Stinks (U)

[redacted]

CT SIGDEV

[redacted]

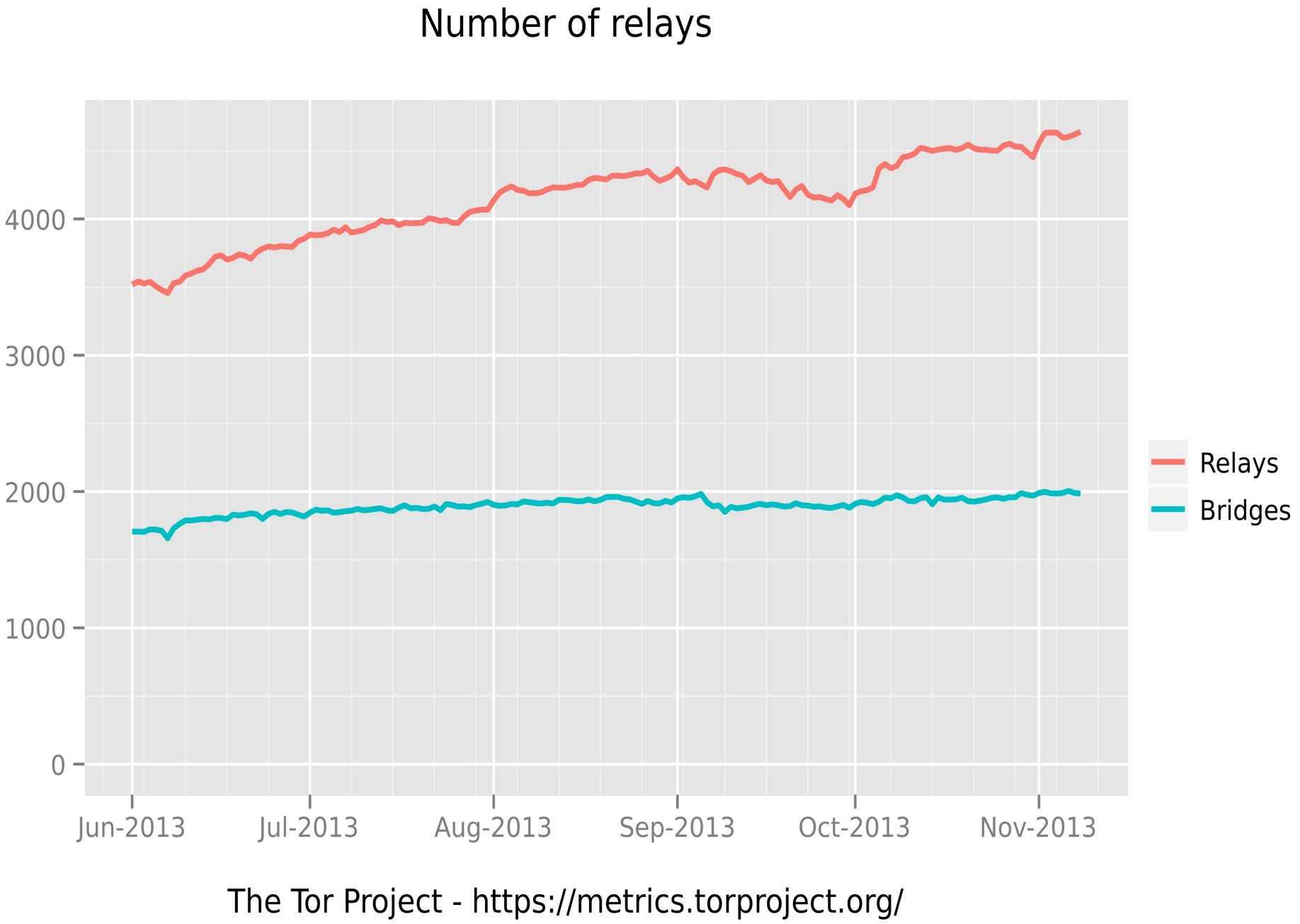
JUN 2012

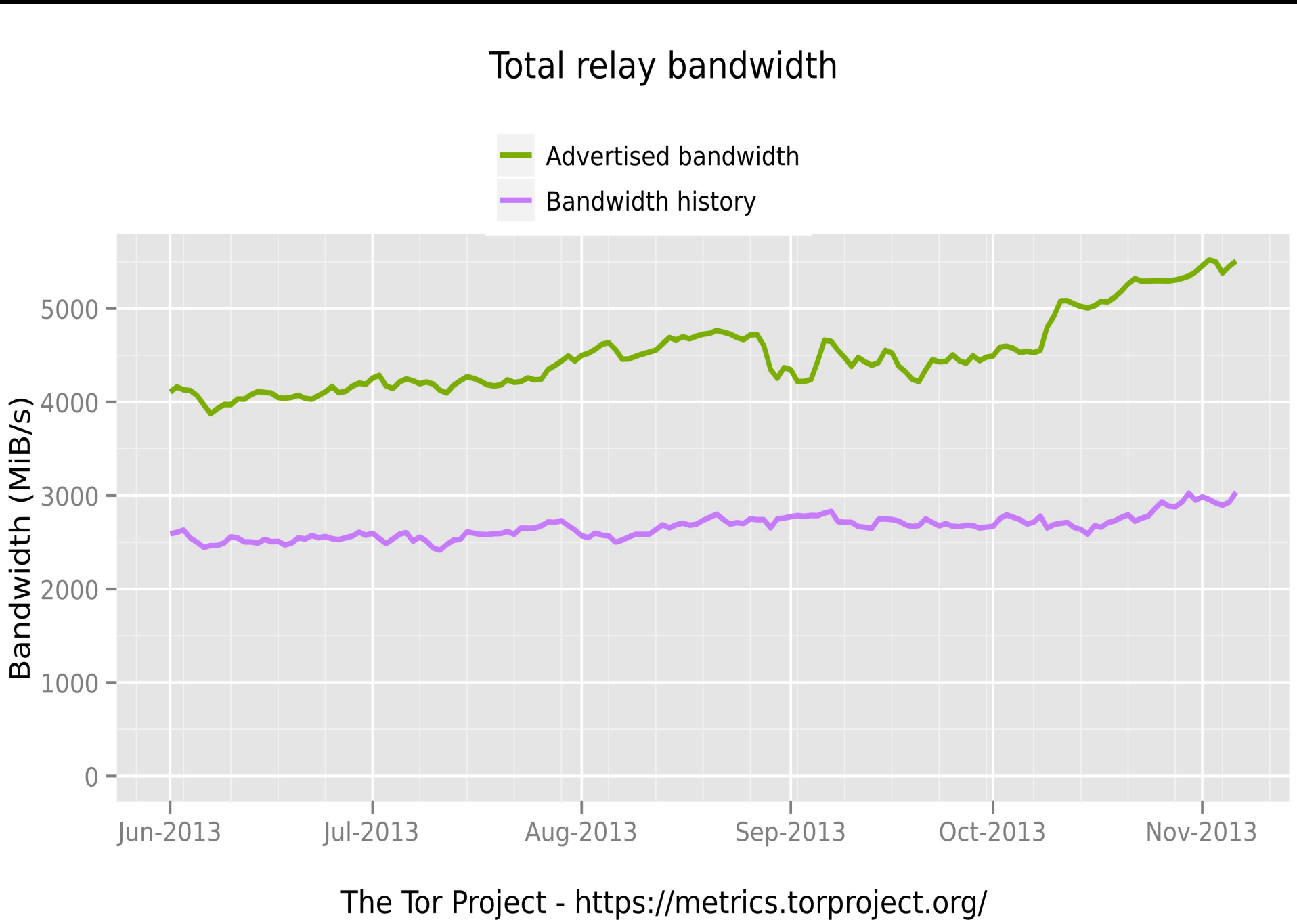
Derived From: [redacted]
Dated: [redacted]
[redacted] On: [redacted]

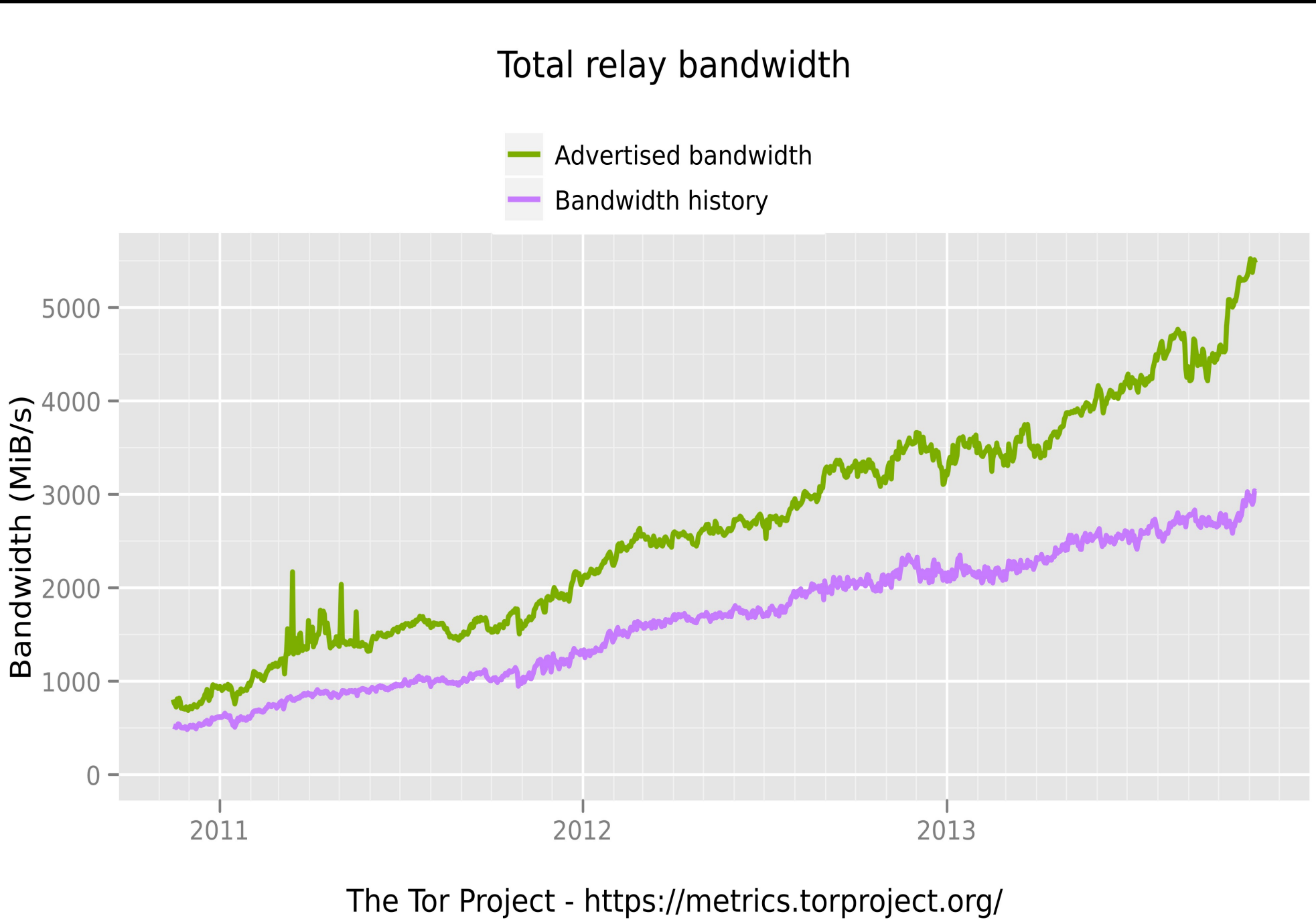
“Still the King of high secure, low latency Internet Anonymity”

Contenders for the throne:

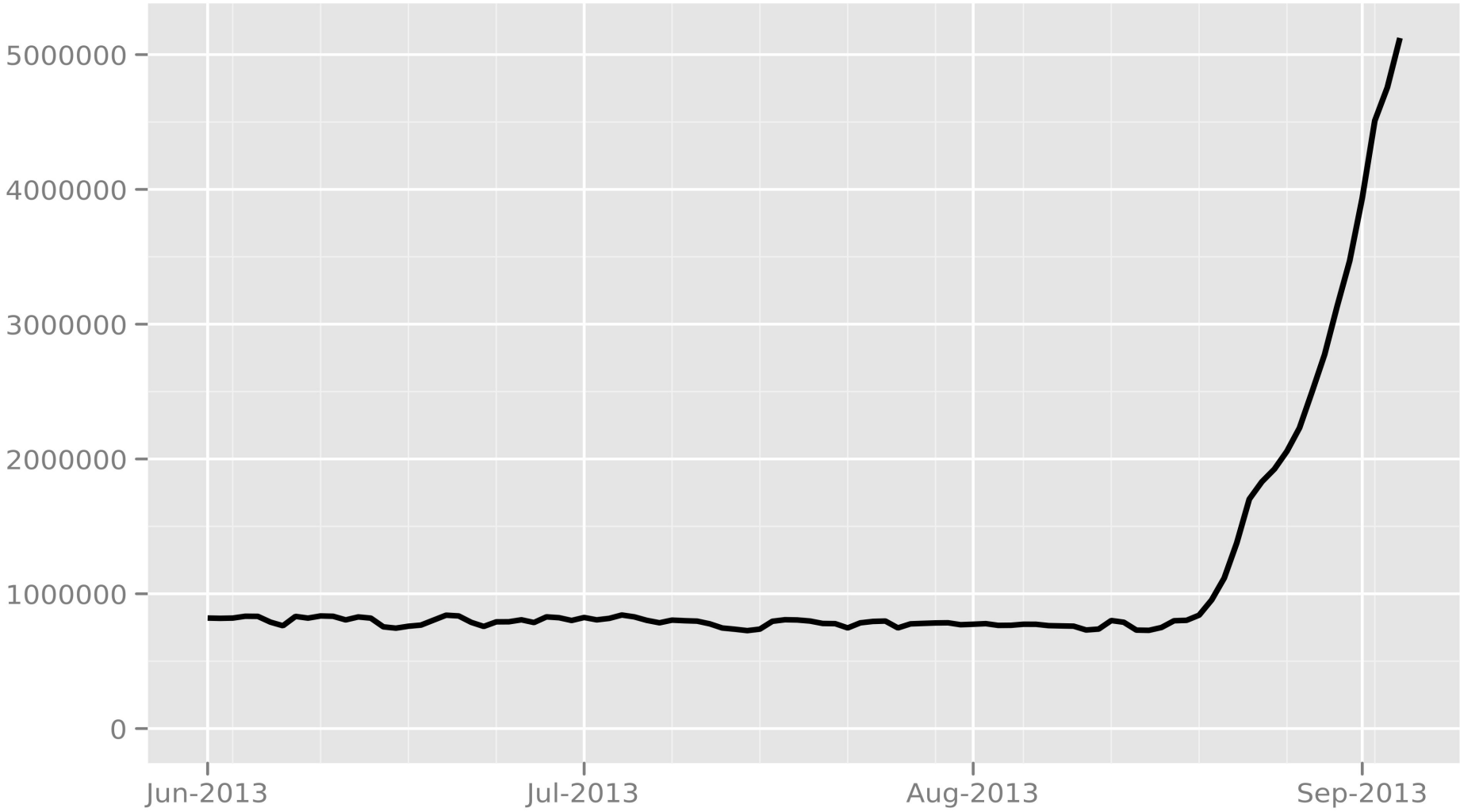
- None


Number of relays
4000
3000
2000
1000
0
Jun-2013
Jul-2013
Aug-2013
Sep-2013
Oct-2013
Nov-2013
Relays
Bridges
The Tor Project - https://metrics.torproject.org/


Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
5000
4000
3000
2000
1000
0
Jun-2013
Jul-2013
Aug-2013
Sep-2013
Oct-2013
Nov-2013
The Tor Project - https://metrics.torproject.org/

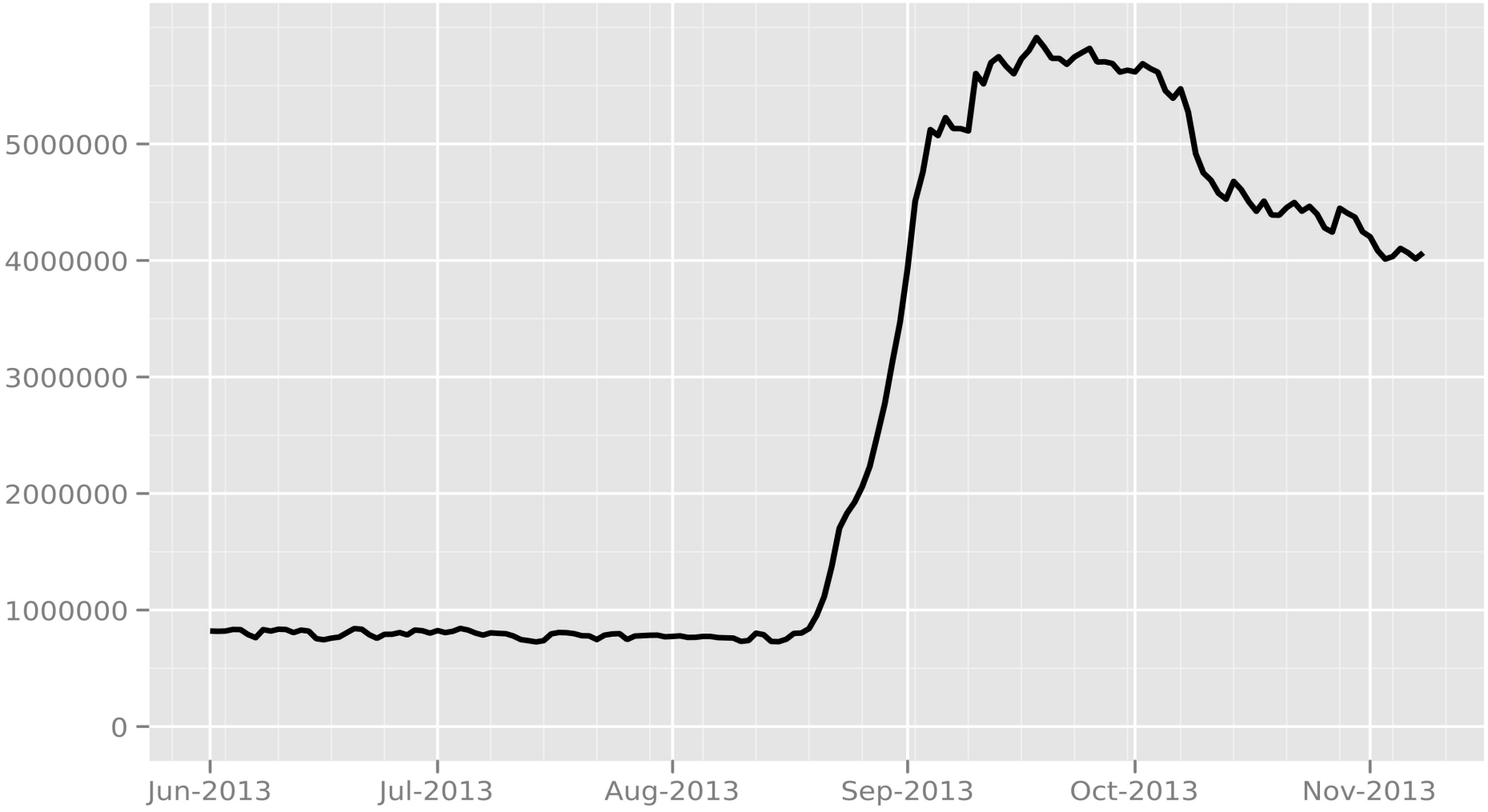

Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
5000
4000
3000
2000
1000
0
2011
2012
2013
The Tor Project - https://metrics.torproject.org/

Number of daily Tor users

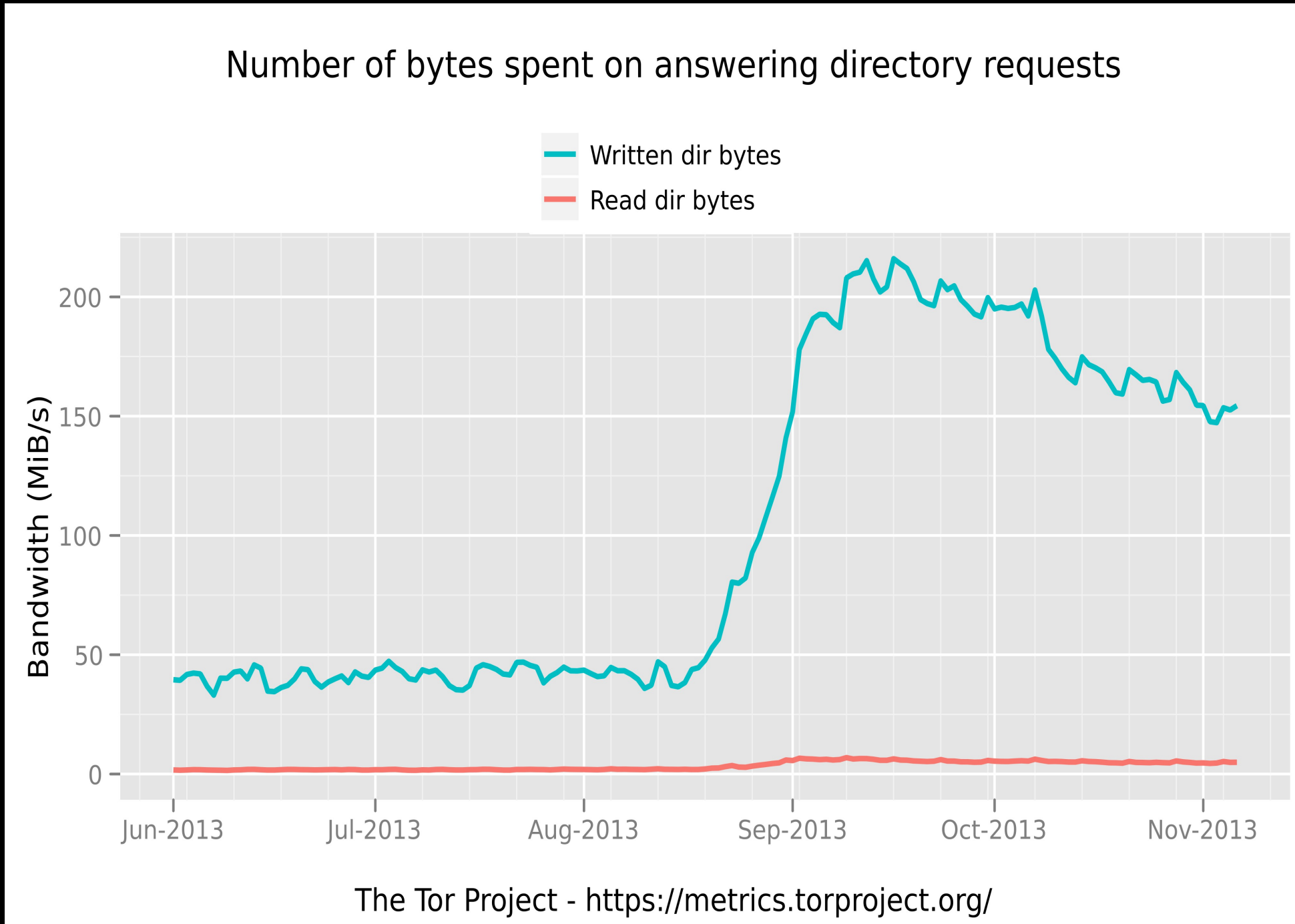


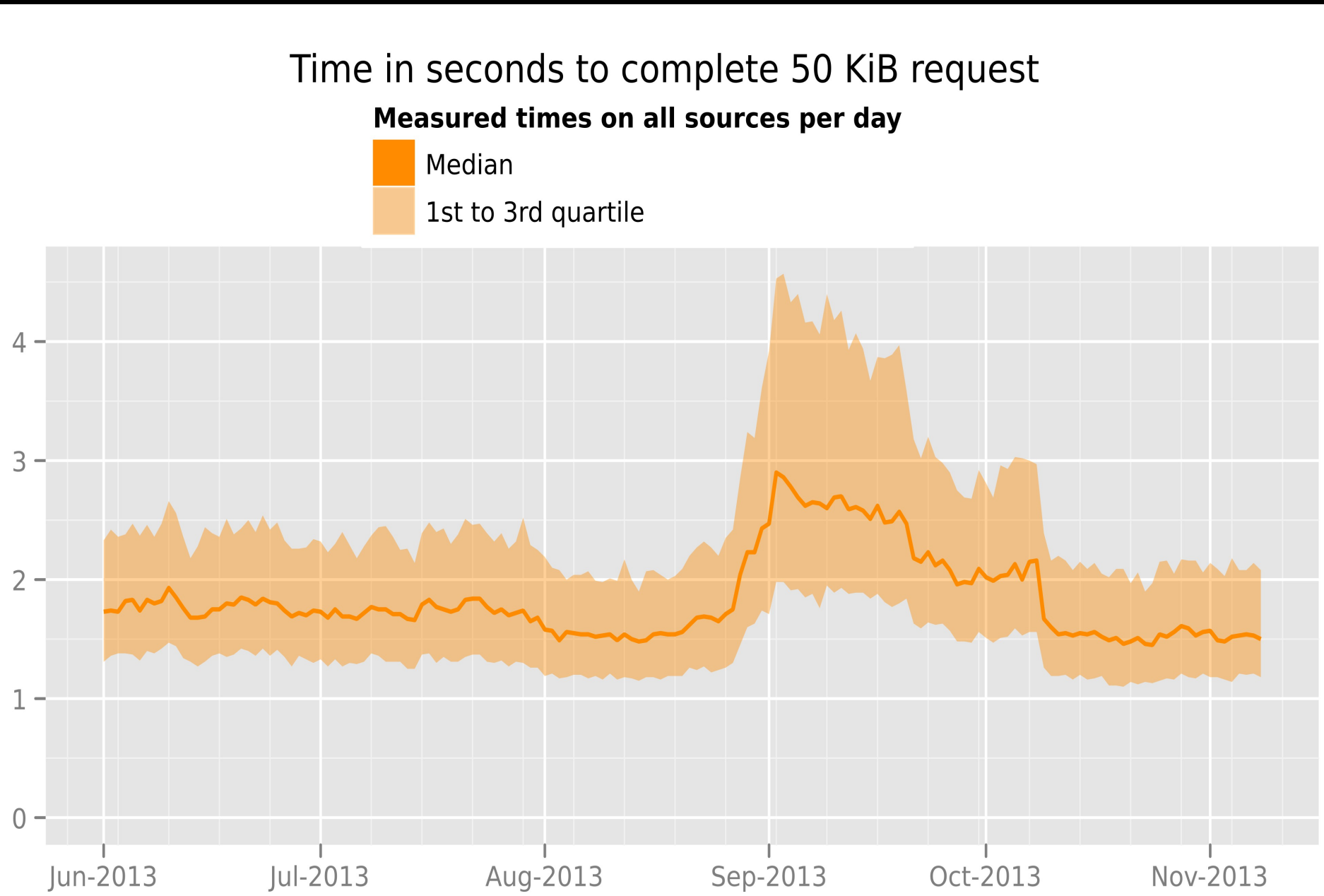
The Tor Project - https://metrics.torproject.org/

Number of daily Tor users

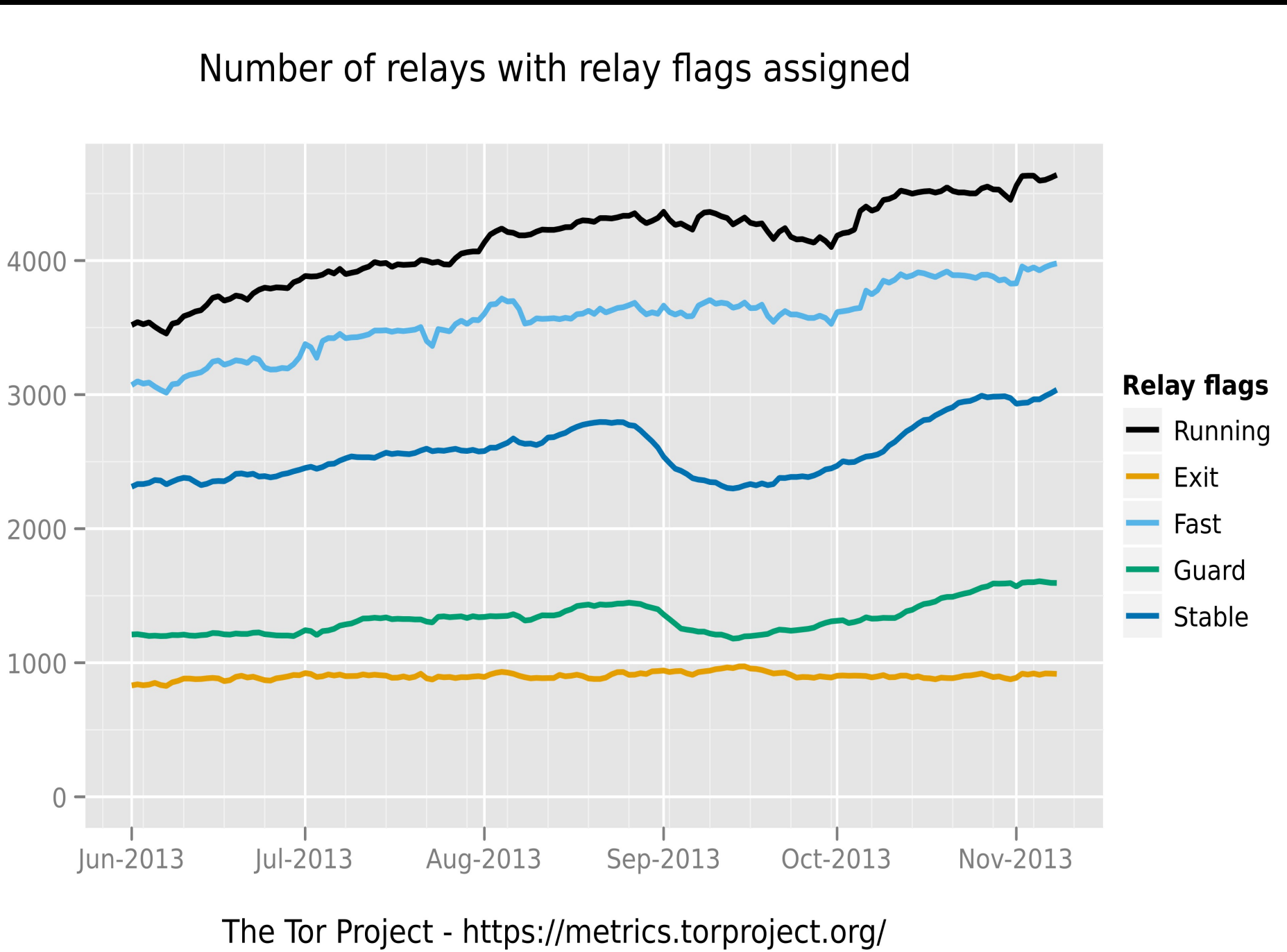


The Tor Project - https://metrics.torproject.org/


Number of bytes spent on answering directory requests
Written dir bytes
Read dir bytes
Bandwidth (MiB/s)
200
150
100
50
0
Jun-2013
Jul-2013
Aug-2013
Sep-2013
Oct-2013
Nov-2013
The Tor Project - https://metrics.torproject.org/



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


Number of relays with relay flags assigned
4000
3000
2000
1000
0
Jun-2013
Jul-2013
Aug-2013
Sep-2013
Oct-2013
Nov-2013
Relay flags
Running
Exit
Fast
Guard
Stable
The Tor Project - https://metrics.torproject.org/

Other world events

- Freedom Hosting
- Silk Road
- NSA / GCHQ articles: QUICK ANT, QUANTUM + FOXACID
- Tor's move to ECC-based TLS/handshakes
- The NSA summer intern 2006 paper

Five performance directions

- Pick the **optimal circuit globally** (and shorter kernel outbufs?)
- Resolve **head-of-line blocking**: Torchestra; Channel abstraction; uTP; Shadow fixes
- Conflux builds **two paths**, load balances
- Static **throttling** (and target bulk transfers?)
- **SPDY** / Caching at exits

Tor 0.2.4.14-alpha .. 0.2.5.1-alpha

- Deal with “too many queued cells” DoS
- Relays prioritize NTor over TAP
- Seccomp2 syscall sandboxing on Linux
- Pluggable transport bridges collect / publish usage stats
- TestingTorNetwork is now smoother
- Many bugfixes

Voice over Tor

- ChatSecure v12 (formerly Gibberbot) for Android now has push-to-talk feature
- Mumble also handles Tor well (but proxy bypass bug)

Pluggable transport news

- Obfs3 observation by Mike Lynn
- Compose Flashproxy + Obfs3
- Flashproxy: Cupcake (Chrome), Badge (FF)
- Obfsproxyssh; pyptlib; goptlib
- Christian Grothoff's auth-in-syn-packet
- uProxy (WebRTC transport)
- 11 criteria for judging a pluggable transport

Tor Browser Bundle 3.x

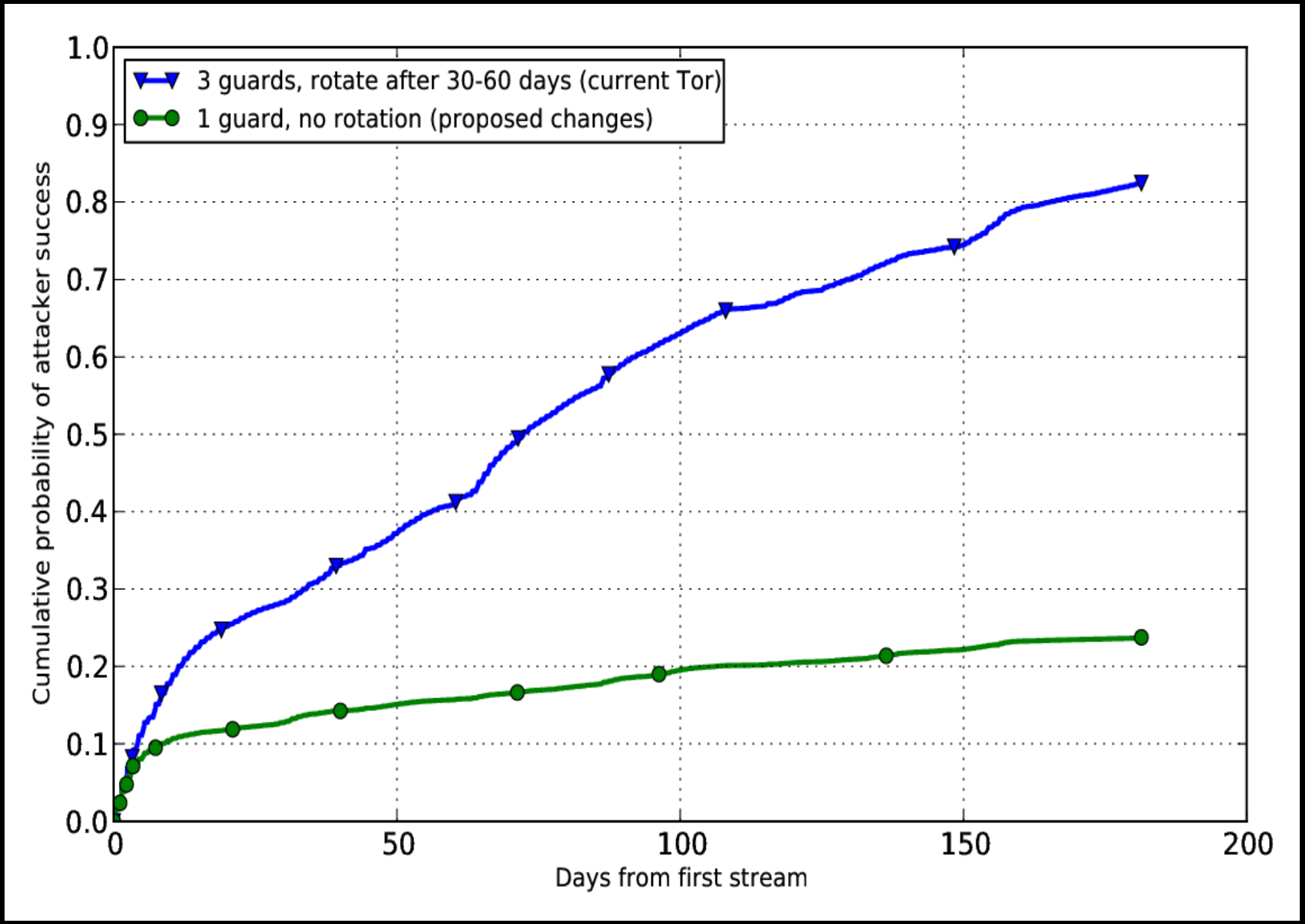
- Deterministic Builds
- “Tor launcher” extension, no Vidalia
- Asks if you want bridges first
- Local homepage, so much faster startup
- Windows NSIS-based extractor
- Security slider (for e.g. JavaScript)
- Privacy fixes, e.g. font enumeration

Hidden service redesign

- Make it hard for HSDir to enumerate .onion addresses
- Hard for attacker to predict HSDir locations into the future
- And stronger keys / handshake

Recent research papers

- Petools, PETS, FOCI, Usenix Security, WPES, CCS
- Scramblesuit, FTE, … 17 new papers on http://freehaven.net/anonbib/ since July
- Remember “Users Get Routed” from Aaron's talk last PI mtg?


3 guards, rotate after 30-60 days (current Tor)
1 guard, no rotation (proposed changes)
Cumulative probability of attacker success
Days from first stream
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1.0
0
50
100
150
200

Other news

- “How to defend Tor against a botnet”
- http://globe.rndm.de/, a new Tor relay metrics visualization tool
- New Stem release (Tor controller lib)
- Tor Browser Bundle forensics tech report
- Torperf redesign tech report
- Roger and Jake in Munich; Jake at CCS

Three ways to destroy Tor

- 1) Legal / policy attacks
- 2) Make ISPs hate hosting exit relays
- 3) Make services hate Tor connections
  - Yelp, Wikipedia, Google, Skype, ...