The Tor Project:

6th QUARTER OF PROJECT, Q1 OF THE YEAR: January, 2016 – March 31, 2016

<table>
<thead>
<tr>
<th>Grantee:</th>
<th>The Tor Project Inc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Title:</td>
<td>Applying Censorship Resistance Research to the Field</td>
</tr>
<tr>
<td>Grant Number:</td>
<td>S-LMAQM-14-GR-1095</td>
</tr>
<tr>
<td>Primary Point of Contact/Title:</td>
<td>Isabela Bagueros / Project Manager</td>
</tr>
<tr>
<td>Email:</td>
<td><a href="mailto:grants@torproject.org">grants@torproject.org</a></td>
</tr>
</tbody>
</table>

Foreign Assistance Framework: Internet-freedom specific indicators

Q1 project timeline (January 1, 2016 – March 31, 2016) – activity summary

Pluggable Transport integration

Project objectives

Outputs for the quarter

Challenges

Testing and network simulation improvements

Project objectives

Outputs for the quarter

Challenges

Enhanced outreach

Project objectives

Outputs for the quarter
Challenges

Press:

Next quarter's planned activities:

- Pluggable Transport integration
- Testing and network simulation improvements
- Enhanced outreach

Foreign Assistance Framework: Internet-freedom specific indicators

Indicator: Number of unique users of circumvention technology or secure communication technology (measured monthly).

Over the last quarter, we've actually seen a slight decrease in users, with the number oscillating just below 2M. We were above 2M for most of 2015, and we are not seeing any change in current trending for April 2016. Further analysis is needed to identify the causes of this decline.

This graph shows the number of users directly connecting on Tor's network (an average calculation, not the unique number of users):

[Graph showing the number of users directly connecting on Tor's network]

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

Q12016
By way of comparison, here is the Q1 2015 graph.

In contrast, the number of users connecting to Tor using a custom bridge has steadily grown over the quarter, nearly doubling:

As we know, bridges are resources used by the most censored user populations. In events where the censor in the country is blocking access to the Tor network, look at the graphs below.
for United Arab Emirates, on the left you will see the red dots showing the censorship event happening, while on the right we see a big increase of bridge users to bypass the censorship.

Most of this growth is due to the release of a new Tor Browser version that is configured to use our new obfs4 bridge servers:

**Indicator:** Number of civil society actors trained in circumvention or digital safety techniques.

**Result:** 820 civil society actors were trained in circumvention or digital safety techniques.
<table>
<thead>
<tr>
<th>Actors trained</th>
<th>Country</th>
<th>Event and/or partner organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>USA</td>
<td>American Library Association</td>
</tr>
<tr>
<td>25</td>
<td>USA</td>
<td>Medford Public Library</td>
</tr>
<tr>
<td>30</td>
<td>USA</td>
<td>Elon University</td>
</tr>
<tr>
<td>45</td>
<td>USA</td>
<td>Idaho Public Library Director's Summit</td>
</tr>
<tr>
<td>60</td>
<td>Canada</td>
<td>Western University</td>
</tr>
<tr>
<td>80</td>
<td>Ireland</td>
<td>Academic and Special Librarians Association</td>
</tr>
<tr>
<td>40</td>
<td>USA</td>
<td>Simmons College, Boston</td>
</tr>
<tr>
<td>30</td>
<td>USA</td>
<td>Long Island Library Association</td>
</tr>
<tr>
<td>450</td>
<td>USA</td>
<td>Keynote: Code4Lib conference;</td>
</tr>
</tbody>
</table>

**Indicator: Number of USG-supported online tools developed or improved to maintain an open Internet.**

**Result:**

- **Highlights for Pluggable Transport (PT):**
  - New bridges added for obfs4
  - Development of obfs5 (new PT)
  - Remove Flashproxy to simplify the UI
- **Highlights for Testing improvements:**
  - Line of code coverage is at 68.9%
  - Improvements on test infrastructure
  - Creation of tools to help with the project of modularization of Core Tor code

**Indicator: Number of individuals or organizations operating in Internet repressive countries that are provided with technical assistance to increase online security.**

**Result:** 12 individuals operating in internet repressive countries were provided with technical assistance.

<table>
<thead>
<tr>
<th>Individuals trained</th>
<th>Country</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Different locations in Latin America</td>
<td>Internet Freedom Festival in Valencia, Spain.</td>
</tr>
</tbody>
</table>
Indicator: USG-assisted campaigns and programs to enhance public understanding, NGO support and media coverage of digital threats and promotion of an open Internet.

Result: We are focusing on four areas of outreach. Highlights of this work in each area:

- Direct work with organizations
  - Facebook launches Android app Tor support and reports that **1 million people access Facebook through Tor each month**.
- Outreach materials
  - Creative Brief for Tor Project Design Guideline
- Social Media
  - Using tweets to give tips to our users.
- Media Support
  - Examples of how we are presenting Tor’s position for media coverage

Indicator: Number of times USG-supported analytic reports are cited by national and international media outlets.

Result: The metrics published by the Tor Project help illustrate stories about the impact of censorship circumvention tools. They also help provide educational information about the Tor network and services to researchers, activists, journalists, government agencies and so on.

It is difficult to keep count of all the articles in which our metrics are cited, but we include here a selection of articles that highlight how the most-used metrics are cited in the media.

<table>
<thead>
<tr>
<th>Title</th>
<th>Media outlet</th>
<th>Metric cited</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Much Of Tor Is Used For Illegal Purposes?</td>
<td>Cyber Matters</td>
<td>Tor bandwidth metrics</td>
<td>02/09/2016</td>
</tr>
<tr>
<td>Russians Find Ways to Bypass Latest Web Ban</td>
<td>Bloomberg</td>
<td>35% increase in Russian users this year alone</td>
<td>02/01/2016</td>
</tr>
<tr>
<td>This stunning map shows the flow of traffic across the globe using the anonymous network Tor</td>
<td>Business Insider</td>
<td>Animated visualization of Tor traffic across the globe</td>
<td>01/18/2016</td>
</tr>
<tr>
<td>Here's What Tor's Data Looks Like as It Flows Around the World</td>
<td>Wired Magazine</td>
<td>Animated visualization of Tor traffic across the globe</td>
<td>01/17/2016</td>
</tr>
</tbody>
</table>
Indicator: Number of times USG-supported analytic reports are discussed in established social media sites.

Result:

Tor metrics are discussed on social media with direct links to our websites or stories published in media outlets about our metrics. With hundreds of millions of users, it is hard to measure the total reach of our metrics-related posts, but a search for keywords such as “#Tor, usage, metrics” on Twitter¹ provides us with some examples of these conversations on social media during Q1 2016:

1. https://twitter.com/search?f=tweets&vertical=default&q=tor%20usage%2C%20OR%20metrics%20%23Tor%20since%20%3A2016-01-01%20until%3A2016-03-31&src=typd

2. https://twitter.com/OyeBenny/status/690355603248668672

Torflow chart²
Q1 project timeline (January 1, 2016 - March 31, 2016): activity summary

Pluggable transport integration

Project objectives

The goal of this project is to separate Tor's anonymity and privacy properties from its censorship-resistance properties: the core Tor software focuses on building Tor circuits and getting the multi-layer encryption right, while the transport layer focuses on preventing an attacker from recognizing or blocking the client's connections to the rest of the Tor network.

This modular approach lets us "plug in" new transports as needed; plus, since the transport layer is a separate program, it can be written in whatever rapid prototyping language is most convenient, allowing Tor to adapt much more quickly to a censor's new Deep Packet Inspection (DPI) tactics without needing to touch the core Tor program at all.

Outputs for the quarter

Task 1 (SponsorT, aka the work we did via the Internews contract):

We are currently starting work on an extension of our contract for sponsorT. This contract contains two new PT evaluations, in addition to our participation and contribution to the Pluggable Transports Implementers Meetings (PTIM).

In Q1 five Tor people participated in the PTIM in Valencia, Spain. Developers discussed three new draft specifications:

- Pluggable Transport new generation specification
- Go Application Programming Interface (API) specification
- User Datagram Protocol (UDP) support specification

These draft specifications were a collaboration between Tor's Nick Mathewson and Google's Ben Schwartz. Both continue to collaborate on building as a follow-up from the previous PTIM in Washington, D.C., December 2015.
Task 2 (SponsorS, aka this direct contract): Maintain and extend obfsproxy, obfs4proxy, obfsclient and other Pluggable Transport codebases as needed, and assist developers and researchers who wish to use Tor frameworks to do relevant research.

We have made great progress with the development of obfs5\(^3\) (working title). As we mentioned on our last report, the design for this PT will dramatically increase link security to the guard, which is the first connection of the user with the Tor network.

We also created new bridges for obfs4 that are faster and have reported great performance. Here is a sample of stats from one of them:

**Bridge #1**

<table>
<thead>
<tr>
<th>month</th>
<th>rx</th>
<th>tx</th>
<th>total</th>
<th>avg. rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb '16</td>
<td>12.07 TiB</td>
<td>13.48 TiB</td>
<td>25.56 TiB</td>
<td>87.62 Mbit/s</td>
</tr>
<tr>
<td>Mar '16</td>
<td>16.81 TiB</td>
<td>18.84 TiB</td>
<td>35.64 TiB</td>
<td>114.31 Mbit/s</td>
</tr>
<tr>
<td>Apr '16</td>
<td>6.87 TiB</td>
<td>7.75 TiB</td>
<td>14.62 TiB</td>
<td>83.42 Mbit/s</td>
</tr>
</tbody>
</table>

Release of the new obfs4 bridges in mid-February resulted in a spike in Tor adoption rates that continued into March:

---

\(^3\) [https://git.schwanenlied.me/explore](https://git.schwanenlied.me/explore)
Task 3 (SponsorS): Tor side pluggable transport related (and other) improvements.

- Tor 0.2.8.2-alpha release
  - Major bugfixes (bridges, pluggable transports)
    - Modify the check for OR connections to private addresses. Allow bridges on private addresses, including pluggable transports that ignore the (potentially private) address in the bridge line. Fixes bug 18517; bugfix on 0.2.8.1-alpha. Reported by gk, patch by teor.
- Tor Browser 5.5 -- January 26 2016
  - Bug 18113: Randomly permute available default bridges of chosen type
  - Bug 17428: Remove Flashproxy to simplify the UI
  - Bug 18072: Change recommended pluggable transport type to obfs4

Task 4 (SponsorS): Pluggable transport R&D (catchall)

For many years Roger Dingledine has been helping a group of researchers from Berkeley University on their recent published Oakland paper. The paper evaluated censorship techniques used over the years against Tor and how we have been addressing them. These techniques include active probing, which China has used to block Tor. As a result, Tor built a way to circumvent active censorship with Pluggable Transports.

Tor is currently contributing to other projects that presented their progress at February’s Tor’s Dev Meeting in Valencia:

- Usability research of Tor Launcher.
  - Researchers from the Berkeley University demonstrated a working prototype of Tor Launcher.
    - Our developers had the chance to review their findings and give feedback.
    - The prototype has been tested again with users and we hope to see the final paper with the results of this usability research during summer.
- Snowflake, a webrtc Pluggable Transport inspired by flashproxy.
  - Serene, the project’s primary developer, demonstrated a working prototype of Snowflake and got everyone excited to see her progress with this project.

---

4 https://blog.torproject.org/blog/tor-0282-alpha-released
5 https://trac.torproject.org/projects/tor/ticket/18517
6 https://trac.torproject.org/projects/tor/ticket/18113
7 https://trac.torproject.org/projects/tor/ticket/17428
8 https://trac.torproject.org/projects/tor/ticket/18072
10 https://trac.torproject.org/projects/tor/wiki/org/meetings/2016WinterDevMeeting/Notes
12 https://trac.torproject.org/projects/tor/wiki/org/meetings/2016WinterDevMeeting/Notes/UXTorLauncher
Our developers have started the discussion of implementing support for Snowflake on Tor Browser.

Challenges

Pluggable Transport developers are currently holding productive discussions, brainstorming technical specifications, and trying to address some known pain points in both the development but the adoption of Pluggable Transports.

This is a challenge because it will require a lot of dedication and coordination with the community, in order to ensure that the results of developer efforts are useful for everyone.

Testing and network simulation improvements

Project objectives

Tor will improve the correctness and stability of the core Tor software by streamlining and automating the process of launching a complete test; designing and scripting an automated test suite to exercise and stress as much of Tor’s functionality as possible; and extending Tor’s controller interface to allow better monitoring.

Outputs for the quarter

Improvements for testing infrastructure:

We wrote implementations for these tickets in Q1, and they were merged in Q2.

- #16792\(^{15}\) - With this work we can let the test coverage code know that certain lines are expected to be unreachable. By marking these lines, we can focus on those untested lines which are testable, and improve our coverage.  
- #18362\(^{16}\) - Was done to avoid having to implement ugly solutions to the problem of objects pointing to other objects they don’t own. Other, more complex approaches have frequently resulted in hard-to-test object relationships.  

We merged numerous small improvements and fixes to our testing infrastructure Other tickets we would like to mention are:

- #18241\(^{17}\) - Assert that event_base is non-null to avoid annoying bugs.
- #17892\(^{18}\) - Make backtrace test verbose on failure.

\(^{15}\) [https://trac.torproject.org/projects/tor/ticket/16792](https://trac.torproject.org/projects/tor/ticket/16792)  
\(^{16}\) [https://trac.torproject.org/projects/tor/ticket/18362](https://trac.torproject.org/projects/tor/ticket/18362)  
\(^{17}\) [https://trac.torproject.org/projects/tor/ticket/18241](https://trac.torproject.org/projects/tor/ticket/18241)  
\(^{18}\) [https://trac.torproject.org/projects/tor/ticket/17892](https://trac.torproject.org/projects/tor/ticket/17892)
- #16794\(^{19}\) - Make sure we can track all cryptography unit test coverage - it should be above 98% coverage.
- #18490\(^{20}\) - Fixing cross-compile unit test failing error.
- #17153\(^{21}\) - Adding IPv6 private address support for network tests.
- #17808\(^{22}\) - Fixing bug Tor 0.2.7.6 doesn't produce a backtrace on gcc 4.9.3 on OS X 10.11.2

**Modularization effort:**

We also did the following code implementations in Q1, which are aimed to make our code more testable. They are not yet merged, but are under review:

- #18363\(^{23}\) - Created a publish/subscribe abstraction - as part of our effort to modularize our code base.
- #18685\(^{24}\) - Fire a ‘STATUS_SERVER’ event when the hibernation state changes.
- #18803\(^{25}\) - We did a lot of work on this ticket, building the tools to manage Tor’s intermodule callgraph. It builds callgraphs by looking at .o files, and figures out how to move code around based on a set of doxygen instructions. Doing these should help us make our code even more testable in the future by decoupling the modules, and helping us refactor our codebase more safely.

**Unit tests implementations:**

We added more unit tests throughout the code, including those in tickets #16831\(^{26}\), #17075\(^{27}\), #17082\(^{28}\), #17084\(^{29}\), #17003\(^{30}\), #17076\(^{31}\), and #17004\(^{32}\).

We also want to highlight ticket #17101\(^{33}\), which was actually a contribution from a volunteer who created some tests that covers the evaluation of an exit address at the function that rewrites addresses and attaches entry connections to circuits. It is great to see our community incorporating the practices we have been promoting with efforts sponsored by this grant.

\(^{19}\) https://trac.torproject.org/projects/tor/ticket/16794
\(^{20}\) https://trac.torproject.org/projects/tor/ticket/18490
\(^{21}\) https://trac.torproject.org/projects/tor/ticket/17153
\(^{22}\) https://trac.torproject.org/projects/tor/ticket/17808
\(^{23}\) https://trac.torproject.org/projects/tor/ticket/18363
\(^{24}\) https://trac.torproject.org/projects/tor/ticket/18685
\(^{25}\) https://trac.torproject.org/projects/tor/ticket/18803
\(^{26}\) https://trac.torproject.org/projects/tor/ticket/16831
\(^{27}\) https://trac.torproject.org/projects/tor/ticket/17075
\(^{28}\) https://trac.torproject.org/projects/tor/ticket/17082
\(^{29}\) https://trac.torproject.org/projects/tor/ticket/17084
\(^{30}\) https://trac.torproject.org/projects/tor/ticket/17003
\(^{31}\) https://trac.torproject.org/projects/tor/ticket/17076
\(^{32}\) https://trac.torproject.org/projects/tor/ticket/17004
\(^{33}\) https://trac.torproject.org/projects/tor/ticket/17101
Challenges

Although we describe many of our goals in terms of testing methodologies and test coverage, these are only a rough metric of the value of a set of tests. It is easy to forget that these metrics matter only to the extent that they correlate with a reduced incidence of flaws in the codebase and increased coding agility.

While we intend to retain a metrics-driven approach, we should continue to look for further metrics and methods to ensure that our testing is focused on improved quality, and not simply on improved testing.

Enhanced outreach

Project objectives

We seek to make more people aware of the benefits of Tor, especially in the scenario that censorship circumvention needs to be combined with privacy and anonymity to extend the time that civil society members can work in Internet-repressive environments.

Outputs for the quarter

Direct work with organizations

Facebook

Facebook released support for users to use Tor with Facebook’s Android App. It’s great to see such a big company recognizing that there is a significant demand from users to access their services over Tor.

Their feature release got great coverage in the media. Recently Facebook published a blog post announcing that 1 million people uses Facebook over Tor every month.

We hope the success of this project and its visibility will help Tor get other services on board with building Tor support for their users.
1 Million People use Facebook over Tor

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've written previously it's important to us to provide methods for people to use our services securely - particularly if they lack reliable methods to do so.

This is why in the last two years we built the Facebook onion site and onion-mobie site, helped standardise the “.onion” domain name, and implemented Tor connectivity for our Android mobile app by enabling connections through Orbot.

LibrePlanet Award and New Hampshire bill over Tor

We are very proud to report that a member of our community, The Library Freedom Project, has received the Free Software Foundation LibrePlanet 2016 Award\(^34\).

\(^{34}\) [https://twitter.com/torproject/status/711307222735822848](https://twitter.com/torproject/status/711307222735822848)
The impact of such program has been enormous. Libraries abroad are copying it and it is also positively impacting public policy as well. New Hampshire State Rep. Keith Ammon (R), with six bipartisan co-sponsors, presented a bill (NH HB 1508\textsuperscript{35}) that would explicitly permit public libraries to "allow the installation and use of cryptographic privacy platforms on public library computers for library patrons use\textsuperscript{36}.

**Google Summer of Code**

We are also excited to work again with Google Summer of Code (GSoC)\textsuperscript{37}! Last year Tor did not participate in the program, because Google wanted to give opportunity to new projects. Instead, we organized our own Summer of Privacy. While our program was a great success, we are thrilled to be working with GSoC again, and we have already picked our seven students!

\textsuperscript{35} http://www.gencourt.state.nh.us/bill_status/billText.aspx?id=796&txtFormat=html
\textsuperscript{36} https://boingboing.net/2016/02/20/nh-bill-would-explicitly-allow.html
\textsuperscript{37} https://blog.torproject.org/blog/tor-google-summer-code-2016
Outreach materials

We are working with Simply Secure on our first design guideline document. This resource will help us keep our brand identify as we design our outreach materials as well as our websites. This is also a step towards defining a cohesive language that can build with our users.

**Media strategy:**

As part of our efforts to take a proactive role in educating the media about Tor, we have published a couple of statements this quarter about Tor facts and our position on emergent events.

Two statements that we believe to be important to highlight in this report are:

- **Tor’s statement on Cloudflare.** We published a statement together with a fact sheet to help educate the media and our users about Cloudflare’s restrictions of Tor traffic. We are also in direct dialogue with Cloudflare. We hope to shortly work out a good solution for all of our stakeholders.

---

38 https://github.com/simplysecure/tor/blob/master/CreativeBriefforTorProjectStyleGuide.pdf

The Trouble with CloudFlare

Wednesday, CloudFlare blogged that 94% of the requests it sees from Tor are “malicious.” We find that unlikely, and we’ve asked CloudFlare to provide justification to back up this claim. We suspect this figure is based on a flawed methodology by which Cloudflare labels all traffic from an IP address that has ever sent spam as “malicious.” Tor IP addresses are conduits for millions of people who are then blocked from reaching websites under CloudFlare’s system.

We’re interested in hearing CloudFlare’s explanation of how they arrived at the 94% figure and why they choose to block so much legitimate Tor traffic. While we wait to hear from CloudFlare, here’s what we know:

- **A Statement from the Tor Project on software integrity and Apple**\(^{40}\). In response to a broad public dialog about Apple’s response to a FBI demand for a way to circumvent device encryption, Tor issued a statement on the integrity of our development processes. Tor applies best practices to ensure our users get the right software when they download our browser, not a modified version or a way for someone to implement such modification.

  As one of the leaders in the security software industry we want to be seen as a benchmark for others to meet. Our statement presented detail on how we approach security and gained some media traction, as well.

---

\(^{40}\) https://blog.torproject.org/blog/statement-tor-project-software-integrity-and-apple
Security

Tor Project works on anti-FBI defenses amid iOS row with Apple

Vows never to add backdoors, improve tamper detection, remove single points of failure

22 Mar 2016 at 21:31, Iain Thomson

Tor Project fortifies its software to quickly catch spies

The organization has worked for three years to improve its ability to catch fraudulent software
Social media

Beyond our ongoing promotion of Tor user stories and news around our community, we would like to highlight the use of our Twitter accounts (in English and Farsi) to give tips to Tor users. These tweets are part of an organization-wide strategy to more proactively support Tor users:

 torproject ◆ @torproject · Mar 13
Can't download Tor because TorProject.org is blocked? Download #Tor by email!

Download Tor Browser via email

Users can communicate with GetTor robot by sending messages via email. Currently, the best known email address to do this is gettor@torproject.org. This should be the most current and stable GetTor robot as it is operated by Tor Project itself.

To ask for Tor Browser, a user should send an email to GetTor robot with one of the following options in the body of the message:

- windows: If the user needs Tor Browser for Windows.
- linux: If the user needs Tor Browser for Linux.
- osx: If the user needs Tor Browser for Mac OS X.

Challenges

We have reorganized internally to dedicate a single person to leading our community team full time and managing most of our outreach efforts. Alison Macrina of the Library Freedom Project,
who has already been working close with Tor and our community for a few years, has taken on this role.

We are already seeing positive results from this realignment. Alison is driving the team and introducing new ideas that have generated great impact in our outreach effort.

Press

<table>
<thead>
<tr>
<th>Date Published</th>
<th>Media Outlet</th>
<th>Article Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016 Jan 8</td>
<td>Salon</td>
<td>This is the web browser you should be using if you at all about security</td>
</tr>
<tr>
<td>2016 Jan 20</td>
<td>PC World</td>
<td>Privacy-conscious users rejoice: Facebook’s Android app now supports Tor</td>
</tr>
<tr>
<td>2016 Jan 20</td>
<td>The Verge</td>
<td>Facebook’s Android app now lets you flip a switch to browse over Tor</td>
</tr>
<tr>
<td>2016 Jan 19</td>
<td>Tech Insider</td>
<td>You can now connect to Facebook on your phone without leaving a digital trail</td>
</tr>
<tr>
<td>2016 Jan 20</td>
<td>China Digital Times</td>
<td>Facebook Makes App that Can Bypass China’s Censors</td>
</tr>
<tr>
<td>2016 Jan 7</td>
<td>The Daily Dot</td>
<td>Everything you need to know about Tor</td>
</tr>
<tr>
<td>2016 Feb 16</td>
<td>The Daily Dot</td>
<td>The woman who aims to take Tor mainstream</td>
</tr>
<tr>
<td>2016 Jan 8</td>
<td>The Guardian</td>
<td>ProPublica launches world’s first major news site for dark web</td>
</tr>
<tr>
<td>2016 Jan 7</td>
<td>Wired</td>
<td>ProPublica Launches the Dark Web’s First Major News Site</td>
</tr>
<tr>
<td>2016 Jan 18</td>
<td>Sky News</td>
<td>Tor Map Reveals Network's Use Across Europe</td>
</tr>
<tr>
<td>2016 Jan 5</td>
<td>The Register</td>
<td>Tor launches invite-only exploit bug bounty</td>
</tr>
<tr>
<td>2016 Jan 22</td>
<td>Ars Technica</td>
<td>Tor Project raises over $200,000 in attempt to “diversify” its funding</td>
</tr>
<tr>
<td>Date</td>
<td>Source</td>
<td>Summary</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2016 Mar 22</td>
<td>The Register</td>
<td>Tor Project works on anti-FBI defenses amid iOS row with Apple</td>
</tr>
<tr>
<td>2016 Mar 22</td>
<td>ComputerWorld</td>
<td>Tor Project says it can quickly catch spying code</td>
</tr>
<tr>
<td>2016 Mar 21</td>
<td>Softpedia</td>
<td>Like Apple, Tor Devs Would Quit Their Jobs If Ordered to Backdoor Their Software</td>
</tr>
</tbody>
</table>

Next quarter’s planned activities

Pluggable Transport integration

- Our Metrics team has been working on the backend of our infrastructure and they start to look at breaking down Pluggable Transports users per country. This will be a great insight of where we are having demand and which researchers can investigate a country use of it with an event for instance.
- We plan to continue to work on obfs5 development
- Stretch goal, make a Tor Browser build that includes an alpha Snowflake transport.
- Publish the next-gen pluggable transport specifications for wider discussion among developers (assuming the other authors accept this plan).
- Getting more publicity and reach for the upcoming Censorship Systemization of Knowledge paper (to be published at Oakland in May).
- Getting the new "Fallback directories" design in and working for the next Tor stable release, so users in situations where the main Tor directory authorities have been blocked will be able to automatically bootstrap into the Tor network using other locations.
- Explore and resolve a possible "distinguisher" that we've found in the obfs4 protocol, which could allow a censor to recognize and block obfs4 traffic without as much collateral damage as we’d previously thought.

Testing and network simulation improvements

As part of our major bug retrospective, Tor has been compiling a survey of which testing methodologies would have prevented which of the major bugs we've discovered and fixed over the last several years. Results should be released within a few weeks. We expect them to drive the direction of much of our test development. In particular, we'll most likely be focusing on raising the coverage in targeted areas of the code where more bugs have occurred in the past.

We'll start using more of our module isolation tools in practice, to continue to make Tor more testable and simplify our module callgraph, without disrupting our development process.

We'll extend our Chutney-based network tests and controller-based network tests to cover a
wider view array of models of actual user behavior.

We'll continue to require tests for all new code introduced to Tor and ensure that writing tests becomes as easy as possible.

Enhanced outreach

Alisson is working together with other members from the community to acquire a grant dedicated to build resources for our community of relay operators. Resources such as dedicated community manager to keep documentation updated, email list moderation, help point people to answers to their questions (legal, technical etc).

We will continue our education campaign with CloudFlare. We hope that by sharing researches as we did, we can help them understand better the Tor network and stop blocking our users. This is something that our community has been very vocal about and we do want to provide as much information to any part, CloudFlare, website owners, media etc. To help people make informed decisions to what is best for the users.

We also hope that our partnership with companies like Facebook gives a good example of how a company can understand the user need and how providing support for Tor is actually a way to meet a very important need that the UN have even expressed as a right. The right of freedom of expression as well as the right to form an opinion. Which for those you must have the freedom to access information and express yourself.