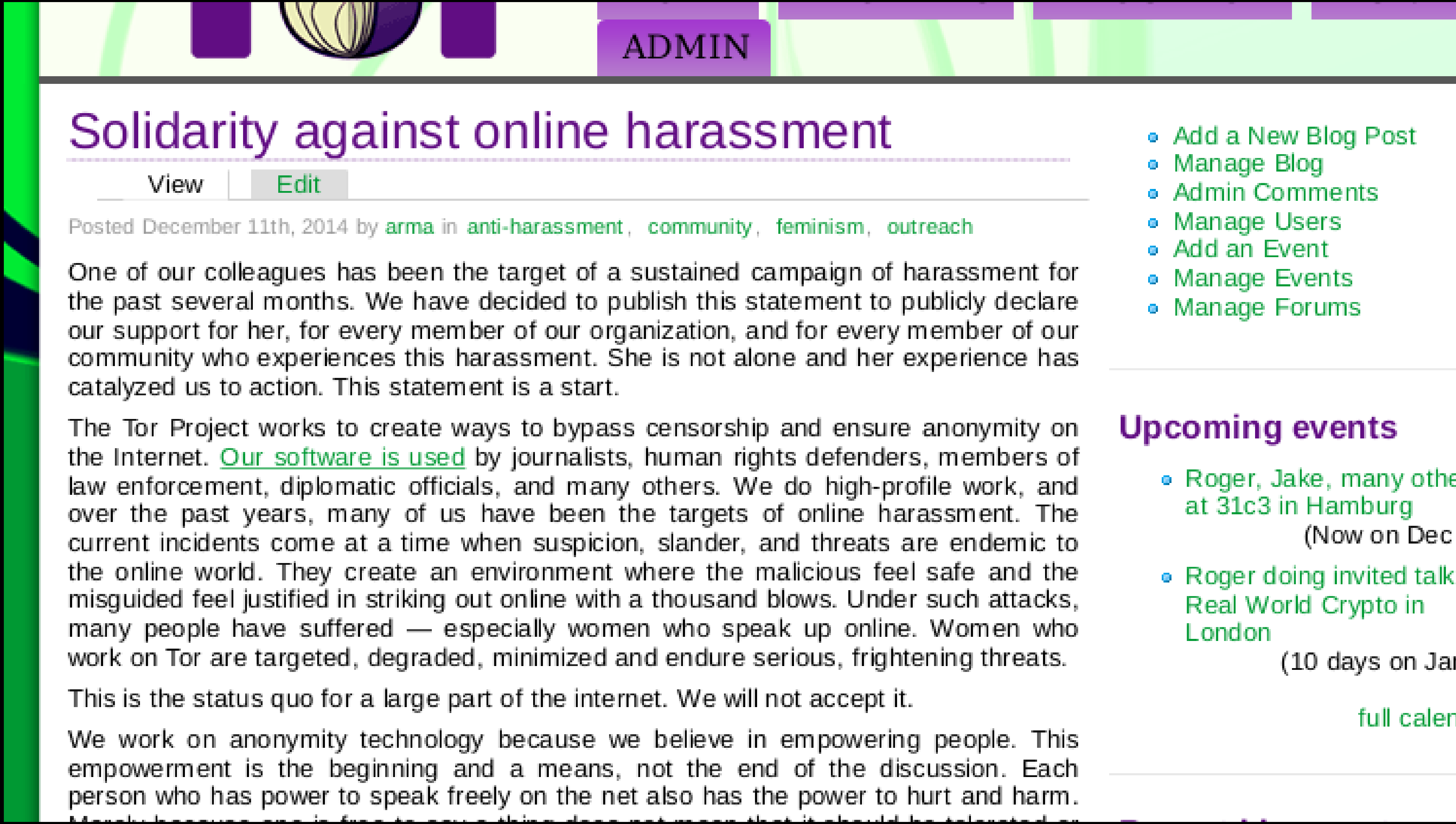
The Tor Project

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.

Tor
I Support Online Rights
ELECTRONIC FRONTIER FOUNDATION EFF.ORG

KEEP THE INTERNET FREE FROM GOVERNMENT CONTROL



Solidarity against online harassment

Posted December 11th, 2014 by arma in anti-harassment, community, feminism, outreach

One of our colleagues has been the target of a sustained campaign of harassment for the past several months. We have decided to publish this statement to publicly declare our support for her, for every member of our organization, and for every member of our community who experiences this harassment. She is not alone and her experience has catalyzed us to action. This statement is a start.

The Tor Project works to create ways to bypass censorship and ensure anonymity on the Internet. Our software is used by journalists, human rights defenders, members of law enforcement, diplomatic officials, and many others. We do high-profile work, and over the past years, many of us have been the targets of online harassment. The current incidents come at a time when suspicion, slander, and threats are endemic to the online world. They create an environment where the malicious feel safe and the misguided feel justified in striking out online with a thousand blows. Under such attacks, many people have suffered — especially women who speak up online. Women who work on Tor are targeted, degraded, minimized and endure serious, frightening threats.

This is the status quo for a large part of the internet. We will not accept it.

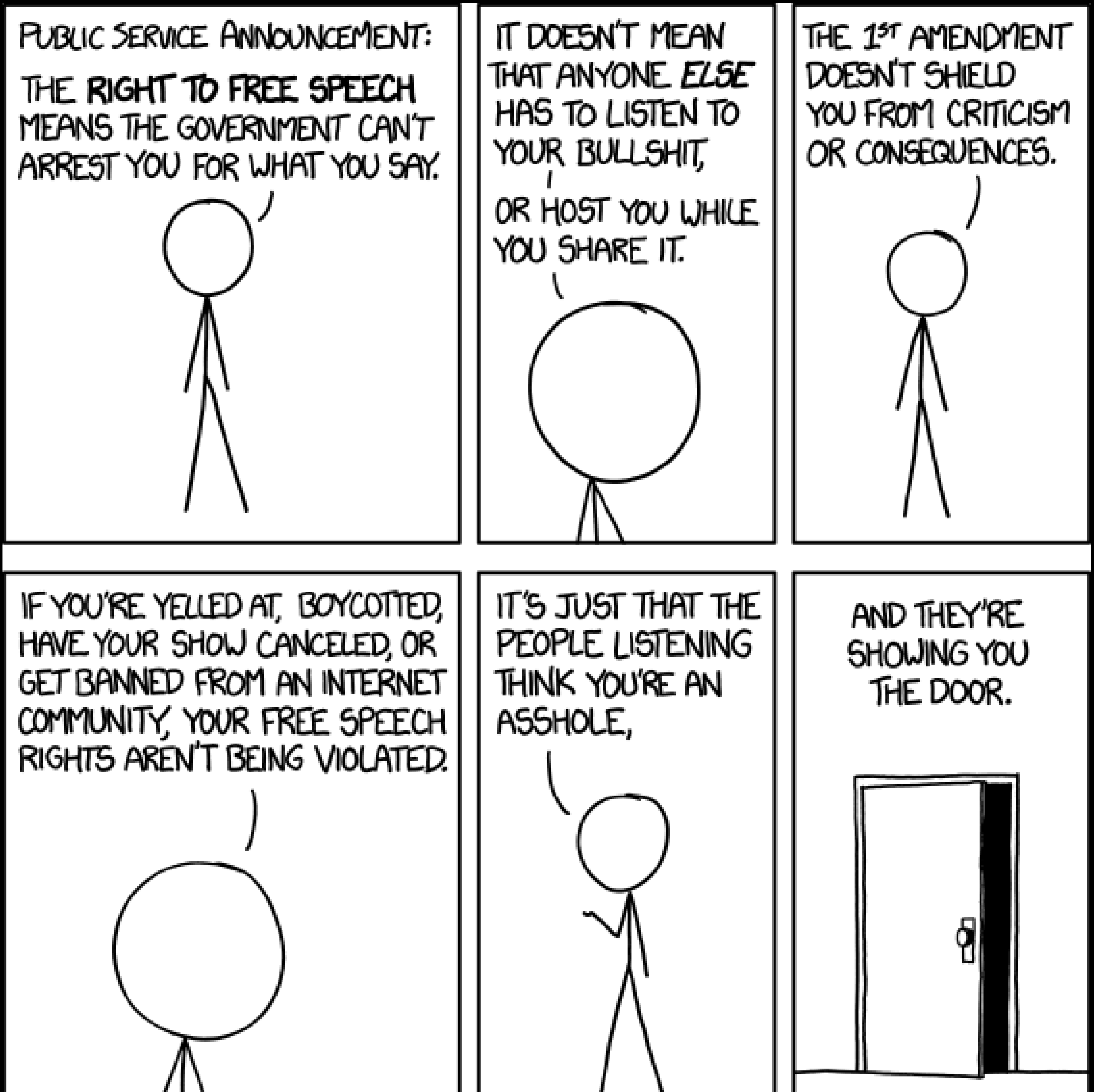
We work on anonymity technology because we believe in empowering people. This empowerment is the beginning and a means, not the end of the discussion. Each person who has power to speak freely on the net also has the power to hurt and harm. Merely because one is free to say a thing does not mean that it should be tolerated or

- Add a New Blog Post
- Manage Blog
- Admin Comments
- Manage Users
- Add an Event
- Manage Events
- Manage Forums

Upcoming events

- Roger, Jake, many othe at 31c3 in Hamburg
  (Now on Dec
- Roger doing invited talk Real World Crypto in London
  (10 days on Jar

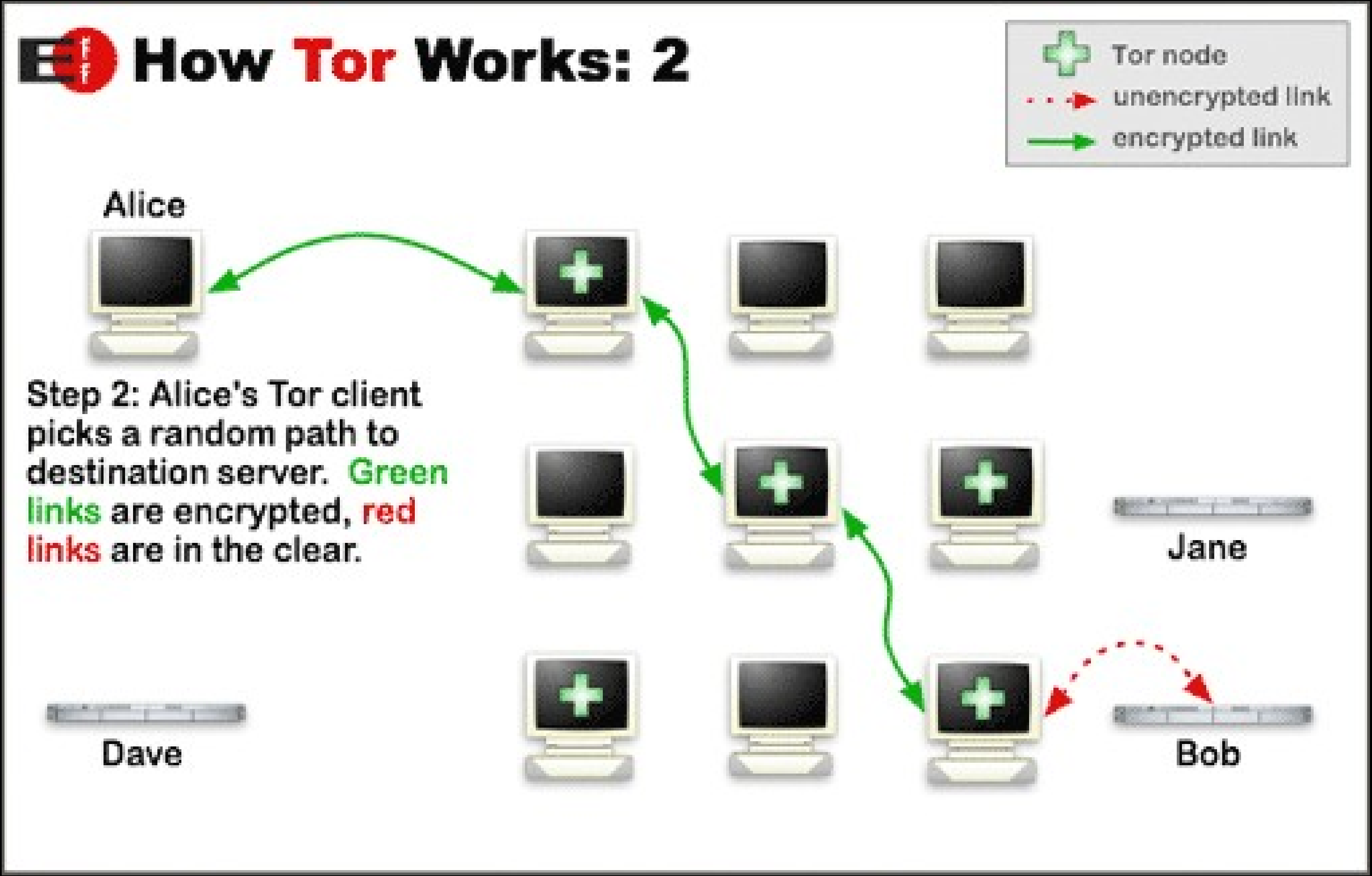
full calen


PUBLIC SERVICE ANNOUNCEMENT:
THE **RIGHT TO FREE SPEECH** MEANS THE GOVERNMENT CAN'T ARREST YOU FOR WHAT YOU SAY.
IT DOESN'T MEAN THAT ANYONE *ELSE* HAS TO LISTEN TO YOUR BULLSHIT,
OR HOST YOU WHILE YOU SHARE IT.
THE 1ST AMENDMENT DOESN'T SHIELD YOU FROM CRITICISM OR CONSEQUENCES.
IF YOU'RE YELLED AT, BOYCOTTED, HAVE YOUR SHOW CANCELED, OR GET BANNED FROM AN INTERNET COMMUNITY, YOUR FREE SPEECH RIGHTS AREN'T BEING VIOLATED.
IT'S JUST THAT THE PEOPLE LISTENING THINK YOU'RE AN ASSHOLE,
AND THEY'RE SHOWING YOU THE DOOR.

We have a press alias now

press@torproject.org

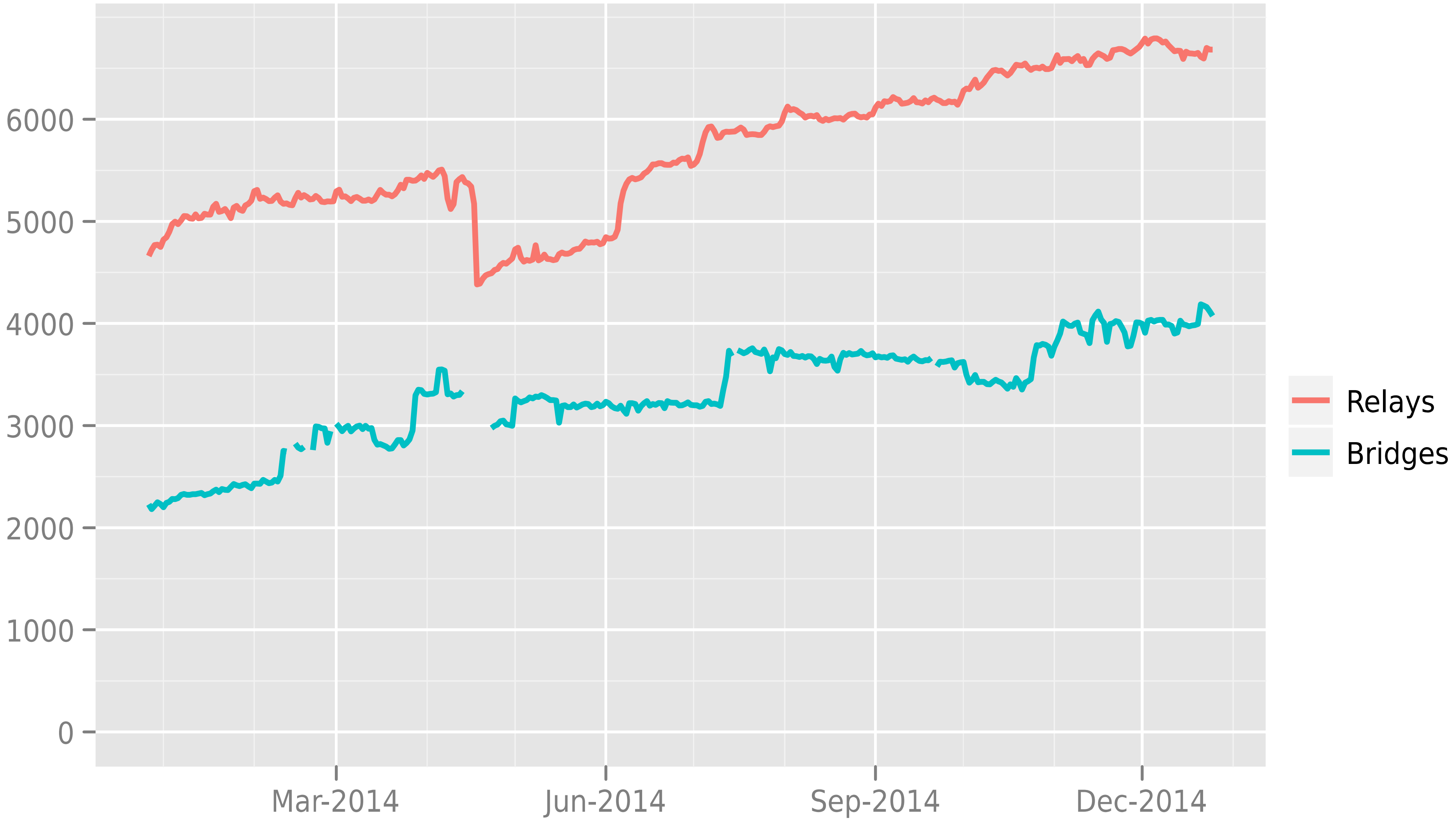
No backdoors ever



How Tor Works: 2

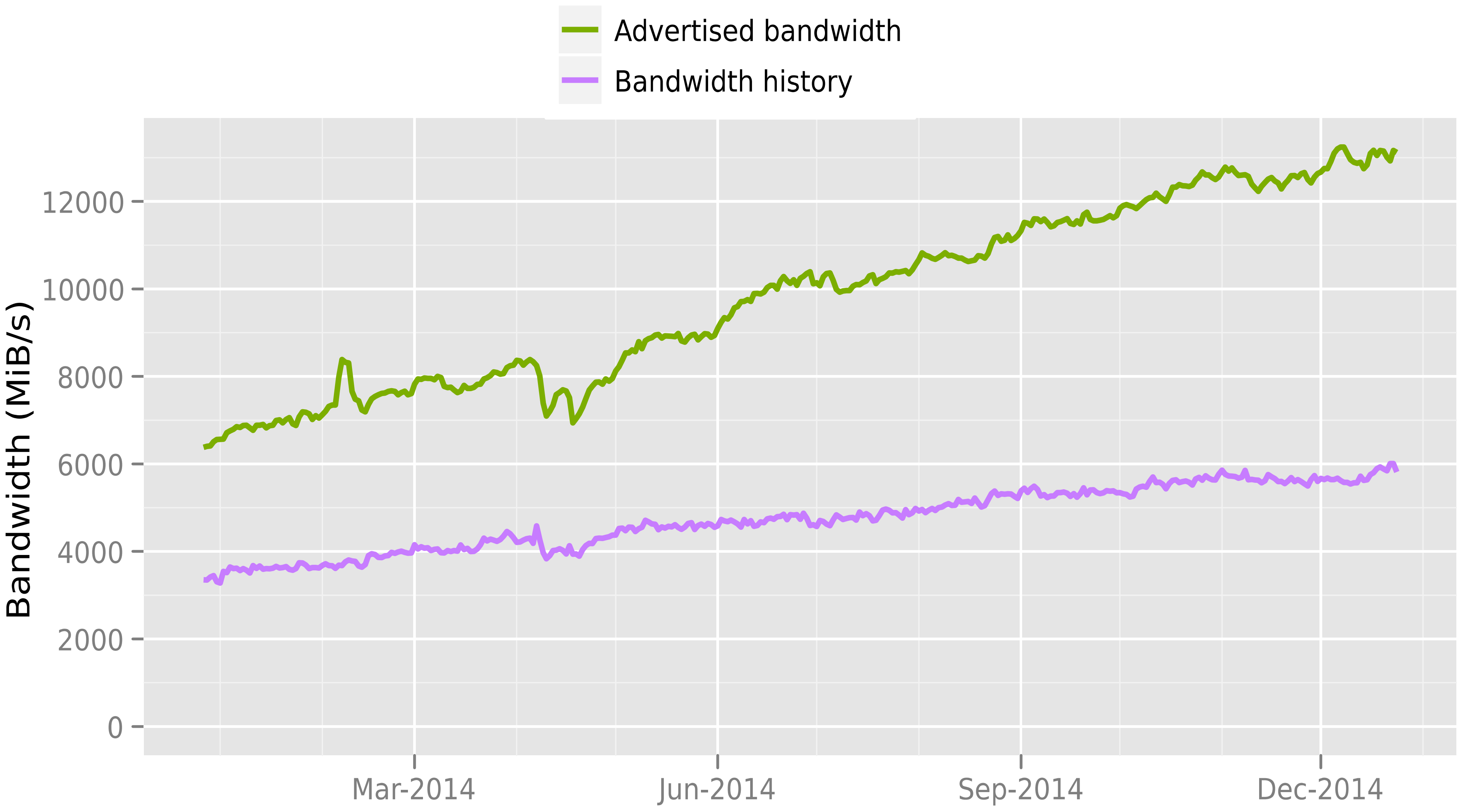
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Number of relays

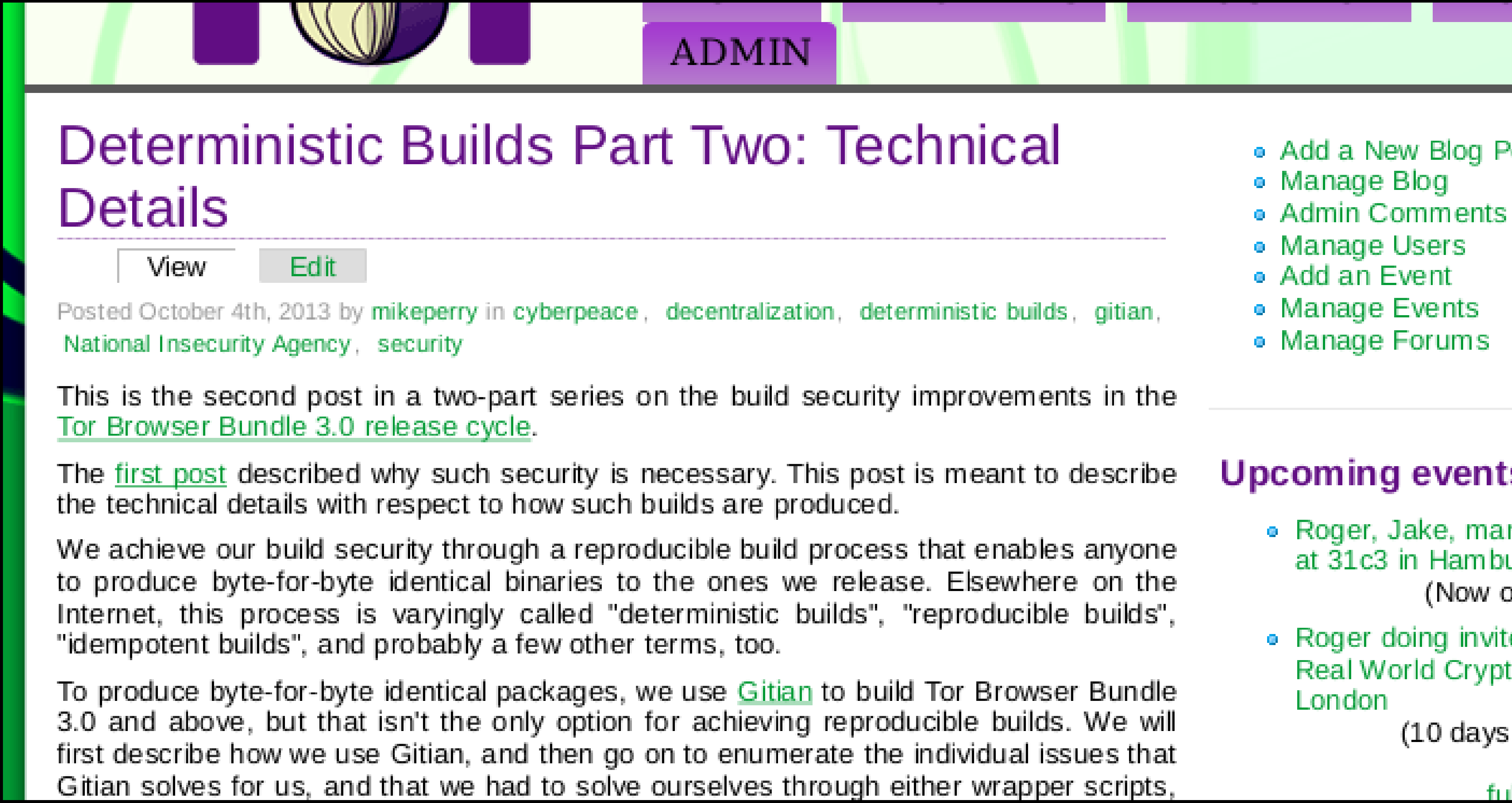


The Tor Project - https://metrics.torproject.org/

Total relay bandwidth



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



Deterministic Builds Part Two: Technical Details

Posted October 4th, 2013 by mikeperry in cyberpeace, decentralization, deterministic builds, gitian, National Insecurity Agency, security

This is the second post in a two-part series on the build security improvements in the Tor Browser Bundle 3.0 release cycle.

The first post described why such security is necessary. This post is meant to describe the technical details with respect to how such builds are produced.

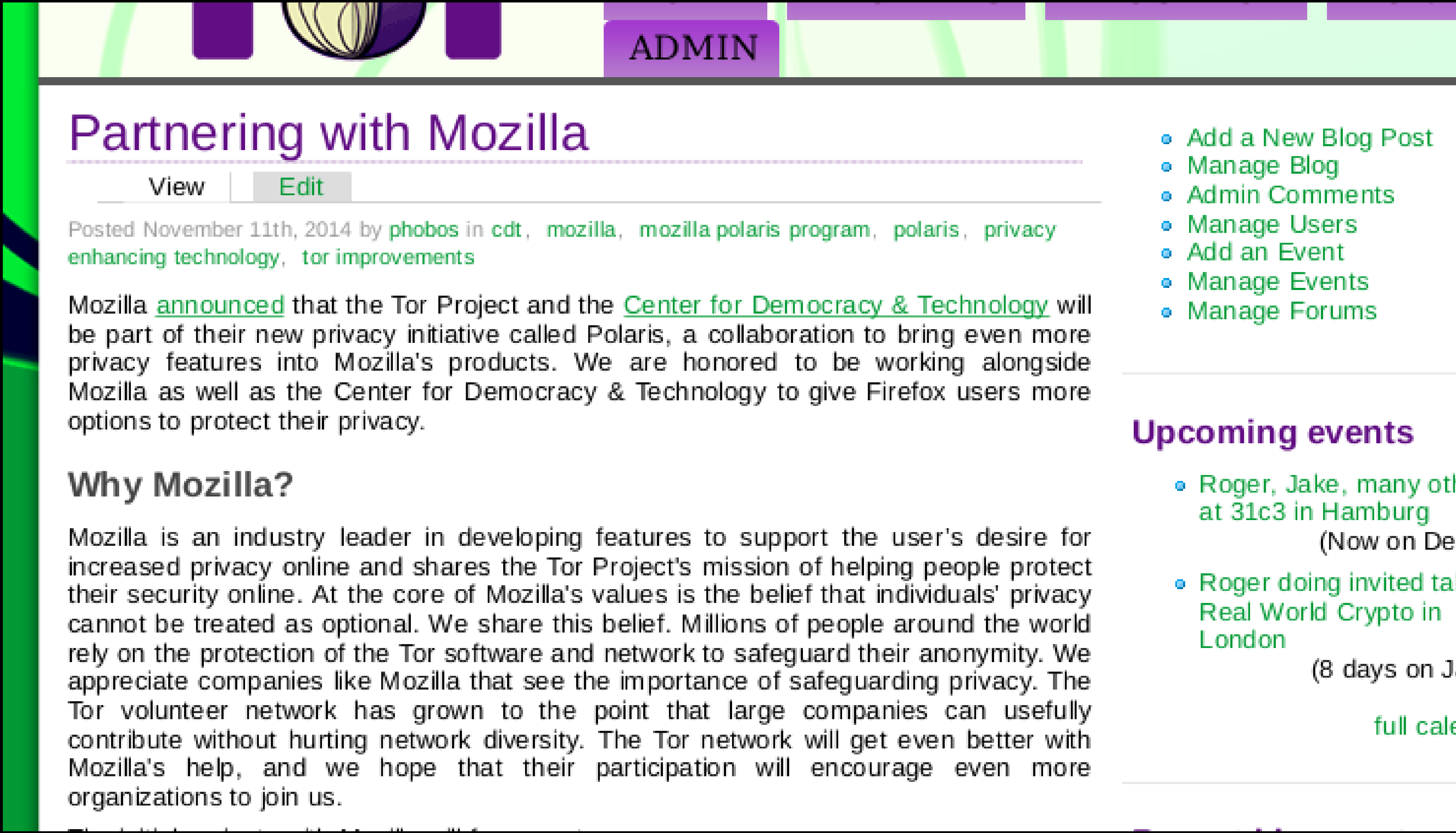
We achieve our build security through a reproducible build process that enables anyone to produce byte-for-byte identical binaries to the ones we release. Elsewhere on the Internet, this process is varyingly called "deterministic builds", "reproducible builds", "idempotent builds", and probably a few other terms, too.

To produce byte-for-byte identical packages, we use Gitian to build Tor Browser Bundle 3.0 and above, but that isn't the only option for achieving reproducible builds. We will first describe how we use Gitian, and then go on to enumerate the individual issues that Gitian solves for us, and that we had to solve ourselves through either wrapper scripts,

Upcoming event

- Roger, Jake, mar at 31c3 in Hambu
  (Now o
- Roger doing invit Real World Crypt London
  (10 days

fu



Partnering with Mozilla

Posted November 11th, 2014 by phobos in cdt, mozilla, mozilla polaris program, polaris, privacy enhancing technology, tor improvements

Mozilla announced that the Tor Project and the Center for Democracy & Technology will be part of their new privacy initiative called Polaris, a collaboration to bring even more privacy features into Mozilla's products. We are honored to be working alongside Mozilla as well as the Center for Democracy & Technology to give Firefox users more options to protect their privacy.

Why Mozilla?

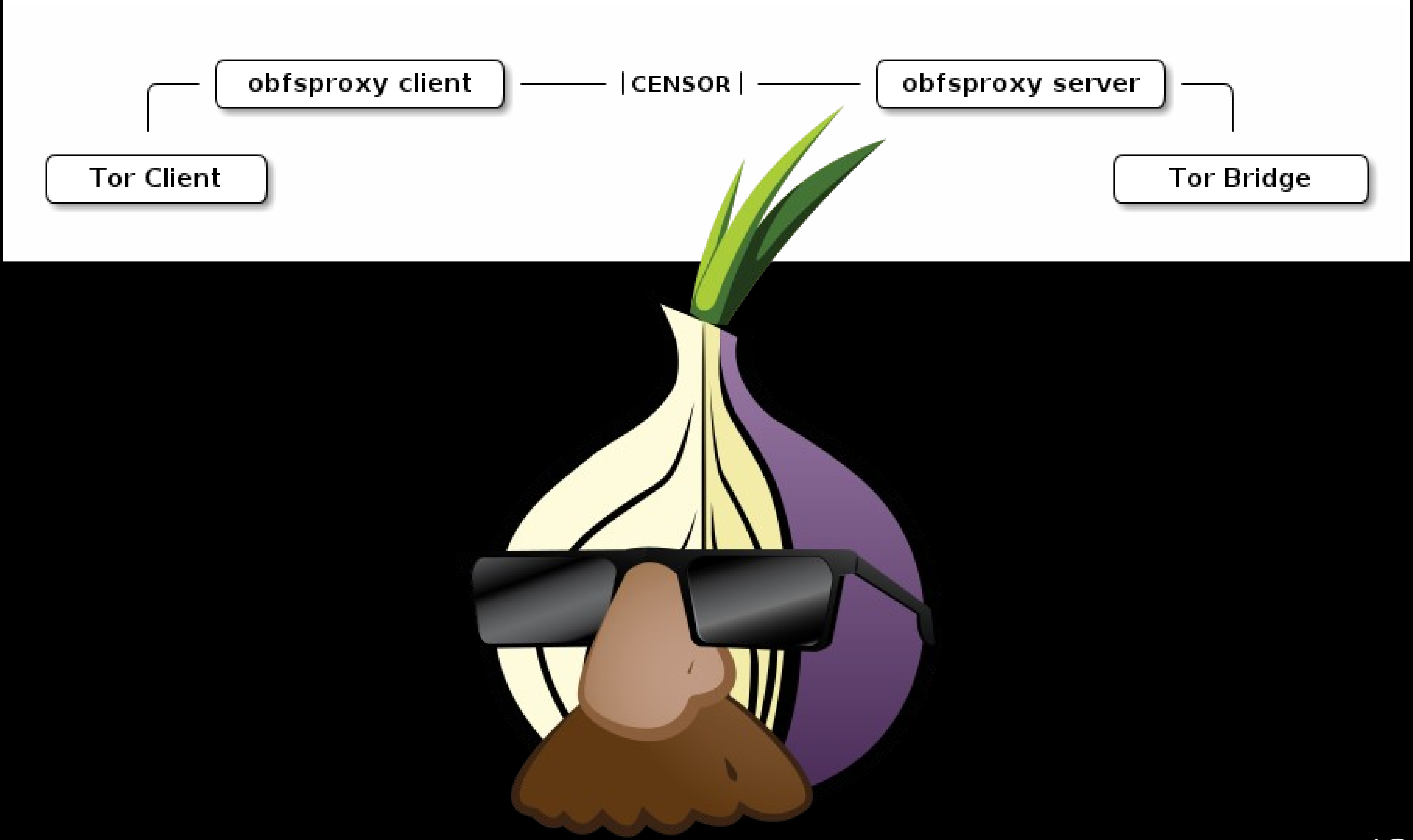
Mozilla is an industry leader in developing features to support the user's desire for increased privacy online and shares the Tor Project's mission of helping people protect their security online. At the core of Mozilla's values is the belief that individuals' privacy cannot be treated as optional. We share this belief. Millions of people around the world rely on the protection of the Tor software and network to safeguard their anonymity. We appreciate companies like Mozilla that see the importance of safeguarding privacy. The Tor volunteer network has grown to the point that large companies can usefully contribute without hurting network diversity. The Tor network will get even better with Mozilla's help, and we hope that their participation will encourage even more organizations to join us.

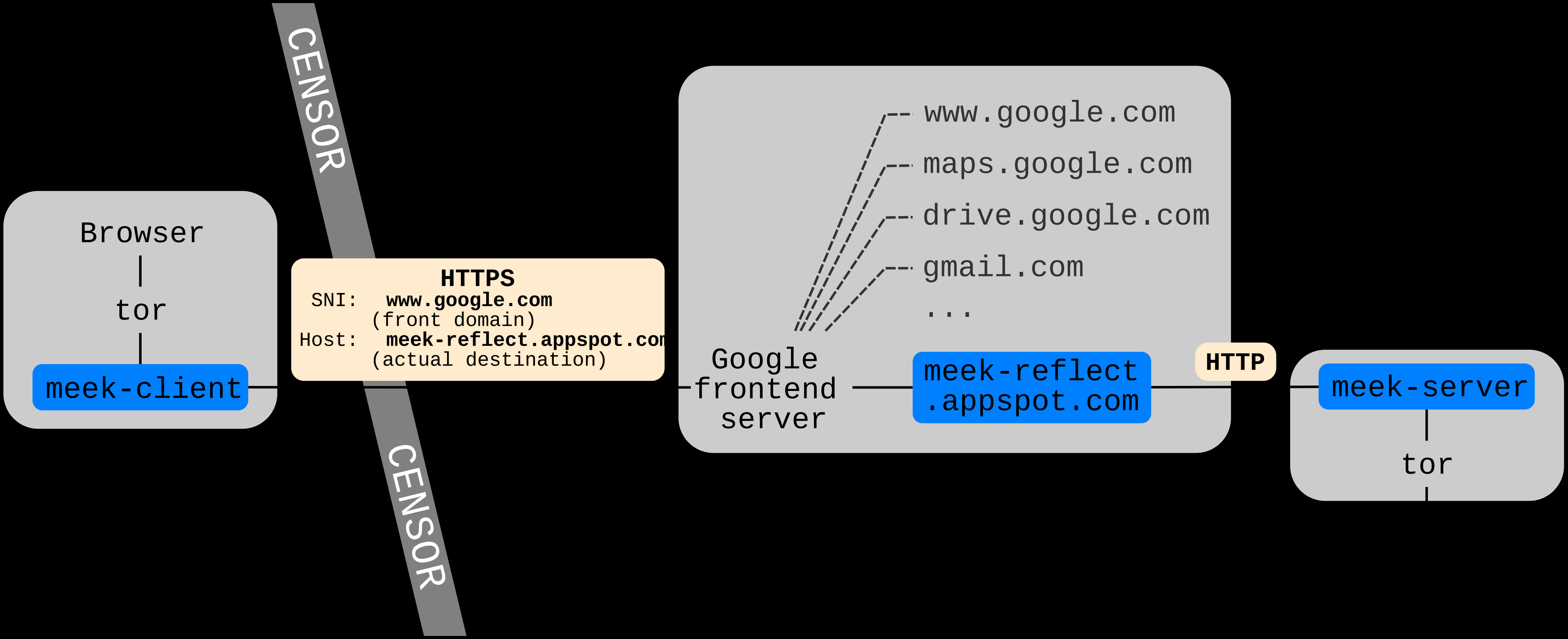
Upcoming events

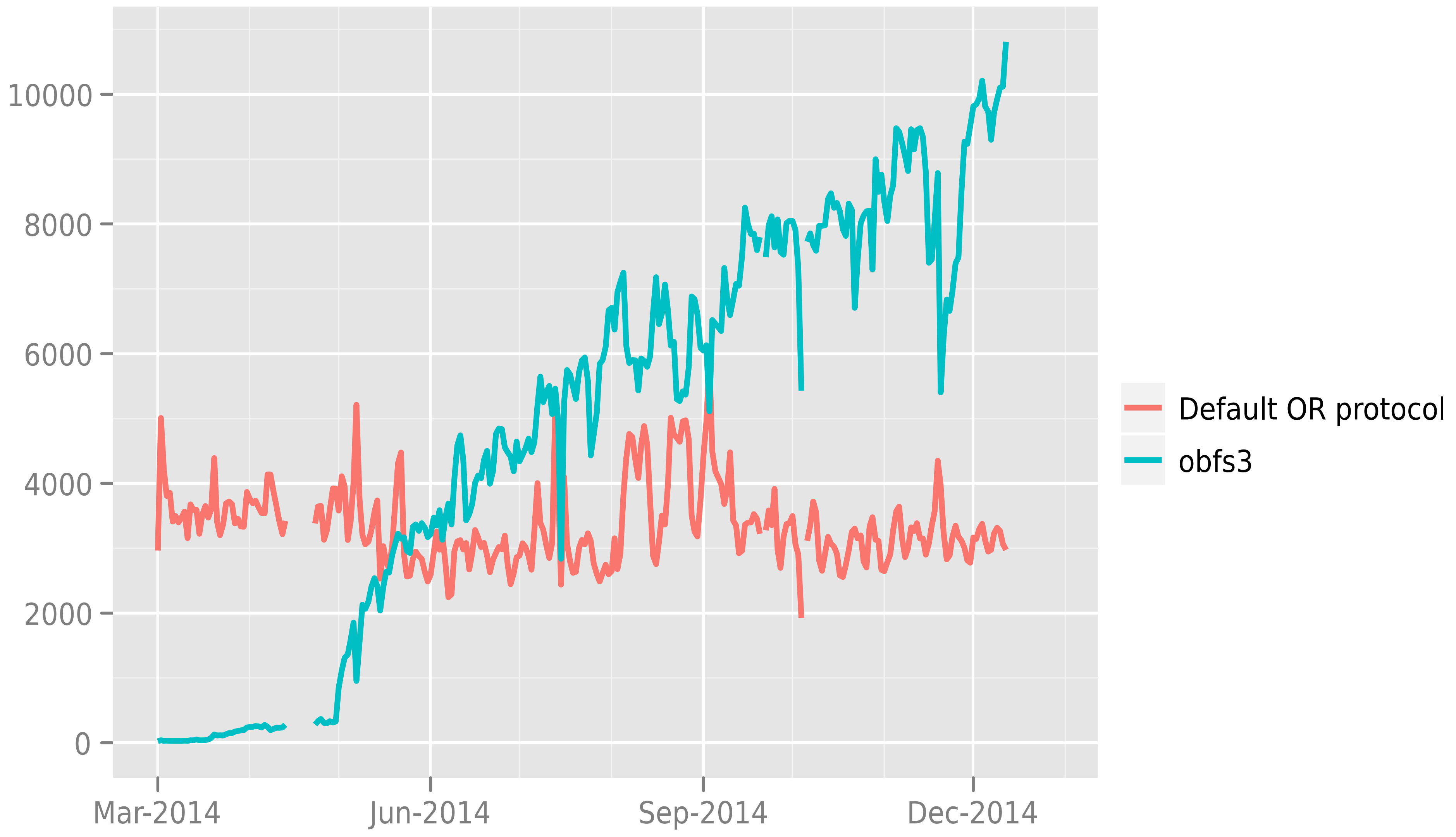
- Roger, Jake, many otl
  at 31c3 in Hamburg
  (Now on De
- Roger doing invited ta
  Real World Crypto in
  London
  (8 days on J

full cale

Pluggable transports




Browser
tor
meek-client
CENSOR
CENSOR
HTTPS
SNI: www.google.com
(front domain)
Host: meek-reflect.appspot.com
(actual destination)
www.google.com
maps.google.com
drive.google.com
gmail.com
...
Google frontend server
meek-reflect .appspot.com
HTTP
meek-server
tor



Bridge users by transport

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

Tor unit tests and refactoring

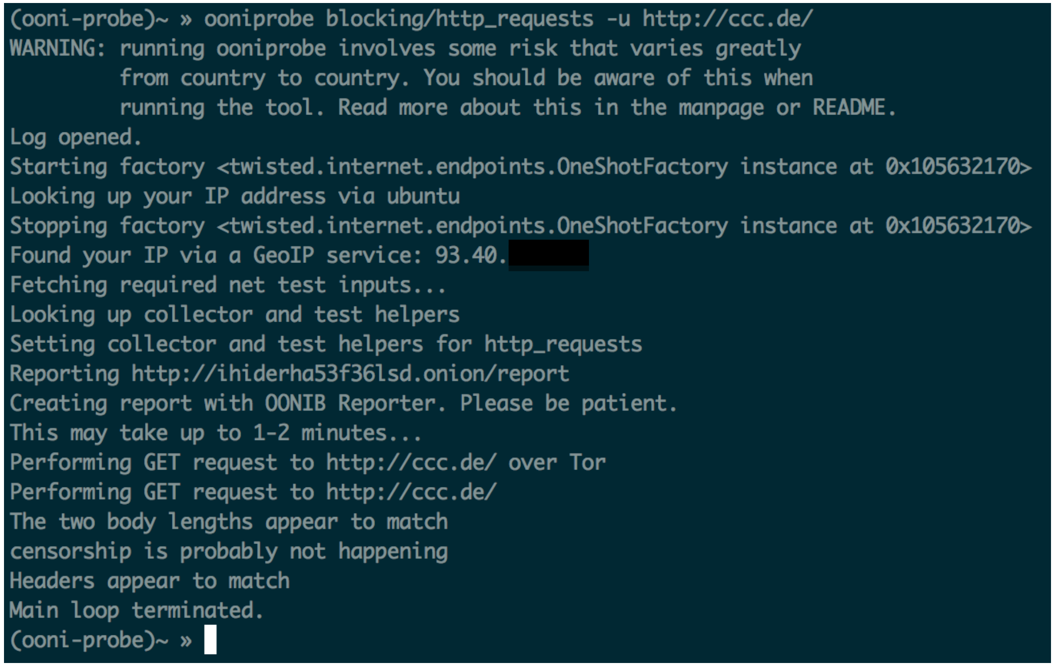
The Tor source code has become much more robust and tested over the past year

OONI: Open Observatory of Network Interference

- It’s a set of principles and test specifications for conducting network measurements.

- Measuring **network irregularities** that can be a symptom of **internet censorship** and **surveillance** since 2012.

- Uses a peer reviewed methodology, implemented using free software and publishing the data.



```
(ooni-probe)~ » ooniprobe blocking/http_requests -u http://ccc.de/
WARNING: running ooniprobe involves some risk that varies greatly
         from country to country. You should be aware of this when
         running the tool. Read more about this in the manpage or README.
Log opened.
Starting factory <twisted.internet.endpoints.OneShotFactory instance at 0x105632170>
Looking up your IP address via ubuntu
Stopping factory <twisted.internet.endpoints.OneShotFactory instance at 0x105632170>
Found your IP via a GeoIP service: 93.40.[redacted]
Fetching required net test inputs...
Looking up collector and test helpers
Setting collector and test helpers for http_requests
Reporting http://ihiderha53f36lsd.onion/report
Creating report with OONIB Reporter. Please be patient.
This may take up to 1-2 minutes...
Performing GET request to http://ccc.de/ over Tor
Performing GET request to http://ccc.de/
The two body lengths appear to match
censorship is probably not happening
Headers appear to match
Main loop terminated.
(ooni-probe)~ »
```

OONI: Learn more & help us!

- Journalists, Researchers, Activists or just citizens need this data to be open.

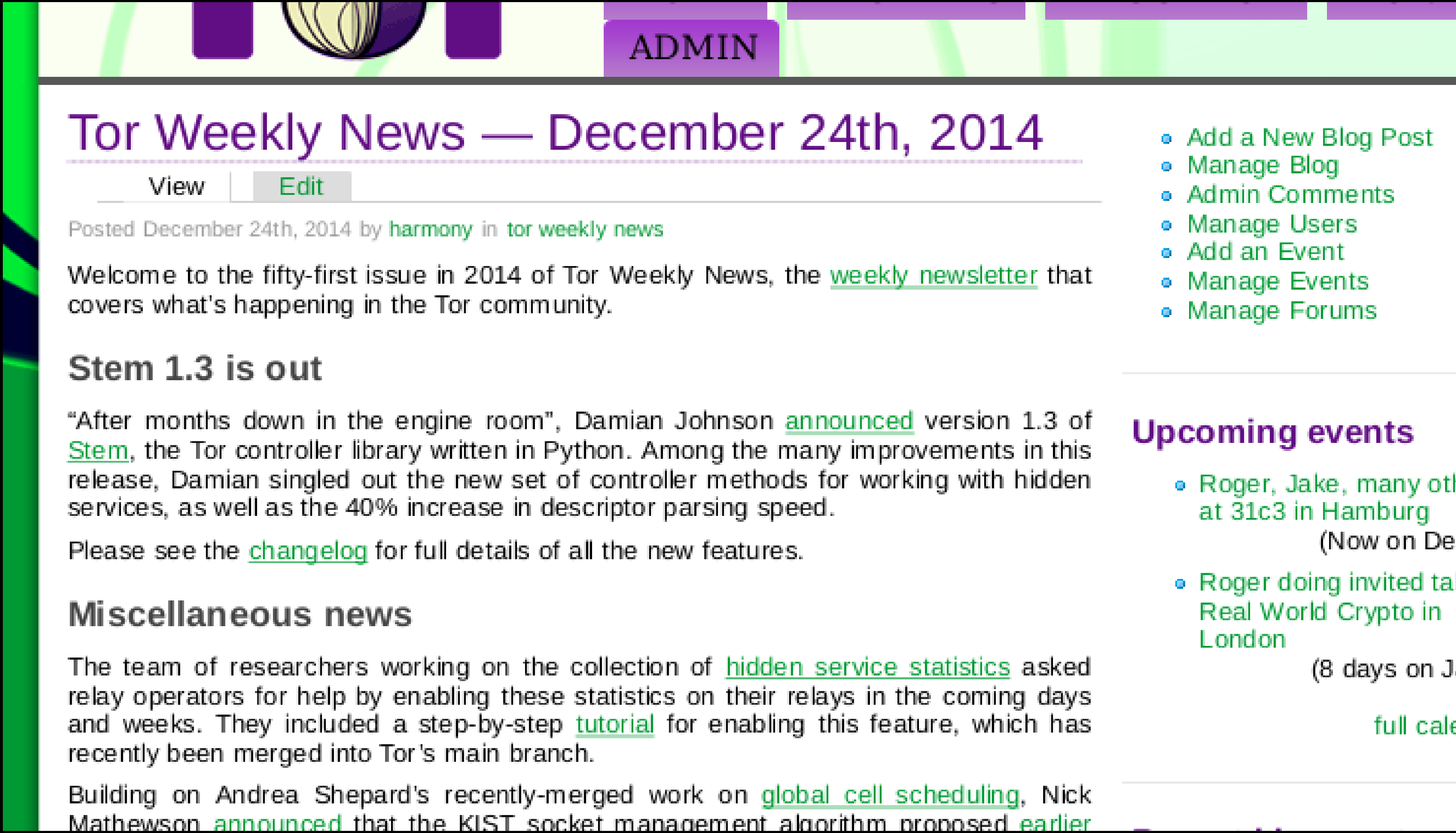
- Historical and data from as many sources as possible is crucial

- Run ooniprobe today!

  ```
  curl https://ooni.torproject.org/install.sh | bash
  ```

- Or Adopt an ooniprobe!

- Come to our Hall13 today at 18:00 to learn more



Tor Weekly News — December 24th, 2014

Posted December 24th, 2014 by harmony in tor weekly news

Welcome to the fifty-first issue in 2014 of Tor Weekly News, the weekly newsletter that covers what's happening in the Tor community.

Stem 1.3 is out

“After months down in the engine room”, Damian Johnson announced version 1.3 of Stem, the Tor controller library written in Python. Among the many improvements in this release, Damian singled out the new set of controller methods for working with hidden services, as well as the 40% increase in descriptor parsing speed.

Please see the changelog for full details of all the new features.

Miscellaneous news

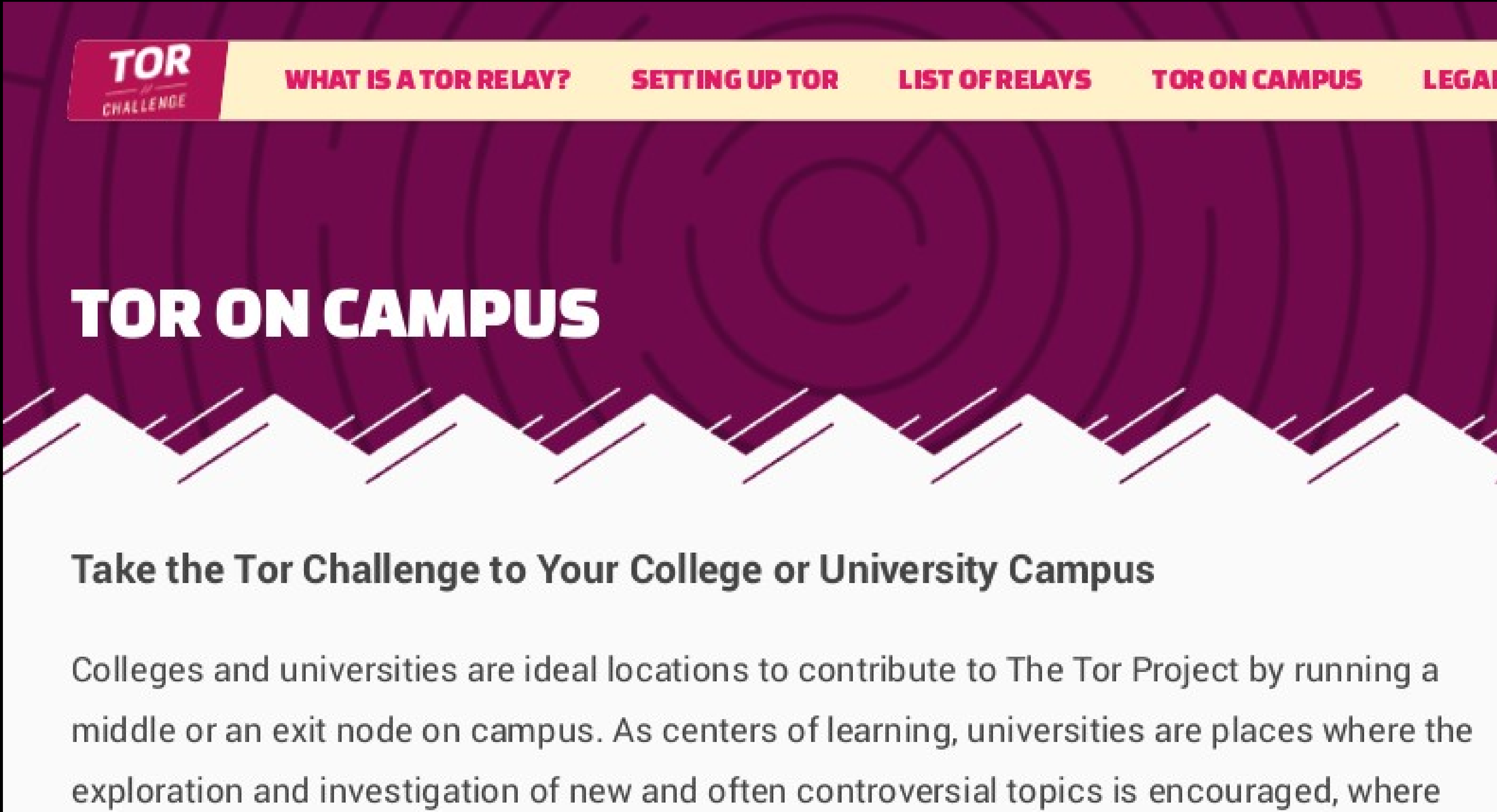
The team of researchers working on the collection of hidden service statistics asked relay operators for help by enabling these statistics on their relays in the coming days and weeks. They included a step-by-step tutorial for enabling this feature, which has recently been merged into Tor's main branch.

Building on Andrea Shepard's recently-merged work on global cell scheduling, Nick Mathewson announced that the KIST socket management algorithm proposed earlier

Upcoming events

- Roger, Jake, many oth at 31c3 in Hamburg
  (Now on De
- Roger doing invited ta Real World Crypto in London
  (8 days on J

full cale

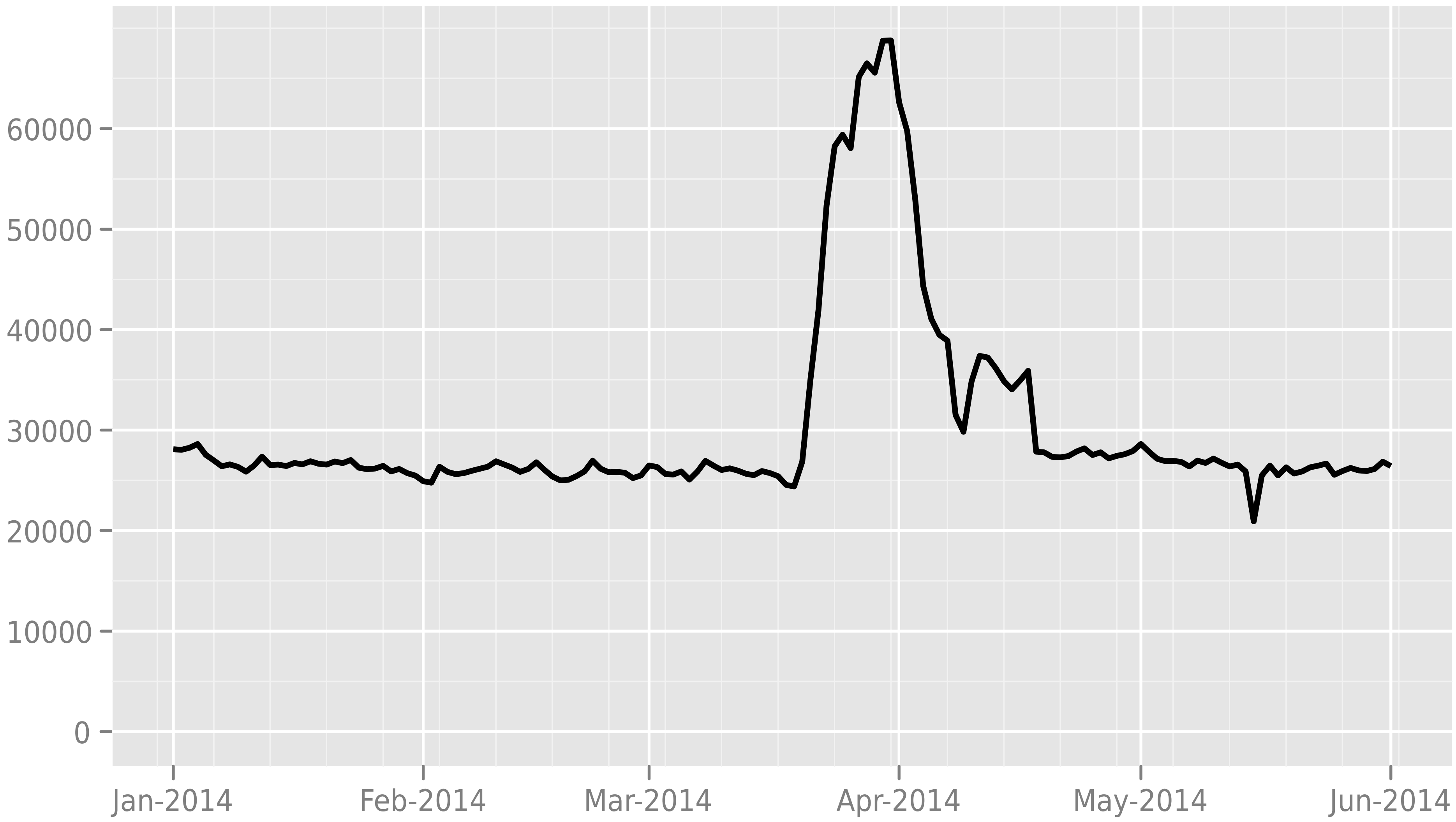


TOR ON CAMPUS

Take the Tor Challenge to Your College or University Campus

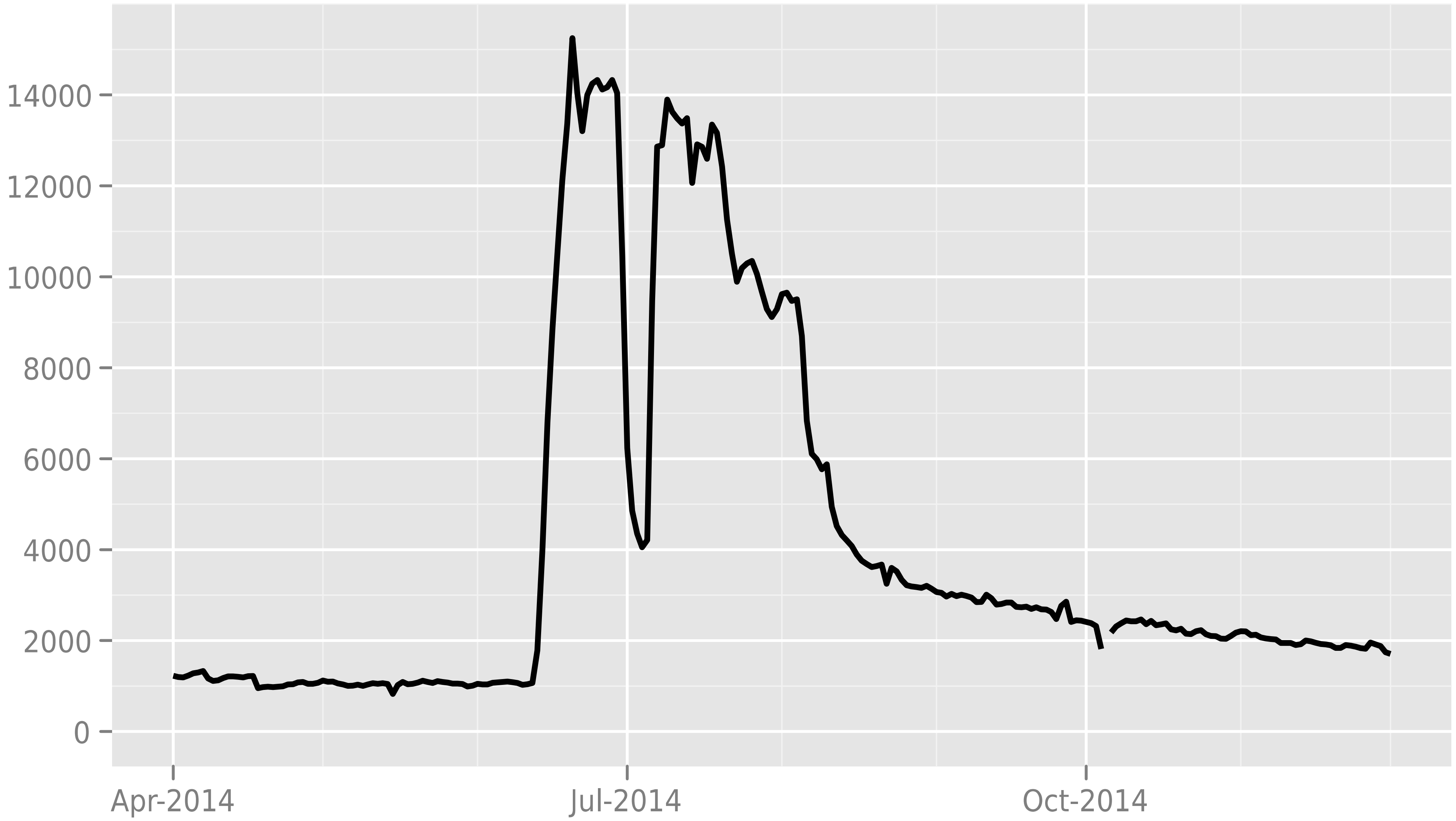
Colleges and universities are ideal locations to contribute to The Tor Project by running a middle or an exit node on campus. As centers of learning, universities are places where the exploration and investigation of new and often controversial topics is encouraged, where

Directly connecting users from Turkey

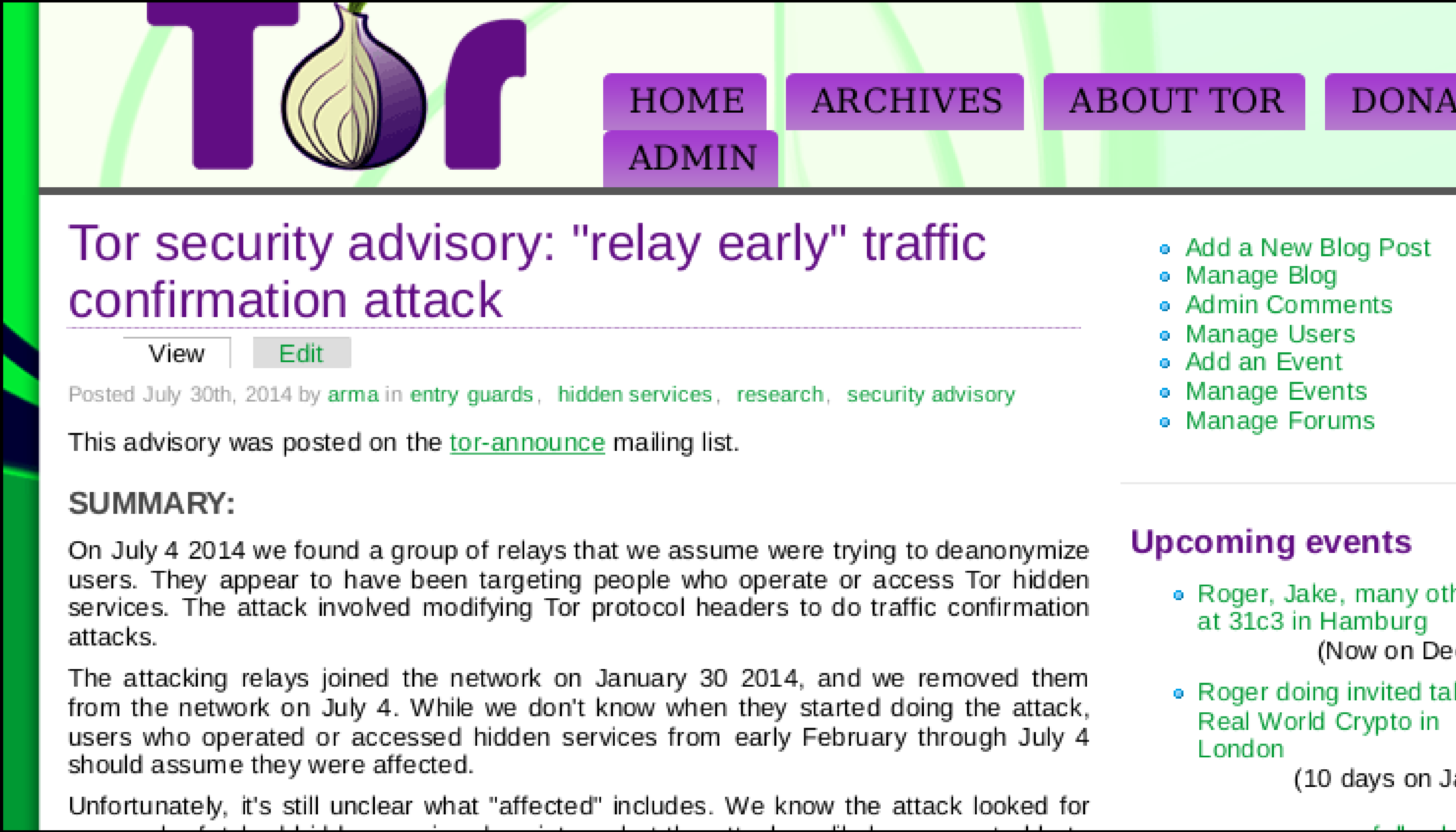


The Tor Project - https://metrics.torproject.org/

Directly connecting users from Iraq



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



Tor security advisory: "relay early" traffic confirmation attack

Posted July 30th, 2014 by arma in entry guards, hidden services, research, security advisory

This advisory was posted on the tor-announce mailing list.

SUMMARY:

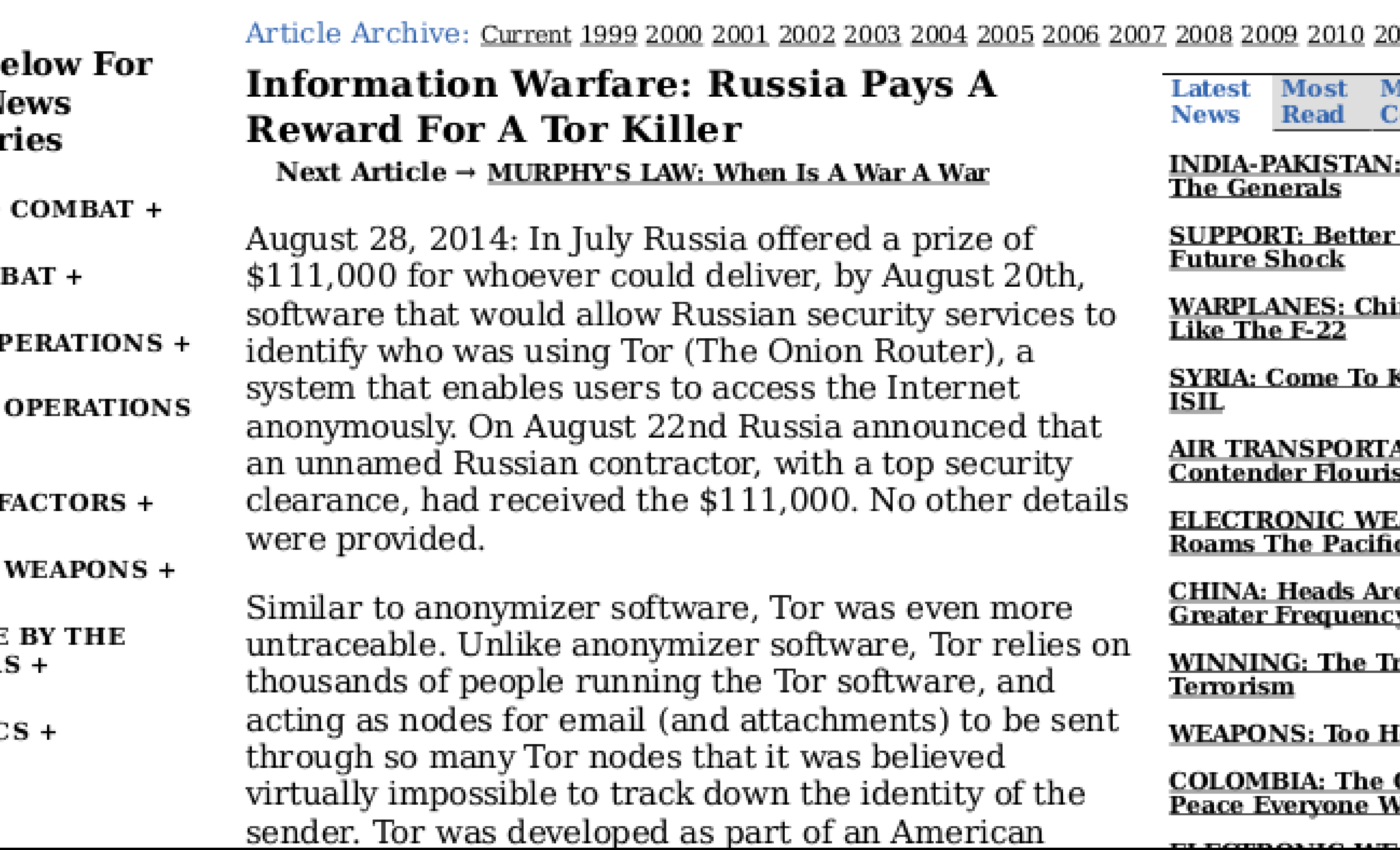
On July 4 2014 we found a group of relays that we assume were trying to deanonymize users. They appear to have been targeting people who operate or access Tor hidden services. The attack involved modifying Tor protocol headers to do traffic confirmation attacks.

The attacking relays joined the network on January 30 2014, and we removed them from the network on July 4. While we don't know when they started doing the attack, users who operated or accessed hidden services from early February through July 4 should assume they were affected.

Unfortunately, it's still unclear what "affected" includes. We know the attack looked for

Upcoming events

- Roger, Jake, many oth at 31c3 in Hamburg (Now on De
- Roger doing invited tal Real World Crypto in London (10 days on Ja



Article Archive: Current 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 20

elow For
lews
ries

COMBAT +

BAT +

PERATIONS +

OPERATIONS

FACTORS +

WEAPONS +

E BY THE
S +

CS +

Information Warfare: Russia Pays A Reward For A Tor Killer

Next Article → MURPHY'S LAW: When Is A War A War

August 28, 2014: In July Russia offered a prize of $111,000 for whoever could deliver, by August 20th, software that would allow Russian security services to identify who was using Tor (The Onion Router), a system that enables users to access the Internet anonymously. On August 22nd Russia announced that an unnamed Russian contractor, with a top security clearance, had received the $111,000. No other details were provided.

Similar to anonymizer software, Tor was even more untraceable. Unlike anonymizer software, Tor relies on thousands of people running the Tor software, and acting as nodes for email (and attachments) to be sent through so many Tor nodes that it was believed virtually impossible to track down the identity of the sender. Tor was developed as part of an American

Latest News | Most Read | M C

INDIA-PAKISTAN: The Generals

SUPPORT: Better Future Shock

WARPLANES: Chi Like The F-22

SYRIA: Come To K ISIL

AIR TRANSPORTA Contender Flouris

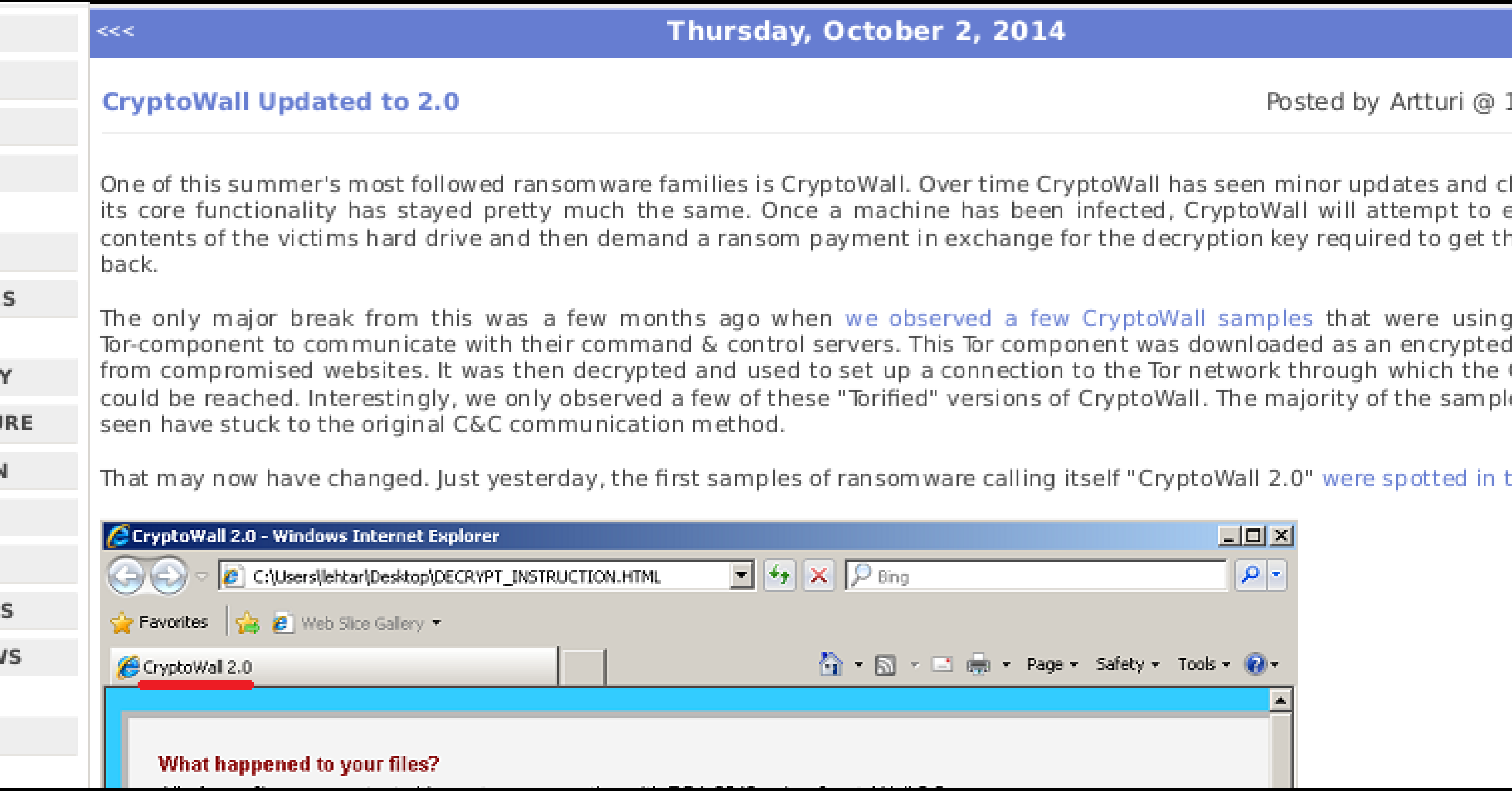
ELECTRONIC WE Roams The Pacific

CHINA: Heads Ar Greater Frequency

WINNING: The Tr Terrorism

WEAPONS: Too H

COLOMBIA: The C Peace Everyone W



Thursday, October 2, 2014

CryptoWall Updated to 2.0

Posted by Artturi @ 1

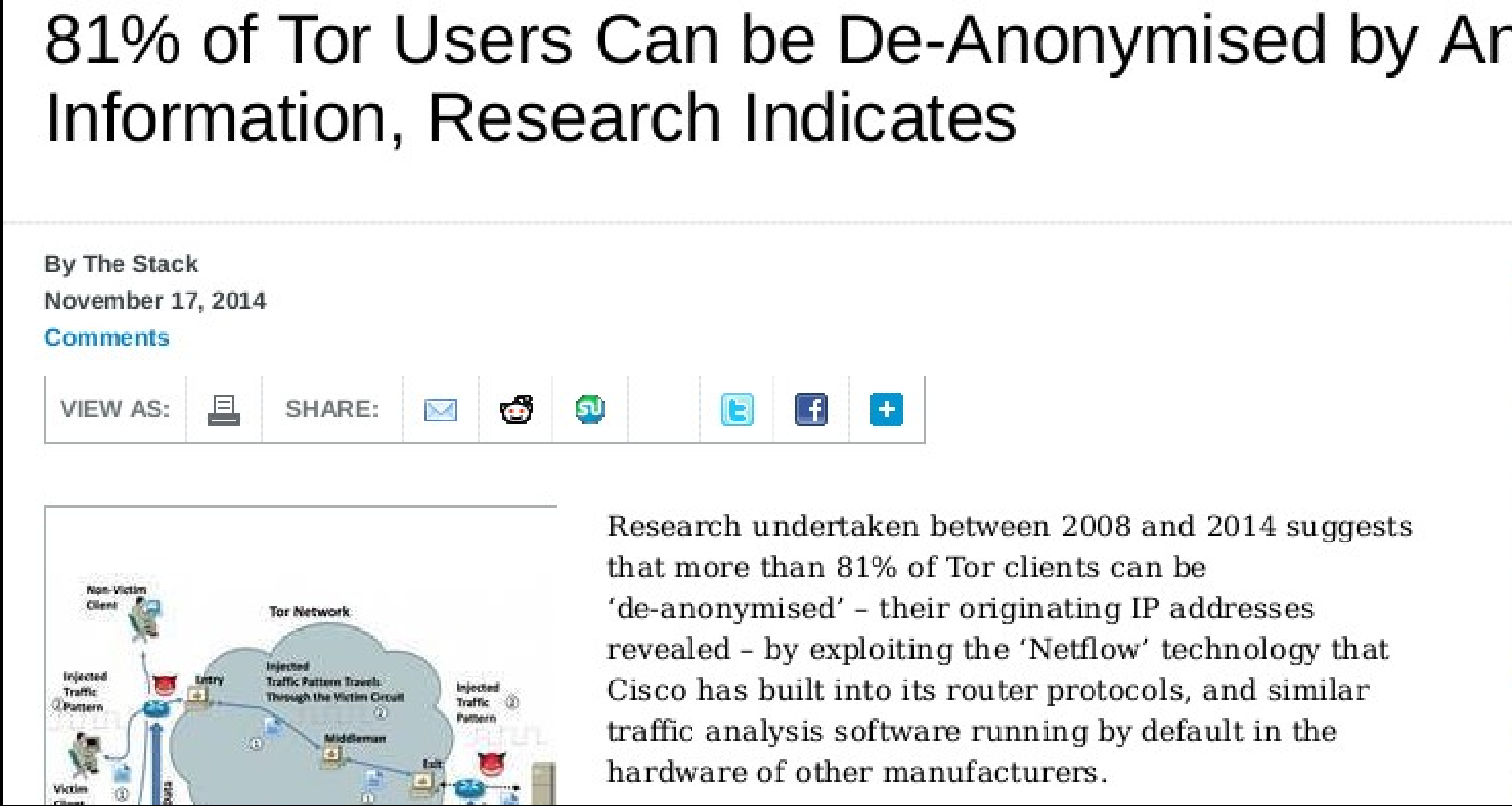
One of this summer's most followed ransomware families is CryptoWall. Over time CryptoWall has seen minor updates and c its core functionality has stayed pretty much the same. Once a machine has been infected, CryptoWall will attempt to e contents of the victims hard drive and then demand a ransom payment in exchange for the decryption key required to get th back.

The only major break from this was a few months ago when we observed a few CryptoWall samples that were using Tor-component to communicate with their command & control servers. This Tor component was downloaded as an encrypted from compromised websites. It was then decrypted and used to set up a connection to the Tor network through which the could be reached. Interestingly, we only observed a few of these "Torified" versions of CryptoWall. The majority of the sampl seen have stuck to the original C&C communication method.

That may now have changed. Just yesterday, the first samples of ransomware calling itself "CryptoWall 2.0" were spotted in t

CryptoWall 2.0 - Windows Internet Explorer
C:\Users\lehtar\Desktop\DECRYPT_INSTRUCTION.HTML
Bing
Favorites
Web Slice Gallery
CryptoWall 2.0
Page
Safety
Tools

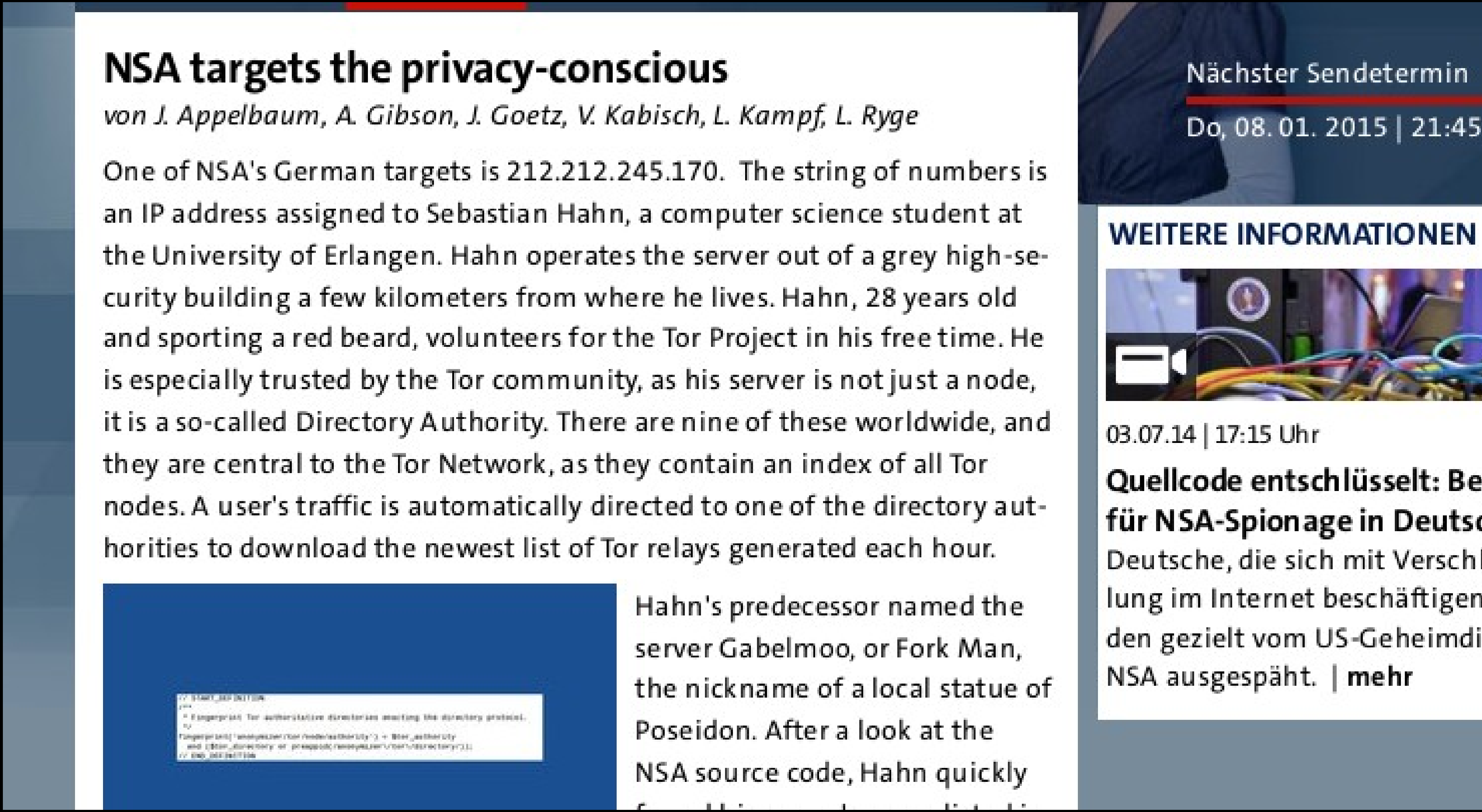
What happened to your files?



81% of Tor Users Can be De-Anonymised by An Information, Research Indicates

By The Stack
November 17, 2014
Comments

Research undertaken between 2008 and 2014 suggests that more than 81% of Tor clients can be ‘de-anonymised’ – their originating IP addresses revealed – by exploiting the ‘Netflow’ technology that Cisco has built into its router protocols, and similar traffic analysis software running by default in the hardware of other manufacturers.



NSA targets the privacy-conscious

von J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge

One of NSA's German targets is 212.212.245.170. The string of numbers is an IP address assigned to Sebastian Hahn, a computer science student at the University of Erlangen. Hahn operates the server out of a grey high-security building a few kilometers from where he lives. Hahn, 28 years old and sporting a red beard, volunteers for the Tor Project in his free time. He is especially trusted by the Tor community, as his server is not just a node, it is a so-called Directory Authority. There are nine of these worldwide, and they are central to the Tor Network, as they contain an index of all Tor nodes. A user's traffic is automatically directed to one of the directory authorities to download the newest list of Tor relays generated each hour.

```
// START_DEFINITION
/**
 * Fingerprint Tor authoritative directories enacting the directory protocol.
 */
fingerprint('anonymizer/tor/node/authority') = $tor_authority
  and ($tor_directory or preappid(/anonymizer\/tor\/directory/));
// END_DEFINITION
```

Hahn's predecessor named the server Gabelmoo, or Fork Man, the nickname of a local statue of Poseidon. After a look at the NSA source code, Hahn quickly

Nächster Sendetermin

Do, 08. 01. 2015 | 21:45

WEITERE INFORMATIONEN

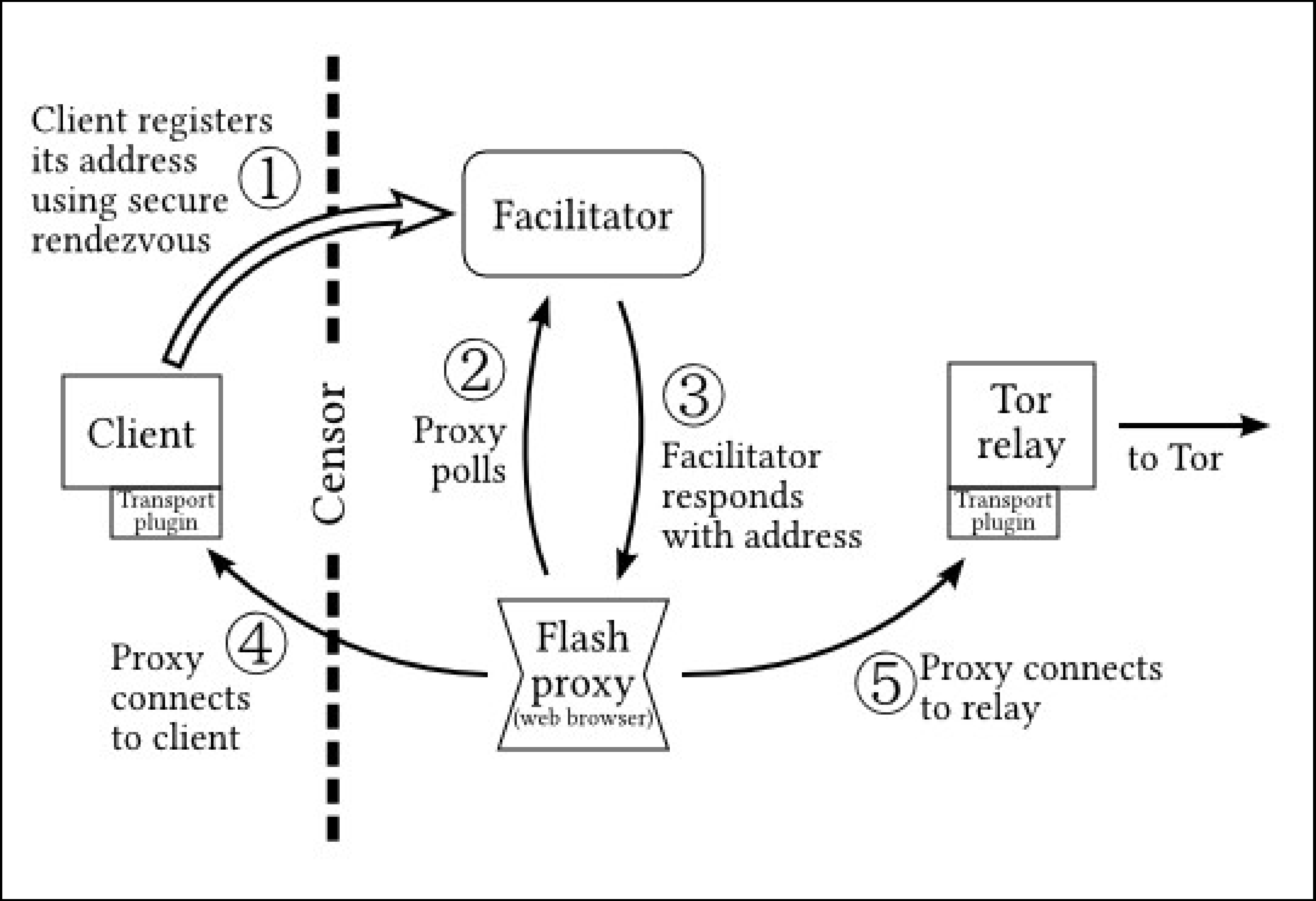
03.07.14 | 17:15 Uhr

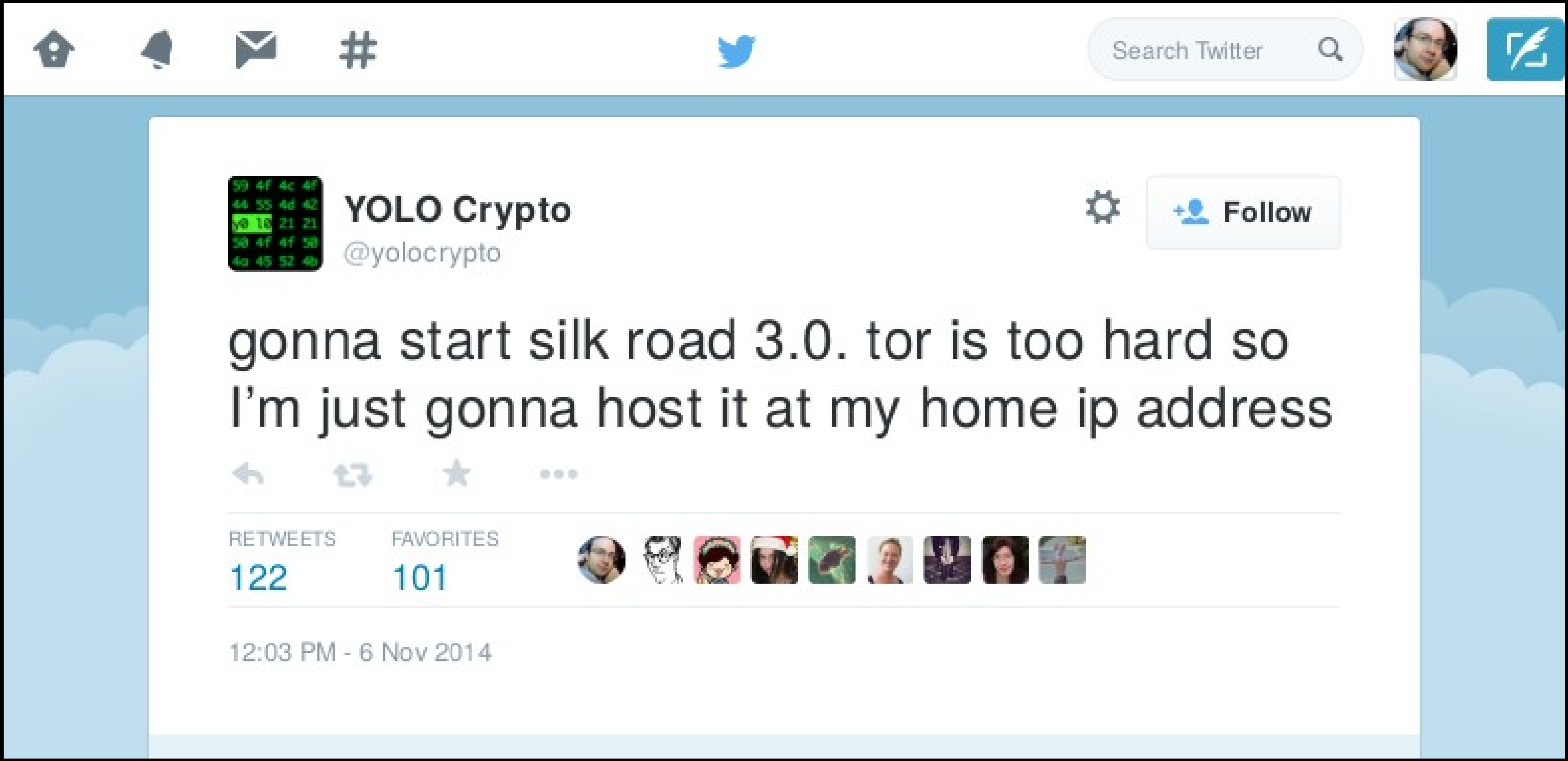
Quellcode entschlüsselt: Be
für NSA-Spionage in Deutsc

Deutsche, die sich mit Verschl
lung im Internet beschäftigen
den gezielt vom US-Geheimdi
NSA ausgespäht. | **mehr**

Pervasive surveillance

- Design changes to improve robustness
- Internet is more centralized than we'd like
- New insight: surveillance (DPI) and censorship (DPI) more related than we realized


Client registers its address using secure rendezvous
1
Censor
Facilitator
2
Proxy polls
3
Facilitator responds with address
Client
Transport plugin
Tor relay
Transport plugin
to Tor
4
Proxy connects to client
Flash proxy
(web browser)
5
Proxy connects to relay



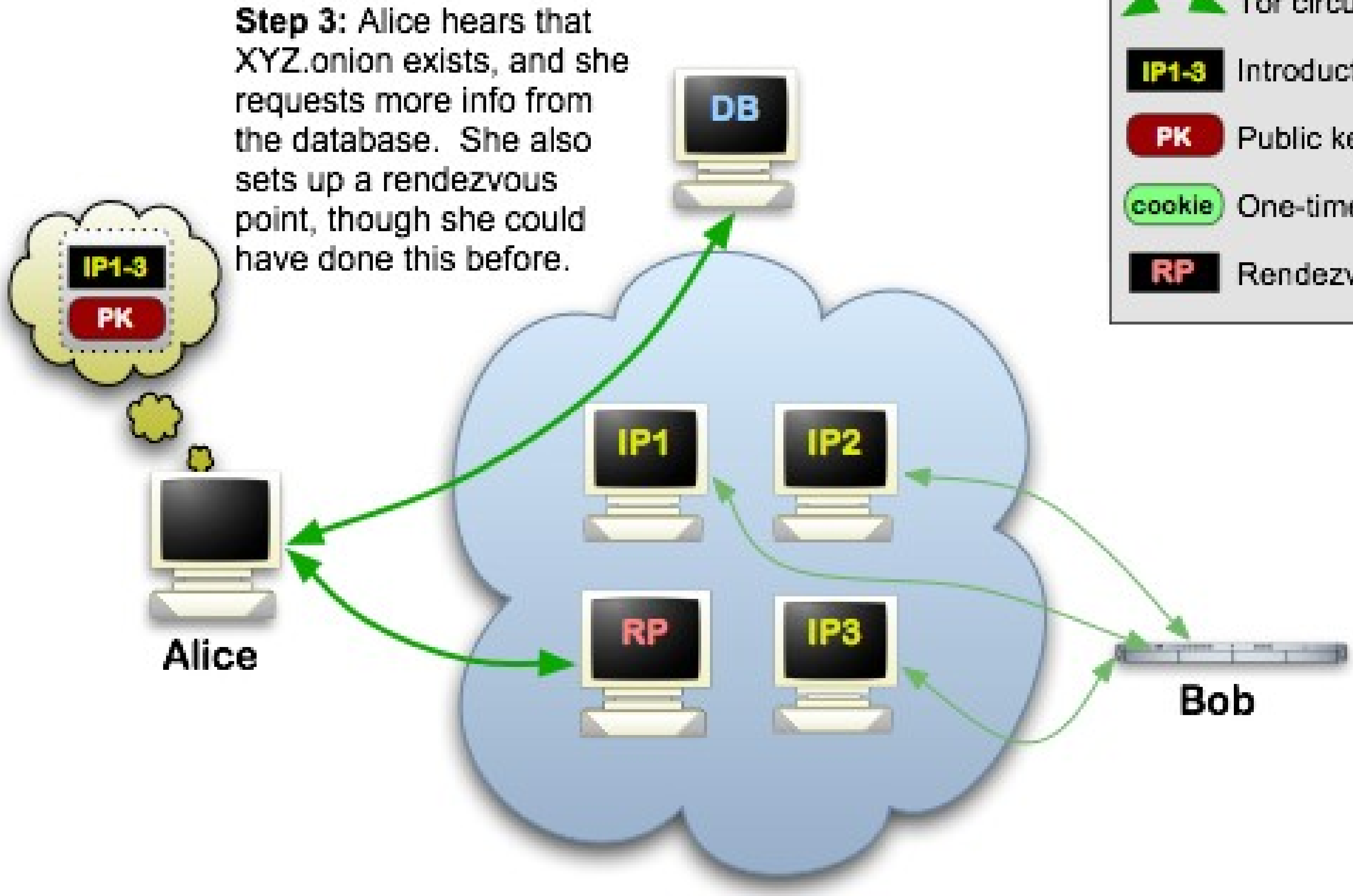
YOLO Crypto
@yolocrypto

gonna start silk road 3.0. tor is too hard so I’m just gonna host it at my home ip address

RETWEETS 122 FAVORITES 101

12:03 PM - 6 Nov 2014

Tor Hidden Services: 3



Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

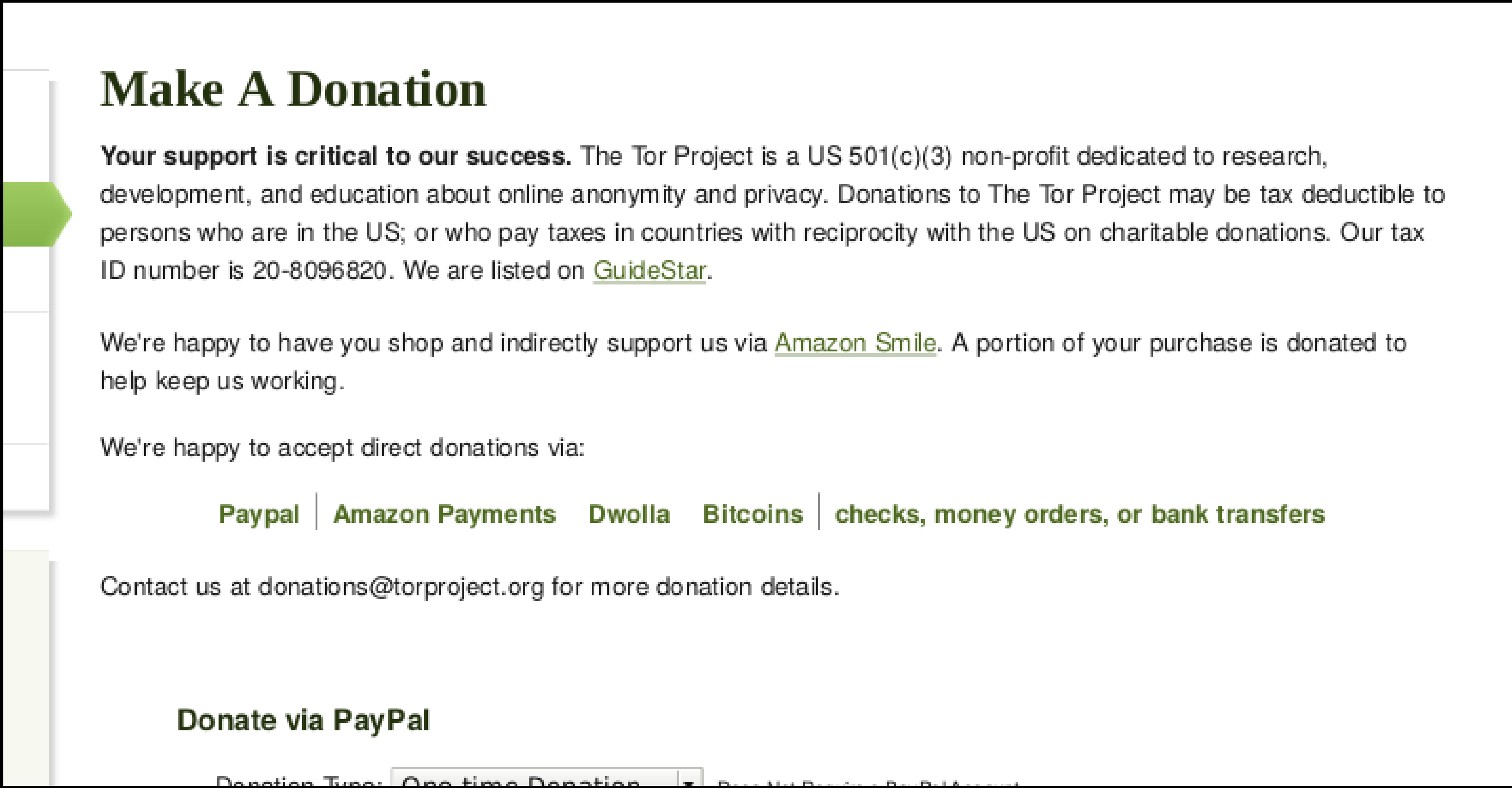
☁	Tor cloud
⤻	Tor circuit
IP1-3	Introduction points
PK	Public key
cookie	One-time secret
RP	Rendezvous point

Please teach your family and friends about the value(s) of Tor

THE HARVEY MILK CITY HALL MEMORIAL

Supervisor Harvey Milk, March 7, 1978

Photo by Daniel Nicoletta



Make A Donation

Your support is critical to our success. The Tor Project is a US 501(c)(3) non-profit dedicated to research, development, and education about online anonymity and privacy. Donations to The Tor Project may be tax deductible to persons who are in the US; or who pay taxes in countries with reciprocity with the US on charitable donations. Our tax ID number is 20-8096820. We are listed on GuideStar.

We're happy to have you shop and indirectly support us via Amazon Smile. A portion of your purchase is donated to help keep us working.

We're happy to accept direct donations via:

Paypal | Amazon Payments Dwolla Bitcoins | checks, money orders, or bank transfers

Contact us at donations@torproject.org for more donation details.

Donate via PayPal

Donation Type: One-time Donation