The Tor Project:

8th QUARTER OF PROJECT, Q34 OF THE YEAR: October 1, 2016 – November 30th, 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>

Q4 project timeline (October 1, 2016 – November 30, 2016): activity summary

Pluggable transport integration

Project objectives

Outputs for the quarter

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.

Task 3 (SponsorS): Tor side pluggable transport related (and other) improvements.

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

Challenges

Testing and network simulation improvements

Project objectives

Outputs for the quarter

Challenges

Enhanced outreach
Project objectives

Outputs for the quarter

Direct work with organizations

Outreach materials

Media strategy:

Social media

Total accumulative numbers for October and November:

Tweets: 81
Tweet impressions: 1.7M
Profile visits: 86.5k
Mentions: 3,057
New followers: 4,200

Challenges

Press

Final report.

Q4 project timeline (October 1, 2016 - November 30, 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
going 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 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 fixed a few bugs on Meek, as part of the new release of it that was merged into Tor Browser release (see Task 3 report)

- **Bug 20250**: meek fails on macOS 10.12 when built with Go 1.4.3 or Go 1.6.3
- **Bug 20451**: The communication stream of managed proxy '/usr/bin/meek-client' is 'closed'

Task 3 (SponsorS): Tor side pluggable transport related (and other) improvements.

- Fixes merged to the following releases - Tor Browser 6.5a4-hardened\(^1\) and Tor Browser 6.5a4\(^2\) and Tor Browser 6.0.6\(^3\):
  - **Bug 20296**: Rotate ports again for default obfs4 bridges
  - **Update meek to 0.25**
    - **Bug 19646**: Wrong location for meek browser profile on OS X
    - **Bug 20030**: Shut down meek-http-helper cleanly if built with Go > 1.5.4
  - **Bug 19838**: Added a new default ofs4 bridge

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

Nothing to report on this.

Challenges

We echo what we stated on our last report. Our main challenge is to have a dedicated person to be Tor representative to lead community efforts around Pluggable Transports.

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

Test coverage:

\(^1\) [https://blog.torproject.org/blog/tor-browser-65a4-hardened-released](https://blog.torproject.org/blog/tor-browser-65a4-hardened-released)
\(^2\) [https://blog.torproject.org/blog/tor-browser-65a4-released](https://blog.torproject.org/blog/tor-browser-65a4-released)
\(^3\) [https://blog.torproject.org/blog/tor-browser-606-released](https://blog.torproject.org/blog/tor-browser-606-released)
We mostly kept working on adding unit tests to new code we created for core tor source.

We also used our testing network to test our 0.2.9 alpha series\(^4\) (which by now is our stable release\(^5\)) helping us discover numerous bugs enabling us to fix them and prepare a stable release in which we were confident could reach production without any big surprises.

**Stem 1.5\(^6\)**

Stem is a Python library for interacting with Tor. This is library can also be used to test Tor in different scenarios and we were happy to have this new version that includes features like Fallback Directory information (we mentioned this new feature on our last report).

**Challenges**

Following up from our last report, we hired a new developer for Core Tor team last year and started the process of hiring a second one in 2017. We hope that adding headcount to the team will help unload some team members who were stretched too thin.

Our next challenge will be to properly onboard our new team members and make sure the team is set to keep up with their good work with the high quality it already has, specially when talking about code tests.

**Enhanced outreach**

**Project objectives**

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

**Outputs for the quarter**

**Direct work with organizations**

**Mozilla - Tor uplifting**

Our work with Mozilla has grown and brought many great results already. For this report we would like to highlight a collaboration we had to fix a zero-day that could be used against Tor Browser and Firefox users. Twelve hours after finding out about the bug the Tor Browser team had a patch for it that Mozilla team upstreamed and both browsers released the fix to their users. This was a great turn around time from both teams, which is great giving the urgency of the matter.

\(^4\) [https://blog.torproject.org/blog/tor-0295-alpha-released-numerous-bugfixes](https://blog.torproject.org/blog/tor-0295-alpha-released-numerous-bugfixes)

\(^5\) [https://blog.torproject.org/blog/tor-0299-released](https://blog.torproject.org/blog/tor-0299-released)

\(^6\) [https://blog.torproject.org/blog/stem-release-15](https://blog.torproject.org/blog/stem-release-15)
Article about the zero day

Mozilla and the Tor Project have acted quickly to patch a zero day bug virtually identical to one used by the FBI a few years ago to unmask users of the anonymizing browser.

It was discovered after the related exploit was posted to a public Tor Project mailing list.

“Exploit took advantage of a bug in Firefox to allow the attacker to execute arbitrary code on the targeted system by having the victim load a web page containing malicious JavaScript and SVG code,” explained Mozilla security lead, Daniel Vesin. “It used this capability to collect the IP and MAC address of the targeted system and report them back to a central server.”

The bug affects Windows, Mac and Linux machines, although the payload of the exploit only

Article about our patch


Working with digital privacy organizations in Chile - Global South Outreach Initiative

Tor has created an effort to build stronger connections with the Global South, we hope to increase awareness around online security, how Tor works, how to become a volunteer and other forms of collaboration with local communities/organizations.

In October Tor was invited by Datos Protegidos, an organization from Chile focus on user privacy, to participate in series of events promoted by them and other organizations.

Workshops:

Tor workshop⁹ on online privacy for librarian students of UTEM (Technological University of Santiago):

We also did workshops for local organizations (no photos) with support of Datos Protegidos, Primavera Hacker (Chile most important grassroots event on online security) and Derechos Digitales (the ‘EFF’ of Latin America). And gave talk explaining Tor to CS students from the Puente Alto Catholic University.

⁹ https://datosprotegidos.org/vigilancia-y-bibliotecas/
Local media coverage

A four page interview with our project manager Isabela Bagueros was published by a local technology magazine, Trend TIC. Isabela talks about the importance of Tor in today’s digital world and clarifies some of the mis-concepts about Tor.

---

10. [https://twitter.com/datospersonales/status/79502797677859072](https://twitter.com/datospersonales/status/79502797677859072)
11. [https://primaverahacker.cl/](https://primaverahacker.cl/)
Outreach materials

Tor Browser User Manual

After months of hard work reviewing and updating the Tor Browser Manual, our Community Team published a new version of it! This new version includes new screenshots, new features information and a complete revision of the language to ensure it was inclusive for all users.

After launching it in English the team exported all strings to Transifex where our community of translators here is a the current localization status of the Manual:

Done:

- Spanish
- French
- Brazilian Portuguese

In progress:

- Arab
- German
- Farsi
- Italian
- Dutch
- Polish
- Russian
- Turkish
- Vietnamese
- Chinese
Announcing the Tor Browser User Manual

The community team is excited to announce the new Tor Browser User Manual! The manual is currently only available in English. We will be adding more languages in the near future, as well as adding the manual to Transifex.

During the creation of this manual, community feedback was requested over various mailing lists / IRC channels. We understand that many people who read this blog are not part of these lists / channels, so we would like to request that if you find errors in the manual or have feedback about how it could be improved, please open a ticket on our bug tracker and set the component to "community".

This manual is part of an ongoing effort to foster wider adoption of Tor, and provide better support to all users, new and old. We'll soon have some more exciting new developments to share about our user support efforts, so stay tuned.

Thanks for using Tor!

phoul's blog

---

Blog post launching new Tor Browser User Manual

Examples of pages inside Tor Browser User Manual

1. Page explaining how to manage identities on Tor Browser

---

[12](https://blog.torproject.org/blog/announcing-tor-browser-user-manual)
Managing identities

When you connect to a website, it is not only the operators of that website who gain record information about your visit. Most websites now use numerous third-party services, including social networking “Like” buttons, analytics trackers, and advertising beacons, all of which can link your activity across different sites.

Using the Tor network helps observers from being able to discover your exact location and IP address, but even without this information they might be able to link different areas of your activity together. For this reason, Tor Browser includes some additional features that help you control what information can be tied to your identity.

The URL bar

Tor Browser centers your web experience around your relationship with the website in the URL bar. Even if you connect to two different sites that use the same third-party tracking service, Tor Browser will force the content to be served over two different Tor circuits, so the tracker will not know that both connections originate from your browser.

On the other hand, all connections to a single website address will be made over the same Tor circuit, meaning you can browse different pages of a single website in separate tabs or windows, without any loss of functionality.

Logging in over Tor

Although Tor Browser is designed to enable total user anonymity on the web, there may be situations in which it makes sense to use Tor with websites that require usernames, passwords, or other identifying information.

If you log into a website using a regular browser, you also reveal your IP address and geographical location to the website. The same is often true when you send an email. Logging into your social networking or email accounts using Tor Browser allows you to choose exactly which information you reveal to the websites you browse. Logging in using Tor Browser is also useful if the website you are trying to reach is censored on your network.

When you log in to a website over Tor, there are several points you should bear in mind:

- See the Secure Connections page for important information on how to secure your connection when logging in.
- Tor Browser often makes your connection appear as though it is coming from an entirely different part of the world. Some websites, such as banks or email providers, might interpret this as a sign that your account has been hacked or compromised, and lock you out. The only way to resolve this is by following the site’s recommended procedure for account recovery, or contacting the operators and explaining the situation.

Changing identities and circuits

Tor Browser features “New Identity” and “New Tor Circuit for this Site” options, located in the Torbutton menu.

New Identity

This option is useful if you want to prevent your subsequent browser activity from being linkable to what you were doing before. Selecting it will close all your open tabs and windows, clear all private information such as cookies and browsing history, and use new Tor circuits for all connections. Tor Browser will warn you that all activity and downloads will be stopped, so take this into account before clicking “New Identity.”

New Tor Circuit for this Site

This option is useful if you are using a service that is unable to connect to the website you require, or is not loading it properly. Selecting it will cause the currently-active tab or window to be reloaded over a new Tor circuit. Other open tabs and windows from the same website will use the new circuit as well once they are reloaded. This option does not clear any private information or undo your activity, nor does it affect your current connections to other websites.

More Information

Tor Browser User Manual
2. Page explaining how Tor Browser updating flow works

Tor Browser User Manual

Updating

Tor Browser must be kept updated at all times. If you continue to use an outdated version of the software, you may be vulnerable to serious security flaws that compromise your privacy and anonymity.

Tor Browser will prompt you to update the software once a new version has been released. The Tor button icon will display a yellow triangle, and you may see a written update indicator when Tor browser opens. You can update either automatically or manually.

Updating Tor Browser automatically

1. Privacy and Security Settings
2. Check for Tor Browser Update

When you are prompted to update Tor Browser, click on the Tor button icon, then select ‘Check for Tor Browser Update’.

When Tor Browser has finished checking for updates, click on the “Update” button.

Wait for the update to download and install, then restart Tor Browser. You will now be running the latest version.

Updating Tor Browser manually

1. When you are prompted to update Tor Browser, finish the browsing session and close the program.
2. Remove Tor Browser from your system by deleting the folder that contains it (see the Uninstalling section for more information).
3. Visit https://www.torproject.org/projects/torbrowser.html.en and download a copy of the latest Tor Browser release, then install it as before.

More Information
Tor Browser User Manual
Media strategy:

The highlights for this period is the buzz around Tor’s ground breaking technology work on Android and the great performance of our teams who worked hard on fixing in matter of hours a zero day security issue that could be used to de-anonymize Tor users.

Android Mission Improbable buzz:

Ars Technica interviewed Mike Perry who worked on a prototype of an Android phone hardened for privacy and security. Mike posted an extensive blog post about his project which together with Ars Technica interview got us a lot of buzz in the media. We are listing some that we have selected at our Press section below.

Buzz on our fix of a zero day that went out in matter of hours:
An email arrived\(^\text{13}\) at our list exposing a zero day that could affect Tor Browser and Firefox users. This was end of day, November 29 EST time zone, and the news got out pretty fast\(^\text{14}\):

During the first hours of November 30, a release with a fix for the issue was published at our blog\(^\text{15}\) and got even more buzz\(^\text{16}\) - we have more references to it at the Press section below as well:

---

\(^{13}\) [link to email]

\(^{14}\) [link to news article]

\(^{15}\) [link to blog post]

\(^{16}\) [link to news article]
Total accumulative numbers for October and November:

- Tweets: 81
- Tweet impressions: 1.7M
- Profile visits: 86.5k
- Mentions: 3,057
- New followers: 4,200

October:

Top mention with over 3k engagements, by Associated Press journalist Frank Bajak. This is a great example of use case for Tor. We often talk about journalists using Tor to talk with their sources and now we can add AP as news outlets that practices that.

To tweet for the month received 55k impressions was another example of journalist / news agency usage of Tor to communicate with their sources:

[Top mention](https://twitter.com/fbajak/status/788646352184016896)

[View Tweet](https://twitter.com/torproject/status/786229910918475776)
November:

Top mention was a tweet from a journalist from Istanbul, Ahmet A. Sabanci, commenting about censorship against VPN services and Tor. The tweet got over 1.8k engagements:

![Tweet from Ahmet A. Sabanci](image)

Top tweet was us announcing our last alpha release on the 0.2.9.x series, the next release would be a ‘rc - release candidate’. The tweet got over 78k impressions:
Challenges

With our Global South initiative part of our Outreach efforts will have evolve the challenge of keeping our message and materials localized. Right now we have a good localization process for Tor Browser and it’s Manual. We are lacking localization for media materials as well as social media. We hope that the effort of having messages for moments of crisis that teaches people about Tor in a database ready to be just copy and pasted and used on social media is a good step towards making it easier for us to reach out communities abroad.

Press

<table>
<thead>
<tr>
<th>Date Published</th>
<th>Media Outlet</th>
<th>Article Title</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 3, 2016</td>
<td>Softpedia</td>
<td>CloudFlare Looking Into New System That Removes CAPTCHAs for Tor Users</td>
<td>“CloudFlare is now researching a new system to protect its clients from malicious Tor traffic, but without bombarding Tor users with endless CAPTCHAs.”</td>
</tr>
<tr>
<td>Oct 4, 2016</td>
<td>The Register UK</td>
<td>Domain name resolution is a Tor attack vector, but don’t worry</td>
<td>Article about scientists research showing possible ways to attack a Tor user using DNS services.</td>
</tr>
<tr>
<td>Oct 5, 2016</td>
<td>SC Magazine</td>
<td>Researchers discover DNS exploit that can identify Tor users</td>
<td>Article about scientists research showing possible ways to attack a Tor user using DNS services.</td>
</tr>
<tr>
<td>Oct 12, 2016</td>
<td>Drexel University</td>
<td>Just Give Me Some Privacy — Anonymous Wikipedia Editors and Tor Users Explain Why They Don’t Want You to Know Who They Are</td>
<td>Article talking about a great research published on why Wikipedia editors chose to use Tor to do their work.</td>
</tr>
<tr>
<td>Oct 13, 2016</td>
<td>Motherboard</td>
<td>Tor Project and Mozilla Making It Harder for Malware to Unmask Users</td>
<td>Article talks about Tor Browser team and Mozilla team collaboration on implementing</td>
</tr>
<tr>
<td>Date</td>
<td>Source</td>
<td>Title</td>
<td>Summary</td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Nov 04, 2016</td>
<td>Yahoo News</td>
<td>Social media interrupted in Turkey after crackdown.</td>
<td>Article about censorship in Turkey. At first there were rumors that Tor was blocked but our OONI team were capable to obtain reports from Turkey that shown Tor was not being blocked. Allowing us to direct users to Tor to bypass the blockade.</td>
</tr>
<tr>
<td>Nov 07, 2016</td>
<td>Motherboard</td>
<td>Turks Are Flocking to Tor After Government Orders Block of Anti-Censorship Tools</td>
<td>Article with updated information and data showing the increase of Tor users coming from Turkey.</td>
</tr>
<tr>
<td>Nov 14, 2016</td>
<td>Forbes</td>
<td>These 6 Simple Tools Help Protect Your Online Privacy.</td>
<td>Article from Forbes showing Tor Browser as their first suggestion on how to protect your online privacy.</td>
</tr>
<tr>
<td>Nov 22, 2016</td>
<td>Ars Technica</td>
<td>Tor phone is antidote to Google “hostility” over Android, says developer</td>
<td>Interview with Mike Perry on his prototype 'Mission Improbable', a more secure option for users of Android phone. Part of our Tor Labs initiative.</td>
</tr>
<tr>
<td>Nov 23, 2016</td>
<td>International Business Times</td>
<td>Tor Phone: Privacy activists developing super private and secure version of Android</td>
<td>Article talking about Mike Perry’s prototype for Android, part of our Tor Labs initiative.</td>
</tr>
<tr>
<td>Nov 23, 2016</td>
<td>iTechPost</td>
<td>Tor Project Is Creating An Ultra Secure And Private Version Of Android</td>
<td>Article talking about Mike Perry’s prototype for Android, part of our Tor Labs initiative.</td>
</tr>
<tr>
<td>Nov 30, 2016</td>
<td>Threat Post</td>
<td>TOR PATCHED AGAINST ZERO DAY UNDER ATTACK</td>
<td>Article talking about our browser update that patches a zero-day vulnerability being exploited in the wild to de-anonymize Tor users.</td>
</tr>
<tr>
<td>Nov 30, 2016</td>
<td>Computer World</td>
<td>Firefox zero-day can be used to unmask Tor browser users</td>
<td>Article talking about zero day vulnerability found on Firefox.</td>
</tr>
<tr>
<td>Nov 30, 2016</td>
<td>The Merkle</td>
<td>Tor Phone Prototype Makes Security And Privacy Accessible To All Smartphone Users</td>
<td>Article talking about Mike Perry’s prototype for Android, part of our Tor Labs initiative.</td>
</tr>
<tr>
<td>Dec 1, 2016</td>
<td>infosecurity</td>
<td>Tor and Mozilla Patch Deanonymizing Zero Day</td>
<td>Article talking about our browser update that patches a zero-day vulnerability being exploited in the wild to de-anonymize Tor users.</td>
</tr>
</tbody>
</table>
Final report.

Work on final report, evaluate our challenges and successes as well as projecting the impact of this work in our future plans.