From: The Tor Project
To: The Tor Community
Date: March 13, 2012

This report documents progress in February 2012.

Research

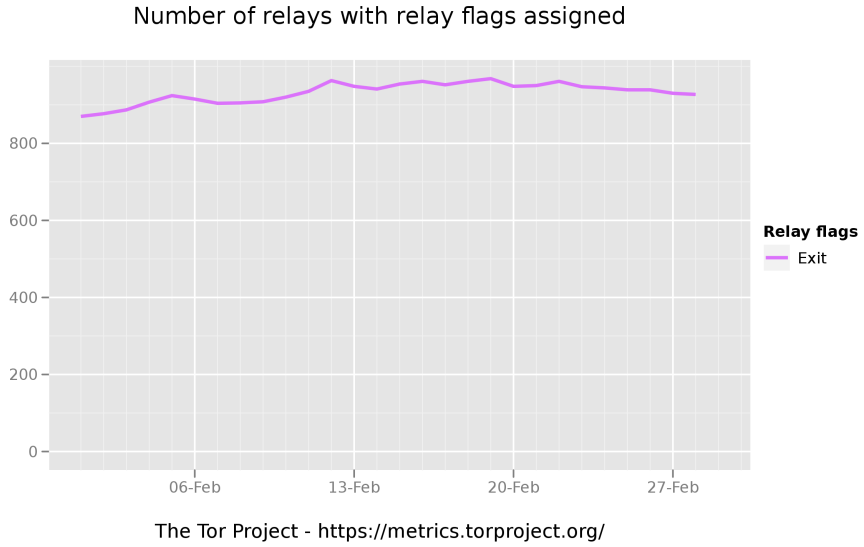
Anonymous Communications

- On February 13, we released a new version of Tor, 0.2.3.12-alpha.

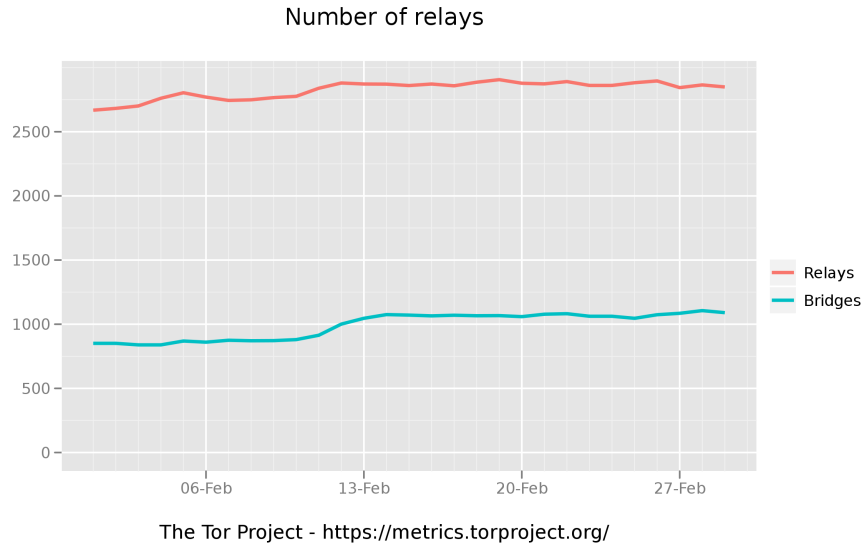
```
Changes in version 0.2.3.12-alpha - 2012-02-13
  Tor 0.2.3.12-alpha lets fast exit relays scale better, allows clients
  to use bridges that run Tor 0.2.2.x, and resolves several big bugs
  when Tor is configured to use a pluggable transport like obfsproxy.

  o Major bugfixes:
    - Fix builds when the path to sed, openssl, or sha1sum contains
      spaces, which is pretty common on Windows. Fixes bug 5065; bugfix
      on 0.2.2.1-alpha.
    - Set the SO_REUSEADDR socket option before we call bind() on outgoing
      connections. This change should allow busy exit relays to stop
      running out of available sockets as quickly. Fixes bug 4950;
      bugfix on 0.2.2.26-beta.
    - Allow 0.2.3.x clients to use 0.2.2.x bridges. Previously the client
      would ask the bridge for microdescriptors, which are only supported
      in 0.2.3.x, and then fail to bootstrap when it didn't get the
      answers it wanted. Fixes bug 4013; bugfix on 0.2.3.2-alpha.
    - Avoid an assert when managed proxies like obfsproxy are configured,
      and we receive HUP signals or configuration values too rapidly. This
      situation happens most commonly when Vidalia tries to attach to
      Tor or tries to configure the Tor it's attached to. Fixes bug 5084;
      bugfix on 0.2.3.6-alpha.
    - Properly set up obfsproxy's environment when in managed mode. The
      Tor Browser Bundle needs LD_LIBRARY_PATH to be passed to obfsproxy,
      and when you run your Tor as a daemon, there's no HOME. Fixes bugs
      5076 and 5082; bugfix on 0.2.3.6-alpha.

  o Minor features:
```

```
  - Use the dead_strip option when building Tor on OS X. This reduces
    binary size by almost 19% when linking openssl and libevent
    statically, which we do for Tor Browser Bundle.
  - Fix broken URLs in the sample torrc file, and tell readers about
    the OutboundBindAddress, ExitPolicyRejectPrivate, and
    PublishServerDescriptor options. Addresses bug 4652.
  - Update to the February 7 2012 Maxmind GeoLite Country database.

o Minor bugfixes:
  - Downgrade the "We're missing a certificate" message from notice
    to info: people kept mistaking it for a real problem, whereas it
    is seldom the problem even when we are failing to bootstrap. Fixes
    bug 5067; bugfix on 0.2.0.10-alpha.
  - Don't put "TOR_PT_EXTENDED_SERVER_PORT=127.0.0.1:4200" in a
    managed pluggable transport server proxy's environment.
    Previously, we would put it there, even though Tor doesn't
    implement an 'extended server port' yet, and even though Tor
    almost certainly isn't listening at that address. For now, we set
    it to an empty string to avoid crashing older obfsproxies. Bugfix
    on 0.2.3.6-alpha.
  - Log the heartbeat message every HeartbeatPeriod seconds, not every
    HeartbeatPeriod + 1 seconds. Fixes bug 4942; bugfix on
    0.2.3.1-alpha. Bug reported by Scott Bennett.
  - Calculate absolute paths correctly on Windows. Fixes bug 4973;
    bugfix on 0.2.3.11-alpha.
  - Update "ClientOnly" man page entry to explain that there isn't
    really any point to messing with it. Resolves ticket 5005.
  - Use the correct CVE number for CVE-2011-4576 in our comments and
    log messages. Found by "fermenthor". Resolves bug 5066; bugfix on
    0.2.3.11-alpha.

o Code simplifications and refactoring:
  - Use the _WIN32 macro throughout our code to detect Windows.
    (Previously we had used the obsolete 'WIN32' and the idiosyncratic
    'MS_WINDOWS'.)
```

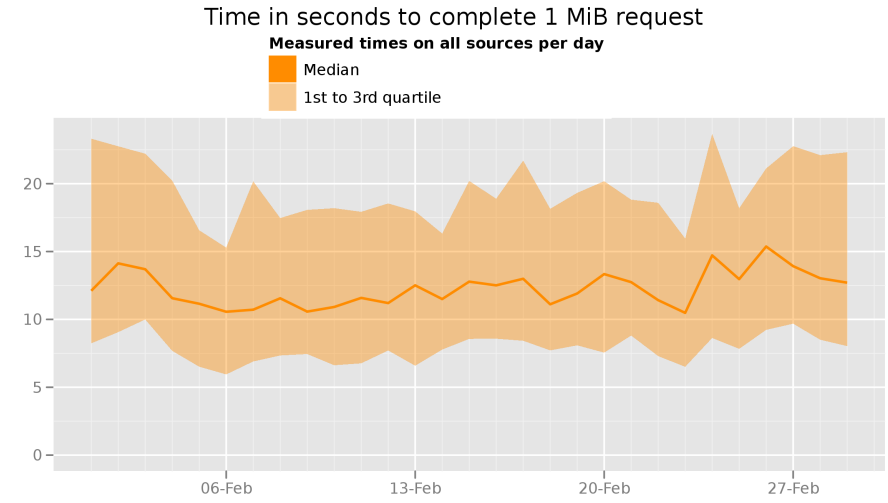
Metrics



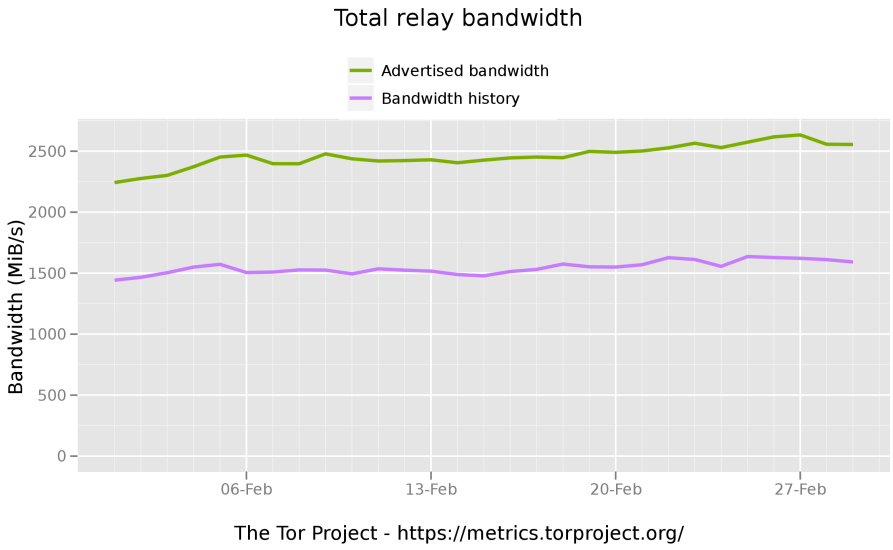
This graph shows the total quantity of exit relays in February 2012.



This graph shows the total quantity of relays and the total quantity of bridges in February 2012.



This graphs shows how many seconds it took to complete a 1 megabyte download from a standard Tor client. We changed from the 50KB download metric to 1 MB because this better reflects real-world web browsing and rich media currently seen on the Internet. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month.

- Karsten, Arturo, and Damian started working on a new Tor Status website, https://atlas.torproject.org/.

Censorship & Circumvention

- On Feb 9, Iran started to filter SSL connections on much of their network. Since the Tor protocol uses SSL, that means Tor stopped working too — even Tor with bridges, since bridges use SSL too.

  We've been quietly developing Obfsproxy, a new tool to make it easier to change how Tor traffic looks on the network. In late 2011 Iran moved into the #2 position in global Tor user count, and several important political events are scheduled in Iran this month and next. This situation seemed like a good time to test our new tool while also helping improve Internet freedom around the world.

  We started with a "Tor Obfsproxy Browser Bundle" with two test obfsproxy bridges in it, to verify that it worked in-country. Then we got over 300 volunteers running more obfsproxy bridges (even with our complex build instructions!), and picked fourteen fast stable trustworthy obfsproxy bridges for an updated bundle which we put out the morning of Feb 11. We spent the weekend fixing usability, stability, and scalability bugs, and put out another bundle on Feb 13 with new versions of Vidalia, Tor, and Obfsproxy.

  Thousands of people in Iran successfully used the Obfsproxy Bundle over the weekend: We did some spot-checking and it seems that the new addresses on Feb 14 are mostly different from the new addresses on Feb 13; but I would guess these are mostly returning users with dynamic IP addresses, rather than actually fresh users. More importantly, these people will be thinking about Obfsproxy next time the filter cracks down — and based on current events, that next time won't be far off. Finally, even though it looks like SSL and Tor are back, I expect Iran will keep throttling SSL traffic as they've been doing for months, so the Obfsproxy bundle will still be more fun to use in Iran than the normal Tor bundles.

  How does it work?

  Deep Packet Inspection (DPI) algorithms classify Internet traffic by protocol. That is, they look at a given traffic flow and decide whether it's http, ssl, bittorrent, vpn, etc. Governments like Iran, China, and Syria increasingly use these tools (and they often purchase them from Western corporations, but that's a different story) to implement their country-wide censorship, either by looking for a given protocol and outright blocking it, or by more subtle mechanisms like squeezing down the bandwidth available to a given protocol to discourage its use.

  Obfsproxy's role is to make it easy for Tor's traffic flows to look like whatever we like. This way Tor can focus on security and anonymity, and Obfsproxy can focus on appearance. The first thing we decided to try looking like was nothing at all: the "obfs2" module adds an encryption wrapper around Tor's traffic, using a handshake that has no recognizable byte patterns.

  It won't work perfectly. For example, the traffic flows will still have recognizable timing, volume, and packet size characteristics; a good entropy test would show that the handshake looks way more random than most handshakes; and the censors could always press the "only allow protocols my DPI box recognizes" panic button. Each step in this arms race aims to force the censor to a) put more development time and DPI resources into examining flows, and b) risk more false positives, that is, risk blocking innocent users that they didn't realize they'd be blocking.

This particular new obfuscating layer isn't the most important feature of Obfsproxy. The best part is that makes it easy to design, deploy, and test other obfuscating layers without messing with the rest of Tor. There's a lot of research into trying to make traffic flows look like other protocols, so for example we could rewrite the Tor flows as valid http that the DPI engine considers harmless. That problem is harder than it sounds — and it sounds hard. But by making a separate component that only has to worry about how the traffic looks, other researchers can try out different strategies without needing to learn so much about the rest of Tor. This approach will also let us easily plug in other transports like Telex, and it will also let other circumvention projects reuse Obfsproxy so they don't have to reinvent our wheels.

Moving forward

One of the choices we faced was how widely and loudly to mention the bundle. While we think it would be hard and/or risky for attackers to block the Obfsproxy protocol, the bundle included 14 preconfigured bridge addresses, and censors could just plug those addresses into their blacklists. We started the weekend telling people to only tell their close friends, but on Sunday we opted for a broader publicity push inside the activist community for two reasons. First, the new Vidalia release (0.2.17) lets users configure their own obfsproxy bridge addresses, so if the preconfigured addresses get blocked the user can just put in new ones. Second, it became clearer that the blocking would let up in a few days once the immediate political pressure was over, and we decided it was more important to get the word out about Obfsproxy in general so these users will know about it next time.

I should point out that I don't think they were targeting Tor here. They were targeting popular websites that use SSL, like Gmail and Facebook. Tor was collateral damage because we opted to make Tor traffic look like SSL. That said, we should not forget that we are on their radar: they targeted Tor by DPI in September 2011, and the Diginotar breakin obtained a fake SSL cert for torproject.org.

The next choice we face is: what other communities should we tell? The bundle works great in China too, where their aggressive censorship has been a real hassle for us the past year or so. Some other countries in Asia appear to be newly using DPI to recognize Tor traffic (more on that in an upcoming blog post). We have more development work to do before we can keep up with the China arms race, including teaching obfsproxy bridges to automatically report their addresses to us and teaching our bridgedb service to give them out, and we need to answer research questions around getting more bridges, giving them out in smarter ways, learning when they get blocked, and making it hard for censors to find them. We also need to spread the word carefully, since the arms race is as much about not drawing the attention of the censors as it is about the technology. But the Obfsproxy Bundle works out of the box right now in every censoring country we know of, so we shouldn't be too quiet about it.

And finally, thanks go to George Kadianakis for taking Obfsproxy on as his Google Summer of Code 2011 Project; to Nick Mathewson for mentoring him and getting the Obfsproxy architecture going in the right direction; to Sebastian Hahn for spending all weekend with me fixing bugs and making packages; and to Karsten Loesing, Erinn Clark, Robert Ransom, Runa Sandvik, Nick, George, and the broader Tor community for stepping up over the weekend to help us take it from "early prototype" to "deployed software in use by 5000+ people" in 72 hours.

Read the full post at https://blog.torproject.org/blog/obfsproxy-next-step-censorship-arms-rac

- In December 2011 we were aware of Kazakhstan increasing Internet censorship in response to some unrest and protests in Zhanaozen in the west. The censorship was then deployed around the country, in many cases with the full support of the populace. The initial invesitgation showed simple IP address blocking coupled with basic dns censorship. Tor continued to work without incident until this week.

  JSC KazTransCom, AS35104, has deployed or begun testing deep packet inspection (dpi) of all Internet traffic. They specifically target SSL-based protocols for blocking. This includes Tor, IPsec, and PPTP-based technologies, as well as some SSL-based VPNs. Business and private users of these technologies are equally affected.

  An example of the censorship, as recorded by volunteers in country, can be found in this network flow diagram. Kazakhstan is identifying and blocking the SSL client key exchange during the setup of an SSL connection. This graph shows the effects of this deployment of censorship based on dpi.

  Luckily, due to our recent experience with Iran we have an answer for people: use obfsproxy. Obfsproxy continues to work in Kazakhstan, as well as Iran. In fact, it works in any country where dpi is used to censor citizens' access to the Internet.

  Thank you to the volunteers for spending their Valentine's Day collecting and analyzing data.

- Two weeks later, we continued research into the censorship in Kazakhstan:

  Two weeks ago we announced the use of deep packet inspection to censor the Internet in Kazakhstan. Over those two weeks we've continued working on how they are blocking native tor connections. The good news is that our obfsproxy bundle continues to work well in country. Thanks to wanoskarnet, ann, and others for their help.

  We have some network-level data captures at both ends to help us assess what is occuring. It seems the Kazakhstan firewall finds something unique in the TLS "Server Hello" message as sent by the Tor relay or bridge and therefore blocks subsequent communications. IP address and TCP port are irrelevant to the censorship. Research continues. Anonymized network flows are available here:

  .kz client to relay: https://media.torproject.org/misc/2012-02-28-tor-kz-client-flow.txt

  and

  the relay view of that same conversation: https://media.torproject.org/misc/2012-02-28-tor-kz-bric
  txt

  Here's a graph of what this censorship looks like nationwide. The red dots are probable censorship events. The full image is here, https://media.torproject.org/image/blog-images/direct-users-off-2011-12-03-on-300-2012-03-02-kz.png.

  Read the full post here, https://blog.torproject.org/blog/updates-kazakhstan-internet-censorshi

Relay

Tor Network

- The Tor Cloud images for all the seven regions have been updated to include the latest cloud image for stable Ubuntu release 10.04.4 LTS (Lucid Lynx). These new images are available on the Tor Cloud website.

  Users who wish to update their existing installations can do so with:

  ```
  apt-get update && apt-get dist-upgrade && reboot.
  ```

Console Client

- Stem development continues, most importantly the implementation and testing of the BaseController class. This is the foundation on which useful controller activity can be based, providing a parallel to TorCtl's asynchronous controller communication (event handling) and sendAndRecv function. Good news is that the BaseController is also designed to be thread safe. Bad news is that getting the deadlocks worked out was difficult and taking over a week.

- Simulated chroot setups for integration testing, https://trac.torproject.org/projects/tor/ticket/4896. This hasn't yet been merged because I haven't added a method for users to provide their chroot prefixes (and hence these integ tests for things like cookie authentication rightfully fail).

- Gave some input on Robert's Safe Cookie proposal and filed a ticket for supporting it in stem, https://trac.torproject.org/projects/tor/ticket/5262. Sathyanarayanan has offered to take the first pass at implementing it.

- Discussions with people helping to make stem better. Sathyanarayanan put the finishing touches on configuration saving, https://trac.torproject.org/projects/tor/ticket/4913, and Neena fixed an integration testing bug, https://trac.torproject.org/projects/tor/ticket/5199.

Tor router

A Onionbox beta program began this month. We shipped Exicto B3 devices off to users to test the user interface and get experience with the general concept of a hardware torouter. We started talking to some hardware engineers about building a base platform for a torouter that can meet our resource requirements for processing the cryptographic calculations, memory consumption, and price point for a commercialized torouter.

Client

- On February 11, we released a new version of the tor controller Vidalia, version 0.2.17.

  ```
  0.2.17  11-Feb-2012
    o Improve the translation policy: do not remove translations that
  ```

are not under 75% done. This re enables Polish and Catalan.

0.2.16 11-Feb-2012

- o Make the default data directory in windows be located in the Local AppData instead of the Roaming one. Fixes bug 2319.
- o Do not launch Firefox with every CIRCUIT_ESTABLISHED signal, do it only if Firefox isn't open yet. Fixes bug 2943.
- o Uses TAKEOWNERSHIP and __OwningControllerProcess to avoid leaving tor running in background if Vidalia exits unexpectedly. Fixes bug 3463.
- o Attempt to remove port.conf file before using it to avoid a race condition between tor and Vidalia. Fixes bug 4048.
- o Do not allow users to check the "My ISP blocks..." checkbox without entering any bridges. Also updates the documentation. Fixes bug 4290.
- o Check that the authentication-cookie file length is exactly 32 bytes long. Fixes bug 4304.
- o Explicitly disable ControlPort auto. Fixes bug 4379.
- o Make the non exit relay option backward compatible with Vidalia < 0.2.14 so that it doesn't confuse users. Fixes bug 4642.
- o Sets the preferred size for the GUI layout so it doesn't squeeze widges when the size isn't big enough. Fixes bug 4656.
- o Removes the option to have only HTTPProxy since it does not work any more as it used to do with older tor versions. Users should use HTTP/HTTPSProxy instead. Fixes bug 4724.
- o Add a hidden configuration option called SkipVersionCheck so systems like Tails can force Vidalia to skip checking tor's version. Resolves ticket 4736.
- o When Tor has cached enough information it bootstraps faster than what takes Vidalia connect to it, so Vidalia does not see the event to update the progress bar. Now Vidalia explicitly asks for bootstrap-phase when it connects to Tor, and updates the progress to what is actually happening instead of hanging in "Authenticating to Tor". Fixes bug 4827.
- o Fix size hints in the main window layout so that tilling window managers display the window properly. Thanks to Mike Warren for the fix. Fixes bug 4907.
- o Vidalia only validates IPv4 bridge lines. IPv6 bridges are now available, and there will be pluggable transport bridge lines. So the validation is now delegated to Tor through SETCONF.
- o Explicitly disable SocksPort auto by setting it to its default (9050). Fixes bug 4598.
- o Sets __ReloadTorrcOnSIGHUP to 0 if SAVECONF failed, which means the user can't write the torrc file. Fixes bug 4833.
- o Enable new translations that are >90% done. The new languages are:

```
    Bulgarian, Czech, Hebrew, Greek, Indonesian, Korean,
    Dutch. Resolves ticket 5051.
  o Remove translations that aren't ready enough: Japanese, Thai,
    Albanian, Vietnamese, Chinese (Taiwan), Polish, Catalan and
    Burmese.
```

Tor Browser

1. On February 3 we released new Tor Browser Bundles.

```
Tor Browser Bundle (2.2.35-5)

    Update Firefox to 10.0
    Update Qt to 4.7.4
    Update OpenSSL to 1.0.0g
    Update zlib to 1.2.6
    Update HTTPS Everywhere to 1.2.2
    Update NoScript to 2.2.8
    New Firefox patches
        Limit the number of fonts per document

Linux changes

    Put documentation in remove-shared-lib-symlinks debug dumps (closes: #4984)

Windows changes

    Make sure mozconfig always gets copied into the Firefox build directory
    (closes: trac ticket #4879)
```

2. On February 13, we released new versions of the Tor Browser Bundle.

```
Tor Browser Bundle (2.2.35-6)

    Update Firefox to 10.0.1
    Update Vidalia to 0.2.17
    Update Libevent to 2.0.17-stable
    Update NoScript to 2.3
```

Obfsproxy

- On February 11, we announced and released alpha versions of obfsproxy tor browser bundles. Learn more at https://www.torproject.org/projects/obfsproxy. We expect to have properly versioned releases of the obfsTBB in March 2012.

Anonymous Computing

No releases this month.

Mobile

We work closely with The Guardian Project to keep tor working on Android and related devices. Learn more about Guardian at https://guardianproject.info.

- The Guardian Project released an updated version of Orbot, version 1.0.7, for Android phones.
- With the public awareness of internet censorship and surveillence growing thanks to SOPA, PIPA and CarrierIQ, not to mention the ongoing unrest in many regions if the world, we have seen a huge spike in interest and download of Orbot, Orweb and Gibberbot. Here are some notable links:
  - http://mobileactive.org/howtos/user-guide-to-orbot
  - http://www.chinagfw.org/2012/01/orbot-tor.html
  - http://geeknews.cz/orbot-svobodnejsi-brouzdani-pro-android/352/
  - http://www.101hacker.com/2012/01/10-must-have-free-android-apps.html

Community

Support

A total of 793 tickets were created in the Tor help desk system this month: 697 tickets are in the queue called help, 29 tickets are in the queue called help-fa, and 67 tickets have been marked as spam.

- The help queue

  697 tickets were created in the help queue this month. 693 of them have been marked as resolved, 4 are currently open and waiting on a reply from a support assistant.

- The help-fa queue

  29 tickets were created in the help-fa queue in December. 28 of them have been marked as resolved, 1 is currently open and waiting on a reply from a support assistant.

- The support requests and other things

  A large number of requests were related to Iran blocking SSL and us building and pushing the obfsproxy Tor Browser Bundle.

Education & Training

No progress this month.

Outreach

1. Andrew, along with Micah Sifry, gave a response to Rebecca McKinnon's Boston Book launch for Consent of the Networked, http://civic.mit.edu/blog/natematias/consent-of-the-networked-the
2. Skep produced some cool graphs of global Tor usage over time, https://media.torproject.org/video/skep/.
3. Andrew was interviewed live by BBC 5 Investigates on the positive uses of the "dark web", http://www.bbc.co.uk/programmes/b01bmpl4.
4. We were featured in a number of news articles about our work in defeating deep packet inspection, starting with recent changes in Iran, https://www.torproject.org/press/inthemedia.html.en.
5. We held a successful hackfest at the University of Washington, https://blog.torproject.org/blog/uw-hackfest-thanks.
6. Jacob spoke at Transmediale, http://www.transmediale.de.
7. Jacob spoke at Technical University of Munich, http://www.tu-berlin.de/.
8. Jacob spoke at University of Luxemborg, http://wwwen.uni.lu/.
9. Jacob presented as a co-author on a paper at Financial Cryptography, http://fc12.ifca.ai/.