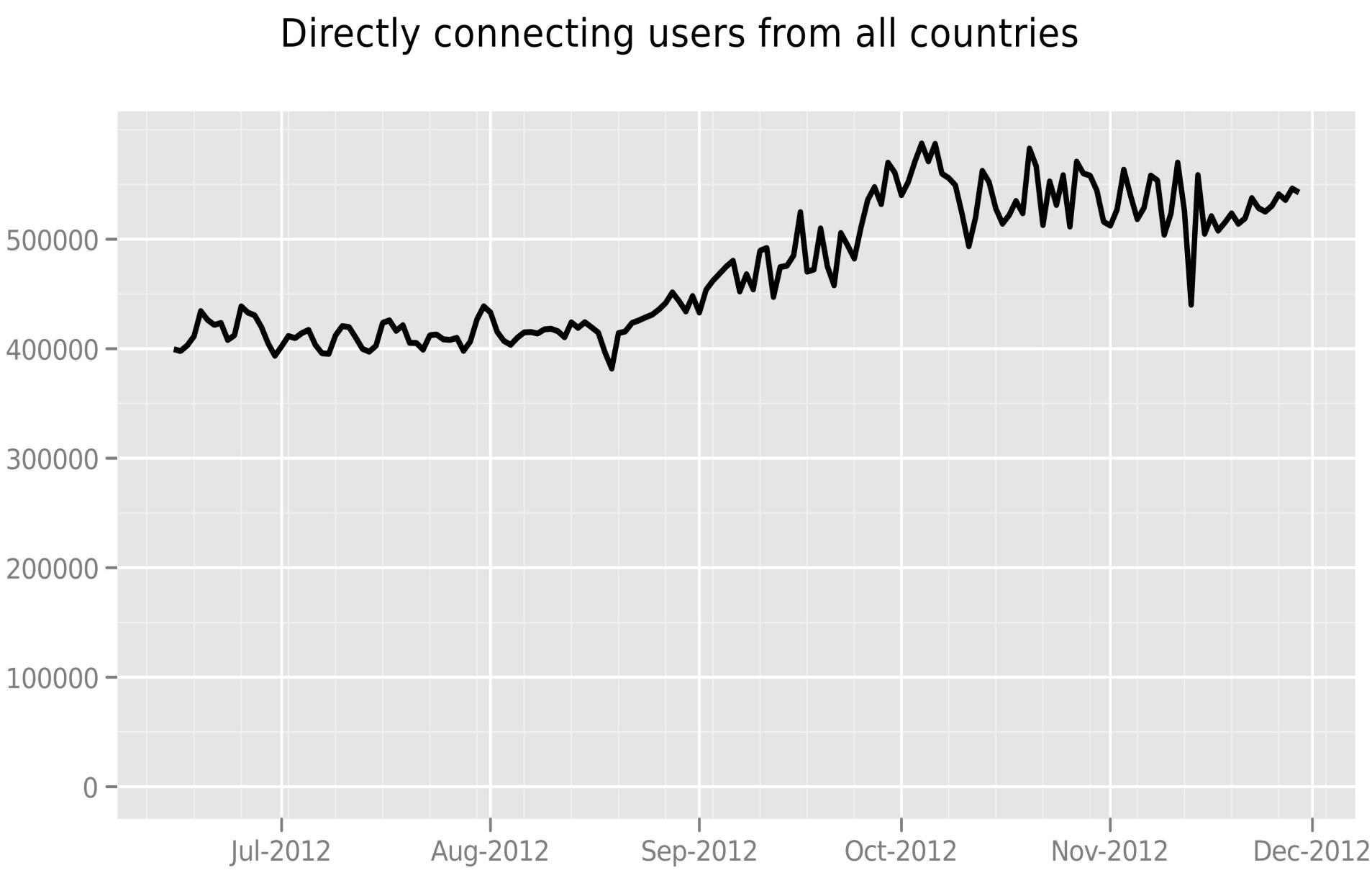


The Tor Project - https://metrics.torproject.org/

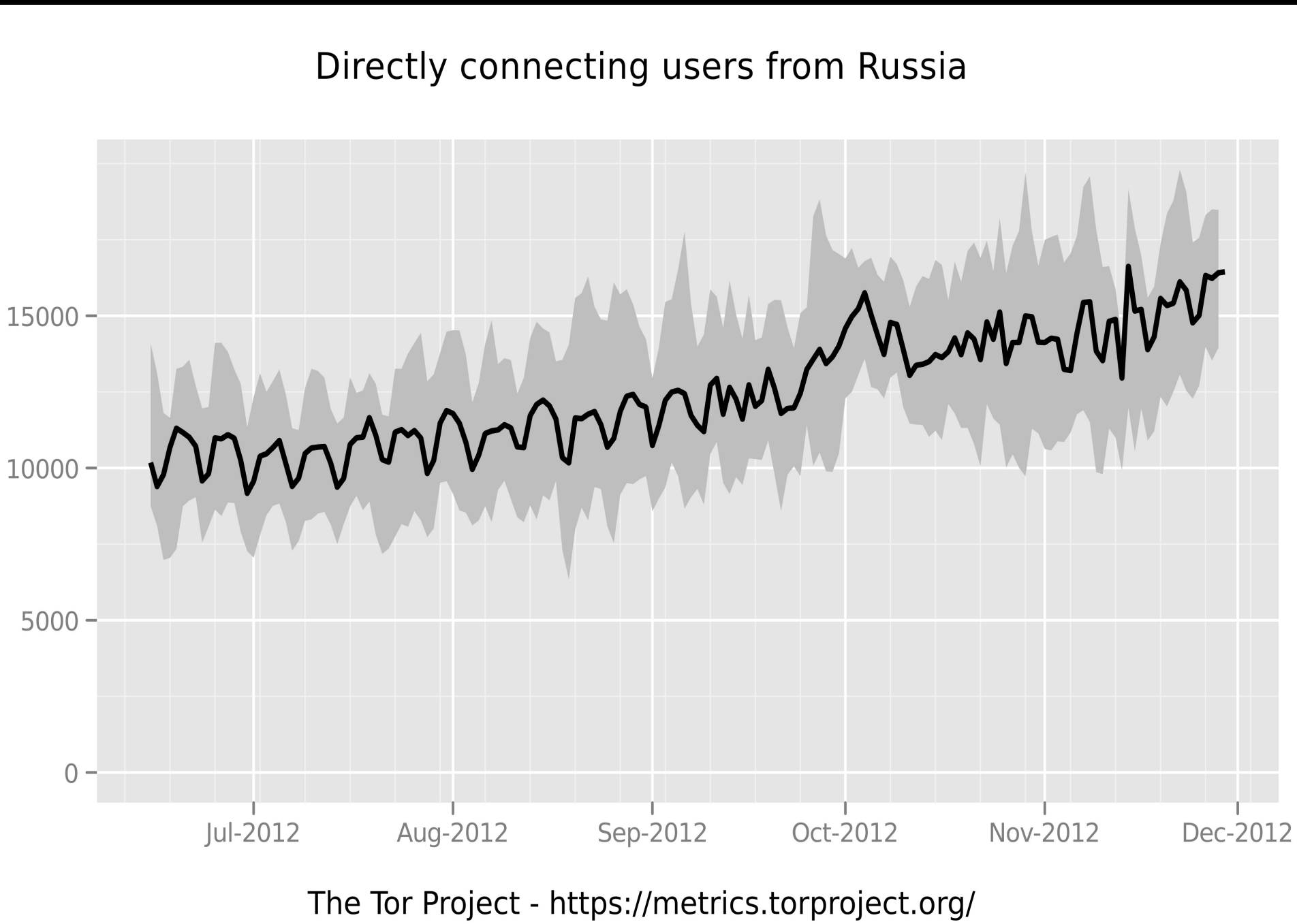

Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
3500
3000
2500
2000
1500
1000
500
0
Jul-2012
Aug-2012
Sep-2012
Oct-2012
Nov-2012
Dec-2012
The Tor Project - https://metrics.torproject.org/

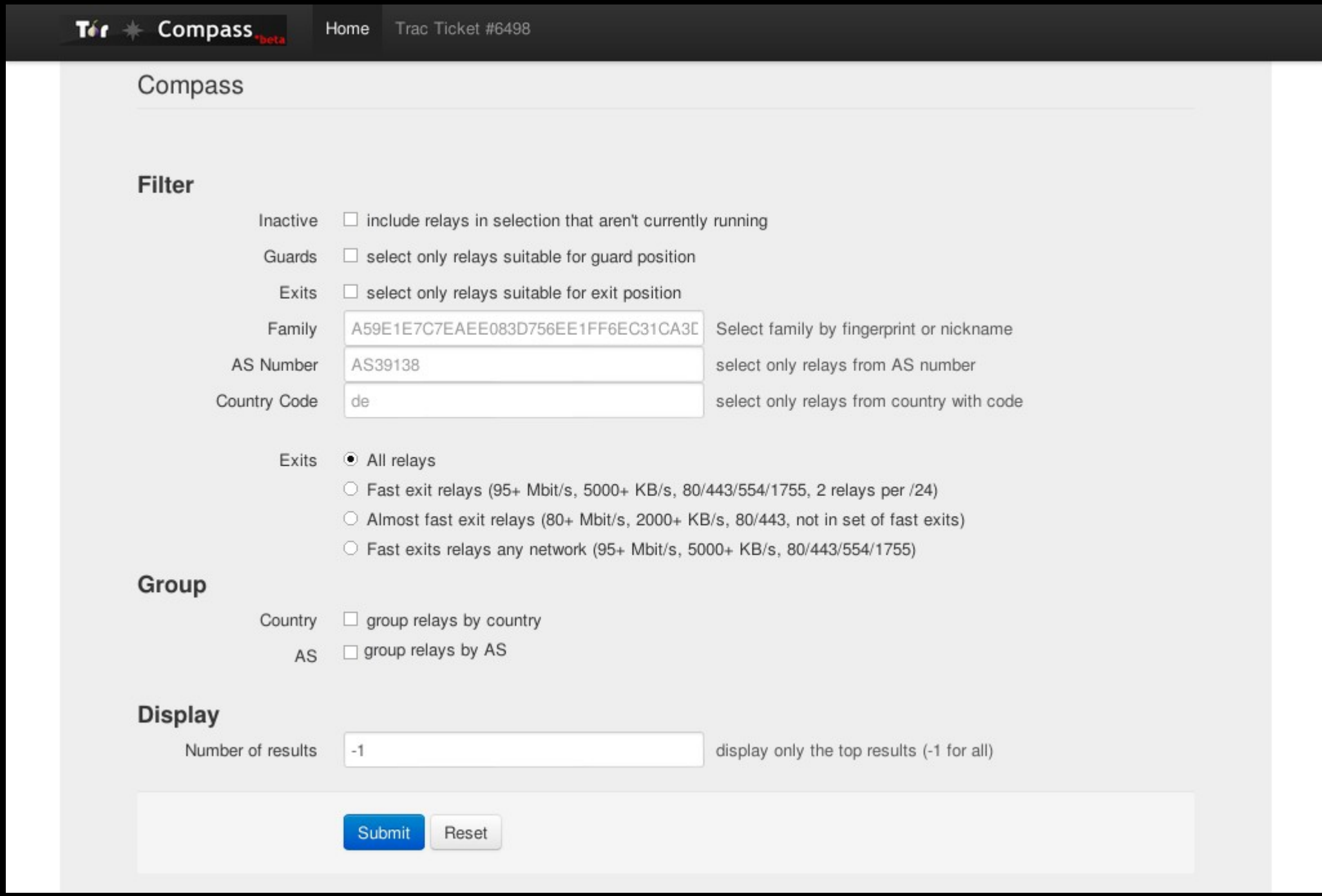

Advertised bandwidth and bandwidth history by relay flags
Guard, advertised bandwidth
Guard, bandwidth history
Exit, advertised bandwidth
Exit, bandwidth history
Bandwidth (MiB/s)
2000
1500
1000
500
0
Jul-2012
Aug-2012
Sep-2012
Oct-2012
Nov-2012
Dec-2012
The Tor Project - https://metrics.torproject.org/


Advertised bandwidth and bandwidth history by relay flags
Guard, advertised bandwidth
Guard, bandwidth history
Exit, advertised bandwidth
Exit, bandwidth history
Bandwidth (MiB/s)
2000
1500
1000
500
0
2011
2012
2013
The Tor Project - https://metrics.torproject.org/



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


Directly connecting users from Russia
15000
10000
5000
0
Jul-2012
Aug-2012
Sep-2012
Oct-2012
Nov-2012
Dec-2012
The Tor Project - https://metrics.torproject.org/


Tor Compass beta
Home
Trac Ticket #6498
Compass
Filter
Inactive
include relays in selection that aren't currently running
Guards
select only relays suitable for guard position
Exits
select only relays suitable for exit position
Family
A59E1E7C7EAEE083D756EE1FF6EC31CA3D
Select family by fingerprint or nickname
AS Number
AS39138
select only relays from AS number
Country Code
de
select only relays from country with code
Exits
All relays
Fast exit relays (95+ Mbit/s, 5000+ KB/s, 80/443/554/1755, 2 relays per /24)
Almost fast exit relays (80+ Mbit/s, 2000+ KB/s, 80/443, not in set of fast exits)
Fast exits relays any network (95+ Mbit/s, 5000+ KB/s, 80/443/554/1755)
Group
Country
group relays by country
AS
group relays by AS
Display
Number of results
-1
display only the top results (-1 for all)
Submit
Reset

Tor Compass beta | Home | Trac Ticket #6498

#	Consensus Weights	Advertised Bandwidth	Guard Probability	Middle Probability	Exit Probability	Nickname	Fingerprint	Exit	Guard	Country	Autonomous System
1	3.2680%	1.0554%	1.6295%	1.6295%	6.5450%	TorLand1	4E377F91	Exit	Guard	??	AS13213 UK-2 Ltd Autonomous System
2	2.9021%	0.9346%	1.4470%	1.4471%	5.8122%	chaoscomputerclub20	CFA48FC3	Exit	Guard	de	AS39138 rrbone UG
3	2.4947%	0.8704%	1.2439%	1.2439%	4.9961%	chaoscomputerclub19	A59E1E7C	Exit	Guard	de	AS39138 rrbone UG
4	1.6714%	1.1596%	0.0000%	3.8116%	1.2026%	manning1	073F2793	Exit	-	us	AS29761 OC3 Networks & Web Solutions, LLC
5	1.4552%	0.9069%	0.7256%	0.7256%	2.9144%	TorLand2	332895D0	Exit	Guard	??	AS13213 UK-2 Ltd Autonomous System
6	1.3638%	1.1625%	0.0000%	3.1100%	0.9812%	dorrisdeebrown	C1E2CF4B	Exit	-	us	AS8100 IPTelligent LLC
7	1.1891%	0.3974%	0.5929%	0.5929%	2.3815%	chaoscomputerclub4	659DF653	Exit	Guard	de	AS20773 Host Europe GmbH
8	1.1143%	0.3121%	0.0000%	2.5411%	0.8017%	Unnamed	2624AE04	Exit	-	se	AS47155 ViaEuropa Sweden
9	1.0478%	0.4420%	0.5224%	0.5224%	2.0984%	kramse	3C5DF71E	Exit	Guard	dk	AS197564 Solido Networks ApS
10	1.0228%	0.5791%	0.5100%	0.5100%	2.0484%	assk	8543536F	Exit	Guard	se	AS51815 Teknikbyran i Sverige AB
11	0.9480%	0.3556%	0.0000%	2.1618%	0.6821%	Unnamed	AE5A97FA	Exit	-	se	AS47155 ViaEuropa

Tor Compass beta | Home | Trac Ticket #6498

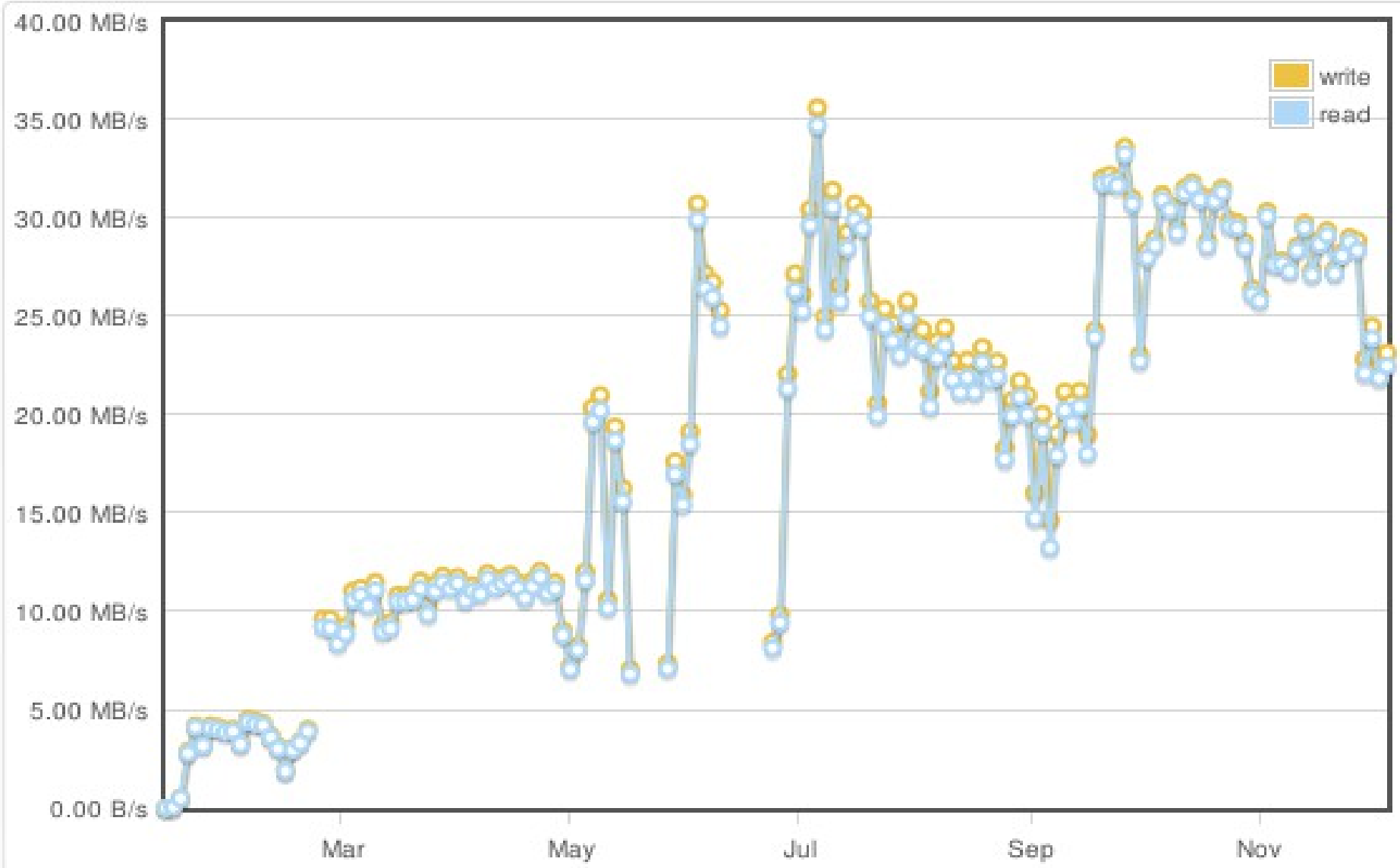
#	Consensus Weights	Advertised Bandwidth	Guard Probability	Middle Probability	Exit Probability	Nickname	Fingerprint	Exit	Guard	Country	Autonomous System
11	16.9410%	9.3179%	7.3388%	12.4071%	31.0763%	*	(93 relays)	(93)	(50)	de	(36)
11	16.4037%	15.9140%	4.2991%	22.0444%	22.8665%	*	(196 relays)	(196)	(58)	us	(94)
11	6.9328%	3.5566%	2.4072%	7.2074%	11.1835%	*	(18 relays)	(18)	(6)	??	(10)
11	5.9957%	3.9851%	1.4297%	8.5637%	7.9934%	*	(35 relays)	(35)	(17)	se	(14)
11	4.3453%	3.6399%	1.1942%	5.6417%	6.1998%	*	(62 relays)	(62)	(18)	nl	(21)
11	2.0473%	1.6717%	0.4237%	3.1546%	2.5635%	*	(69 relays)	(69)	(13)	fr	(15)
11	1.5967%	1.0994%	0.7739%	0.8758%	3.1405%	*	(23 relays)	(23)	(11)	ca	(13)
11	1.5656%	3.3506%	0.7397%	0.9267%	3.0302%	*	(15 relays)	(15)	(10)	ro	(5)
11	1.3084%	0.7519%	0.6420%	0.6896%	2.5936%	*	(14 relays)	(14)	(6)	dk	(8)
11	0.7217%	1.2861%	0.1452%	1.1270%	0.8928%	*	(134 relays)	(134)	(13)	ru	(49)
11	0.7048%	0.6389%	0.3347%	0.4111%	1.3686%	*	(12 relays)	(12)	(5)	ch	(5)
11	0.6985%	0.3215%	0.3387%	0.3826%	1.3742%	*	(28 relays)	(28)	(5)	gb	(16)
11	0.6395%	0.7764%	0.2571%	0.5397%	1.1218%	*	(26 relays)	(26)	(6)	ua	(17)
11	0.6238%	0.6516%	0.1891%	0.7468%	0.9354%	*	(21 relays)	(21)	(2)	lu	(2)
11	0.4634%	0.4638%	0.2308%	0.2320%	0.9274%	*	(14 relays)	(14)	(12)	cz	(8)
11	0.4285%	0.2444%	0.2136%	0.2141%	0.8580%	*	(3 relays)	(3)	(2)	gr	(2)
11	0.3941%	0.2973%	0.1961%	0.1979%	0.7883%	*	(2 relays)	(2)	(1)	a2	(2)
11	0.3166%	0.5118%	0.0431%	0.5680%	0.3388%	*	(8 relays)	(8)	(1)	eu	(5)
11	0.2070%	0.2899%	0.1022%	0.1070%	0.4119%	*	(10 relays)	(10)	(3)	pl	(7)
11	0.0730%	0.1709%	0.0010%	0.1630%	0.0551%	*	(9 relays)	(9)	(1)	at	(5)
11	0.0510%	0.1195%	0.0000%	0.1162%	0.0367%	*	(4 relays)	(4)	(0)	lv	(4)
11	0.0235%	0.0295%	0.0117%	0.0117%	0.0471%	*	(1 relays)	(1)	(1)	md	(1)

Tor Compass *beta | Home | Trac Ticket #6498

#	Consensus Weights	Advertised Bandwidth	Guard Probability	Middle Probability	Exit Probability	Nickname	Fingerprint	Exit	Guard	Country	Autonomous System
14	9.4299%	3.5801%	4.7018%	4.7020%	18.8854%	*	(4 relays)	(4)	(4)	de	AS39138 rrbone UG
15	6.4778%	2.9081%	2.3550%	6.3564%	10.7218%	*	(3 relays)	(3)	(2)	??	AS13213 UK-2 Ltd Autonomous System
17	5.0251%	4.8345%	0.8015%	8.5954%	5.6782%	*	(7 relays)	(7)	(4)	us	AS29761 OC3 Networks & Web Solutions, LLC
14	3.6971%	1.8147%	1.8434%	1.8435%	7.4043%	*	(6 relays)	(6)	(6)	de	AS20773 Host Europe GmbH
14	3.5358%	2.7354%	1.1278%	4.0330%	5.4464%	*	(5 relays)	(5)	(3)	nl	AS43350 NFOrce Entertainment BV
13	2.9845%	3.5895%	0.0000%	6.8059%	2.1473%	*	(3 relays)	(3)	(0)	us	AS8100 IPTelligent LLC
13	2.8958%	1.7706%	0.7035%	4.0899%	3.8940%	*	(33 relays)	(33)	(11)	fr	AS16276 OVH Systems
14	2.8739%	2.1561%	1.4329%	1.4330%	5.7556%	*	(8 relays)	(8)	(8)	us	AS22219 Applied Operations, LLC
13	2.6111%	1.0402%	0.0000%	5.9544%	1.8786%	*	(3 relays)	(3)	(0)	se	AS47155 ViaEuropa Sweden
15	1.8436%	1.1358%	0.9192%	0.9193%	3.6922%	*	(2 relays)	(2)	(2)	se	AS51815 Teknikbyran i Sverige AB
13	1.6806%	3.5000%	0.7199%	1.2600%	3.0618%	*	(13 relays)	(13)	(8)	ro	AS39743 Voxility SRL
14	1.0478%	0.4420%	0.5224%	0.5224%	2.0984%	*	(1 relays)	(1)	(1)	dk	AS197564 Solido Networks ApS

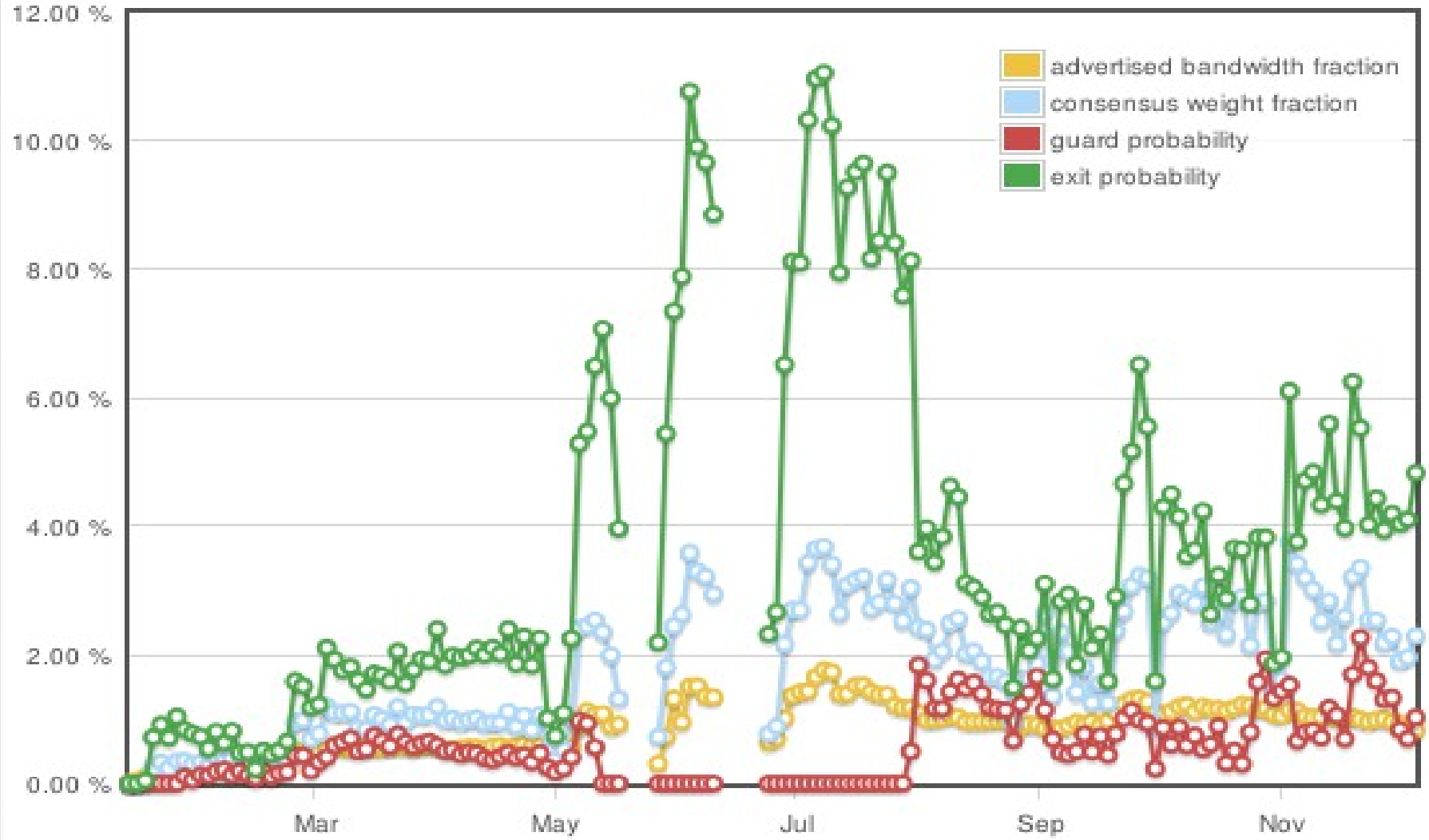
Tor Status *beta

Home About Search



1 Year graph

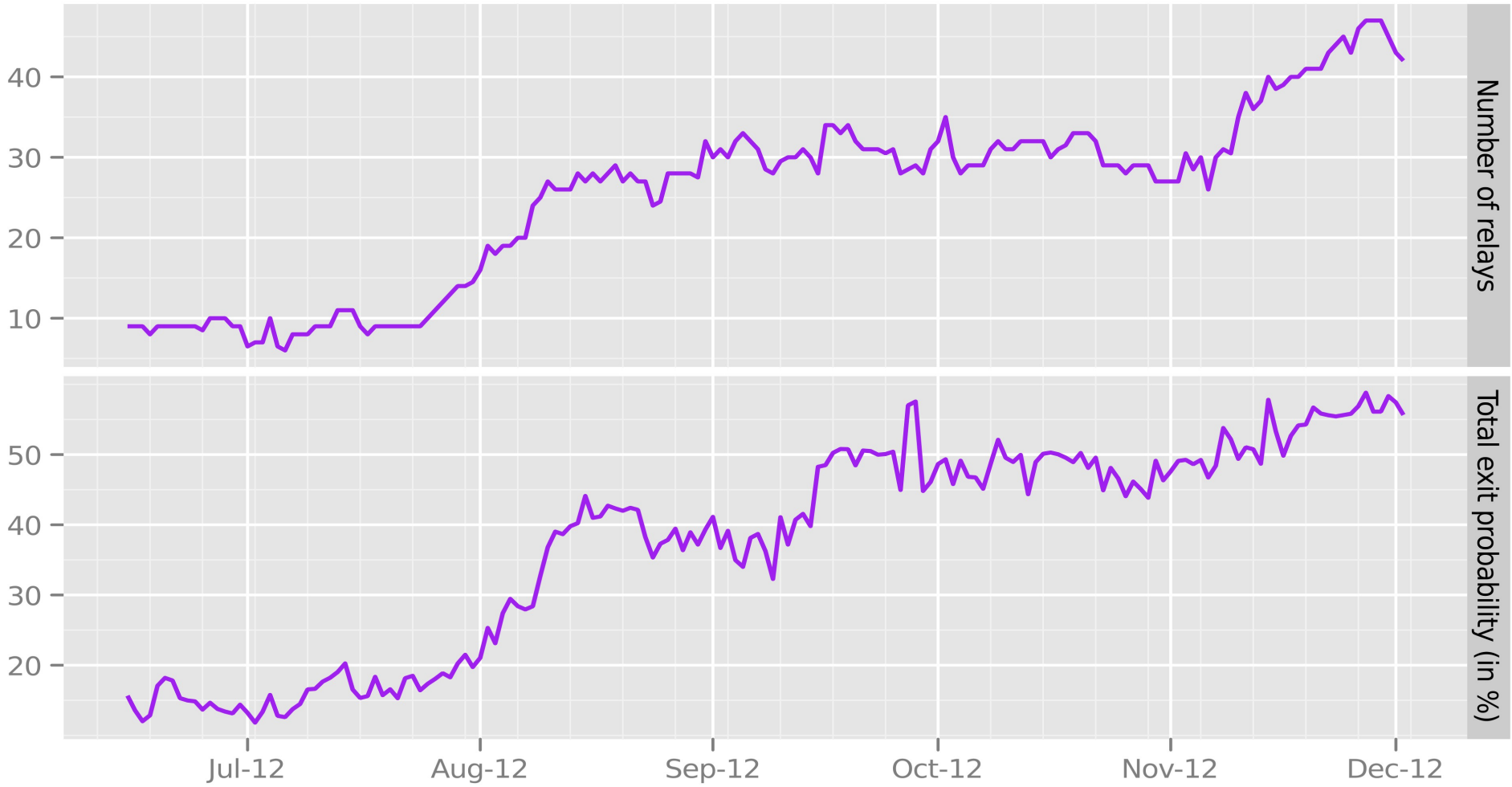
Save Graph



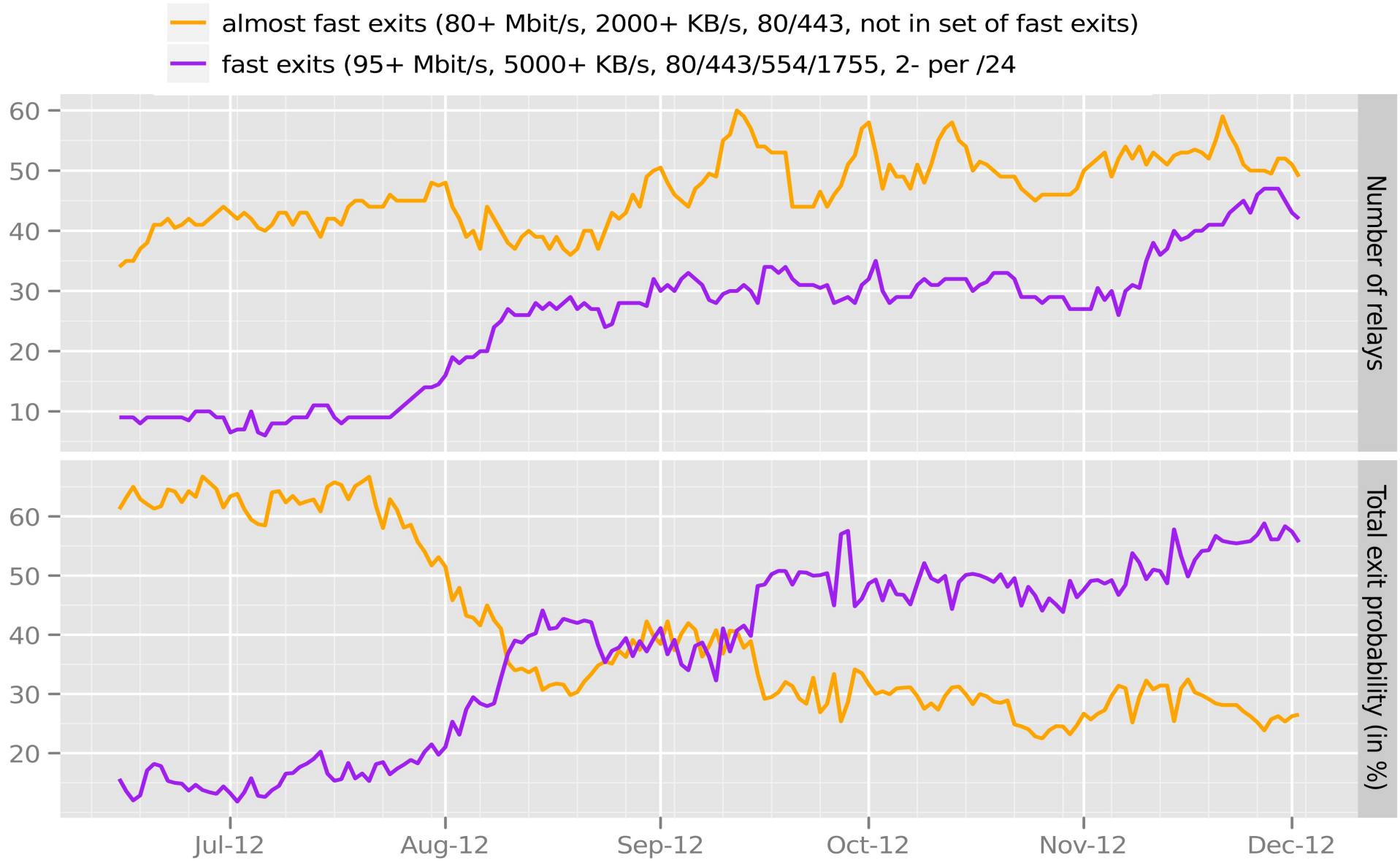
1 Year graph

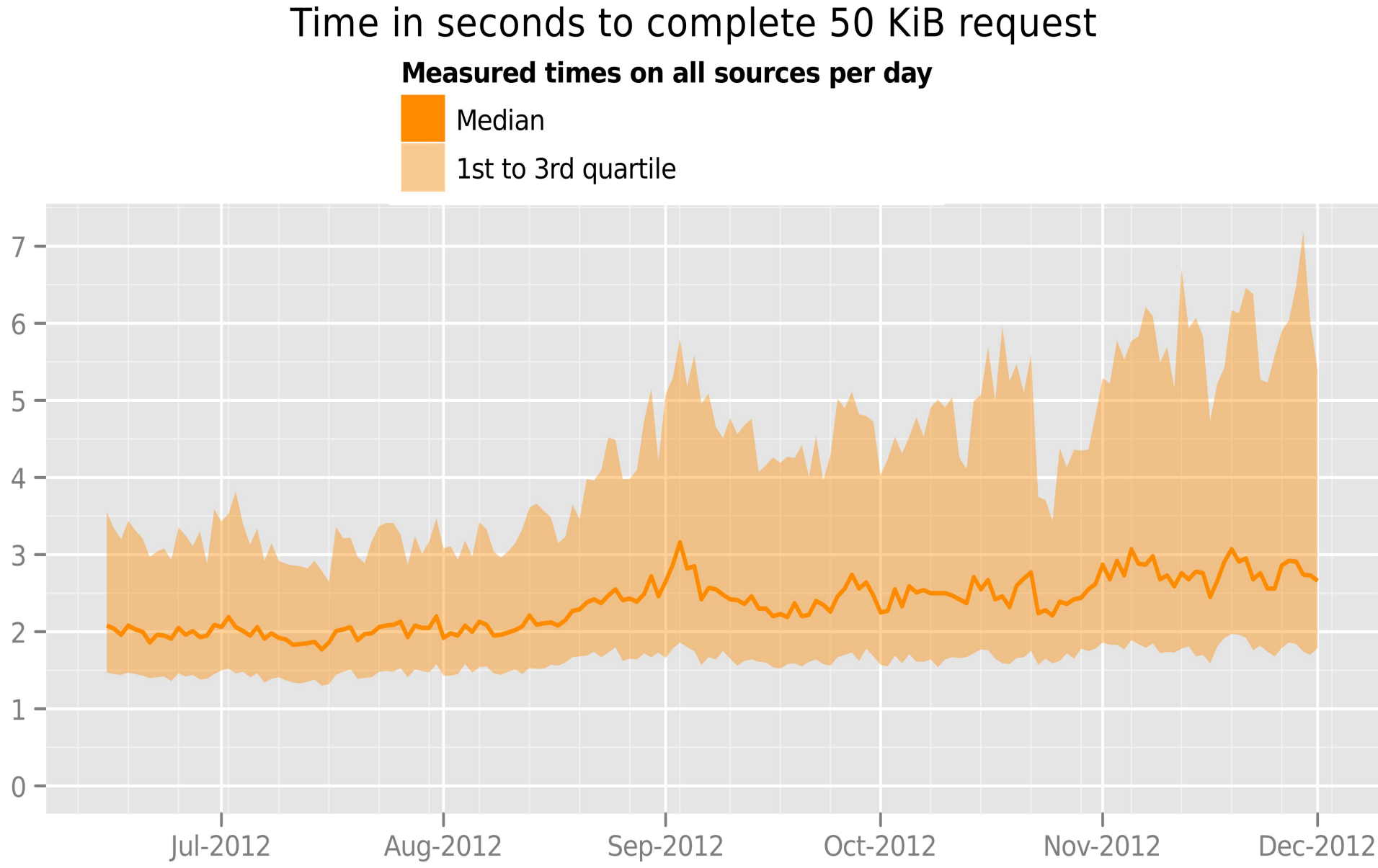
Save Graph

Fast exits (95+ Mbit/s configured bandwidth rate,
5000+ KB/s advertised bandwidth capacity,
exit to ports 80, 443, 554, and 1755,
at most 2 relays per /24 network)

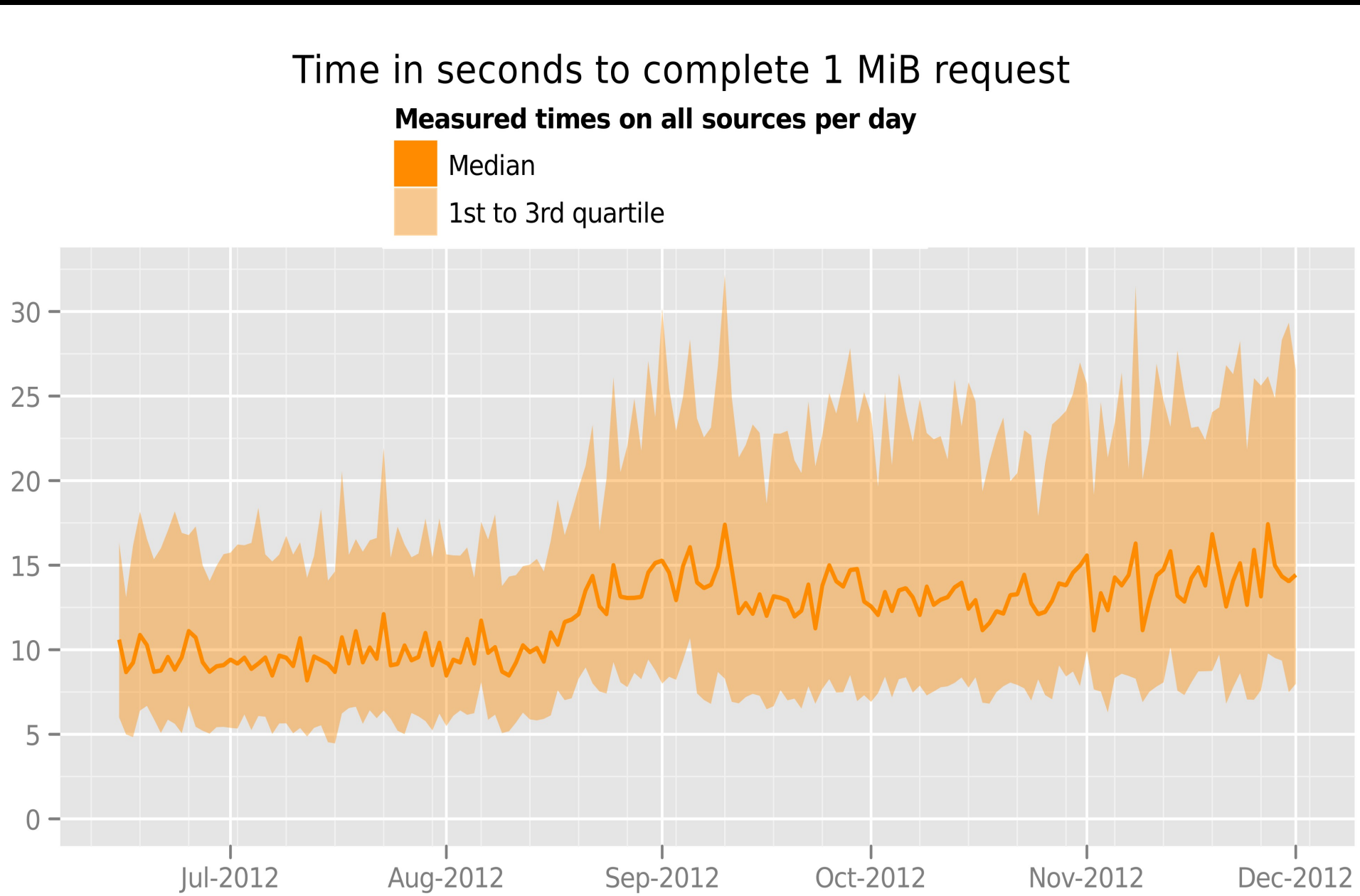


Relays almost meeting the fast-exit requirements





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



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

Today's plan

- ~~0) Crash course on Tor~~
- ~~1) Recent censorship~~
- ~~2) Pluggable transport work~~
- ~~3) Simulations / Performance~~
- ***4) Attacks on low-latency anonymity***

Operational attacks

- You need to use https – correctly.
- Don't use Flash.
- Who runs the relays?
- What local traces does Tor leave on the system?
- ...Different talks.

Traffic confirmation (1)

- If you can see the flow into Tor and the flow out of Tor, simple math lets you correlate them.
- “Passive Attack Analysis for Connection-Based Anonymity”, 2003
- Window-based analysis (2004)

Countermeasures?

- Defensive dropping (2004)? Adaptive padding (2006)?
- Traffic morphing (2009), Johnson (2010)
- Tagging attack, traffic watermarking

Traffic confirmation (2)

- Feamster's AS-level attack (2004), Edman's followup (2009), Murdoch's sampled traffic analysis attack (2007).
- Mid-latency systems (e.g. alpha-mixing, 2006) a solution?
- Drac (2010) for VoIP

Traffic confirmation (3)

- How about adding padding?
  - Really expensive
  - Need to send consistently, even when offline
  - Webserver needs to pad too
  - And even then, active attacks
- How about caching at exits?

Congestion attacks (1)

- Murdoch-Danezis attack (2005) sent constant traffic through every relay, and when Alice made her connection, looked for a traffic bump in three relays.
- Couldn't identify Alice – just the relays she picked.

Congestion attacks (2)

- Hopper et al (2007) extended this to (maybe) locate Alice based on latency.
- Chakravarty et al (2008) extended this to (maybe) locate Alice via bandwidth tests.
- Evans et al (2009) showed the original attack doesn't work anymore (too many relays, too much noise) – but “infinite length circuit” makes it work again?

Congestion attacks (3)

- Packet-spinning (2008) just used the congestion attack to knock out all the honest relays.

Throughput fingerprinting

- Mittal et al, CCS 2011
- Build a test path through the network. See if you picked the same bottleneck node as Alice picked.

Anonymity / load balancing

- Give more load to fast relays, but less anonymity
- Client-side network observations, like circuit-build-timeout or congestion-aware path selection

Bandwidth measurement

- Bauer et al (WPES 2009)
- Clients used the bandwidth as reported by the relay
- So you could sign up tiny relays, claim huge bandwidth, and get lots of traffic
- Fix is active measurement.

  (Centralized vs distributed?)

Tor gives three anonymity properties

- **#1**: A local network attacker can't learn, or influence, your destination.
- **#2**: No single router can link you to your destination.
- **#3**: The destination, or somebody watching it, can't learn your location.

Tor's safety comes from diversity

- #1: Diversity of relays. The more relays we have and the more diverse they, the fewer attackers are in a position to do traffic confirmation.
- #2: Diversity of users and reasons to use it. 60000 users in Iran means almost all of them are normal citizens.

Long-term passive attacks

- Matt Wright's predecessor attack
- Overlier and Syverson, Oakland 2006
- The more circuits you make, the more likely one of them is bad
- The fix: guard relays
- But: guard churn so old guards don't accrue too many users

Website fingerprinting

- If you can see an SSL-encrypted link, you can guess what web page is inside it based on size.
- Does this attack work on Tor? Open-world vs closed-world analysis.
- Considering multiple pages (e.g. via hidden Markov models) would probably make the attack even more effective.

Denial of service as denial of anonymity

- Borisov et al, CCS 2007
- If you can't win against a circuit, kill it and see if you win the next one
- Guard relays also a good answer here.

Epistemic attacks on route selection

- Danezis/Syverson (PET 2008)
- If the list of relays gets big enough, we'd be tempted to give people random subsets of the relay list
- But, partitioning attacks
- Anonymous lookup? DHT? PIR?

Profiling at exit relays

- Tor reuses the same circuit for 10 minutes before rotating to a new one.
- (It used to be 30 seconds, but that put too much CPU load on the relays.)
- If one of your connections identifies you, then the rest lose too.
- What's the right algorithm for allocating connections to circuits safely?

Declining to extend

- Tor's directory system prevents an attacker from spoofing the whole Tor network.
- But your first hop can still say “sorry, that relay isn't up. Try again.”
- Or your local network can restrict connections so you only reach relays they like.

Attacks on Tor

- Pretty much any Tor bug seems to turn into an anonymity attack.
- Many of the hard research problems are attacks against all low-latency anonymity systems. Tor is still the best that we know of – other than not communicating.
- People find things because of the openness and thoroughness of our design, spec, and code. We'd love to hear from you.