Hello Ken and Kelly,

Meet Erinn. Erinn is our main packaging person for just about everything users download and run. She's also become a recent public speaker about Tor, having done a number of recent talks in Chile, Sweden, and Portugal.

She is currently in Russia and did a talk at Moscow State University on Tor. She's received some good feedback and introductions to other people in the larger Russian citizen journalism sphere. In the past you've mentioned that BBG is concerned about what is going on in Russia, even if it's isn't the hot country according to the US media.

Erinn met someone who works with citizen journalists in the Caucasus (http://www.eng.kavkaz-uzel.ru/) and deals with the kinds of activists who'd be squarely within Tor's targets. That said, he's really interested in working on training materials with Tor, the kind that can be generalized enough that they're easy to adapt for specific regions.

Can you help us better engage with the larger ex-Soviet sphere of journalists? Are there related materials you've already created and distributed to help us jumpstart such an effort?

I'm planning on being in DC in early January 2011. If you're around, I can stop by and we can talk more about a plan to move forward with such an engagement.

--
Andrew
pgp 0x74ED336B

Hi folks,

Attached is our August report. The highlights are:
A) Lots of new versions of Tor components -- in particular, the Tor
0.2.0.x tree has finally been declared stable.
B) Outreach is continuing to ramp up, now that we have Jacob on board.
C) The "iFree" project is beginning! More on that in September.

My next task in the 'reports' category is to come up with a research and
development roadmap that covers all the topics we're working on now and
want to work on soon -- for DRL, for BBG, for NRL, for NLnet, for Google,
etc -- not just a description of the task, but also how much they cost,
in what timeframe we're aiming to land results, and so on. This should let
BBG see where it fits in the puzzle (right in the middle!), and should
also give us a good way to be more transparent with our community about
where Tor is now and where it's going.

Thanks!
--Roger

Hi folks,

Here's the December Tor report. We can chat more about it, and our other recent projects, on Friday.

Thanks!
--Roger

Hi folks,

I'm about to get on an airplane, and it may be a little while until I
get the January report finalized. So I decided to send most of it now,
and leave the "gossip" section (C.2.10) until later. Hopefully this will
have enough info in it to tide you over.

Andrew, please turn it into a shiny .doc file at your leisure.

Thanks,
--Roger

C.2.0. New releases, new hires, new funding

Tor 0.2.1.10-alpha (released January 6) fixes two major bugs in bridge
relays (one that would make the bridge relay not so useful if it had
DirPort set to 0, and one that could let an attacker learn a little bit
of information about the bridge's users), and a bug that would cause your
Tor relay to ignore a circuit create request it can't decrypt (rather
than reply with an error). It also fixes a wide variety of other bugs.
http://archives.seul.org/or/talk/Jan-2009/msg00078.html

Tor 0.2.1.11-alpha (released Jan 20) finishes fixing the "if your Tor is
off for a week it will take a long time to bootstrap again" bug. It also
fixes an important security-related bug reported by Ilja van Sprundel. You
should upgrade. (We'll send out more details about the bug once people
have had some time to upgrade.)
http://archives.seul.org/or/talk/Jan-2009/msg00171.html

Tor 0.2.0.33 (released Jan 21) fixes a variety of bugs that were making
relays less useful to users. It also finally fixes a bug where a relay or
client that's been off for many days would take a long time to bootstrap.
http://archives.seul.org/or/announce/Jan-2009/msg00000.html

Tor Browser Bundle 1.1.8 (released Jan 22) updates Tor to 0.2.1.11-alpha
(security update), updates OpenSSL to 0.9.8j (security update), updates
Firefox to 3.0.5, updates Pidgin to 2.5.4, and updates libevent to 1.4.9.
https://svn.torproject.org/svn/torbrowser/trunk/README

This month we also hired three new people: Martin Peck is working on
Tor VM, a new way of packaging Tor on Windows that will let people use
Youtube safely again; Mike Perry is working on Torbutton maintenance
and development and on Torflow, a set of scripts to do measurements on
the Tor network; and Andrew Lewman is our new executive director.

C.2.1. Design, develop, and implement enhancements that make Tor a better
tool for users in censored countries.

We continued enhancements to the Chinese and Russian Tor website
translations. Our Farsi translation from this summer is slowly becoming

obsolete; we should solve that at some point.

Major bugfixes in the Tor 0.2.1.10-alpha and 0.2.0.33 releases:
- If the cached networkstatus consensus is more than five days old,
  discard it rather than trying to use it. In theory it could be useful
  because it lists alternate directory mirrors, but in practice it just
  means we spend many minutes trying directory mirrors that are long
  gone from the network. Helps bug 887 a bit; bugfix on 0.2.0.x.

Tor 0.2.1.10-alpha contains cleanups that let Tor build on Google's
Android phone:
- Change our header file guard macros to be less likely to conflict
  with system headers. Adam Langley noticed that we were conflicting
  with log.h on Android.

Major bugfixes in the Tor 0.2.1.11-alpha and 0.2.0.33 releases:
- Discard router descriptors as we load them if they are more than
  five days old. Otherwise if Tor is off for a long time and then
  starts with cached descriptors, it will try to use the onion
  keys in those obsolete descriptors when building circuits. Bugfix
  on 0.2.0.x. Fixes bug 887.

Security bugfixes in the Tor 0.2.1.11-alpha and 0.2.0.33 releases:
- Fix a heap-corruption bug that may be remotely triggerable on
  some platforms. Reported by Ilja van Sprundel.

C.2.2. Architecture and technical design docs for Tor enhancements
related to blocking-resistance.

Proposal 158 ("Clients download consensus + microdescriptors") suggests a
new way forward for reducing directory overhead for clients, and replaced
part of proposal 141. Rather than modifying the circuit-building protocol
to fetch a server descriptor inline at each circuit extend, we instead put
all of the information that clients need either into the consensus itself,
or into a new set of data about each relay called a microdescriptor.
https://svn.torproject.org/svn/tor/trunk/doc/spec/proposals/158-microdescriptors.txt

C.2.5. Hide Tor's network signature.

From the 0.2.0.33 ChangeLog:
- Never use OpenSSL compression: it wastes RAM and CPU trying to compress
  cells, which are basically all encrypted, compressed, or both. It also
  made us stand out from other applications on the wire.

Nobody has blocked the new signature, as far as we know.

We have built a plan for how to address potential ways for people to
block Tor based on its network signature. We are aiming to have an
internal list of known potential vulnerabilities by early 2009, along
with suggested paths to addressing each. Then we can react to actual
blocking as it occurs, and periodically update our list of potential
flaws and intended solutions as we get more intuition.

More on that in February.

C.2.10. Grow the Tor network and user base. Outreach.

Jillian York continued blogging for us about the good uses of Tor:
http://www.knightpulse.org/blog/tor

"Federico Heinz advocates anonymous browsing in Argentina", Jan 8
http://www.knightpulse.org/blog/09/01/08/federico-heinz-advocates-anonymous-browsing-argentina

"Human Rights Organizations in Argentina welcome anonymous browsing", Jan 25
http://www.knightpulse.org/blog/09/01/25/human-rights-organizations-argentina-welcome-anonymous-browsing

"Watch how you get around", Jan 30
http://www.knightpulse.org/blog/09/01/30/watch-how-you-get-around

[more soon]

C.2.11. Preconfigured privacy (circumvention) bundles for USB or LiveCD.

Tor Browser Bundle 1.1.8 (released Jan 22) updates Tor to 0.2.1.11-alpha
(security update), updates OpenSSL to 0.9.8j (security update), updates
Firefox to 3.0.5, updates Pidgin to 2.5.4, and updates libevent to 1.4.9.
https://svn.torproject.org/svn/torbrowser/trunk/README

We continued work on Vidalia features to support where we want Tor
Browser Bundle to go. In particular, we're changing it to be able to
launch Firefox natively, rather than use the "PortableFirefox" pile of
complex scripts. We hope this change will also let users run a normal
Firefox alongside TBB. More on that in February.

We also continued work on Tor VM, a new way of packaging Tor on
Windows that will (among other things) let people use Youtube safely
again. Hopefully we'll have some simple instructions up about that in
February too.

C.2.12. Bridge relay and bridge authority work.

Major bugfixes in the Tor 0.2.1.10-alpha and 0.2.0.33 releases:
- Bridge relays that had DirPort set to 0 would stop fetching
  descriptors shortly after startup, and then briefly resume
  after a new bandwidth test and/or after publishing a new bridge
  descriptor. Bridge users that try to bootstrap from them would
  get a recent networkstatus but would get descriptors from up to
  18 hours earlier, meaning most of the descriptors were obsolete
  already. Reported by Tas; bugfix on 0.2.0.13-alpha.
- Prevent bridge relays from serving their 'extrainfo' document
  to anybody who asks, now that extrainfo docs include potentially
  sensitive aggregated client geoip summaries. Bugfix on
  0.2.0.13-alpha.

Bugfixes in the Tor 0.2.1.10-alpha release:
- When we made bridge authorities stop serving bridge descriptors over
  unencrypted links, we also broke DirPort reachability testing for
  bridges. So bridges with a non-zero DirPort were printing spurious
  warns to their logs. Bugfix on 0.2.0.16-alpha. Fixes bug 709.

New feature in Tor 0.2.1.10-alpha:
- New controller event "clients_seen" to report a geoip-based summary
  of which countries we've seen clients from recently. Now controllers
  like Vidalia can show bridge operators that they're actually making
  a difference.
Vidalia will add support for this feature in February.

Karsten began to crunch the numbers on all our historical bridge relay
information, to look for trends, and to start being able to display the

database more graphically. We sent some graphs about this in January, but we're aiming to have improved graphs in February.

C.2.13. Scalability, load balancing, directory overhead, efficiency.

Circuit-building speedups in Tor 0.2.1.10-alpha:
- When a relay gets a create cell it can't decrypt (e.g. because it's using the wrong onion key), we were dropping it and letting the client time out. Now actually answer with a destroy cell. Fixes bug 904. Bugfix on 0.0.2pre8.

Scalability fixes from the Tor 0.2.0.33 ChangeLog:
- Clip the MaxCircuitDirtiness config option to a minimum of 10 seconds, and the CircuitBuildTimeout to a minimum of 30 seconds. Warn the user if lower values are given in the configuration. These fixes prevent a user from rebuilding circuits too often, which can be a denial-of-service attack on the network.
- When a stream at an exit relay is in state "resolving" or "connecting" and it receives an "end" relay cell, the exit relay would silently ignore the end cell and not close the stream. If the client never closes the circuit, then the exit relay never closes the TCP connection. Bug introduced in Tor 0.1.2.1-alpha; reported by "wood".
- When sending CREATED cells back for a given circuit, use a 64-bit connection ID to find the right connection, rather than an addr:port combination. Now that we can have multiple OR connections between the same ORs, it is no longer possible to use addr:port to uniquely identify a connection.

Bootstrapping speedups in Tor 0.2.1.11-alpha:
- When our circuit fails at the first hop (e.g. we get a destroy cell back), avoid using that OR connection anymore, and also tell all the one-hop directory requests waiting for it that they should fail. Bugfix on 0.2.1.3-alpha.

Sent my geoip-counting patches to Karsten so he can begin playing around with trying to estimate the number of Tor users in each country. Wrote some very simple notes on where I think we're undercounting and where I think we're overcounting with the patch. More on that in January.

C.2.14. Incentives work.

I've summarized our current status here:
https://blog.torproject.org/blog/two-incentive-designs-tor

C.2.15. More reliable (e.g. split) download mechanism.

Our "gettor" email auto-responder is up and working:
https://svn.torproject.org/svn/projects/gettor/README
https://www.torproject.org/finding-tor#Mail

Thandy itself is working smoothly at this point too -- it can contact the central repository, check all the keys, look in the registry and compare the currently installed version to the new choices, fetch the right packages, check all the signatures, and launch the install.

As of December we only had a new MSI-based installer for Tor, but not for Vidalia, Torbutton, or Polipo. Now we do, though it's still in testing:
https://data.peertech.org/torbld

C.2.16. Footprints from Tor Browser Bundle.

No changes.

C.2.17. Translation work, ultimately a browser-based approach.

Our translation server is up and online:
https://translation.torproject.org/
https://www.torproject.org/translation-portal

Hi Kelly,

I have the July .doc file pretty much ready, but a lot of non-development outreach stuff has been going on lately that isn't captured in the current draft of the status report. So I'm going to stall another day or so in order to put more of it in.

Let me know if you instead need it ASAP (in which case I've attached a copy with an empty C.2.10).

Thanks!
--Roger

Hi folks,

Here's the November Tor report.

Sorry for the delay again -- I've been trying a policy lately of actually
answering all of my interesting mail (rather than the previous policy
of meaning to answer it but then forgetting about it and never looking
back). Which means that more things get done rather than dropped, but
with higher latency. :)

Thanks (and happy holidays),
--Roger

Hi folks,

Here's the November Tor report.

Sorry for the delay again -- I've been trying a policy lately of actually
answering all of my interesting mail (rather than the previous policy
of meaning to answer it but then forgetting about it and never looking
back). Which means that more things get done rather than dropped, but
with higher latency. :)

Thanks (and happy holidays),
--Roger

Here is the much-awaited October report. Hope it is useful!

Thanks,
--Roger

Here is the much-awaited October report. Hope it is useful!

Thanks,
--Roger

Hi folks,

Attached is our September report. The highlights are:

A) We started working with iFree to figure out what we'll be doing with
them over the next few years, and how to tie that into the IBB work.
B) We finished the first go at the roadmap-full.pdf, which lists all
the development items we'd like to get to in the next few years. First
we can use this to provide more transparency to our funders (you),
and next we hope to use it for transparency in our broader community.
C) Outreach continues apace.

Kelly, did we make any progress getting IBB translators interested in
our online translation process, or verifying our current translations?

I've scheduled to meet with Jeremiah Young in San Diego next week. I've
also just scheduled to meet with Shiyu Zhou in NYC on Nov 4 ish.

Let me know if you've had time to look over the roadmap-full, and/or
if I should schedule another time to drop by so we can discuss in more
detail. For example, I'm going to be in Alexandria for a conference from
Oct 27-30, and could conceivably stick around an extra half-day to meet
on the 31st.

I hope you're enjoying your government holiday. :)

Thanks!
--Roger

Hi Kelly,

I just got a call from a friend of mine who works at Akamai. He can't have an official conversation with you, but he pointed out that you could set up a voanews.com/twitter page which took in twitter credentials and then passed traffic to twitter. In effect that would make every akamai node into a proxy for folks who can't reach twitter directly. And you could do it just by modifying the content on your side, and not need to involve akamai in any way.

I don't know the twitter API to know how complex a page this would be to write. You'd want to get some engineers on your side to ponder whether it's *actually* a good idea, if you decide that it appears to be a good idea. :)

In any case my job is to be the messenger. I'm happy to hook you up with him in an unofficial way if you want to ask questions.

Hope you're having an exciting week,
--Roger

Not a full reply to your email yesterday, but just a couple things...

I think the language translations that would be good to have from our point of view at this time are just Simplified Chinese and Persian.

You also asked about documentation licensing, I think using the FreeBSD Documentation License probably makes the most sense.

Stay tuned, I should have a draft Statement of Work for you to review later today.

-k

Hi Kelly, Ken, Sho,

Here's a brief update on how things are going with Tor. We've been busy
the past week helping users in Iran set up Tor, and users out of Iran
set up Tor bridges and relays.

We're seeing a serious up-tick in Tor use from Iran:
https://blog.torproject.org/blog/measuring-tor-and-iran
I haven't yet made an updated version of that graph, but it dips a bit
and then goes even higher. I estimate there are between 1000 and 10000
people actively using Tor from Iran each day (plus another 250-1000 or
so bridge users, but those are much harder to count). It's not a million,
but it's clearly enough to get a lot of info to/from people inside.

Karsten made some graphs of the number of relays and number of bridges
running:
https://blog.torproject.org/blog/recent-growth-tor-network
and that article links two pdf's with much more detail:
https://git.torproject.org/checkout/metrics/master/report/dirarch/dirarch-2009-06-22.pdf
https://git.torproject.org/checkout/metrics/master/report/bridges/bridges-2009-06-22.pdf

We've been in the press a bunch. I've left that to Andrew, who I think
has managed to divert all of the "Tor takes on Iran, and wins!!!" stories
that journalists wanted to write. Yay.

I cleaned up the Tor relay / bridge setup instructions:
https://www.torproject.org/docs/tor-doc-relay

Note that the Tor network is not blocked from Iran right now. So people
can just fetch Tor and use it -- the bridges are backups for a) in case
the Tor network does get blocked, and b) people who want more security
because they're worried somebody will recognize that it's a Tor relay
IP address they're contacting.

Some nice fellow in Iran helped us clean up our Tor Browser Bundle
Farsi page:
https://www.torproject.org/torbrowser/index.html.fa
We had the right-to-left screwed up in some places, and nobody had told
us before this week. Oops.

We also put out an emergency Tor Browser Bundle update today with the
newly released Pidgin 2.5.7: apparently a) Yahoo broke Yahoo Messenger
for all clients except their official one, and they chose the past few
days to do it, and b) Yahoo Messenger is the IM client of choice in Iran.
Boo for Yahoo.

We're continuing to make progress on the performance questions. Karsten
has set up a "torperf" program fetching three files periodically via Tor:
50KB, 1MB, and 5MB. You can see the results here:
https://git.torproject.org/checkout/metrics/master/report/performance/torperf-2009-06-24.pdf
Page 3 shows the 1st quartile, median, and 3rd quartile of total download
time. So 50KB downloads generally take 5-15 seconds to download; 1MB

downloads take 40-100 seconds; and 5MB downloads take 150-450 seconds.
Conclusion: the bulk downloads are surprisingly good, and the tiny
download is surprisingly bad. We need to get that round-trip time down.

And last, our gettor email service has gone nuts in the past few days:
https://www.torproject.org/finding-tor#Mail
Jake did a training in Hong Kong a few days ago, and somebody there
fanfou'd the gettor address, and it took off from there. We've sent
about 1400 Tor Browser Bundles via email in the past two days, and we're
answering about 1 request per minute at this point -- a bit under 1
megabyte per second being dumped on gmail. I've contacted some friends
at google to make sure they know it's happening. :)

More later,
--Roger

Hi Ken, Kelly,

Vidalia has a dozen translations so far, but no Farsi. I think it would
be handy to get that started. Plus, the RSF folks we're working with
are focusing on Iran and they'd be happy to see a translation.

Do you have any Farsi translators who are at least mildly technically
inclined and could help us out?

Check out http://trac.vidalia-project.net/wiki/Translations for details of
how it works. Just translating the ".ts" file is the right step for now --
I hope to revise the help documents a lot in the next few months.

Let me know if you know anybody interested and suitable and we'll go
from there.

Thanks!
--Roger

Hi Kelly,

Thanks for the phone call last week. I've been working feverishly since then to get all the topics organized in my mind and then on paper. I think we've done a pretty good job with the attached document.

(I'm sorry it's so long. As they say, I haven't had time to make it shorter. :)

Shall we schedule a time for me and Andrew to come down and walk you through it, answer questions, and figure out how this matches up with your priorities and preferences? I'm available March 13-17 inclusive, and March 26-April 1 inclusive.

Thanks!
--Roger

Hello Kelly,

The Wall Street Journal is doing a write-up on Tor. They're wondering if they can interview your org as a funding org and why Tor.

Are you interested?

Thanks!

--
Andrew
http://tpo.is/contact
pgp 0x6B4D6475

From: Roger Dingledine
To: Kelly DeYoe; Ken Berman
Subject: (FWD) Re: Vidalia and Torbutton localization
Date: Wednesday, June 11, 2008 8:18:15 AM

Chris has found us a Farsi translator who is comfortable with text
editors, so we're working on getting more Tor components translated
into Farsi.

In other news, we've finally found a web-based translation project
that doesn't suck. It's called Pootle. You can check out the editing
interface at
http://translation.torproject.org/de/vidalia/translate.html?editing=1&blank=1

and you can compare the Farsi, Russian, and Chinese translation progress
at a glance:
http://translation.torproject.org/projects/torbutton/
http://translation.torproject.org/projects/vidalia/
http://translation.torproject.org/projects/torcheck/
though there are still some kinks to iron out -- for example it looks
like it can't find the zh-CN vidalia translation file, even though there
is one:
https://svn.torproject.org/svn/translation/trunk/projects/vidalia/zh_cn/vidalia.po

Plus it can commit changes directly to our SVN repository, so we don't
have to deal with manually importing and exporting "po" string files
all the time.

(Pootle can handle the string formats for Vidalia, Torbutton, and
Torcheck, but it can't yet handle the wml files that we use for our
website. So we have directed one of our Google Summer of Code students
to work for the summer on teaching Pootle how to handle wml files.)

We've only found it in the past week, so all of this set-up is very new.
We hope to clean it up in the next few weeks and then have it go 'live',
meaning we will actually encourage translators to show up and help out.

--Roger

----- Forwarded message from Jacob Appelbaum < [(b) (6)] > -----

From: Jacob Appelbaum < [(b) (6)]
To: Shahab Gashti < [(b) (6)]
CC: Chris Walker < [(b) (6)]
        'Roger Dingledine' < [(b) (6)]
Subject: Re: Vidalia and Torbutton localization
Delivery-Date: Tue, 10 Jun 2008 19:27:09 -0400

We do have a new process that will hopefully be "officially" launched in
the next few days. We're planning on merging all of the translation
files for Vidalia, Torbutton and any other projects (currently just
TorCheck) into a single website. Translators will be able to download
.po files for editing as they prefer or by using a website directly.

Currently, I'm working on a few details to ensure this rolls out
smoothly and I'll be documenting the process once we've agreed on a
solid one.

The website is up and running, though users can really only translate into German at the moment (this limitation is to make testing more manageable and not a permanent issue). The website is also synced with subversion, so users no longer need to know anything about subversion or diffing files unless they directly want to do so. This is the subversion repository:
https://tor-svn.freehaven.net/svn/translation/trunk/

If you'd like to see how the translation website works, this is the current version of the website, possibly as we will deploy it in the next few days:
http://translation.torproject.org/

You'll need to sign up for an account and register it before you'll be able to make translations. As I said above, only German is available for translation at the moment but it should work well for demonstration purposes.

This is the German section of the website, listing all projects:
http://translation.torproject.org/de_DE/index.html

This is the German section of the website, listing only files for Torbutton:
http://translation.torproject.org/de_DE/torbutton/

If there is a specific language, we can easily enable it for testing purposes and hopefully we'll be able to test a full translation from start to re-integration with upstream.

I hope this is helpful. I'm excited to see this new website and these new processes in place!

Please do send me any feedback and do not hesitate to ask questions, I'm all ears!

Regards,
Jacob Appelbaum

----- End forwarded message -----

I asked Wendy to take a look at the FISMA situation. Here's her answer.

--Roger

----- Forwarded message from Wendy Seltzer <​ ██████ (b) (6) ██████ ​> -----

From: Wendy Seltzer <​ ████ (b) (6) ████ ​>
To: ██████ (b) (6) ██████
Subject: FISMA -- I think we're clear
Delivery-Date: Fri, 06 Aug 2010 07:07:14 -0400

I did a very brief review of the Federal Information Security Management
Act (44 U.S.C. s 3541-49), as Roger said Ken was wondering whether it
applied to Tor. From my read of the statute, some White House and OMB
guidance memos, and the FIPS 199 standard, I'd say that FISMA does not
apply to Tor because Tor doesn't process "Federal Information."

FISMA is designed to assure the security, integrity, and availability of
federal information, whether that information is processed by federal
agencies or by third-party contractors. It makes agency heads
responsible for information risk management. It doesn't put any direct
obligations on federal contractors, but it might induce agencies to do
so when the contractors process government information.

Tor doesn't process any federal information; we can't breach anyone's
privacy, lose any federal secrets, or interfere with federal business
even if the network goes down. I think that should mean that Tor is
out-of-scope from Ken's FISMA obligations. That conclusion comes both
from the design of the Tor network (we can't learn anything about
individuals whom the government might want using the network), and the
nature of the services we're providing.

Happy to send pointers or do more analysis if you think it's useful.

--Wendy

§ 3544. Federal agency responsibilities
(a) In General.? The head of each agency shall?
(1) be responsible for?
(A) providing information security protections commensurate with the
risk and magnitude of the harm resulting from unauthorized access, use,
disclosure, disruption, modification, or destruction of?
(i) information collected or maintained by or on behalf of the agency; and
(ii) information systems used or operated by an agency or by a
contractor of an agency or other organization on behalf of an agency;
... <http://www.law.cornell.edu/uscode/44/3544.html>
--
Wendy Seltzer -- ██████ (b) (6) ██████
phone: + ████ (b) (6) ████
Fellow, Silicon Flatirons Center at University of Colorado Law School
Fellow, Berkman Center for Internet & Society at Harvard University
http://cyber.law.harvard.edu/seltzer.html

http://www.chillingeffects.org/
https://www.torproject.org/

----- End forwarded message -----

I asked Wendy to take a look at the FISMA situation. Here's her answer.

--Roger

----- Forwarded message from Wendy Seltzer < [(b) (6)] -----

From: Wendy Seltzer < [(b) (6)]
To: [(b) (6)]
Subject: FISMA -- I think we're clear
Delivery-Date: Fri, 06 Aug 2010 07:07:14 -0400

I did a very brief review of the Federal Information Security Management
Act (44 U.S.C. s 3541-49), as Roger said Ken was wondering whether it
applied to Tor. From my read of the statute, some White House and OMB
guidance memos, and the FIPS 199 standard, I'd say that FISMA does not
apply to Tor because Tor doesn't process "Federal Information."

FISMA is designed to assure the security, integrity, and availability of
federal information, whether that information is processed by federal
agencies or by third-party contractors. It makes agency heads
responsible for information risk management. It doesn't put any direct
obligations on federal contractors, but it might induce agencies to do
so when the contractors process government information.

Tor doesn't process any federal information; we can't breach anyone's
privacy, lose any federal secrets, or interfere with federal business
even if the network goes down. I think that should mean that Tor is
out-of-scope from Ken's FISMA obligations. That conclusion comes both
from the design of the Tor network (we can't learn anything about
individuals whom the government might want using the network), and the
nature of the services we're providing.

Happy to send pointers or do more analysis if you think it's useful.

--Wendy

§ 3544. Federal agency responsibilities
(a) In General.? The head of each agency shall?
(1) be responsible for?
(A) providing information security protections commensurate with the
risk and magnitude of the harm resulting from unauthorized access, use,
disclosure, disruption, modification, or destruction of?
(i) information collected or maintained by or on behalf of the agency; and
(ii) information systems used or operated by an agency or by a
contractor of an agency or other organization on behalf of an agency;
... <http://www.law.cornell.edu/uscode/44/3544.html>
--
Wendy Seltzer -- [(b) (6)]
phone: + [(b) (6)]
Fellow, Silicon Flatirons Center at University of Colorado Law School
Fellow, Berkman Center for Internet & Society at Harvard University
http://cyber.law.harvard.edu/seltzer.html

http://www.chillingeffects.org/
https://www.torproject.org/

----- End forwarded message -----

Hi Ken, Kelly,

I just learned that you folks have probably been left out of the loop
on this. Here are the details as I understand them, the key detail being
"http://cyber.law.harvard.edu/oniconference07/". Let me know if you want
me to introduce you to any of them. I hear they're mighty disorganized
(even mightier than normal I mean :).

--Roger

----- Forwarded message from Catherine Bracy < (b) (6) -----

From: Catherine Bracy < (b) (6)
To: (b) (6)
Subject: Invitation to Circumvention Tools Meeting in Oxford, May 17-18
Delivery-Date: Fri, 23 Mar 2007 17:20:25 -0400

March 23, 2007

Mr. Roger Dingledine
TOR
via email to: (b) (6)

Dear Roger:

The Berkman Center for Internet & Society at Harvard Law School is
hosting a meeting to discuss current circumvention tools and technology
on May 17 and 18 in Oxford, England. The meeting will gather together
developers of some of the most popular and interesting circumvention
tools along with many of the world's experts on internet filtering. The
purpose of the meeting will be to review the results of the center's
private circumvention tools study and to discuss shared issues including
possibilities for technology integration, strategies for blocking
resistance, likely future changes in filtering and blocking, and
practical needs of filtering users.

There will be a private meeting with just the circumvention project
leaders on May 17 to cover technical issues, followed by a breakout
session on May 18 in which we are joined by other people interested in
filtering to cover larger filtering and usage issues. The breakout is
part of a day-long conference on filtering, to which you are cordially
invited (more information will be available soon here:
http://cyber.law.harvard.edu/oniconference07).

We are able to pay for round-trip coach airfare to London, train from
London to Oxford, and two nights lodging in Oxford. We sincerely hope
you're available to attend. Please RSVP to me by Thursday, March 29 so
we can secure your place at the meeting and conference. Please let me
know if you have any questions.

Sincerely,

Catherine Bracy
Administrative Manager
Berkman Center for Internet & Society
Harvard Law School
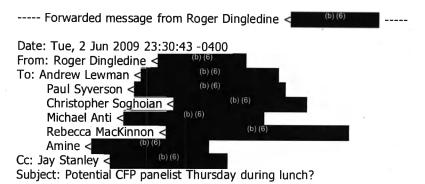
----- End forwarded message -----

Hi Kelly,

Want to drop by GWU tomorrow and be on a panel / breakout discussion about the need for tools like Tor around the world?

It's tomorrow, 12:15-13:30. It's an emergency replacement panel, so we're quite flexible about what it turns into. :)
http://www.cfp2009.org/wiki/index.php/Program

(Registration is free for gov't employees, so feel free to drop by even if the panel answer is no.)

--Roger

----- Forwarded message from Roger Dingledine < ​(b) (6)​ > -----

Date: Tue, 2 Jun 2009 23:30:43 -0400
From: Roger Dingledine < (b) (6)
To: Andrew Lewman < (b) (6)
      Paul Syverson < (b) (6)
      Christopher Soghoian < (b) (6)
      Michael Anti < (b) (6)
      Rebecca MacKinnon < (b) (6)
      Amine < (b) (6)
Cc: Jay Stanley < (b) (6)
Subject: Potential CFP panelist Thursday during lunch?

Hi folks,

Jay mentioned yesterday that the Egypt panel on Thursday flaked. Stephanie Perrin suggested that "the Tor guys" use the space. I'm thinking it would be nice to do a breakout session where we talk about all the various people in the world who need tools like Tor, and why. So that would mean:

- Andrew and me to give an overview of what Tor is, what it isn't, and why our strategy should be "bring all these different groups into the same network".

- Michael Anti and/or Rebecca to talk about circumvention in China (how pervasive it is, what sorts of things are filtered, and why Tor is a good solution for some situations and the wrong solution for others)

- Amine to say as much as he's willing to about the situation in Tunisia (e.g. why it's bad that so few people are coordinated bloggers)

- Paul to talk a bit about why governments and militaries need communications privacy

- Chris to talk about why ordinary people in the US and Europe really need *technology* to ensure their privacy (folks at CFP already believe that policy and laws are the way to solve problems, but do they think

enough about the tech side?)

I'm figuring it should be an actual breakout, where rather than doing
15 minute talks each and then running out of time, we do much shorter
introductions (unless you want more) and then start bringing the
audience in.

I know there are a bunch of related panels on Thursday. This panel would
follow naturally from the two "grand ballroom" panels; and the breakout
sessions later in the day are all about "activism", which I expect will
at best touch briefly on government filtering and mechanisms to get
around it.

So, what do you think? If we have enough interest, we should do it. If
you can't make it but you know the perfect person who should, please ask
them. If we don't have enough interest, we can let Jay know that we're
not the right panel. I think the conference would survive fine with just
the other breakout sessions at that point.

Paul: I think it should be pretty easy to make a "no cspan" rule, so if
you have any problems with officially being on a panel, that should be
a solvable problem. (If you want to be extra safe, we can seat you in
the front row and use you to jumpstart the audience discussion.)

Jay wanted to decide the fate of the panel slot by Wednesday at noon.
I'll plan to arrive before noon tomorrow (I'm not sure how much before
noon though :), and will check the email discussion and sort things
out then.

--Roger

----- End forwarded message -----

Hi folks,

Here's a snapshot of bridge progress from a development perspective.

--Roger

----- Forwarded message from Roger Dingledine < ███████ (b) (6) ███████ -----

From: Roger Dingledine < ███████ (b) (6) ███████
To: ███████ (b) (6) ███████
Subject: Re: bridge and bridge authority proposal
Delivery-Date: Sun, 11 Nov 2007 15:59:53 -0500

On Sun, May 06, 2007 at 11:42:25PM -0400, Roger Dingledine wrote:
> Here are some details on my plans for bridges and bridge authorities.
> They're still fluid because I haven't actually built it, so it's hard
> to know if they will turn out to be the right plans when it comes down
> to coding, but it's at least a start.

Here is a much more fleshed out version, describing the current design
as well as the current state of implementation.

Behavior for bridge users, bridge relays, and bridge authorities

0. Preface

  This document describes the design decisions around support for bridge
  users, bridge relays, and bridge authorities. It acts as an overview
  of the bridge design and deployment for developers, and it also tries
  to point out limitations in the current design and implementation.

  For more details on what all of these mean, look at blocking.tex in
  /doc/design-paper/

1. Bridge relays

  Bridge relays are just like normal Tor relays except they don't publish
  their server descriptors to the main directory authorities.

1.1. PublishServerDescriptor

  To configure your relay to be a bridge relay, just add
    PublishServerDescriptor bridge
  to your torrc. This will cause your relay to publish its descriptor
  to the bridge authorities rather than to the default authorities.

  Alternatively, you can say
    PublishServerDescriptor 0
  which will cause your relay to not publish anywhere. This could be
  useful for private bridges.

1.2. Defining DirPort

Bridges need to answer BEGIN_DIR requests, both so they can answer
"/server/authority" questions ("what's your descriptor?") and so they
can supply their bridge users with cached copies of all the various
Tor network information.

Right now (0.2.0.11-alpha) we require that bridges turn their DirPort on
-- which means both that we answer BEGIN_DIR requests and that we fetch
and cache directory information in an aggressive way like other servers.

But:
a) we don't enforce that DirPort is on, since it's not clear how to
detect if the user meant to be a bridge. So it's easy to set up a bridge
relay that silently refuses BEGIN_DIR requests and is thus useless.
b) We don't actually care if they have an open or reachable DirPort. So
at some point we should separate having an open DirPort from answering
directory questions. Which leads to:
c) We need to investigate if there are any anonymity worries with
answering BEGIN_DIR requests when our DirPort is off. If there aren't,
we should drop the DirPort requirement.

I claim that we don't open any new attacks by answering BEGIN_DIR
questions when DirPort is off: it's still a fine question to ask what
partitioning attacks there are when you can query a Tor client about
its current directory opinions, but these attacks already exist when
DirPort is on.

We need to answer this issue in 0.2.0.x.

1.3. Exit policy

Bridge relays should use an exit policy of "reject *:*". This is
because they only need to relay traffic between the bridge users
and the rest of the Tor network, so there's no need to let people
exit directly from them.

1.4. RelayBandwidthRate / RelayBandwidthBurst

We invented the RelayBandwidth* options for this situation: Tor clients
who want to allow relaying too. See proposal 111 for details. Relay
operators should feel free to rate-limit their relayed traffic.

1.5. Helping the user with port forwarding, NAT, etc.

Just as for operating normal relays, our documentation and hints for
how to make your ORPort reachable are inadequate for normal users.

We need to work harder on this step, perhaps in 0.2.1.x.

1.6. Vidalia integration

Vidalia 0.0.15 has turned its "Relay" settings page into a tri-state
"Don't relay" / "Relay for the Tor network" / "Help censored users".

If you click the third choice, it forces your exit policy to reject *:*,
and it forces your DirPort to 9030 (but see Sec 1.2 above about DirPort).

If all the bridges end up on port 9001, that's not so good. On the
other hand, putting the bridges on a low-numbered port in the Unix
world requires jumping through extra hoops. The current compromise is

that Vidalia makes the ORPort default to 443 on Windows, and 9001 on
other platforms.

At the bottom of the relay config settings window, Vidalia displays
the bridge identifier to the operator (see Section 3.1) so he can pass
it on to bridge users.

1.7. What if the default ORPort is already used?

If the user already has a webserver or some other application
bound to port 443, then Tor will fail to bind it and complain to the
user, probably in a cryptic way. Rather than just working on a better
error message (though we should do this), we should consider an
"ORPort auto" option that tells Tor to try to find something that's
bindable and reachable. This would also help us tolerate ISPs that
filter incoming connections on port 80 and port 443. But this should
be a different proposal, and can wait until 0.2.1.x.

2. Bridge authorities.

Bridge authorities are like normal directory authorities, except they
don't create their own network-status documents or votes. So if you
ask an authority for a network-status document or consensus, they
behave like a directory mirror: they give you one from one of the main
authorities. But if you ask the bridge authority for the descriptor
corresponding to a particular identity fingerprint, it will happily
give you the latest descriptor for that fingerprint.

To become a bridge authority, add these lines to your torrc:
    AuthoritativeDirectory 1
    BridgeAuthoritativeDir 1

Right now there's one bridge authority, running on the Tonga relay.

2.1. Exporting bridge-purpose descriptors

We've added a new purpose for server descriptors: the "bridge"
purpose. With the new router-descriptors file format that includes
annotations, it's easy to look through it and find the bridge-purpose
descriptors.

We should work with Tonga to export its router-descriptors file to
some place where we can distribute the bridge addresses according to
the policies in blocking.pdf. It might even be easier to have it write
out a separate file, just for export, that includes only the bridge
descriptors; or maybe a six-liner perl postprocessing script is the
better plan there to create a file for export.

2.2. Reachability/uptime testing

Right now the bridge authorities just passively collect bridge
descriptors, and give them out on request. At some point we are going
to want to recommend new bridges to users, and we'll want to have
some way of deciding which ones are up right now, which ones have
been around for a while, etc. We should have the bridge authorities
do active measurements of bridges just as the normal authorities do
active measurements of normal relays. Then we can export the results
just like in Section 2.1. above.

In the design document, we suggested that bridges should publish

anonymously (i.e. via Tor) to the bridge authority, so somebody watching
the bridge authority can't just enumerate all the bridges. But if we're
doing active measurement, the game is up. Perhaps we should back off on
this goal, or perhaps we should do our active measurement anonymously?

Answering this issue is scheduled for 0.2.1.x.

2.3. Migrating to multiple bridge authorities

Having only one bridge authority is both a trust bottleneck (if you
break into one place you learn about every single bridge we've got)
and a robustness bottleneck (when it's down, bridge users become sad).

Right now if we put up a second bridge authority, all the bridges would
publish to it, and (assuming the code works) bridge users would query
a random bridge authority. This resolves the robustness bottleneck,
but makes the trust bottleneck even worse.

In 0.2.1.x and later we should think about better ways to have multiple
bridge authorities.

3. Bridge users.

Bridge users are like ordinary Tor users except they use encrypted
directory connections by default, and they use bridge relays as both
entry guards (their first hop) and directory guards (the source of
all their directory information).

To become a bridge user, add the following two lines to your torrc:

    UseBridges 1
    TunnelDirConns 1

and then add at least one "Bridge" line to your torrc based on the
format below.

3.1. Format of the bridge identifier.

The canonical format for a bridge identifier contains an IP address,
an ORPort, and an identity fingerprint:
    bridge 128.31.0.34:9009 4C17 FB53 2E20 B2A8 AC19 9441 ECD2 B017 7B39 E4B1

However, the identity fingerprint can be left out, in which case the
bridge user will connect to that relay and use it as a bridge regardless
of what identity key it presents:
    bridge 128.31.0.34:9009
This might be useful for cases where only short bridge identifiers
can be communicated to bridge users.

In a future version we may also support bridge identifiers that are
only a key fingerprint:
    bridge 4C17 FB53 2E20 B2A8 AC19 9441 ECD2 B017 7B39 E4B1
and the bridge user can fetch the latest descriptor from the bridge
authority (see Section 3.4).

3.2. Bridges as entry guards

For now, bridge users add their bridge relays to their list of "entry
guards" (see path-spec.txt for background on entry guards). They are
managed by the entry guard algorithms exactly as if they were a normal

entry guard -- their keys and timing get cached in the "state" file,
etc. This means that when the Tor user starts up with "UseBridges"
disabled, he will skip past the bridge entries since they won't be
listed as up and usable in his networkstatus consensus. But to be clear,
the "entry_guards" list doesn't currently distinguish guards by purpose.

Internally, each bridge user keeps a smartlist of "bridge_info_t"
that reflects the "bridge" lines from his torrc along with a download
schedule (see Section 3.5 below). When he starts Tor, he attempts
to fetch a descriptor for each configured bridge (see Section 3.4
below). When he succeeds at getting a descriptor for one of the bridges
in his list, he adds it directly to the entry guard list using the
normal add_an_entry_guard() interface. Once a bridge descriptor has
been added, should_delay_dir_fetches() will stop delaying further
directory fetches, and the user begins to bootstrap his directory
information from that bridge (see Section 3.3).

Currently bridge users cache their bridge descriptors to the
"cached-descriptors" file (annotated with purpose "bridge"), but
they don't make any attempt to reuse descriptors they find in this
file. The theory is that either the bridge is available now, in which
case you can get a fresh descriptor, or it's not, in which case an
old descriptor won't do you much good.

We could disable writing out the bridge lines to the state file, if
we think this is a problem.

As an exception, if we get an application request when we have one
or more bridge descriptors but we believe none of them are running,
we mark them all as running again. This is similar to the exception
already in place to help long-idle Tor clients realize they should
fetch fresh directory information rather than just refuse requests.

3.3. Bridges as directory guards

In addition to using bridges as the first hop in their circuits, bridge
users also use them to fetch directory updates. Other than initial
bootstrapping to find a working bridge descriptor (see Section 3.4
below), all further non-anonymized directory fetches will be redirected
to the bridge.

This means that bridge relays need to have cached answers for all
questions the bridge user might ask. This makes the upgrade path
tricky --- for example, if we migrate to a v4 directory design, the
bridge user would need to keep using v3 so long as his bridge relays
only knew how to answer v3 queries.

In a future design, for cases where the user has enough information
to build circuits yet the chosen bridge doesn't know how to answer a
given query, we might teach bridge users to make an anonymized request
to a more suitable directory server.

3.4. How bridge users get their bridge descriptor

Bridge users can fetch bridge descriptors in two ways: by going directly
to the bridge and asking for "/tor/server/authority", or by going to
the bridge authority and asking for "/tor/server/fp/ID". By default,
they will only try the direct queries. If the user sets
   UpdateBridgesFromAuthority 1
in his config file, then he will try querying the bridge authority

first for bridges where he knows a digest (if he only knows an IP
address and ORPort, then his only option is a direct query).

If the user has at least one working bridge, then he will do further
queries to the bridge authority through a full three-hop Tor circuit.
But when bootstrapping, he will make a direct begin_dir-style connection
to the bridge authority.

As of Tor 0.2.0.10-alpha, if the user attempts to fetch a descriptor
from the bridge authority and it returns a 404 not found, the user
will automatically fall back to trying a direct query. Therefore it is
recommended that bridge users always set UpdateBridgesFromAuthority,
since at worst it will delay their fetches a little bit and notify
the bridge authority of the identity fingerprint (but not location)
of their intended bridges.

3.5. Bridge descriptor retry schedule

Bridge users try to fetch a descriptor for each bridge (using the
steps in Section 3.4 above) on startup. Whenever they receive a
bridge descriptor, they reschedule a new descriptor download for 1
hour from then.

If on the other hand it fails, they try again after 15 minutes for the
first attempt, after 15 minutes for the second attempt, and after 60
minutes for subsequent attempts.

In 0.2.1.x we should come up with some smarter retry schedules.

3.6. Vidalia integration

Vidalia 0.0.15 has a new checkbox in its Network config window called
"My ISP blocks connections to the Tor network." Users who click that
box change their configuration to:
  TunnelDirConns 1
  PreferTunneledDirConns 1

Once the box is checked, there is also a section for adding bridge
identifiers. When at least one bridge identifier is present, Vidalia
also changes their config to:
  UseBridges 1
  UpdateBridgesFromAuthority 1
and updates their Bridge config option accordingly.

3.7. When should we make TunnelDirConns default?

Right now Tor's directory requests can be filtered on the network,
and some tools used by Middle Eastern governments even do this. A user
who wants to circumvent these filters should click the above box in
Vidalia 0.0.15. But at what point should we make tunneled directory
requests the default?

Once proposal 124 (modified TLS handshake) is in place, we should
consider doing the switch. This might even be in the 0.2.0.x timeframe.

----- End forwarded message -----

----- Forwarded message from Roger Dingledine < [(b) (6)] -----

Here's another snapshot, again representing about 150000 Tor clients
seen during a given 24 hour period.

--Roger

May 30 18:00:00.325 [notice] Clients seen:
de=38039(25.755%)
us=23234(15.731%)
cn=17392(11.775%)
it=7332(4.964%)
fr=4974(3.368%)
gb=4835(3.274%)
ca=3238(2.192%)
ru=3155(2.136%)
pl=3128(2.118%)
es=2775(1.879%)
jp=2666(1.805%)
tr=2619(1.773%)
br=2153(1.458%)
at=2091(1.416%)
au=1663(1.126%)
se=1583(1.072%)
nl=1569(1.062%)
tw=1463(0.991%)
ch=1367(0.926%)
mx=1101(0.745%)
in=899(0.609%)
ar=880(0.596%)
ro=870(0.589%)
ua=826(0.559%)
no=789(0.534%)
cz=756(0.512%)
fi=733(0.496%)
cl=726(0.492%)
be=705(0.477%)
vn=697(0.472%)
gr=629(0.426%)
ir=599(0.406%)
hk=582(0.394%)
id=559(0.378%)
hu=546(0.370%)
dk=538(0.364%)
th=527(0.357%)
sg=523(0.354%)
pt=510(0.345%)
kr=508(0.344%)
my=491(0.332%)
sa=484(0.328%)
il=471(0.319%)
sk=339(0.230%)
co=335(0.227%)

```
ie=332(0.225%)
ve=327(0.221%)
bg=305(0.207%)
ph=305(0.207%)
nz=295(0.200%)
lt=276(0.187%)
hr=227(0.154%)
pe=198(0.134%)
qa=198(0.134%)
by=190(0.129%)
cs=190(0.129%)
si=180(0.122%)
lv=172(0.116%)
kw=136(0.092%)
ee=132(0.089%)
pk=123(0.083%)
md=114(0.077%)
lu=95(0.064%)
ps=91(0.062%)
do=90(0.061%)
ge=86(0.058%)
pr=86(0.058%)
kz=84(0.057%)
cr=80(0.054%)
mk=73(0.049%)
jo=71(0.048%)
ae=69(0.047%)
gt=67(0.045%)
sv=66(0.045%)
uy=61(0.041%)
pa=57(0.039%)
ba=56(0.038%)
sy=55(0.037%)
om=51(0.035%)
rs=49(0.033%)
ec=45(0.030%)
lb=44(0.030%)
bo=42(0.028%)
cy=41(0.028%)
is=36(0.024%)
uz=36(0.024%)
bh=33(0.022%)
lk=29(0.020%)
py=29(0.020%)
hn=27(0.018%)
jm=26(0.018%)
mt=23(0.016%)
bd=22(0.015%)
az=21(0.014%)
ye=20(0.014%)
iq=19(0.013%)
mo=19(0.013%)
ni=19(0.013%)
tt=16(0.011%)
al=15(0.010%)
an=14(0.009%)
bb=13(0.009%)
cu=13(0.009%)
am=12(0.008%)
me=12(0.008%)
```

bs=11(0.007%)
kh=11(0.007%)
bn=10(0.007%)
ng=8(0.005%)
pf=8(0.005%)
bm=7(0.005%)
gu=7(0.005%)
ky=7(0.005%)
fj=6(0.004%)
li=6(0.004%)
mn=6(0.004%)
ax=5(0.003%)
mv=5(0.003%)
sm=5(0.003%)
ag=4(0.003%)
bz=4(0.003%)
kg=4(0.003%)
la=4(0.003%)
mc=4(0.003%)
zm=4(0.003%)
bt=3(0.002%)
gy=3(0.002%)
mp=3(0.002%)
mq=3(0.002%)
np=3(0.002%)
pg=3(0.002%)
vi=3(0.002%)
aw=2(0.001%)
gl=2(0.001%)
gp=2(0.001%)
ke=2(0.001%)
mg=2(0.001%)
nc=2(0.001%)
tm=2(0.001%)
ad=1(0.001%)
af=1(0.001%)
bj=1(0.001%)
cd=1(0.001%)
ck=1(0.001%)
fk=1(0.001%)
gd=1(0.001%)
gi=1(0.001%)
ht=1(0.001%)
kn=1(0.001%)
lc=1(0.001%)
ly=1(0.001%)
ma=1(0.001%)
mm=1(0.001%)
mw=1(0.001%)
mz=1(0.001%)
pw=1(0.001%)
sb=1(0.001%)
sr=1(0.001%)
tj=1(0.001%)
to=1(0.001%)
vc=1(0.001%)
vu=1(0.001%)
za=1(0.001%)

On Sun, Apr 13, 2008 at 02:26:45AM -0400, Roger Dingledine wrote:

```
> Apr 13 02:00:00.643 [notice] Clients seen:
> de=42875(28.030%)
> us=24099(15.755%)
> cn=18617(12.171%)
> it=6022(3.937%)
> fr=4904(3.206%)
> gb=4778(3.124%)
> ca=3449(2.255%)
> pl=3378(2.208%)
> jp=3033(1.983%)
> ru=2709(1.771%)
> es=2594(1.696%)
> at=2286(1.494%)
> tr=2270(1.484%)
> br=1918(1.254%)
> se=1748(1.143%)
> tw=1726(1.128%)
> au=1720(1.124%)
> nl=1503(0.983%)
> ch=1460(0.954%)
> mx=1078(0.705%)
> ir=885(0.579%)
> in=874(0.571%)
> ro=859(0.562%)
> ar=834(0.545%)
> cz=811(0.530%)
> fi=789(0.516%)
> be=782(0.511%)
> no=763(0.499%)
> ua=742(0.485%)
> hk=699(0.457%)
> vn=618(0.404%)
> gr=587(0.384%)
> dk=580(0.379%)
> cl=576(0.377%)
> sg=573(0.375%)
> hu=572(0.374%)
> il=570(0.373%)
> pt=562(0.367%)
> my=467(0.305%)
> th=457(0.299%)
> id=390(0.255%)
> sk=360(0.235%)
> ie=333(0.218%)
> co=324(0.212%)
> lt=320(0.209%)
> ph=320(0.209%)
> bg=284(0.186%)
> nz=282(0.184%)
> ve=265(0.173%)
> sa=260(0.170%)
> hr=231(0.151%)
> qa=222(0.145%)
> si=207(0.135%)
> pe=180(0.118%)
> cs=177(0.116%)
> kr=177(0.116%)
> lv=166(0.109%)
> kw=163(0.107%)
> ee=136(0.089%)
```

> ag=4(0.003%)
> ax=4(0.003%)
> dz=4(0.003%)
> fo=4(0.003%)
> kh=4(0.003%)
> mc=4(0.003%)
> mq=4(0.003%)
> cd=3(0.002%)
> dm=3(0.002%)
> ng=3(0.002%)
> np=3(0.002%)
> re=3(0.002%)
> sm=3(0.002%)
> tj=3(0.002%)
> ad=2(0.001%)
> eg=2(0.001%)
> ht=2(0.001%)
> la=2(0.001%)
> ne=2(0.001%)
> sr=2(0.001%)
> tm=2(0.001%)
> zm=2(0.001%)
> zw=2(0.001%)
> bj=1(0.001%)
> cg=1(0.001%)
> ck=1(0.001%)
> cv=1(0.001%)
> fk=1(0.001%)
> gh=1(0.001%)
> gi=1(0.001%)
> gq=1(0.001%)
> gy=1(0.001%)
> ke=1(0.001%)
> kg=1(0.001%)
> lc=1(0.001%)
> mh=1(0.001%)
> mm=1(0.001%)
> mp=1(0.001%)
> mz=1(0.001%)
> nc=1(0.001%)
> sb=1(0.001%)
> tc=1(0.001%)
> tv=1(0.001%)
> tz=1(0.001%)
> vc=1(0.001%)
> vg=1(0.001%)
> vi=1(0.001%)
> za=1(0.001%)
>
> On Wed, Dec 12, 2007 at 08:41:40PM -0500, Roger Dingledine wrote:
> > Dec 12 20:36:06.977 [notice] 97125 Total
> > Dec 12 20:36:06.977 [notice] 21672 DE (22.314%)
> > Dec 12 20:36:06.977 [notice] 17028 US (17.532%)
> > Dec 12 20:36:06.977 [notice] 16679 CN (17.173%)
> > Dec 12 20:36:06.977 [notice] 3666 FR (3.775%)
> > Dec 12 20:36:06.977 [notice] 3528 IT (3.632%)
> > Dec 12 20:36:06.978 [notice] 2746 GB (2.827%)
> > Dec 12 20:36:06.978 [notice] 2561 CA (2.637%)
> > Dec 12 20:36:06.978 [notice] 2139 JP (2.202%)
> > Dec 12 20:36:06.978 [notice] 2082 PL (2.144%)

> > Dec 12 20:36:06.978 [notice] 1911 TW (1.968%)
> > Dec 12 20:36:06.978 [notice] 1482 ES (1.526%)
> > Dec 12 20:36:06.978 [notice] 1328 BR (1.367%)
> > Dec 12 20:36:06.978 [notice] 1303 RU (1.342%)
> > Dec 12 20:36:06.978 [notice] 1120 AU (1.153%)
> > Dec 12 20:36:06.978 [notice] 1090 AT (1.122%)
> > Dec 12 20:36:06.978 [notice] 959 UN (0.987%)
> > Dec 12 20:36:06.978 [notice] 952 SE (0.980%)
> > Dec 12 20:36:06.978 [notice] 899 NL (0.926%)
> > Dec 12 20:36:06.978 [notice] 778 CH (0.801%)
> > Dec 12 20:36:06.978 [notice] 685 TR (0.705%)
> > Dec 12 20:36:06.978 [notice] 598 CZ (0.616%)
> > Dec 12 20:36:06.978 [notice] 543 MX (0.559%)
> > Dec 12 20:36:06.978 [notice] 528 NO (0.544%)
> > Dec 12 20:36:06.978 [notice] 524 IN (0.540%)
> > Dec 12 20:36:06.978 [notice] 522 IR (0.537%)
> > Dec 12 20:36:06.979 [notice] 509 BE (0.524%)
> > Dec 12 20:36:06.979 [notice] 463 RO (0.477%)
> > Dec 12 20:36:06.979 [notice] 451 AR (0.464%)
> > Dec 12 20:36:06.979 [notice] 440 FI (0.453%)
> > Dec 12 20:36:06.979 [notice] 409 DK (0.421%)
> > Dec 12 20:36:06.979 [notice] 404 TH (0.416%)
> > Dec 12 20:36:06.979 [notice] 383 PT (0.394%)
> > Dec 12 20:36:06.979 [notice] 358 IL (0.369%)
> > Dec 12 20:36:06.979 [notice] 351 SG (0.361%)
> > Dec 12 20:36:06.979 [notice] 336 GR (0.346%)
> > Dec 12 20:36:06.980 [notice] 326 UA (0.336%)
> > Dec 12 20:36:06.980 [notice] 316 MY (0.325%)
> > Dec 12 20:36:06.980 [notice] 315 HK (0.324%)
> > Dec 12 20:36:06.980 [notice] 311 VN (0.320%)
> > Dec 12 20:36:06.980 [notice] 282 LT (0.290%)
> > Dec 12 20:36:06.980 [notice] 280 SK (0.288%)
> > Dec 12 20:36:06.980 [notice] 276 HU (0.284%)
> > Dec 12 20:36:06.980 [notice] 225 CL (0.232%)
> > Dec 12 20:36:06.980 [notice] 201 PH (0.207%)
> > Dec 12 20:36:06.980 [notice] 199 NZ (0.205%)
> > Dec 12 20:36:06.980 [notice] 191 IE (0.197%)
> > Dec 12 20:36:06.980 [notice] 165 CO (0.170%)
> > Dec 12 20:36:06.980 [notice] 163 ID (0.168%)
> > Dec 12 20:36:06.980 [notice] 143 BG (0.147%)
> > Dec 12 20:36:06.980 [notice] 142 KR (0.146%)
> > Dec 12 20:36:06.980 [notice] 138 SA (0.142%)
> > Dec 12 20:36:06.980 [notice] 129 HR (0.133%)
> > Dec 12 20:36:06.980 [notice] 129 VE (0.133%)
> > Dec 12 20:36:06.980 [notice] 104 PE (0.107%)
> > Dec 12 20:36:06.980 [notice] 99 SI (0.102%)
> > Dec 12 20:36:06.980 [notice] 92 CS (0.095%)
> > Dec 12 20:36:06.980 [notice] 83 QA (0.085%)
> > Dec 12 20:36:06.980 [notice] 80 LV (0.082%)
> > Dec 12 20:36:06.981 [notice] 72 BY (0.074%)
> > Dec 12 20:36:06.981 [notice] 72 KW (0.074%)
> > Dec 12 20:36:06.981 [notice] 71 EE (0.073%)
> > Dec 12 20:36:06.981 [notice] 62 PK (0.064%)
> > Dec 12 20:36:06.981 [notice] 50 SY (0.051%)
> > Dec 12 20:36:06.981 [notice] 48 PR (0.049%)
> > Dec 12 20:36:06.981 [notice] 46 LU (0.047%)
> > Dec 12 20:36:06.981 [notice] 40 JO (0.041%)
> > Dec 12 20:36:06.981 [notice] 40 GT (0.041%)
> > Dec 12 20:36:06.981 [notice] 39 OM (0.040%)
> > Dec 12 20:36:06.981 [notice] 39 DO (0.040%)

```
> > Dec 12 20:36:06.981 [notice] 37 CR (0.038%)
> > Dec 12 20:36:06.981 [notice] 35 MK (0.036%)
> > Dec 12 20:36:06.981 [notice] 31 AE (0.032%)
> > Dec 12 20:36:06.981 [notice] 29 KZ (0.030%)
> > Dec 12 20:36:06.981 [notice] 29 SV (0.030%)
> > Dec 12 20:36:06.981 [notice] 29 UY (0.030%)
> > Dec 12 20:36:06.981 [notice] 28 EC (0.029%)
> > Dec 12 20:36:06.981 [notice] 28 RS (0.029%)
> > Dec 12 20:36:06.981 [notice] 28 BA (0.029%)
> > Dec 12 20:36:06.981 [notice] 28 PA (0.029%)
> > Dec 12 20:36:06.981 [notice] 24 BO (0.025%)
> > Dec 12 20:36:06.982 [notice] 21 BH (0.022%)
> > Dec 12 20:36:06.982 [notice] 20 CY (0.021%)
> > Dec 12 20:36:06.982 [notice] 19 LK (0.020%)
> > Dec 12 20:36:06.982 [notice] 17 PY (0.018%)
> > Dec 12 20:36:06.982 [notice] 17 MD (0.018%)
> > Dec 12 20:36:06.982 [notice] 16 UZ (0.016%)
> > Dec 12 20:36:06.982 [notice] 16 MT (0.016%)
> > Dec 12 20:36:06.982 [notice] 15 PS (0.015%)
> > Dec 12 20:36:06.982 [notice] 14 NI (0.014%)
> > Dec 12 20:36:06.982 [notice] 13 LB (0.013%)
> > Dec 12 20:36:06.982 [notice] 13 YE (0.013%)
> > Dec 12 20:36:06.982 [notice] 12 HN (0.012%)
> > Dec 12 20:36:06.982 [notice] 12 MO (0.012%)
> > Dec 12 20:36:06.982 [notice] 12 BD (0.012%)
> > Dec 12 20:36:06.982 [notice] 11 IQ (0.011%)
> > Dec 12 20:36:06.982 [notice] 9 BB (0.009%)
> > Dec 12 20:36:06.982 [notice] 9 BN (0.009%)
> > Dec 12 20:36:06.982 [notice] 9 GE (0.009%)
> > Dec 12 20:36:06.982 [notice] 9 AL (0.009%)
> > Dec 12 20:36:06.982 [notice] 8 IS (0.008%)
> > Dec 12 20:36:06.983 [notice] 6 TT (0.006%)
> > Dec 12 20:36:06.983 [notice] 6 CU (0.006%)
> > Dec 12 20:36:06.983 [notice] 6 PF (0.006%)
> > Dec 12 20:36:06.983 [notice] 6 MV (0.006%)
> > Dec 12 20:36:06.983 [notice] 5 BM (0.005%)
> > Dec 12 20:36:06.983 [notice] 5 KH (0.005%)
> > Dec 12 20:36:06.983 [notice] 5 BS (0.005%)
> > Dec 12 20:36:06.983 [notice] 5 GU (0.005%)
> > Dec 12 20:36:06.983 [notice] 5 AN (0.005%)
> > Dec 12 20:36:06.983 [notice] 5 JM (0.005%)
> > Dec 12 20:36:06.983 [notice] 5 AZ (0.005%)
> > Dec 12 20:36:06.983 [notice] 4 LI (0.004%)
> > Dec 12 20:36:06.983 [notice] 4 FJ (0.004%)
> > Dec 12 20:36:06.983 [notice] 4 AX (0.004%)
> > Dec 12 20:36:06.983 [notice] 3 NG (0.003%)
> > Dec 12 20:36:06.983 [notice] 3 AF (0.003%)
> > Dec 12 20:36:06.983 [notice] 3 KY (0.003%)
> > Dec 12 20:36:06.983 [notice] 3 MC (0.003%)
> > Dec 12 20:36:06.983 [notice] 3 MN (0.003%)
> > Dec 12 20:36:06.983 [notice] 3 SM (0.003%)
> > Dec 12 20:36:06.983 [notice] 3 NC (0.003%)
> > Dec 12 20:36:06.984 [notice] 2 KG (0.002%)
> > Dec 12 20:36:06.984 [notice] 2 ME (0.002%)
> > Dec 12 20:36:06.984 [notice] 2 NP (0.002%)
> > Dec 12 20:36:06.984 [notice] 2 AW (0.002%)
> > Dec 12 20:36:06.984 [notice] 2 VC (0.002%)
> > Dec 12 20:36:06.984 [notice] 2 GY (0.002%)
> > Dec 12 20:36:06.984 [notice] 2 AD (0.002%)
> > Dec 12 20:36:06.984 [notice] 2 AM (0.002%)
```

```
> > Dec 12 20:36:06.984 [notice] 2 AG (0.002%)
> > Dec 12 20:36:06.984 [notice] 2 EG (0.002%)
> > Dec 12 20:36:06.984 [notice] 2 VI (0.002%)
> > Dec 12 20:36:06.984 [notice] 1 LC (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 GL (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 CK (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 DM (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 MZ (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 LY (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 PG (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 GI (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 ST (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 DZ (0.001%)
> > Dec 12 20:36:06.984 [notice] 1 KE (0.001%)
> > Dec 12 20:36:06.985 [notice] 1 GN (0.001%)
> > Dec 12 20:36:06.985 [notice] 1 BZ (0.001%)
> > Dec 12 20:36:06.985 [notice] 1 ZM (0.001%)
> > Dec 12 20:36:06.985 [notice] 1 FO (0.001%)
> > Dec 12 20:36:06.985 [notice] 1 MA (0.001%)
> > Dec 12 20:36:06.985 [notice] 1 FK (0.001%)
> > Dec 12 20:36:06.985 [notice] 1 TL (0.001%)
>
----- End forwarded message -----
```

Here are the 13 Apr stats also, with some discussion that goes
along with them.

--Roger

----- Forwarded message from Roger Dingledine <[(b) (6)] -----

Date: Sun, 13 Apr 2008 02:26:45 -0400
From: Roger Dingledine <[(b) (6)]
To: Chris Walker <[(b) (6)]   Kelly DeYoe <[(b) (6)]
    Ken Berman <[(b) (6)]   [(b) (6)]
Subject: Re: December GeoIP stats

Four months later produces some very interesting stats. The percentage
of German Tor users has gone up relative to the other users. But the
total number of users in each country has gone up. Compared to the 97125
Tor clients that we glimpsed in mid December, we're now glimpsing a bit
over 150000.

Does that mean the number of running Tor clients has gone up by 50%
in the past four months? Remember that my measurements are still pretty
rough, but it seems that there's a serious increase across the board,
and a huge increase in Germany.

Note that we changed our geoip code since December, so this new count is
leaving out about 1200 IP addresses that our geoip db doesn't recognize.
Manually checking a few of them makes me think these are still mostly
African countries. (These were lumped into country-code "UN" in previous
batches.)

I'm going to try to think up some smarter tests, to see if we can figure
out if this is a fluke or if we really did grow that much. :)

--Roger

Apr 13 02:00:00.643 [notice] Clients seen:
de=42875(28.030%)
us=24099(15.755%)
cn=18617(12.171%)
it=6022(3.937%)
fr=4904(3.206%)
gb=4778(3.124%)
ca=3449(2.255%)
pl=3378(2.208%)
jp=3033(1.983%)
ru=2709(1.771%)
es=2594(1.696%)
at=2286(1.494%)
tr=2270(1.484%)
br=1918(1.254%)
se=1748(1.143%)
tw=1726(1.128%)
au=1720(1.124%)

```
nl=1503(0.983%)
ch=1460(0.954%)
mx=1078(0.705%)
ir=885(0.579%)
in=874(0.571%)
ro=859(0.562%)
ar=834(0.545%)
cz=811(0.530%)
fi=789(0.516%)
be=782(0.511%)
no=763(0.499%)
ua=742(0.485%)
hk=699(0.457%)
vn=618(0.404%)
gr=587(0.384%)
dk=580(0.379%)
cl=576(0.377%)
sg=573(0.375%)
hu=572(0.374%)
il=570(0.373%)
pt=562(0.367%)
my=467(0.305%)
th=457(0.299%)
id=390(0.255%)
sk=360(0.235%)
ie=333(0.218%)
co=324(0.212%)
lt=320(0.209%)
ph=320(0.209%)
bg=284(0.186%)
nz=282(0.184%)
ve=265(0.173%)
sa=260(0.170%)
hr=231(0.151%)
qa=222(0.145%)
si=207(0.135%)
pe=180(0.118%)
cs=177(0.116%)
kr=177(0.116%)
lv=166(0.109%)
kw=163(0.107%)
ee=136(0.089%)
pk=132(0.086%)
ge=118(0.077%)
by=112(0.073%)
md=93(0.061%)
pr=88(0.058%)
lu=87(0.057%)
gt=85(0.056%)
kz=85(0.056%)
sv=79(0.052%)
cr=73(0.048%)
do=72(0.047%)
rs=71(0.046%)
jo=70(0.046%)
mk=67(0.044%)
ae=63(0.041%)
uy=58(0.038%)
sy=57(0.037%)
om=56(0.037%)
```

```
pa=49(0.032%)
ps=49(0.032%)
ec=48(0.031%)
cy=44(0.029%)
ba=43(0.028%)
jm=41(0.027%)
uz=40(0.026%)
bo=36(0.024%)
is=36(0.024%)
mt=32(0.021%)
az=31(0.020%)
bh=30(0.020%)
lb=30(0.020%)
py=28(0.018%)
bd=25(0.016%)
hn=21(0.014%)
lk=20(0.013%)
ni=19(0.012%)
mo=18(0.012%)
mv=15(0.010%)
al=14(0.009%)
me=14(0.009%)
tt=14(0.009%)
am=13(0.008%)
iq=11(0.007%)
bs=10(0.007%)
mn=10(0.007%)
ye=10(0.007%)
cu=9(0.006%)
li=9(0.006%)
bb=8(0.005%)
bm=7(0.005%)
ky=7(0.005%)
aw=6(0.004%)
bn=6(0.004%)
fj=6(0.004%)
gu=6(0.004%)
af=5(0.003%)
an=5(0.003%)
bz=5(0.003%)
gl=5(0.003%)
pf=5(0.003%)
ag=4(0.003%)
ax=4(0.003%)
dz=4(0.003%)
fo=4(0.003%)
kh=4(0.003%)
mc=4(0.003%)
mq=4(0.003%)
cd=3(0.002%)
dm=3(0.002%)
ng=3(0.002%)
np=3(0.002%)
re=3(0.002%)
sm=3(0.002%)
tj=3(0.002%)
ad=2(0.001%)
eg=2(0.001%)
ht=2(0.001%)
la=2(0.001%)
```

ne=2(0.001%)
sr=2(0.001%)
tm=2(0.001%)
zm=2(0.001%)
zw=2(0.001%)
bj=1(0.001%)
cg=1(0.001%)
ck=1(0.001%)
cv=1(0.001%)
fk=1(0.001%)
gh=1(0.001%)
gi=1(0.001%)
gq=1(0.001%)
gy=1(0.001%)
ke=1(0.001%)
kg=1(0.001%)
lc=1(0.001%)
mh=1(0.001%)
mm=1(0.001%)
mp=1(0.001%)
mz=1(0.001%)
nc=1(0.001%)
sb=1(0.001%)
tc=1(0.001%)
tv=1(0.001%)
tz=1(0.001%)
vc=1(0.001%)
vg=1(0.001%)
vi=1(0.001%)
za=1(0.001%)

On Wed, Dec 12, 2007 at 08:41:40PM -0500, Roger Dingledine wrote:
> Dec 12 20:36:06.977 [notice] 97125 Total
> Dec 12 20:36:06.977 [notice] 21672 DE (22.314%)
> Dec 12 20:36:06.977 [notice] 17028 US (17.532%)
> Dec 12 20:36:06.977 [notice] 16679 CN (17.173%)
> Dec 12 20:36:06.977 [notice] 3666 FR (3.775%)
> Dec 12 20:36:06.977 [notice] 3528 IT (3.632%)
> Dec 12 20:36:06.978 [notice] 2746 GB (2.827%)
> Dec 12 20:36:06.978 [notice] 2561 CA (2.637%)
> Dec 12 20:36:06.978 [notice] 2139 JP (2.202%)
> Dec 12 20:36:06.978 [notice] 2082 PL (2.144%)
> Dec 12 20:36:06.978 [notice] 1911 TW (1.968%)
> Dec 12 20:36:06.978 [notice] 1482 ES (1.526%)
> Dec 12 20:36:06.978 [notice] 1328 BR (1.367%)
> Dec 12 20:36:06.978 [notice] 1303 RU (1.342%)
> Dec 12 20:36:06.978 [notice] 1120 AU (1.153%)
> Dec 12 20:36:06.978 [notice] 1090 AT (1.122%)
> Dec 12 20:36:06.978 [notice] 959 UN (0.987%)
> Dec 12 20:36:06.978 [notice] 952 SE (0.980%)
> Dec 12 20:36:06.978 [notice] 899 NL (0.926%)
> Dec 12 20:36:06.978 [notice] 778 CH (0.801%)
> Dec 12 20:36:06.978 [notice] 685 TR (0.705%)
> Dec 12 20:36:06.978 [notice] 598 CZ (0.616%)
> Dec 12 20:36:06.978 [notice] 543 MX (0.559%)
> Dec 12 20:36:06.978 [notice] 528 NO (0.544%)
> Dec 12 20:36:06.978 [notice] 524 IN (0.540%)
> Dec 12 20:36:06.978 [notice] 522 IR (0.537%)
> Dec 12 20:36:06.979 [notice] 509 BE (0.524%)
> Dec 12 20:36:06.979 [notice] 463 RO (0.477%)

```
> Dec 12 20:36:06.979 [notice] 451 AR (0.464%)
> Dec 12 20:36:06.979 [notice] 440 FI (0.453%)
> Dec 12 20:36:06.979 [notice] 409 DK (0.421%)
> Dec 12 20:36:06.979 [notice] 404 TH (0.416%)
> Dec 12 20:36:06.979 [notice] 383 PT (0.394%)
> Dec 12 20:36:06.979 [notice] 358 IL (0.369%)
> Dec 12 20:36:06.979 [notice] 351 SG (0.361%)
> Dec 12 20:36:06.979 [notice] 336 GR (0.346%)
> Dec 12 20:36:06.980 [notice] 326 UA (0.336%)
> Dec 12 20:36:06.980 [notice] 316 MY (0.325%)
> Dec 12 20:36:06.980 [notice] 315 HK (0.324%)
> Dec 12 20:36:06.980 [notice] 311 VN (0.320%)
> Dec 12 20:36:06.980 [notice] 282 LT (0.290%)
> Dec 12 20:36:06.980 [notice] 280 SK (0.288%)
> Dec 12 20:36:06.980 [notice] 276 HU (0.284%)
> Dec 12 20:36:06.980 [notice] 225 CL (0.232%)
> Dec 12 20:36:06.980 [notice] 201 PH (0.207%)
> Dec 12 20:36:06.980 [notice] 199 NZ (0.205%)
> Dec 12 20:36:06.980 [notice] 191 IE (0.197%)
> Dec 12 20:36:06.980 [notice] 165 CO (0.170%)
> Dec 12 20:36:06.980 [notice] 163 ID (0.168%)
> Dec 12 20:36:06.980 [notice] 143 BG (0.147%)
> Dec 12 20:36:06.980 [notice] 142 KR (0.146%)
> Dec 12 20:36:06.980 [notice] 138 SA (0.142%)
> Dec 12 20:36:06.980 [notice] 129 HR (0.133%)
> Dec 12 20:36:06.980 [notice] 129 VE (0.133%)
> Dec 12 20:36:06.980 [notice] 104 PE (0.107%)
> Dec 12 20:36:06.980 [notice] 99 SI (0.102%)
> Dec 12 20:36:06.980 [notice] 92 CS (0.095%)
> Dec 12 20:36:06.980 [notice] 83 QA (0.085%)
> Dec 12 20:36:06.980 [notice] 80 LV (0.082%)
> Dec 12 20:36:06.981 [notice] 72 BY (0.074%)
> Dec 12 20:36:06.981 [notice] 72 KW (0.074%)
> Dec 12 20:36:06.981 [notice] 71 EE (0.073%)
> Dec 12 20:36:06.981 [notice] 62 PK (0.064%)
> Dec 12 20:36:06.981 [notice] 50 SY (0.051%)
> Dec 12 20:36:06.981 [notice] 48 PR (0.049%)
> Dec 12 20:36:06.981 [notice] 46 LU (0.047%)
> Dec 12 20:36:06.981 [notice] 40 JO (0.041%)
> Dec 12 20:36:06.981 [notice] 40 GT (0.041%)
> Dec 12 20:36:06.981 [notice] 39 OM (0.040%)
> Dec 12 20:36:06.981 [notice] 39 DO (0.040%)
> Dec 12 20:36:06.981 [notice] 37 CR (0.038%)
> Dec 12 20:36:06.981 [notice] 35 MK (0.036%)
> Dec 12 20:36:06.981 [notice] 31 AE (0.032%)
> Dec 12 20:36:06.981 [notice] 29 KZ (0.030%)
> Dec 12 20:36:06.981 [notice] 29 SV (0.030%)
> Dec 12 20:36:06.981 [notice] 29 UY (0.030%)
> Dec 12 20:36:06.981 [notice] 28 EC (0.029%)
> Dec 12 20:36:06.981 [notice] 28 RS (0.029%)
> Dec 12 20:36:06.981 [notice] 28 BA (0.029%)
> Dec 12 20:36:06.981 [notice] 28 PA (0.029%)
> Dec 12 20:36:06.981 [notice] 24 BO (0.025%)
> Dec 12 20:36:06.982 [notice] 21 BH (0.022%)
> Dec 12 20:36:06.982 [notice] 20 CY (0.021%)
> Dec 12 20:36:06.982 [notice] 19 LK (0.020%)
> Dec 12 20:36:06.982 [notice] 17 PY (0.018%)
> Dec 12 20:36:06.982 [notice] 17 MD (0.018%)
> Dec 12 20:36:06.982 [notice] 16 UZ (0.016%)
> Dec 12 20:36:06.982 [notice] 16 MT (0.016%)
```

```
> Dec 12 20:36:06.982 [notice] 15 PS (0.015%)
> Dec 12 20:36:06.982 [notice] 14 NI (0.014%)
> Dec 12 20:36:06.982 [notice] 13 LB (0.013%)
> Dec 12 20:36:06.982 [notice] 13 YE (0.013%)
> Dec 12 20:36:06.982 [notice] 12 HN (0.012%)
> Dec 12 20:36:06.982 [notice] 12 MO (0.012%)
> Dec 12 20:36:06.982 [notice] 12 BD (0.012%)
> Dec 12 20:36:06.982 [notice] 11 IQ (0.011%)
> Dec 12 20:36:06.982 [notice] 9 BB (0.009%)
> Dec 12 20:36:06.982 [notice] 9 BN (0.009%)
> Dec 12 20:36:06.982 [notice] 9 GE (0.009%)
> Dec 12 20:36:06.982 [notice] 9 AL (0.009%)
> Dec 12 20:36:06.982 [notice] 8 IS (0.008%)
> Dec 12 20:36:06.983 [notice] 6 TT (0.006%)
> Dec 12 20:36:06.983 [notice] 6 CU (0.006%)
> Dec 12 20:36:06.983 [notice] 6 PF (0.006%)
> Dec 12 20:36:06.983 [notice] 6 MV (0.006%)
> Dec 12 20:36:06.983 [notice] 5 BM (0.005%)
> Dec 12 20:36:06.983 [notice] 5 KH (0.005%)
> Dec 12 20:36:06.983 [notice] 5 BS (0.005%)
> Dec 12 20:36:06.983 [notice] 5 GU (0.005%)
> Dec 12 20:36:06.983 [notice] 5 AN (0.005%)
> Dec 12 20:36:06.983 [notice] 5 JM (0.005%)
> Dec 12 20:36:06.983 [notice] 5 AZ (0.005%)
> Dec 12 20:36:06.983 [notice] 4 LI (0.004%)
> Dec 12 20:36:06.983 [notice] 4 FJ (0.004%)
> Dec 12 20:36:06.983 [notice] 4 AX (0.004%)
> Dec 12 20:36:06.983 [notice] 3 NG (0.003%)
> Dec 12 20:36:06.983 [notice] 3 AF (0.003%)
> Dec 12 20:36:06.983 [notice] 3 KY (0.003%)
> Dec 12 20:36:06.983 [notice] 3 MC (0.003%)
> Dec 12 20:36:06.983 [notice] 3 MN (0.003%)
> Dec 12 20:36:06.983 [notice] 3 SM (0.003%)
> Dec 12 20:36:06.983 [notice] 3 NC (0.003%)
> Dec 12 20:36:06.984 [notice] 2 KG (0.002%)
> Dec 12 20:36:06.984 [notice] 2 ME (0.002%)
> Dec 12 20:36:06.984 [notice] 2 NP (0.002%)
> Dec 12 20:36:06.984 [notice] 2 AW (0.002%)
> Dec 12 20:36:06.984 [notice] 2 VC (0.002%)
> Dec 12 20:36:06.984 [notice] 2 GY (0.002%)
> Dec 12 20:36:06.984 [notice] 2 AD (0.002%)
> Dec 12 20:36:06.984 [notice] 2 AM (0.002%)
> Dec 12 20:36:06.984 [notice] 2 AG (0.002%)
> Dec 12 20:36:06.984 [notice] 2 EG (0.002%)
> Dec 12 20:36:06.984 [notice] 2 VI (0.002%)
> Dec 12 20:36:06.984 [notice] 1 LC (0.001%)
> Dec 12 20:36:06.984 [notice] 1 GL (0.001%)
> Dec 12 20:36:06.984 [notice] 1 CK (0.001%)
> Dec 12 20:36:06.984 [notice] 1 DM (0.001%)
> Dec 12 20:36:06.984 [notice] 1 MZ (0.001%)
> Dec 12 20:36:06.984 [notice] 1 LY (0.001%)
> Dec 12 20:36:06.984 [notice] 1 PG (0.001%)
> Dec 12 20:36:06.984 [notice] 1 GI (0.001%)
> Dec 12 20:36:06.984 [notice] 1 ST (0.001%)
> Dec 12 20:36:06.984 [notice] 1 DZ (0.001%)
> Dec 12 20:36:06.984 [notice] 1 KE (0.001%)
> Dec 12 20:36:06.985 [notice] 1 GN (0.001%)
> Dec 12 20:36:06.985 [notice] 1 BZ (0.001%)
> Dec 12 20:36:06.985 [notice] 1 ZM (0.001%)
> Dec 12 20:36:06.985 [notice] 1 FO (0.001%)
```

> Dec 12 20:36:06.985 [notice] 1 MA (0.001%)
> Dec 12 20:36:06.985 [notice] 1 FK (0.001%)
> Dec 12 20:36:06.985 [notice] 1 TL (0.001%)

----- End forwarded message -----

I consider this my proof. :) Make of it what you will.

Oh, another result that will come out of the Oxford conference that I
forgot to mention -- there's a fellow named Hal Roberts who was funded
to compile a "state of the circumvention technologies" report, and he
hopes to publish it in the next little while. (He's going to send us
an early draft of our chapter so we can point out any problems, so the
actual publishing won't be until at least after that.)

--Roger

----- Forwarded message from Ethan Zuckerman ◁   (b) (6)   ▷ -----

From: Ethan Zuckerman ◁   (b) (6)
To: Roger Dingledine ◁   (b) (6)
Subject: Re: Hivos a secular humanist organization?
Delivery-Date: Mon, 04 Jun 2007 16:23:30 -0400

Nope, that's exactly right. The government gives charitable money to several
different religions, including the secular humanists, and HIVOS is their
charitable arm.

'

-E

On 6/4/07, Roger Dingledine ◁   (b) (6)   ▷ wrote:
>
>Hi Ethan,
>
>I have a vague memory in the back of my head that somebody in Oxford
>told me that Hivos is actually funded by the .nl govt as a religious
>organization -- and the religion they represent is secular humanism.
>
>Am I on crack? Do you remember this too? :)
>
>Thanks,
>--Roger
>
>

--
Ethan Zuckerman | (b) (6)
Research Fellow, Berkman Center for Internet and Society
   (b) (6) | http://www.ethanzuckerman.com/blog
http://globalvoicesonline.org | http://worldchanging.com

----- End forwarded message -----

Hi folks,

Can you recommend anybody who A) could make it to a hearing on Tuesday in DC, B) could actually be useful at said hearing, and C) has first-hand clue about what Cisco is really up to in China?

My net isn't so good here so make sure to include Colin in your response.

--Roger

----- Forwarded message from colin maclay < ███████████ (b) (6) ██████ -----

From: colin maclay < ████████ (b) (6) ██████
To: Roger Dingledine < ██████ (b) (6) ███
Subject: Re: random cisco question...
Delivery-Date: Fri, 16 May 2008 11:44:26 -0400

business clue - what is cisco up to in china wrt great firewall...

they are trying to figure out what to do w/them in legislative terms. it's a hard question, but imp to know how naughty they are being - how proactively they are enabling censorship and surveillance. they are familiar w/the allegations, but it's hard to find anyone that can really confirm.

hearing is on tues.

best,

c

On May 16, 2008, at 10:25 AM, Roger Dingledine wrote:

>On Tue, May 13, 2008 at 02:58:23PM -0400, colin maclay wrote:
>>do you know anyone who would talk to congress about cisco and
>>censorship/surveillance, and know anything more than the hearsay we
>>are all familiar with?
>
>What did you have in mind in particular? You want technical clue
>about how
>cisco boxes work? Business clue about what Cisco the corporation is
>up to?
>Technical clue about how various govt firewalls work?
>
>Once I have a few more details, I will fwd your mail to a few people I
>know who are likely to know the right people.
>
>--Roger

----- End forwarded message -----