

Freedom of Speech

Tor
&
Ανωνυμία στο Internet

Freedom of Speech

Ποιός ;
&
Γιατί ;

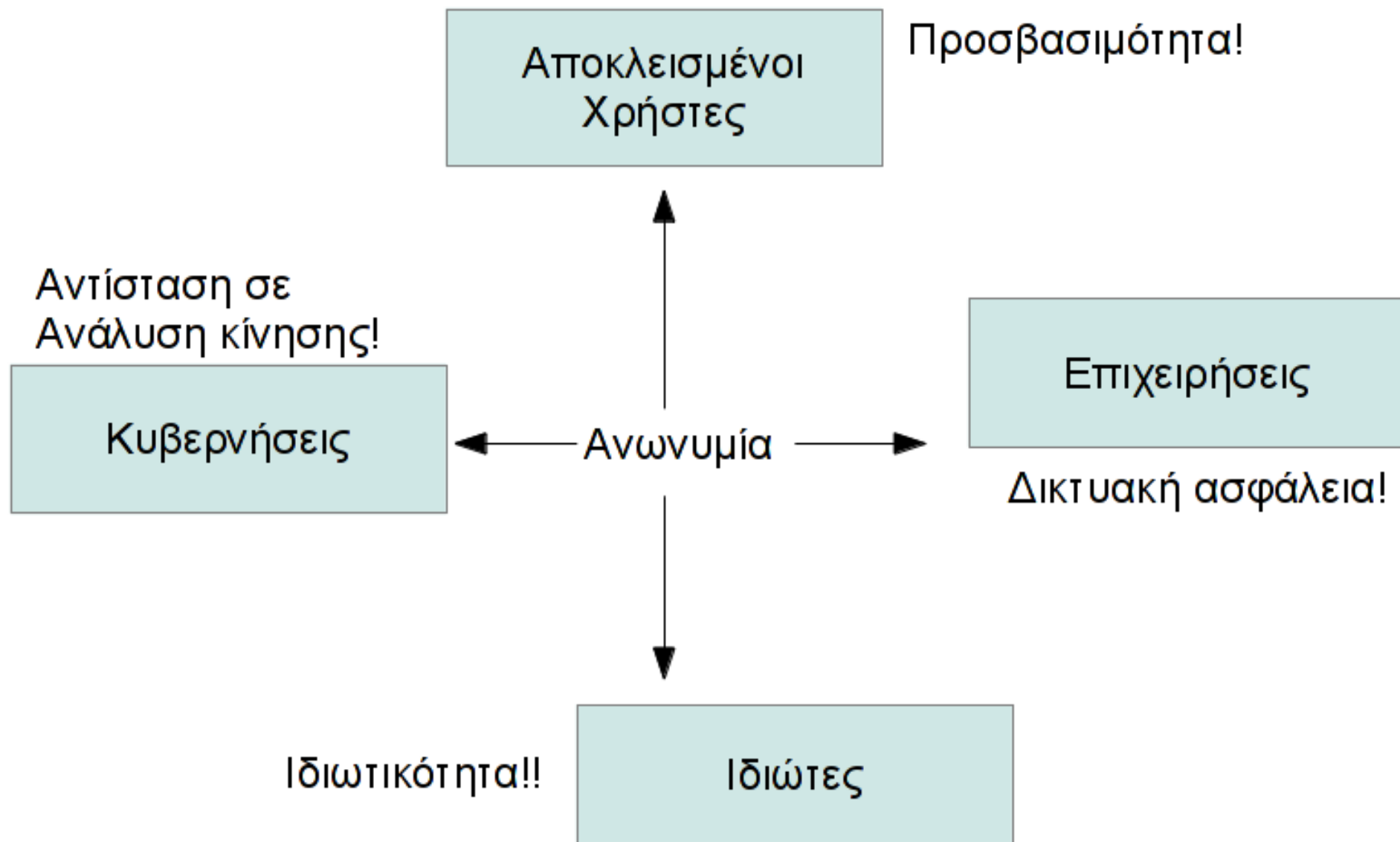
Εισαγωγή
Λογοκρισία
Το δίκτυο Tor
Χρήση
Demo
Πώς να βοηθήσετε

Ασφαλείς vs Ανώνυμες επικοινωνίες

ΔΕΝ είναι το ίδιο!

Υπάρχει **ανάγκη** για χρήση και των δύο
ταυτόχρονα!

Ανωνυμία ? Γιατί ?



Εισαγωγή

- Tor: σύστημα που επιτρέπει την ανώνυμη επικοινωνία στο Internet χρησιμοποιώντας onion routing
- Πρώτη ανακοίνωση: 20/09/2002 – “Tor: The Second-Generation Onion router” - 13ο Usenix
 - Roger Dingledine, Nick Mathewson and Paul Syverson
- Αρχικοί Χορηγοί: 2002-2003: US Naval Research Laboratory, 2004+: EFF
- 2006: ΜΚΟ με έδρα Αμερική
- Τωρινοί χορηγοί:
 - Οργανισμοί: Broadcasting Board of Governors, Swedish International Development Cooperation Agency, Naval Research, EFF, Google, Human Rights Watch, DARPA ,
 - Χρήστες

Χορηγοί

- US Dept. Defense + EFF; Πώς γίνεται ;
 - Το δίκτυο δεν ξεχωρίζει τους χρήστες! Όλοι ίσοι!
 - Ο καθένας χρησιμοποιεί το δίκτυο για δικούς του σκοπούς!
 - Ποικιλία χρηστών: Πολύ σημαντική σε ένα anonymity network
- Γιατί ;
 - **Η ελευθερία δεν πρέπει να θεωρείται δεδομένη**
 - Οργανισμοί που ενδιαφέρονται για ανθρώπινα δικαιώματα σε όλο το κόσμο βοηθούν το Tor ώστε να κρατούν επαφή με κόσμο σε καταπιεσμένες χώρες.

- Ανοιχτή προτυποποίηση
- Ακαδημαϊκή έρευνα (Μαθηματικά μοντέλα, ασφάλεια, ανωνυμία, επιθέσεις, κτλ)
- Open Source, πολλαπλές υλοποιήσεις (C, Java, κτλ) Tor clients
 - Διασημότερο: Tor - torproject.org
 - Κώδικας: <https://gitweb.torproject.org/tor.git>
- Πολύ μεγάλη συμμετοχή της κοινότητας
- 20 developers επί πληρωμή + εθελοντές
- 2011: FSF Award: Project of Social Benefit

Χρήστες

- | | |
|------------------------------------|---------------------------------|
| • Χρήστες για λόγους ιδιωτικότητας | • Αστυνομία/Νόμος |
| • Στρατιωτικοί | • Ακτιβιστές/
whistleblowers |
| • Δημοσιογράφοι | • Ερευνητές |
| • Ακαδημαϊκοί | • Επιχειρήσεις |

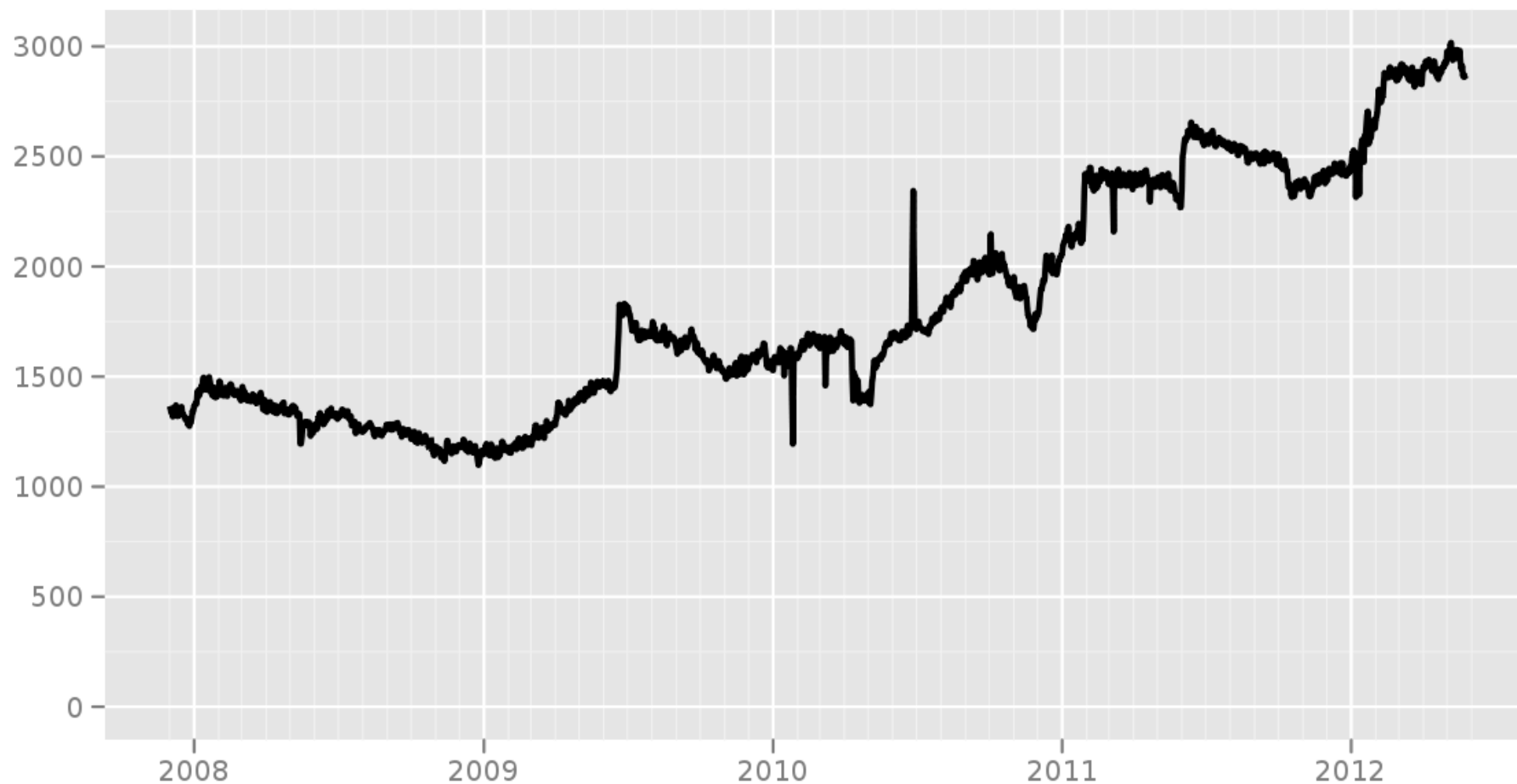
Όποιος άλλος το έχει ανάγκη
για πολιτικούς, θρησκευτικούς, κτλ λόγους ☺

🍇 Μεγέθη:

- 🍇 ~3000 ενεργοί “relay” κόμβοι
- 🍇 ~400.000 ενεργοί χρήστες
- 🍇 ~12Gbps

Χρήστες

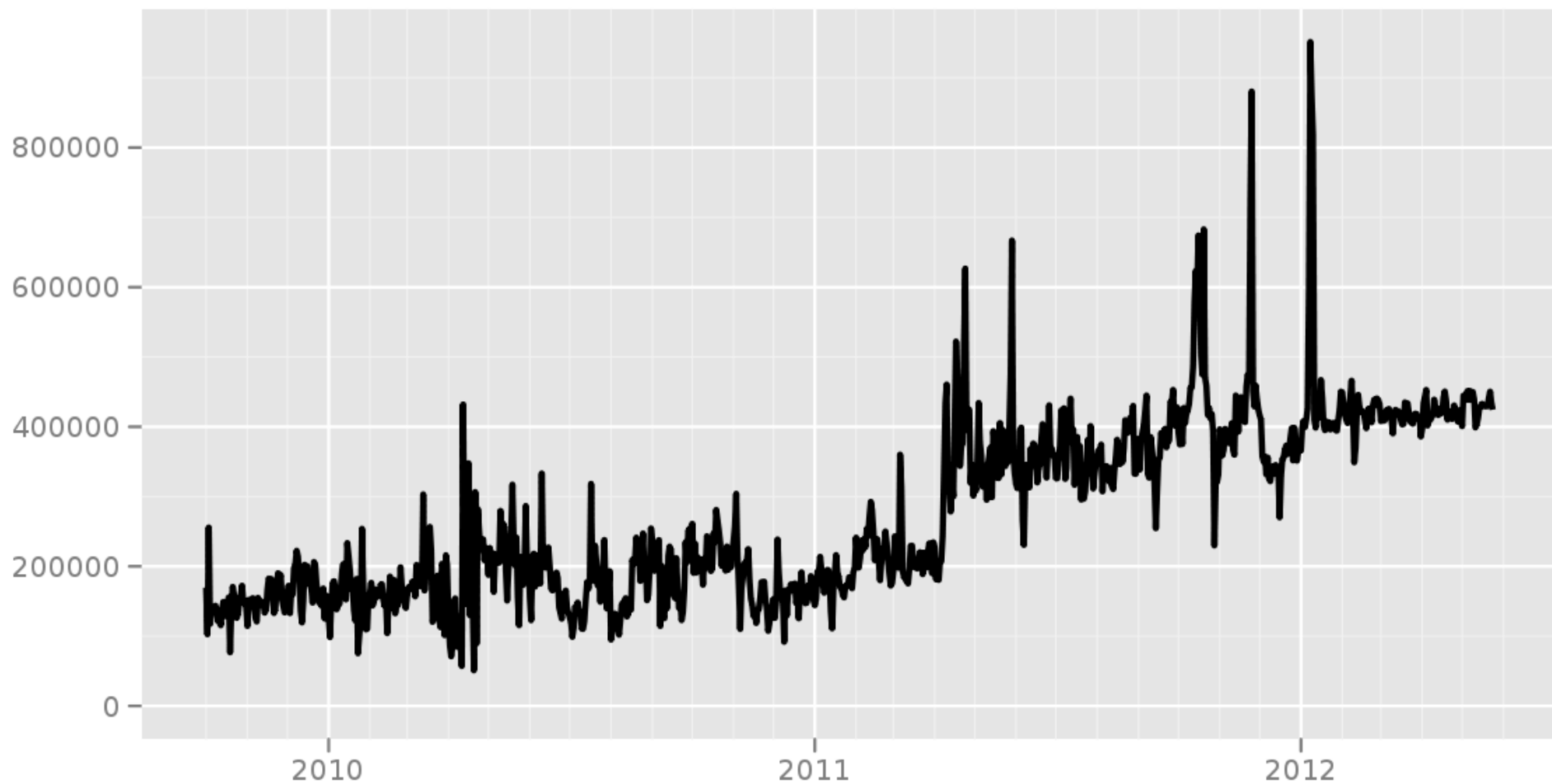
Number of relays in all countries



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

Χρήστες

Directly connecting users from all countries



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

Λογοκρισία

- Λογοκρισία: **Έλεγχος του λόγου και άλλων μορφών ανθρώπινης έκφρασης**
 - Κράτη περιορίζουν την πρόσβαση σε δικτυακούς κόμβους για πολιτικούς, θρησκευτικούς, οικονομικούς, κ.α λόγους
 - Πολύ πιο συχνή από όσο νομίζουμε (εμείς της “πολιτισμένης Δύσης”)
 - Επίπεδο λογοκρισίας χωρών:
 - **Μεγάλο:** Bahrain, Belarus, Burma, Cuba, Iran, North Korea, Saudi Arabia, Syria, Turkmenistan, Uzbekistan, Vietnam
 - **Μεσαίο:** Australia, Egypt, France, India, Kazakhstan, Malaysia, Russia, South Korea, Sri Lanka, Thailand, Tunisia, Turkey, United Arab Emirates
- Πηγή:** http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf
- Περιορισμός στην ταχύτητα == Λογοκρισία!

Λογοκρισία

خطر!

تصفح بأمان!

عذرا، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.

تشكل شبكة الإنترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية، وقد تم حجب الموقع الذي ترغب بدخوله لاحتوائه محتوى مدرج تحت "فئات المحتويات المخطورة" حسب تصنيف "السياسة التنظيمية لإدارة الملفد للأنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

إذا كانت لديك وجهة نظر مختلفة، الرجاء انقر هنا.

Surf Safely!

This website is not accessible in the UAE.

The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the 'Internet Access Management Regulatory Policy' of the Telecommunications Regulatory Authority of the United Arab Emirates.

If you believe the website you are trying to access does not contain any such content, please [click here](#).

© 2008 Lemnatech IT LLC.

يالله بالسستر...!

ببيرة المتحدة.

وخدمة متطلبات بدخوله لاحتوائه "ة" حسب تصنيف تنظيم الاتصالات

Surf Safe

This website is

The Internet is a p serving our daily le access contains co

<http://torproject.org/>

1 3G 9:28 AM

Site Blocke... x

<http://torproject.org/>

Site Blocked

Web site has been blocked for violating laws and laws of Kingdom of Bahrain.

واين في مملكة

believe the requested page should be blocked please [click here](#).

محب تفعل [بالضغط](#)

Notice...

تم حظر هذا الموقع بسبب احتوائه على محتويات تعارض مع قوانين السلطنة. عليه يرجى تعبئة الاستمارة أدناه اذا كنت تعتقد بان الموقع لا يتضمن أي من هذه المحتويات.

This site has been blocked due to content that is contrary to the laws of the Sultanate. If you believe that the website you are trying to access does not contain any such content, please fill in and submit the form below:

WebSite*

Email Address*

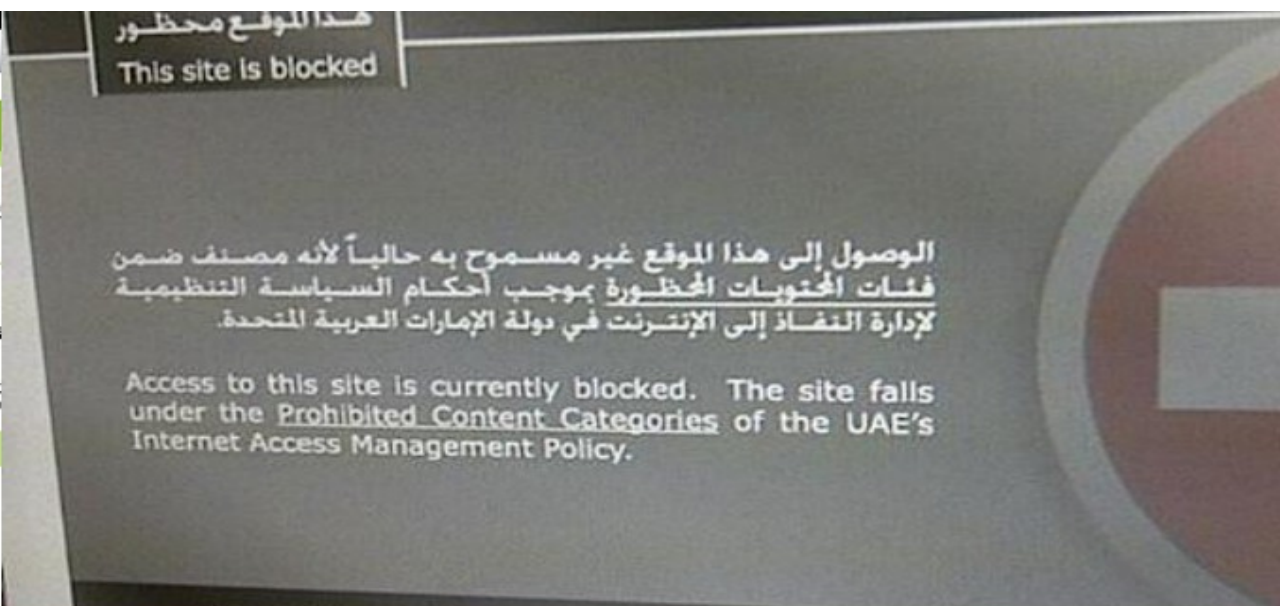
Comments*

غير متاح.

ي أن لا تُحجب

المملكة العربية www.internet.gov

Λογοκρισία



Μερικά παραδείγματα

- Κίνα...
- Ιραν + SSL != ♥ (SSL Blocking + SSL Throttling)
- Ιταλία: bookmakers, The pirate Bay
- Μ. Βρετανία: T-Mobile, Vodafone block TPB
- Ν. Κορέα: block sites σχετ. με porn + Β.Κορέα(!?)
- Σε αρκετές Αραβικές χώρες απαγορεύονται πολιτικά και porn sites.
- ΗΠΑ: T-mobile Webguard
- Ελλάδα: 4658/2012 (ellinadiko.com/music-bazaar.com)

Παρακολούθηση παγκόσμιας λογοκρισίας

• OpenNet Initiative

- Ετήσιες επιθεωρήσεις
- Χάρτες

• Δημοσιογράφοι χωρίς Σύνορα (RWB)

• Εργαλεία:

- Censorsweeper (buggy)
- Open Observatory of Network Interference (OONI)
- Glasnost
- metrics.torproject.org (Anomaly-based censorship-detection system for Tor - George Danezis)

Μπορεί να νικήθει η λογοκρισία ?

- “When politics fail; technology comes in”
- Αρκούν τα (single hop) Proxies/VPNs ?
 - Δεν είναι ασφαλή!
 - Ούτε αποτελεσματικά...
- Χρειάζεται ένα **κατανεμημένο** σύστημα ανά τον κόσμο που να μην (μπορεί να) είναι **υπό τον έλεγχο κανενός → Tor!**

Bonus!

Single Hop Proxy

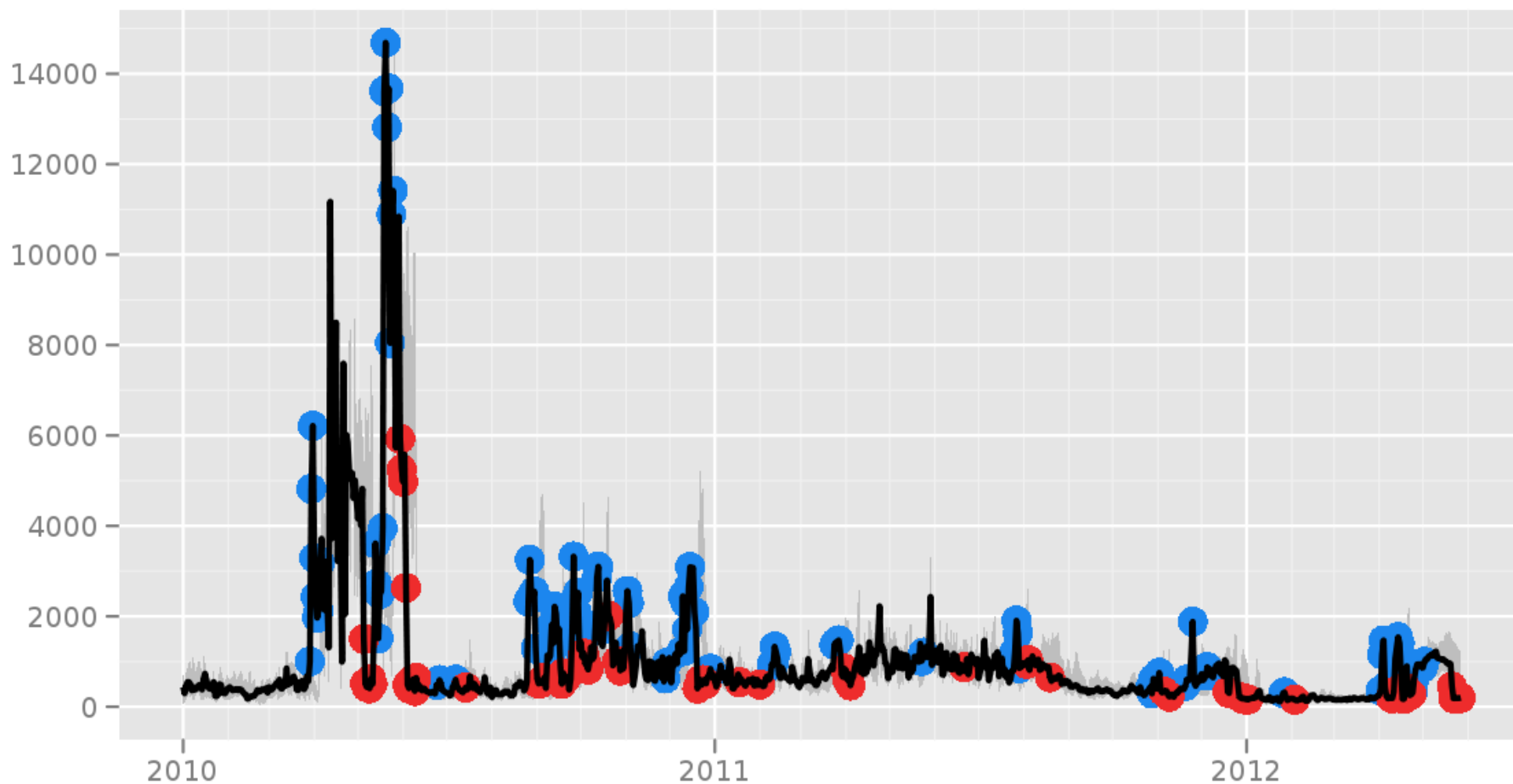
- Δεν φτάνει ένα VPN ή ένα proxy ; **OXI**
 - Single Hop Proxy == Single point of **Failure**
- Τι γίνεται αν ο διαχειριστής του VPN/proxy κόμβου αρχίσει να παρεμβαίνει στην κίνηση ;
- Τι γίνεται αν ο συγκεκριμένος κόμβος “πέσει” ή γίνει block από κάποιον ;
- Ποιοί και πόσοι διαχειριστές των proxies/VPNs έχουν πρόσβαση στα δεδομένα των χρηστών ;

Ανταγωνισμός εξοπλισμών / Arms Race

- Κράτη μπλοκάρουν το <http://torproject.org> → Δημιουργία του gettor (αποστολή email: gettor @ torproject.org)
- Δημόσιες IP των relays → Κράτη μπορούν να μπλοκάρουν τις IPs των relays (Κίνα)
- Tor Bridges: Tor relays με μη-δημόσιες IP, χρήστες μαθαίνουν IPs από το <http://bridges.torproject.org> → Κράτη μαθαίνουν τα bridges (botnets !?) και τα μπλοκάρουν και αυτά (Κίνα) → Χρήστες δημιουργούν “ιδιωτικά”/non-shared bridges και τα μοιράζονται μεταξύ τους
- Κράτη κόβουν το HTTPS/SSL (Ιράν) → obfsproxy (pluggable transports) - traffic transformation

Λογοκρισία

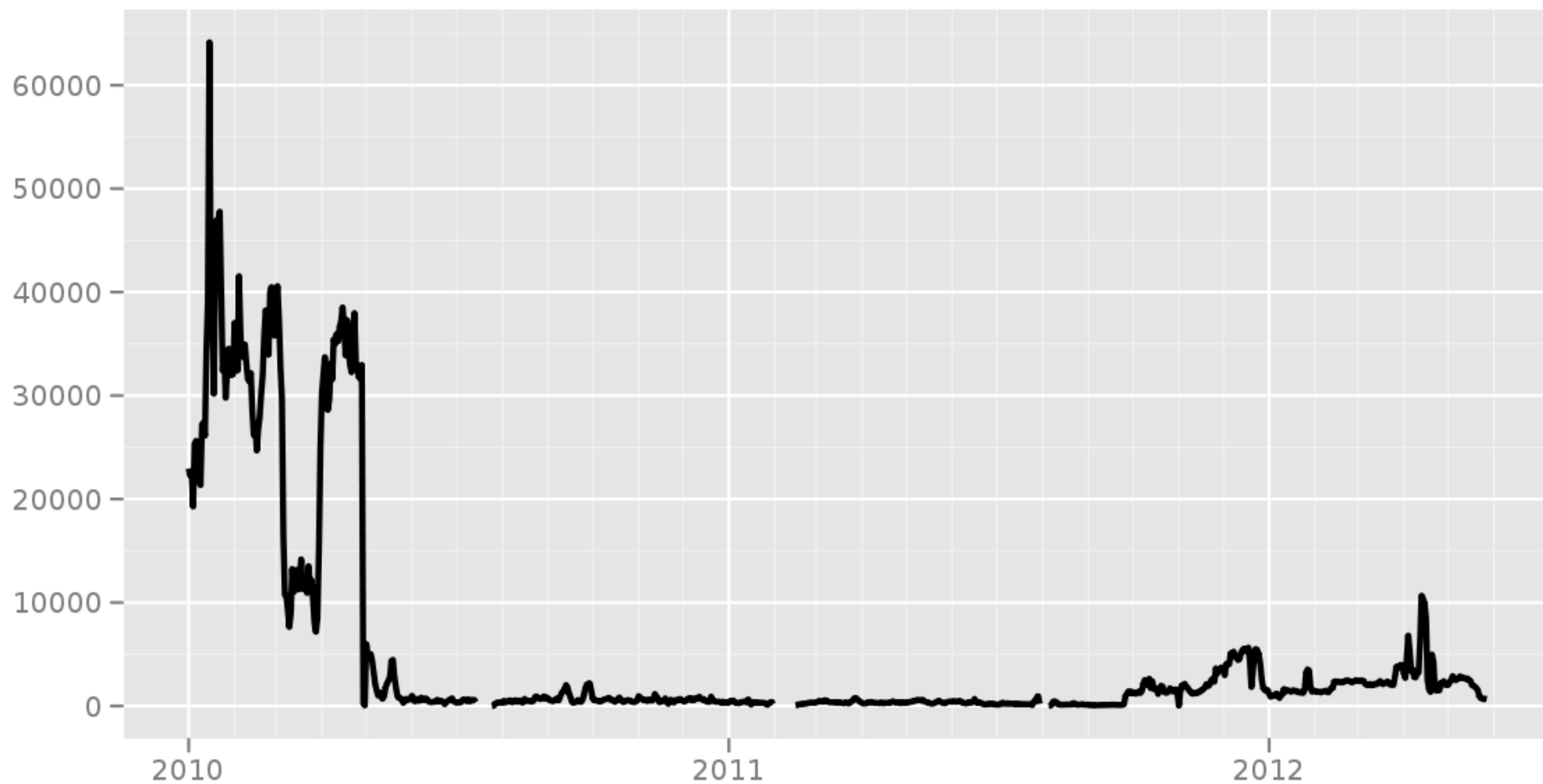
Directly connecting users from China



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

Λογοκρισία

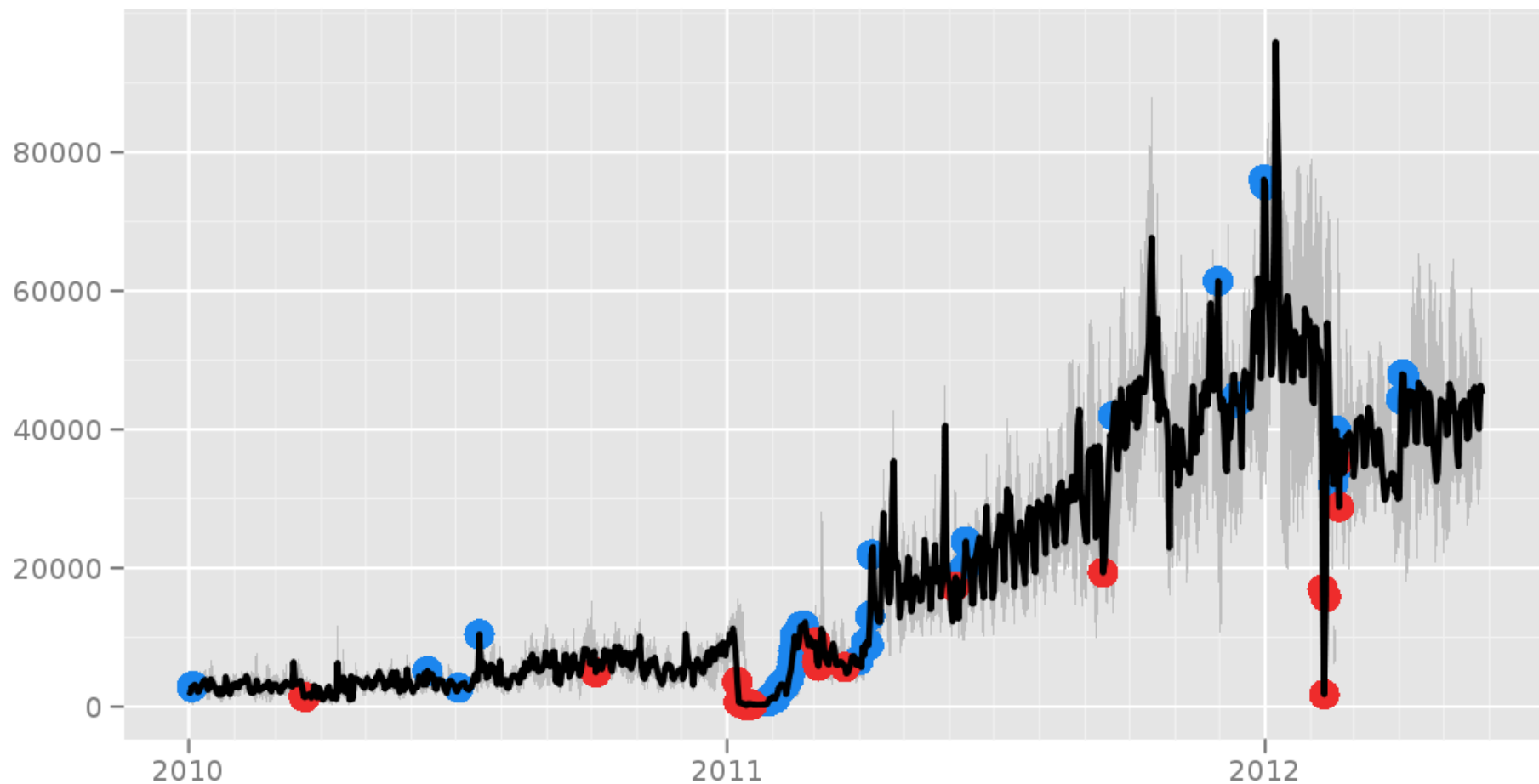
Bridge users from China



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

Λογοκρισία

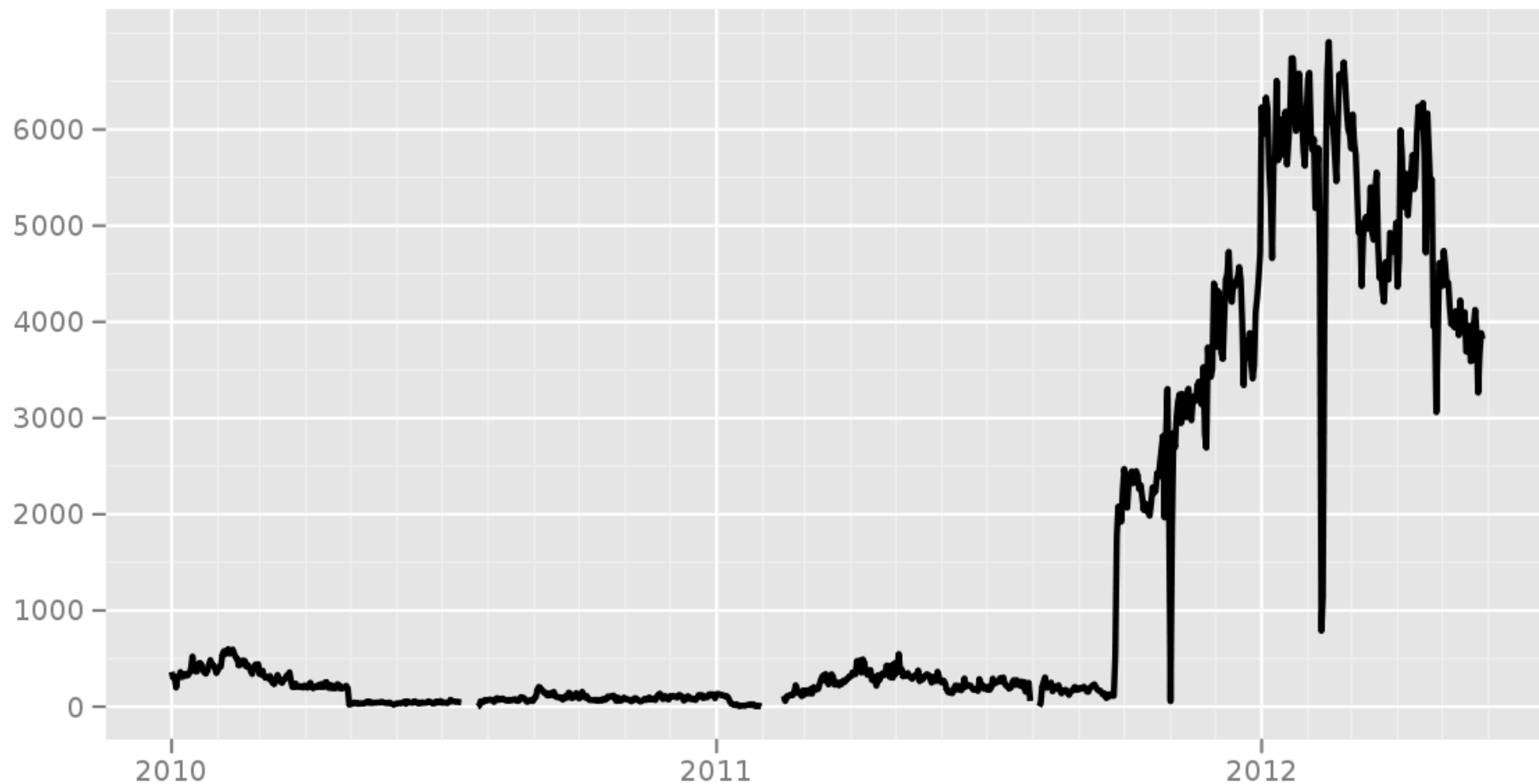
Directly connecting users from Iran



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

Λογοκρισία

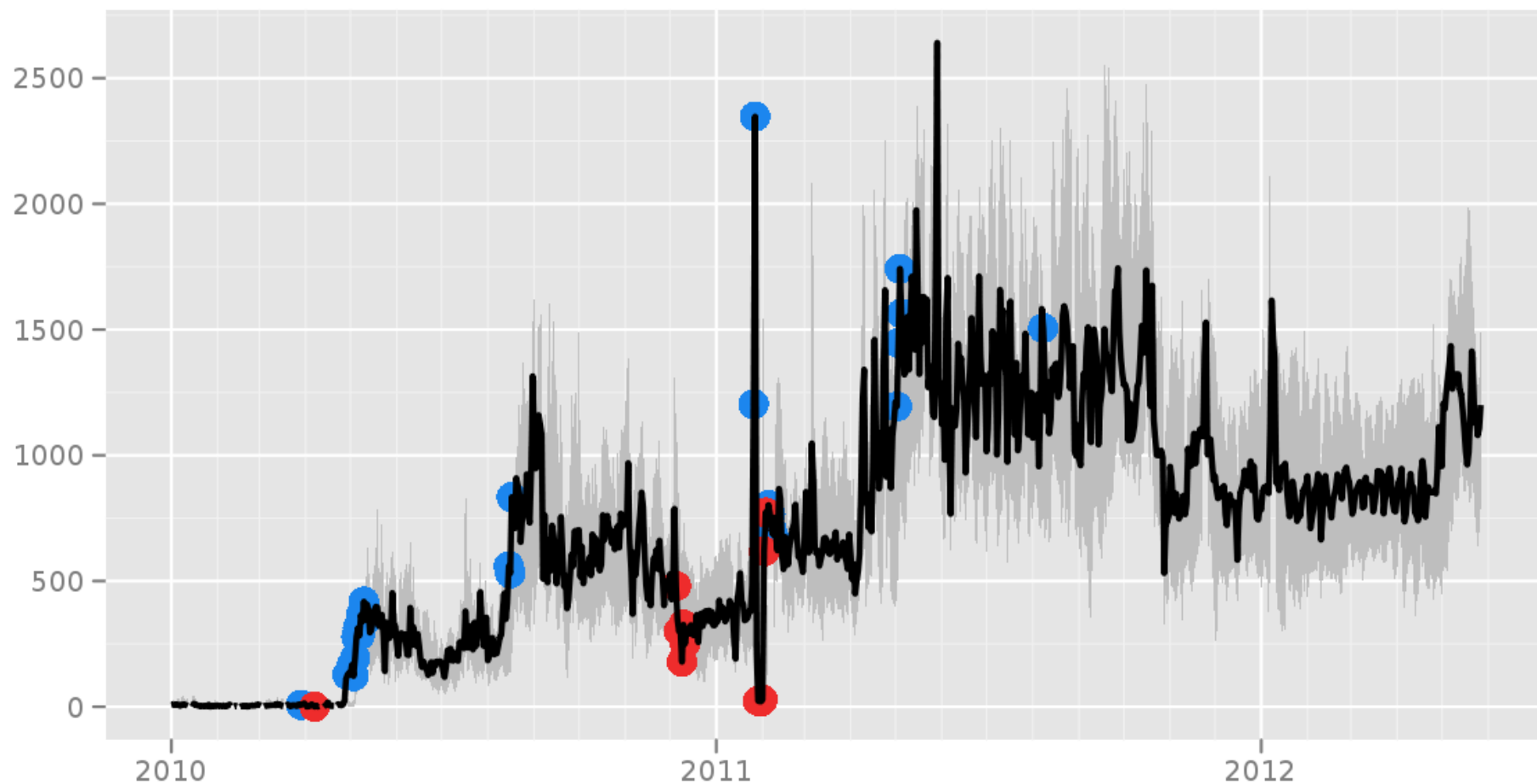
Bridge users from Iran



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

Λογοκρισία

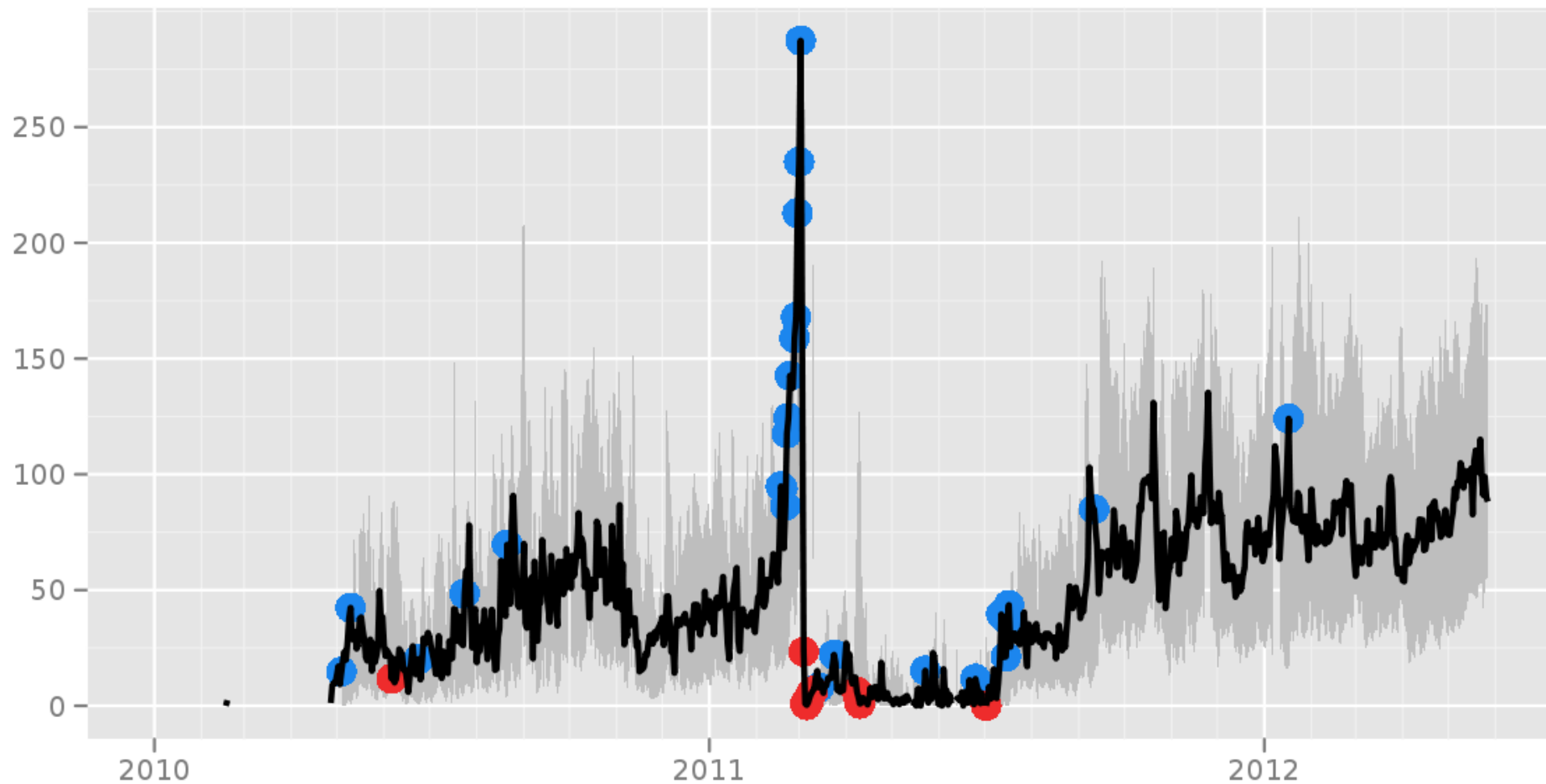
Directly connecting users from Egypt



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

Λογοκρισία

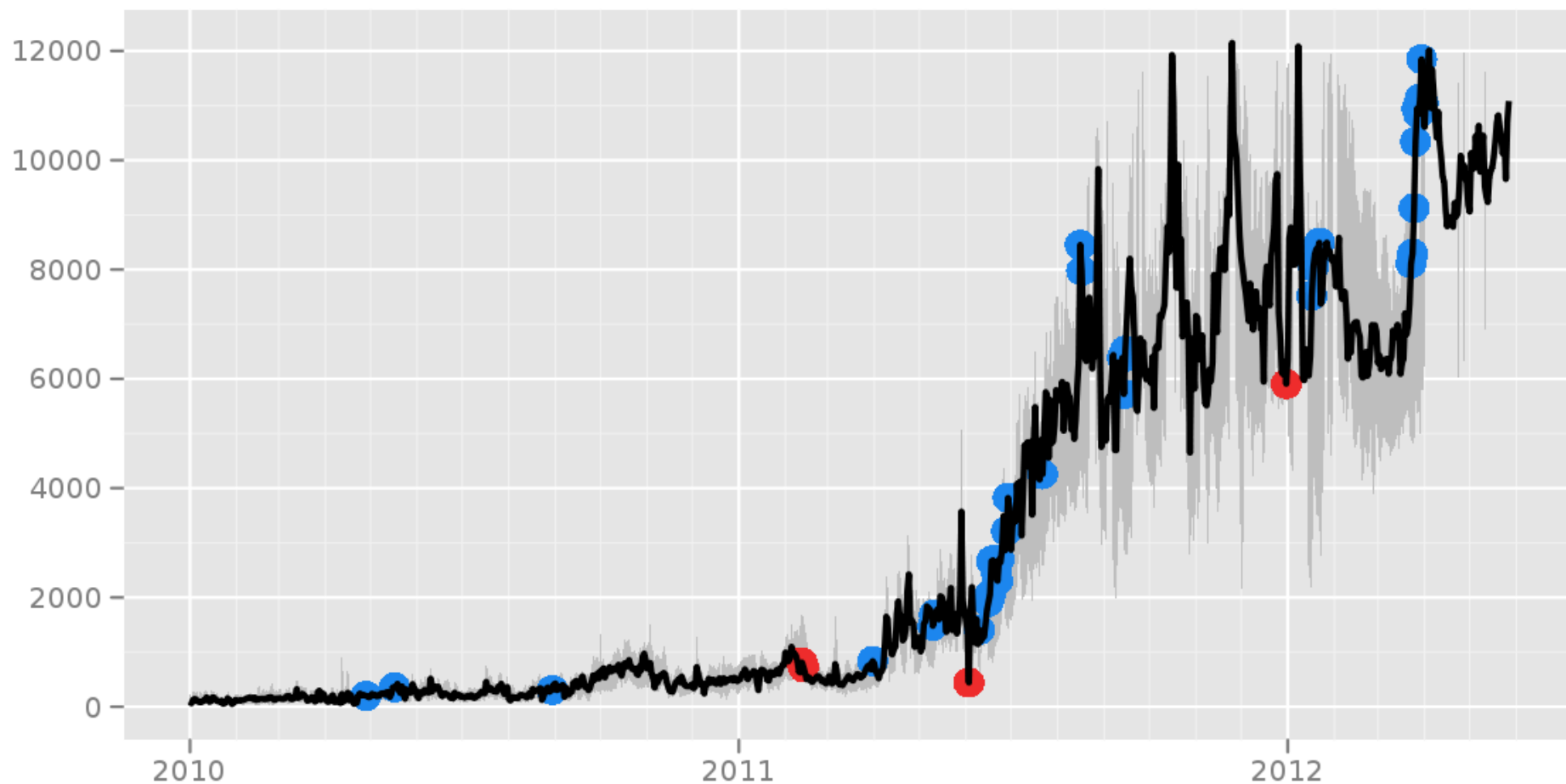
Directly connecting users from Libya



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

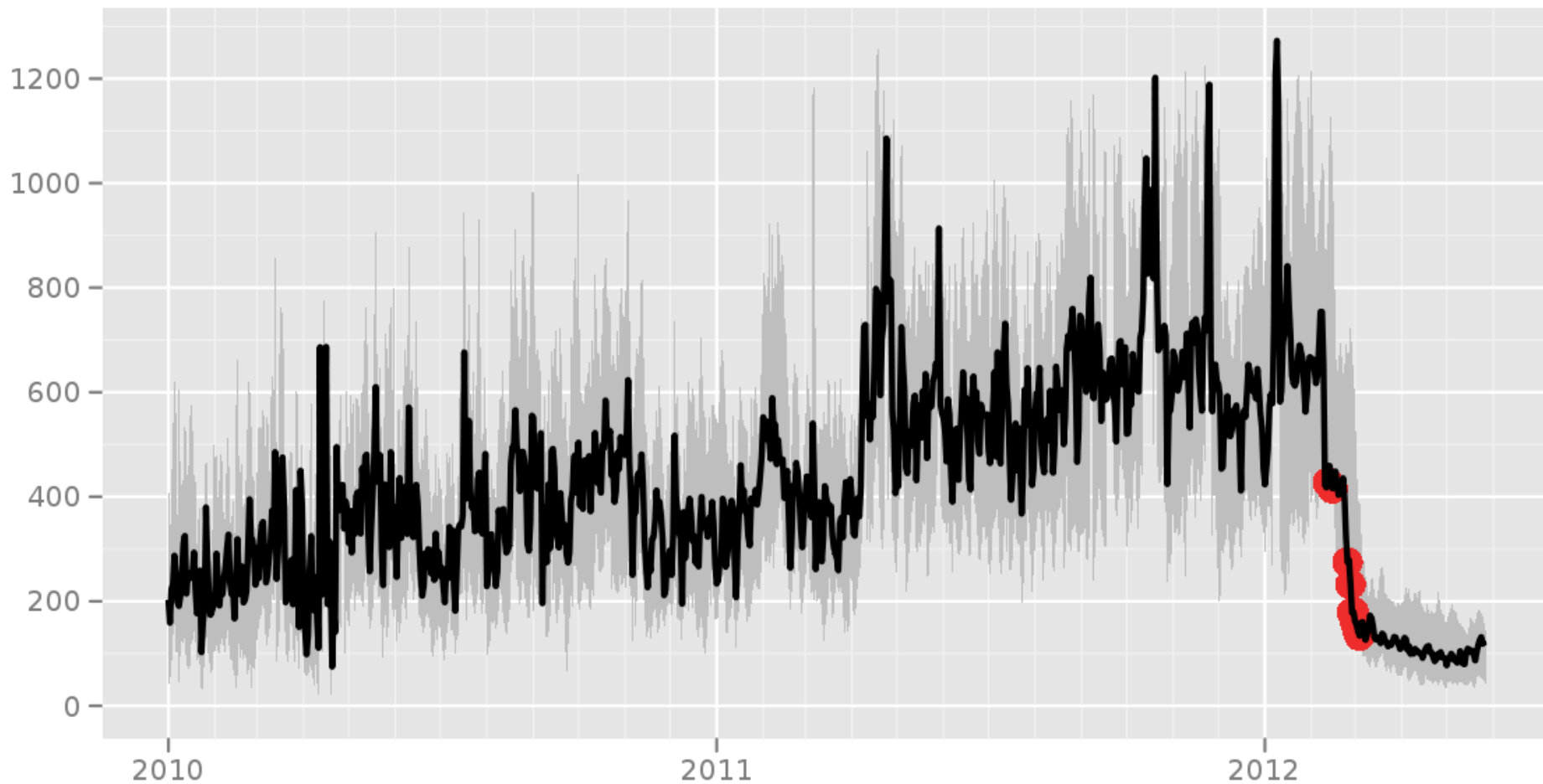
Λογοκρισία

Directly connecting users from the Syrian Arab Republic



Λογοκρισία

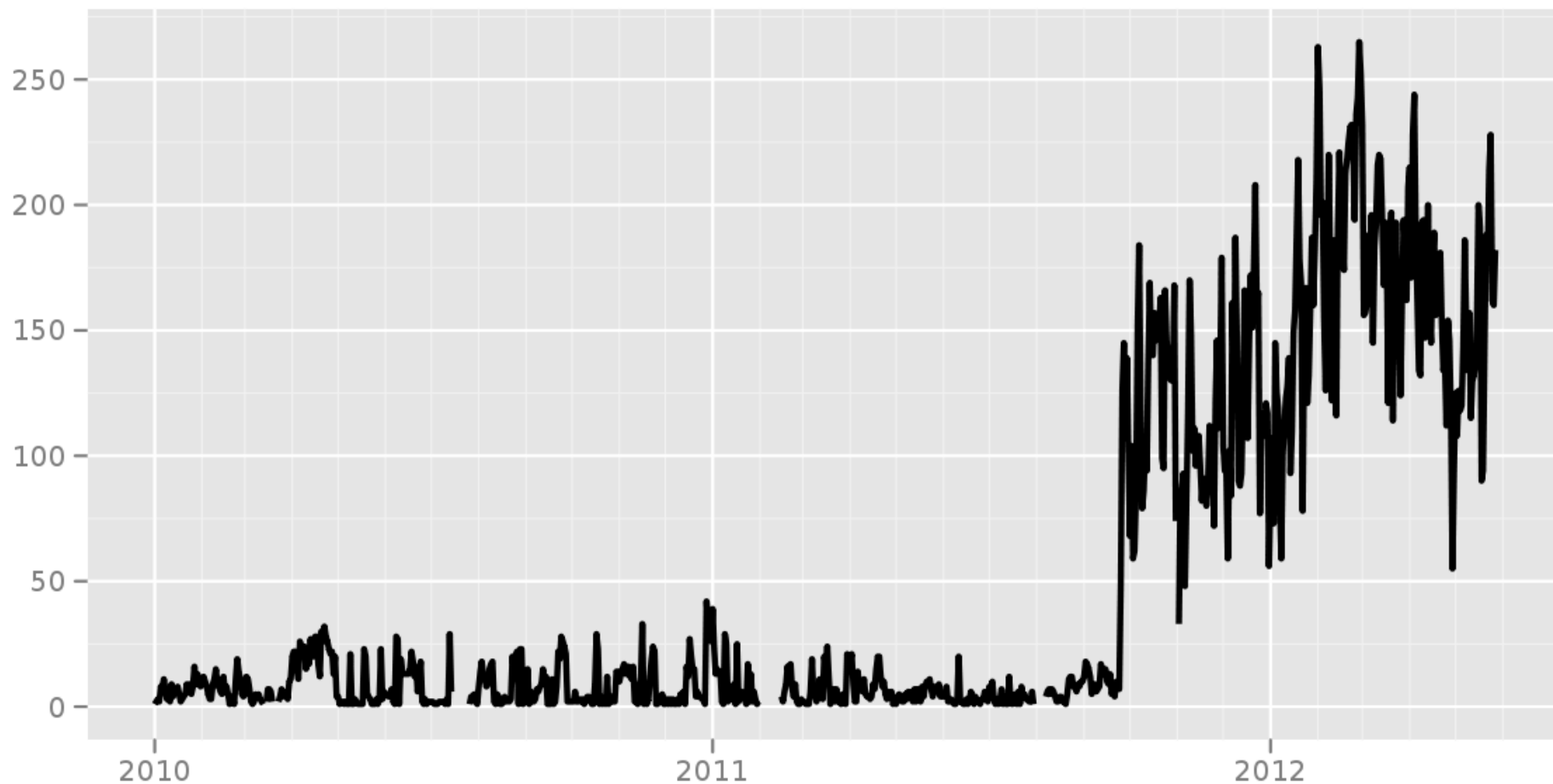
Directly connecting users from Kazakhstan



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

Λογοκρισία

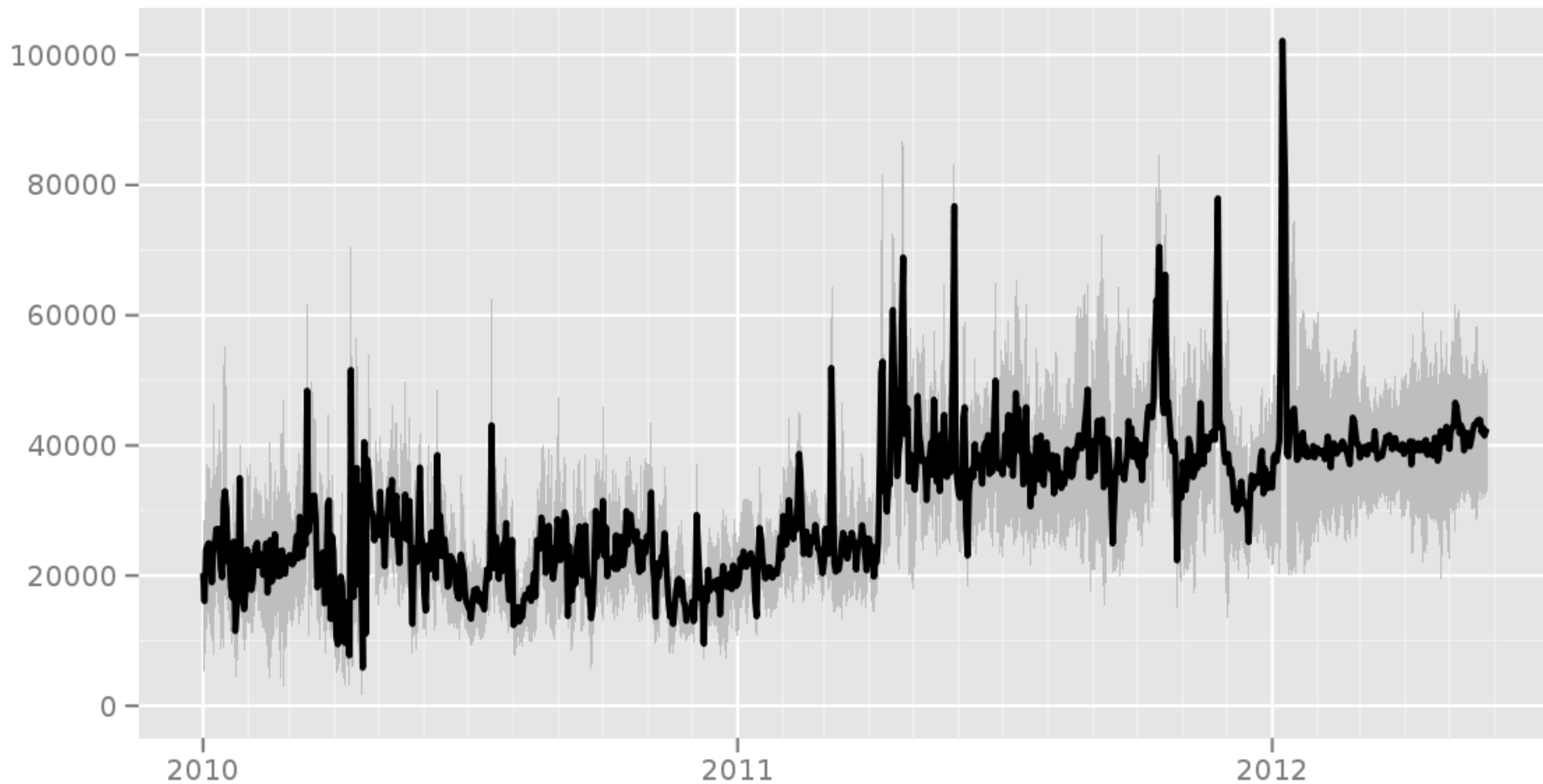
Bridge users from Kazakhstan



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

Λογοκρισία

Directly connecting users from Germany



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

Tor Network

- P2P δίκτυο επικεντρωμένο στην ανωνυμία, ιδιωτικότητα και την “ασφάλεια”
- Ανωνυμία σε **TCP** συνδέσεις.
- Tor relays:
 - 3000+ nodes σε όλο το κόσμο
 - Onion routers – Πολυεπίπεδη (multi-layered) κρυπτογράφηση
 - Perfect Forward Secrecy!
 - Οι IP διευθύνσεις τους είναι **δημόσιες!**
 - Στέλνουν τα στοιχεία τους στα “Directory authorities”

- 🍇 Tor Nodes:

- 🍇 Tor Relays

- 🍇 Guard nodes – Πρώτος κόμβος εισόδου στο δίκτυο

- 🍇 Middle nodes

- 🍇 Exit nodes – Τα μόνα που βγάζουν κίνηση προς το κανονικό Internet

- 🍇 Bridges: μη-δημόσια/κρυφά relays

- 🍇 <https://bridges.torproject.org>

- 🍇 Email: bridges @ torproject.org (yahoo, gmail)

- 🍇 Directory Authorities

- 🍇 Πελάτες/Clients

- 🍇 Δεν υπάρχουν logins, κωδικοί, χρεώσεις, κόστη

Bonus!

Guard Nodes

- Αν κάποιος ελέγχει C από τα N συνολικά nodes, τότε υπάρχει πιθανότητα $(C/N)^2$ να μπορεί να παρακολουθεί την κίνηση ενός client
- Αν γίνεται αλλαγή entry node συνέχεια η πιθανότητα ο attacker να δει (κάποια) κίνηση τείνει στο 1
- Άρα χρήση 3 σταθερών Guard Nodes κάθε φορά. Αν κάποιος πέσει, προστίθεται στην λίστα ένας νέος. Αν δεν υπάρχουν τουλάχιστον 2 δεν γίνεται σύνδεση στο δίκτυο Tor

Bonus!

Directory Authorities

- 🍇 Μαζεύουν πληροφορίες για τα relays
- 🍇 Αποφασίζουν ποιά relays του δικτύου είναι προσβάσιμα και “ασφαλή” και δημιουργούν το “consensus” (μτφ: συναίνεση)

```
r barbastrumf A37UTGfb5AMT8LMr0zGQx9BHTOg AOJoyabcdefZzrbU0Y4tjE 2012-05-11 10:42:18 1.2.3.5
443 0
s Fast Running Stable Unnamed Valid
v Tor 0.2.3.11-alpha
w Bandwidth=11230
p accept 22,53,1194,5222-5223,8333
```

🍇 Πελάτες/Clients

- 🍇 Κατεβάζουν το consensus
- 🍇 Αποφασίζουν ποια relays θα χρησιμοποιήσουν
- 🍇 Φτιάχνουν κύκλωμα (circuit) με τα επιλεγμένα relays

Onion Routing

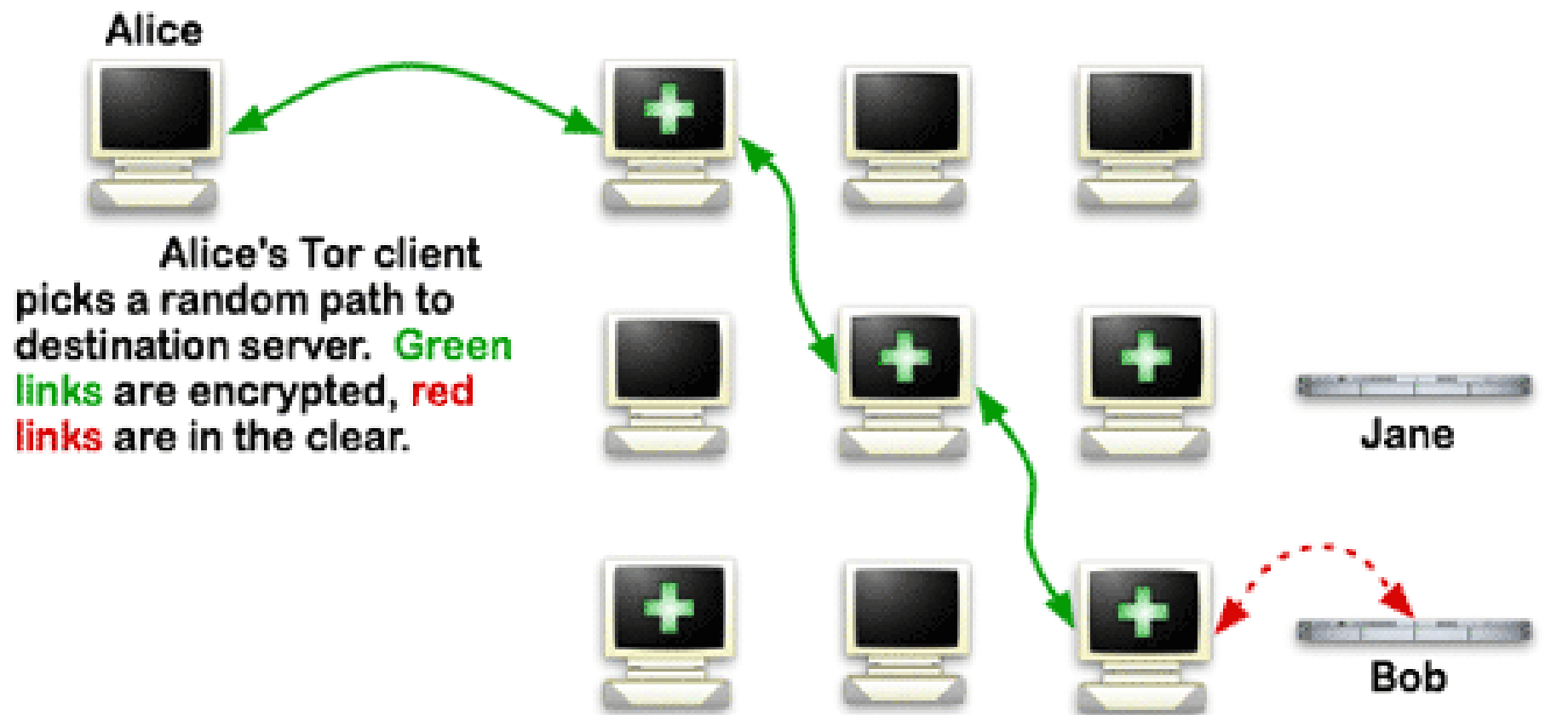
- Τεχνική δρομολόγησης για ανώνυμη επικοινωνία
- Public-key crypto → Διατήρηση ταυτότητας δρομολογητή
- Multi-layered encryption → Αποφυγή διαρροής πληροφορίας (Single layered encryption == Single point of **Failure**)

Tor

- Χρησιμοποιεί 3-hop circuits

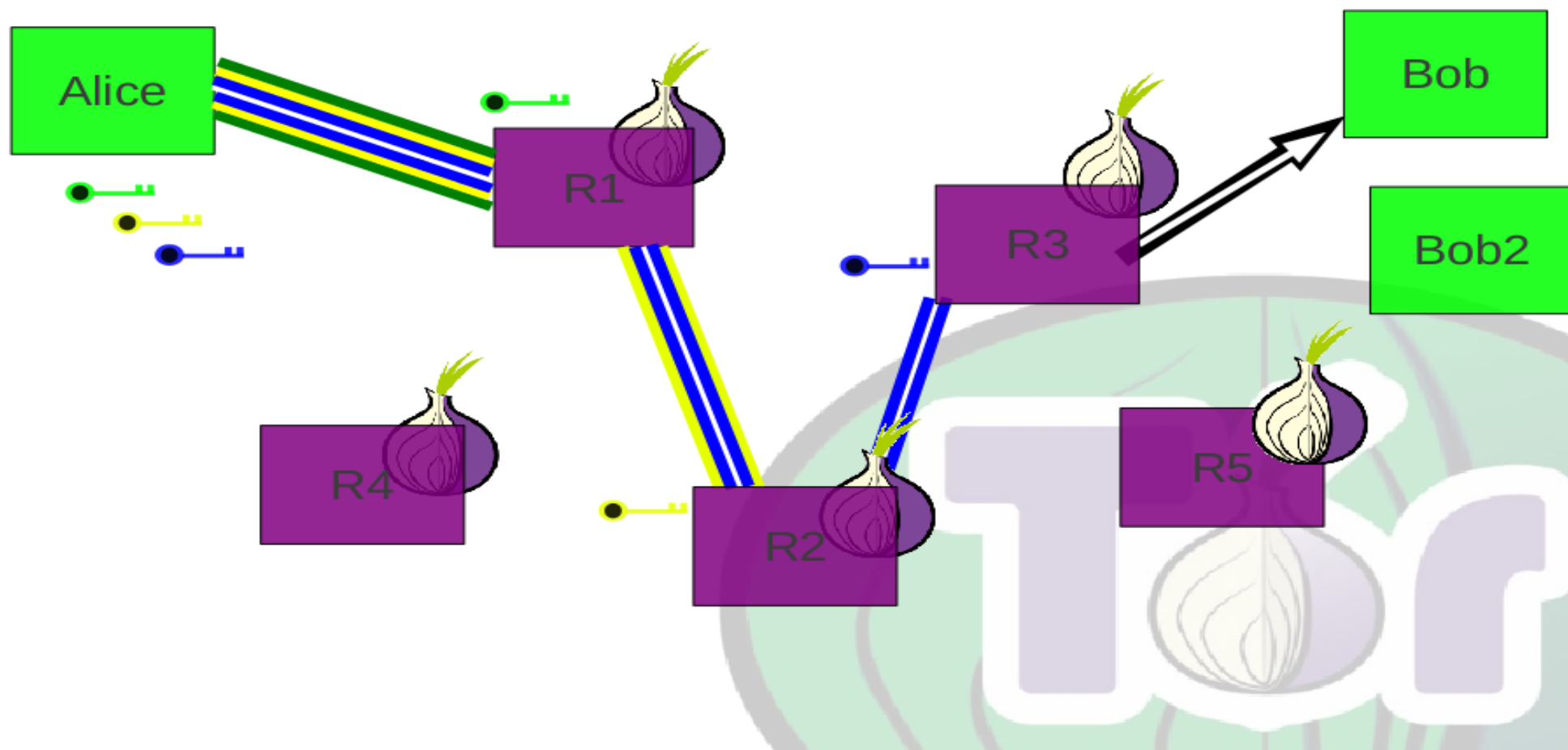
Tor Network

How Tor Works

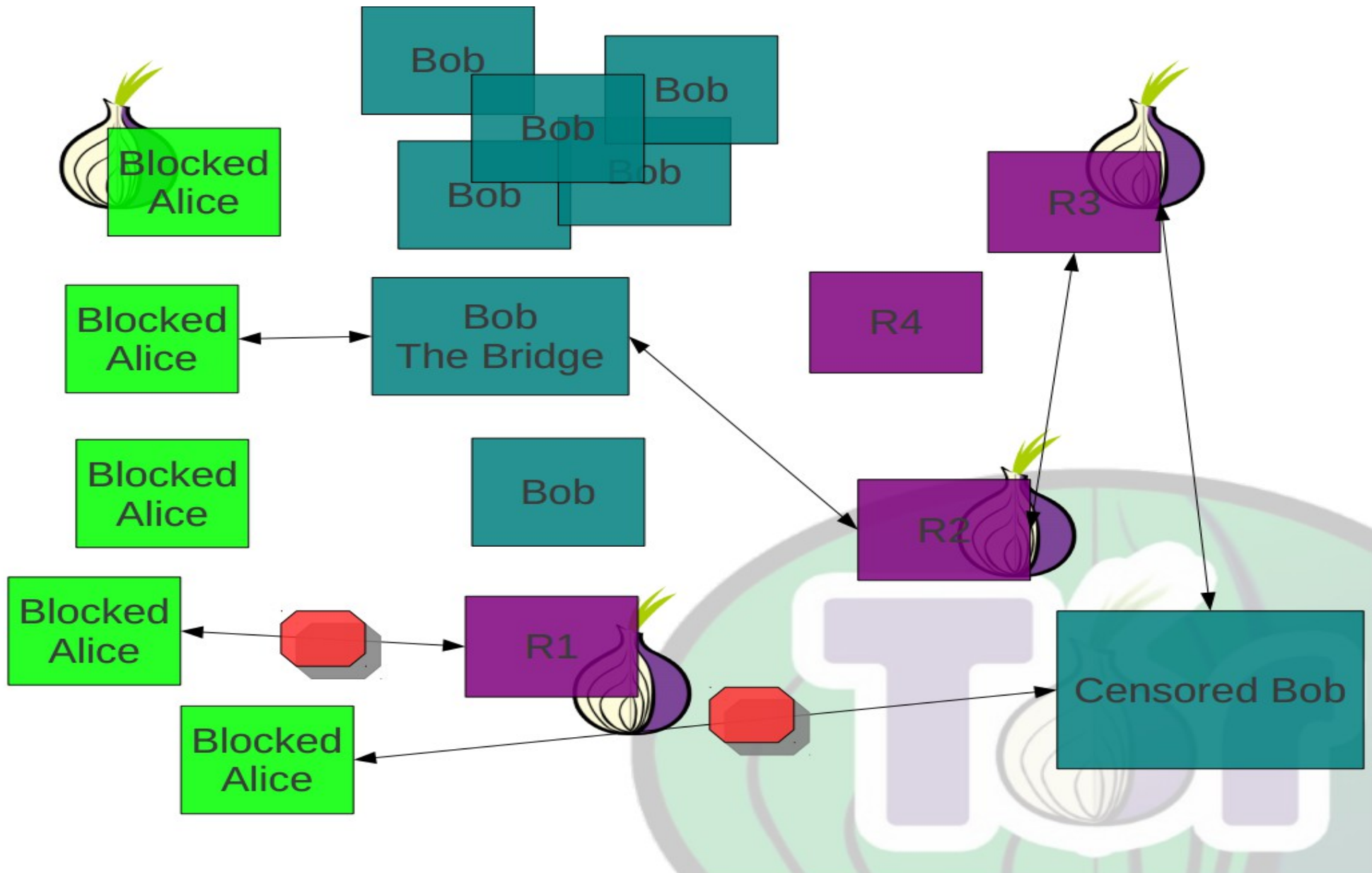


Tor Network

**Tor avoids the single hop paradigm;
This is Privacy by Design!**



Tor Network



Hidden Services

- Ανώνυμα TCP services
 - HTTP, IRC, κ.α
 - Ειδικές “.onion” διευθύνσεις: <http://idnxcnkne4qt76tg.onion/>
- Χρησιμοποιεί
 - Rendezvous points
 - Introduction points

“It's complicated”

Περισσότερα στο:

<https://www.torproject.org/docs/hidden-services.html.en>

Χρήσιμοιώντας Tor

- 🔧 **Socks Server** που περνάει την κίνηση στο δίκτυο Tor
- 🔧 **TorBrowserBundle**
 - 🔧 Vidalia: Γραφικό interface διαχείρισης Tor node
 - 🔧 Πακέτο Firefox με ειδικά patches και extensions σχετικά με ιδιωτικότητα
 - 🔧 ~~TorButton~~ (έχει καταργηθεί → διαρροή πληροφορίας!)
- 🔧 Χρήση άλλων προγραμμάτων με Tor
 - 🔧 Socks support → Κατάλληλες ρυθμίσεις socks port
 - 🔧 torify “command”
- 🔧 **Προσοχή** σε πιθανά Proxy/DNS Leaks!
 - 🔧 Unity drag-n-drop leak
 - 🔧 Websockets
 - 🔧 Pidgin filetransfer proxy bypass

Άλλα προγράμματα

- Torbutton for Thunderbird (torbutton-birdy)
 - Δοκιμές χρήσης
- Tor IM Browser Bundle
 - Temp. discontinued (Pidgin DNS leaks)

Hidden Services

- Σύνδεση χρησιμοποιώντας .onion διευθύνσεις
 - <http://idnxcnkne4qt76tg.onion/> - Torproject
 - <http://3g2upl4pq6kufc4m.onion/> - DuckDuckGo
 - <http://duskgytldkxiuqc6.onion/> - Example
 - <http://izrhvy5nxc6ody5x.onion/> - AnonPad
 - <http://leakager742hufco.onion/> - Cable Viewer (wikileaks)
- Χρήσεις:
 - Ιδιώτες: δημοσιογράφοι, δικηγόροι, ακτιβιστές, whistleblowers, bloggers
 - Οργανισμοί: wikileaks, indymedia
 - “Deep web”

Χρήσιμοιώντας Tor



The Hidden Wiki

navigation

- [Main page](#)
- [All pages](#)
- [Recent changes](#)
- [Random page](#)

search

[Go](#) [Search](#)

toolbox

- [What links here](#)
- [Related changes](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)

[category](#) [discussion](#) [edit](#) [history](#)

Category:How to Exit the Matrix

(Redirected from [How to Exit the Matrix](#))

Privacy and anonymity have been poop to the point of non-existence in recent years. Our personal, private information is [stockpiled and sold](#) to the highest bidder like so much inventory at a warehouse. [National Security Letters](#) are written to make [countless](#) requests for records from our search engines, libraries, and [book stores](#) with no court oversight. [Email](#) and especially [searchable data](#) is practically unprotected from anyone who might ask to have it. All our electronic communications are [tapped](#). Massive [governmental data mining schemes](#) are being built to record everything we publish on the web. In many workplaces, employers spy on and control their employees' Internet access, and this practice is widely considered to be acceptable.

These are dark times. [The Fourth Amendment](#) has all but disappeared, thanks to the Wars on Drugs, Porn, and Terror. Any practicing trial lawyer will tell you that you can no longer rely on unreasonable search to be the basis for excluding evidence, especially for [digital evidence](#) in the hands of a [third party](#). Likewise the First Amendment has been shredded with [exceptions](#) and [provisos](#), and is only truly available to those with the money to fight costly (and [usually frivolous](#)) court battles against large corporations. In short, you can say what you want so long as it [doesn't affect corporate profits](#).

How we got to a legal state where this all this activity is the accepted norm, I'm not quite sure. It seems to stem from an underlying assumption that our function at work and at home is that of a diligent slave - a single unit of economic output under the direct watch and total control of our superiors at all times; that we should accept this surveillance because we should have nothing to hide from our benevolent overlords who are watching us merely to protect us from evil.

I believe this view is wrong. Moreover, I believe it is time to reverse the tide. This document seeks to provide the means to protect your right to privacy, freedom of speech, and anonymous net access even under the most draconian of conditions - including, but not limited to, both private and criminal investigation (which happens far more often to innocent people than one might like to think). "So what are you saying? That I can dodge bullets?" "No.. What I am trying to tell you is that when you're ready, you won't have to."

Contents [\[hide\]](#)

- [1 Document Organization](#)
- [2 Where to find this Document](#)
- [3 License](#)
- [4 Credits](#)
- [5 Feedback and Assistance](#)

Welcome to the first day of the rest of your life.

Document Organization [\[edit\]](#)

This document is organized into seven chapters. The first chapter is an introductory philosophical discussion, and the next six are based on the six main ways you can leak information about who you are onto your network connection, or to an attentive individual.

- [1. The Matrix](#)**

A discussion of what the Matrix is, how it functions, and how to resist and subvert it. This forms the philosophical underpinnings of this HOWTO and the driving force behind the author's motivation to work ceaselessly on this document for over a year, and then proceed to give it away for free. Not required reading, but strongly recommended.
- [2. Network Attributes of your computer](#)**

This includes your network hardware (MAC) address, your IP address, and your 802.11 nickname. This section describes ways of obfuscating each of these attributes, as well as your network data itself.

Άλλοι τρόποι χρήσης

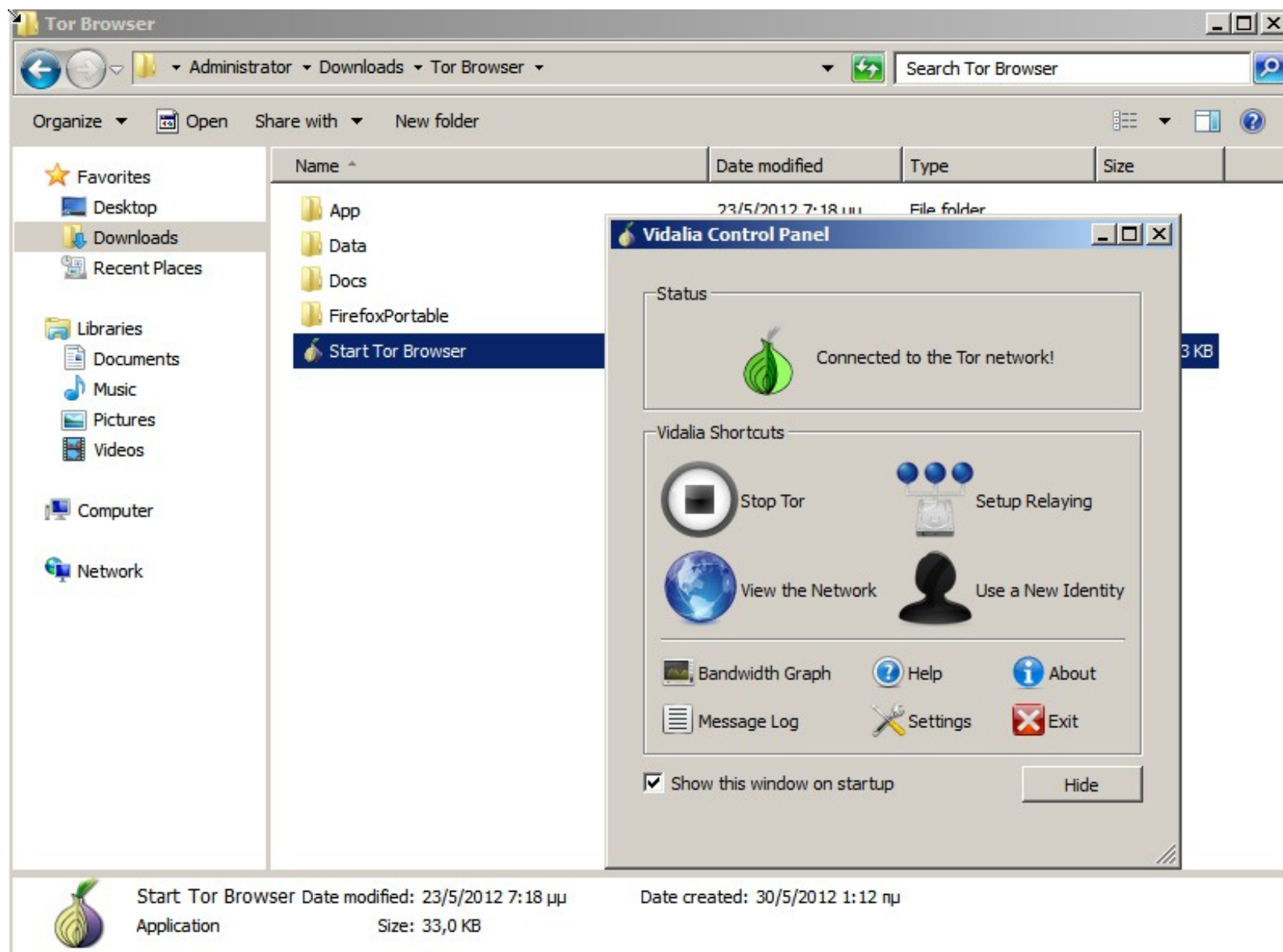
- TAILS (The Amnesic Incognito Live System)
 - LiveCD με ιδιαίτερο ενδιαφέρον σχετικά με την ιδιωτικότητα / ασφάλεια
- Εργαλεία Tor για Android
 - Orbot → Tor app
 - Orweb → Browser με Tor

Χρήσιμοιώντας Tor

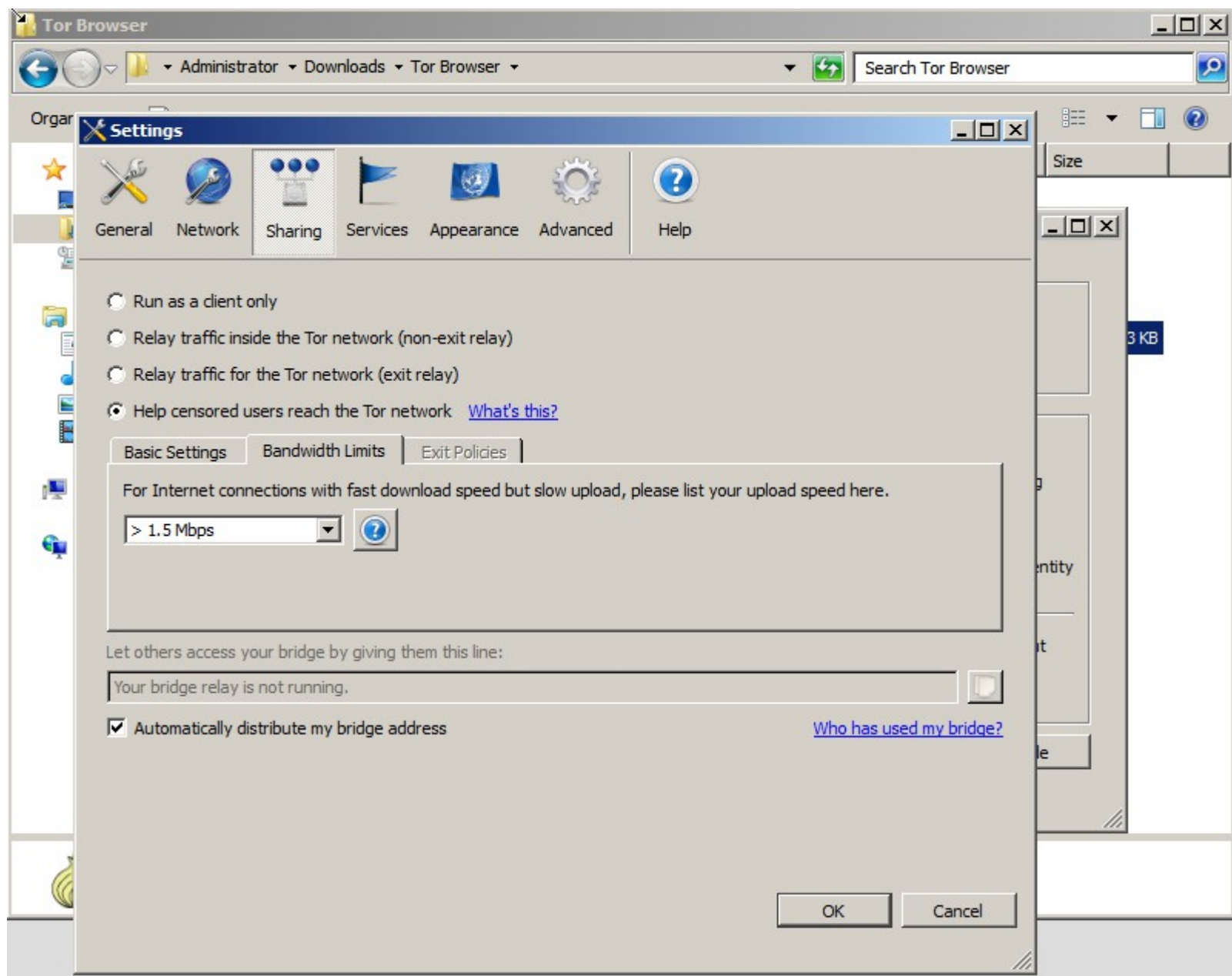
Get it, use it!

- Κατεβάστε το Tor Browser Bundle!
- Τρέξτε το .exe ή αποσυμπιέστε το .tar.gz
- Τρέξτε το “Start Tor Browser”

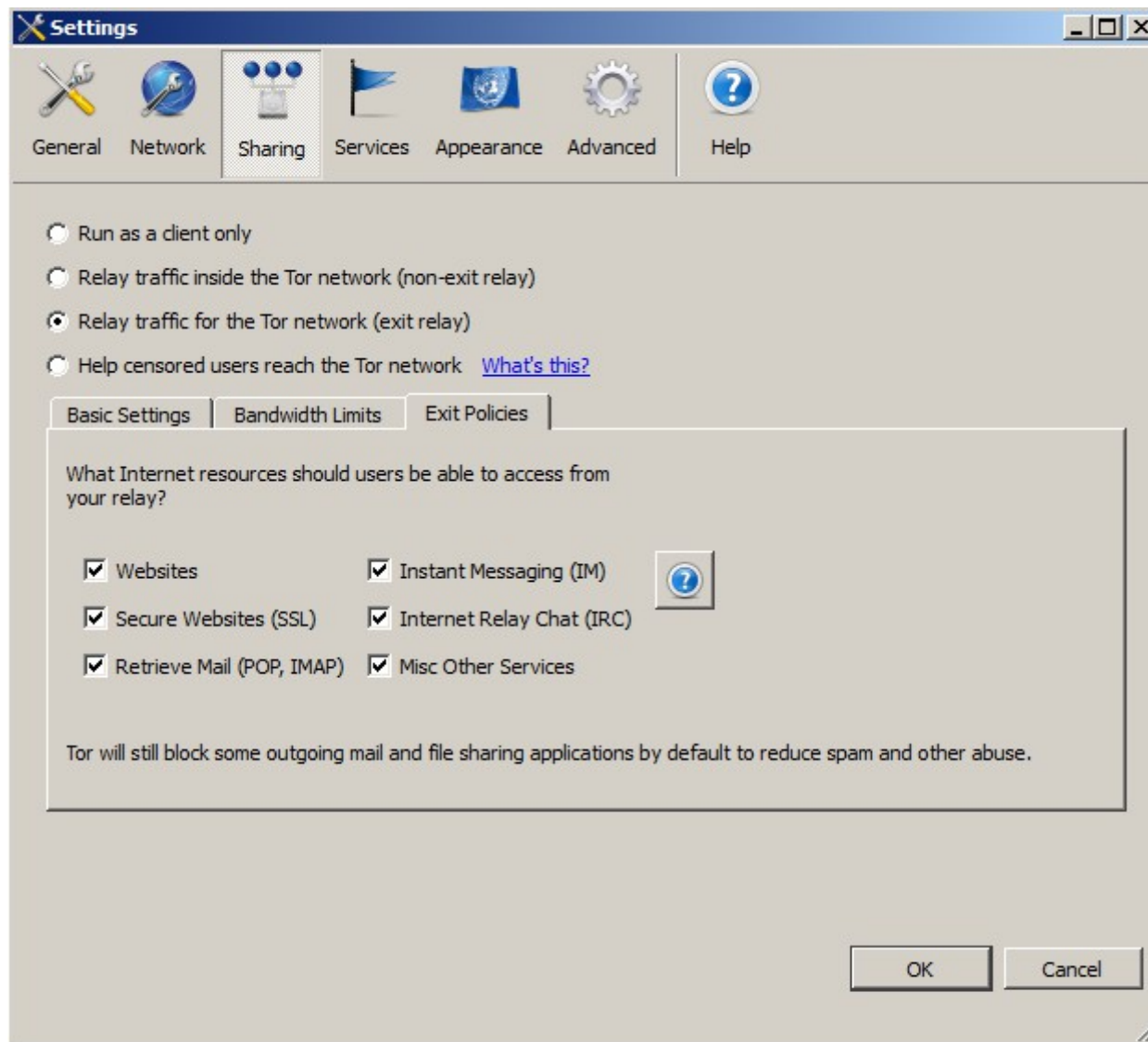
Χρήσιμοιώντας Tor



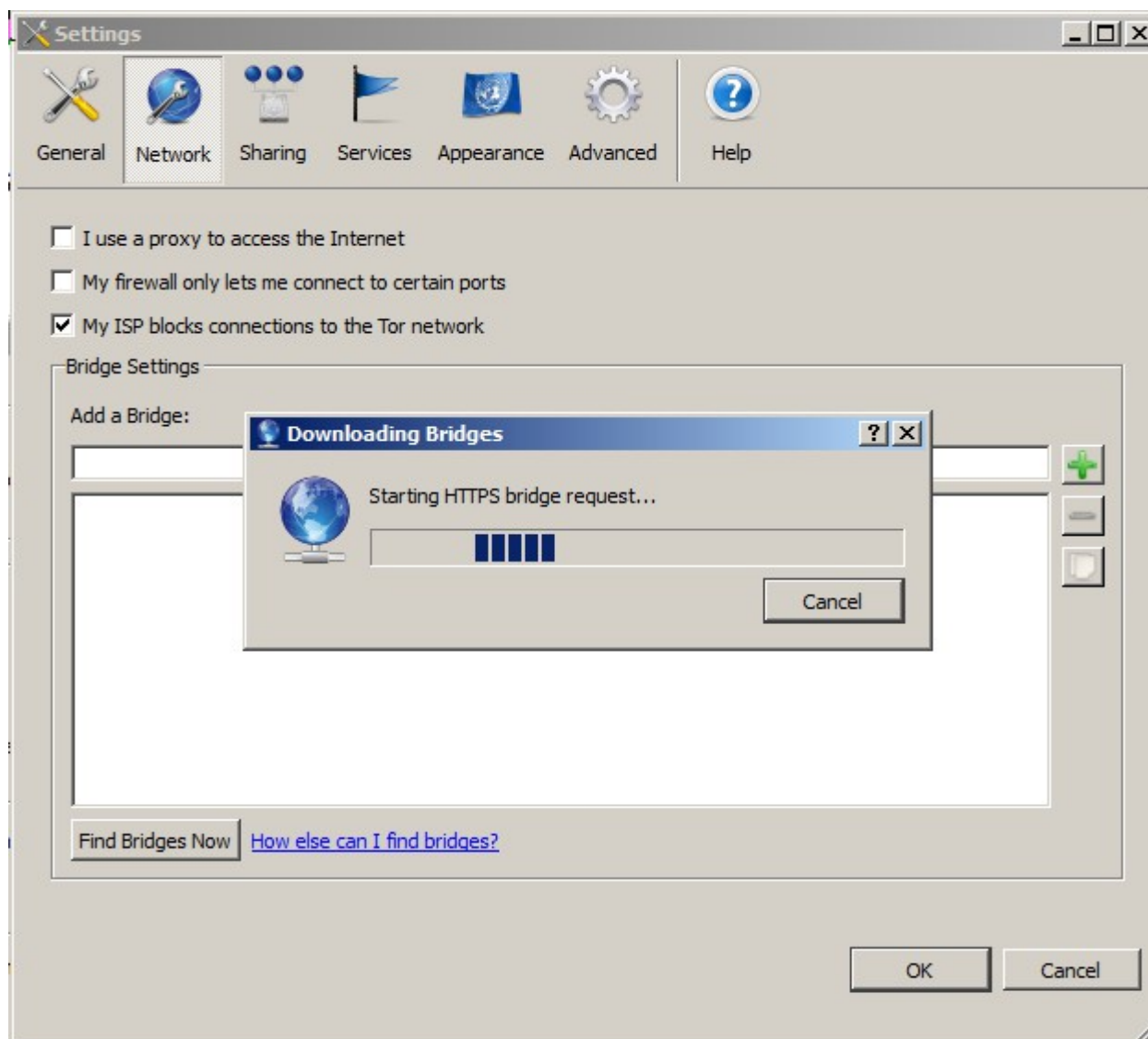
Χρήσιμοιώντας Tor



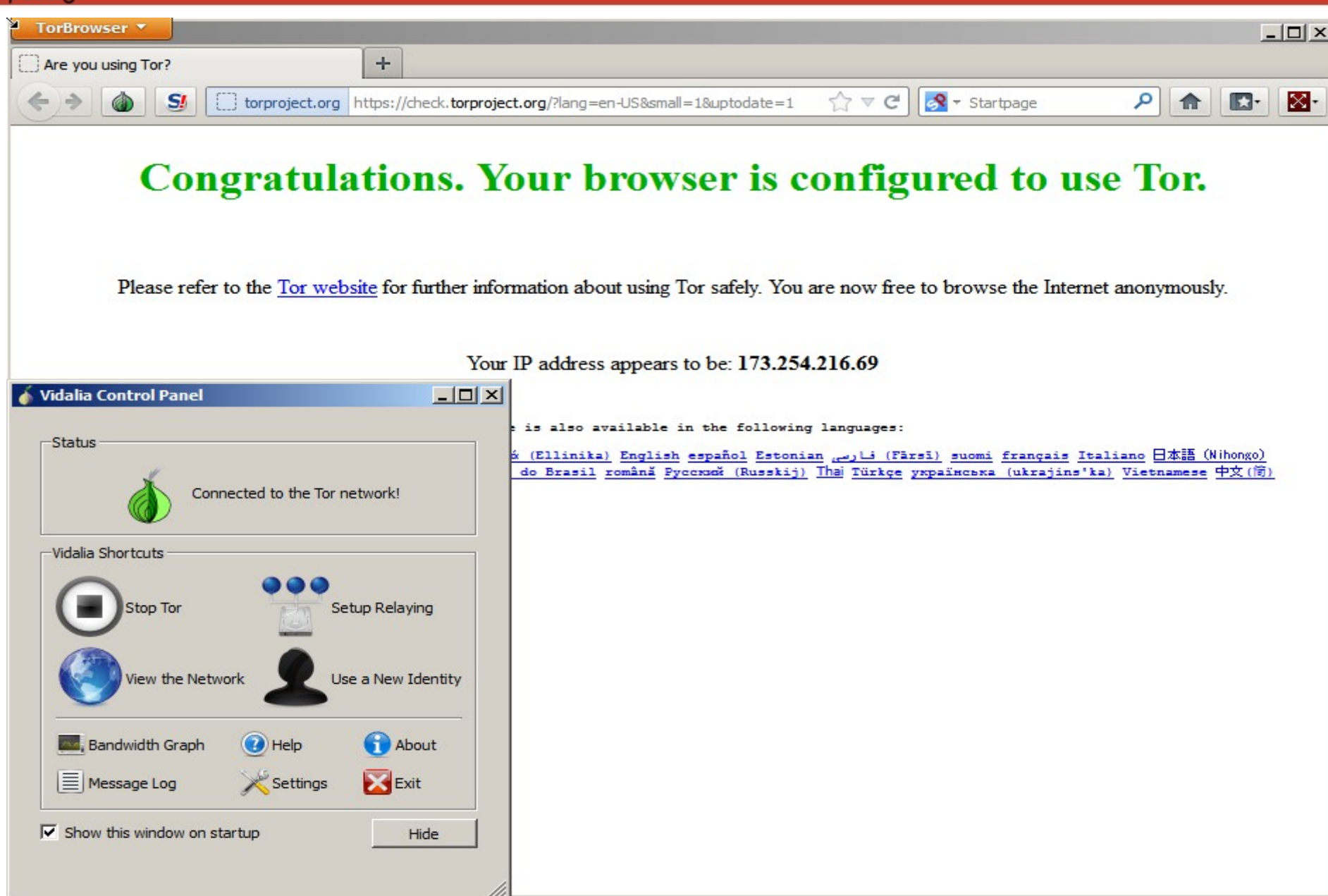
Χρησιμοποιώντας Tor



Χρήσιμποιώντας Tor



Χρήσιμοιώντας Tor



The image shows a screenshot of a computer screen with two windows. The top window is the TorBrowser, which displays a confirmation message in green text: "Congratulations. Your browser is configured to use Tor." Below this, it says "Please refer to the [Tor website](https://check.torproject.org/?lang=en-US&small=1&uptodate=1) for further information about using Tor safely. You are now free to browse the Internet anonymously." The browser's address bar shows the URL "https://check.torproject.org/?lang=en-US&small=1&uptodate=1". Below the main message, it states "Your IP address appears to be: 173.254.216.69".

The bottom window is the Vidalia Control Panel. It has a "Status" section with a green onion icon and the text "Connected to the Tor network!". Below this is a "Vidalia Shortcuts" section with several icons and labels: "Stop Tor" (a square with a circle), "Setup Relaying" (a network diagram), "View the Network" (a globe), "Use a New Identity" (a person icon), "Bandwidth Graph" (a line graph), "Help" (a question mark), "About" (an information icon), "Message Log" (a list icon), "Settings" (a wrench and screwdriver), and "Exit" (a red X). At the bottom of the panel, there is a checkbox labeled "Show this window on startup" which is checked, and a "Hide" button.

Συμβουλές χρήσης Tor

- Χρήση Tor != απόλυτη ασφάλεια
- **Plaintext over Tor == Plaintext** (στο exit node)
- Human-layer leaks (πχ social media logins!)
- Το Tor αφήνει αποτυπώματα στο δίκτυο
 - Μπορεί να εντοπιστεί η χρήση του αλλά όχι το περιεχόμενο της επικοινωνίας
- Διαφορετικό threat model για κάθε χρήστη == διαφορετική χρήση του tor για τον καθένα
 - Πρέπει να ξέρεις από τι θέλεις/πρέπει να προστατευτείς!

Συμβουλές χρήσης Tor

<https://www.eff.org/pages/tor-and-https>

Freedom of Speech

Demo time!

Βοηθήστε το Tor!

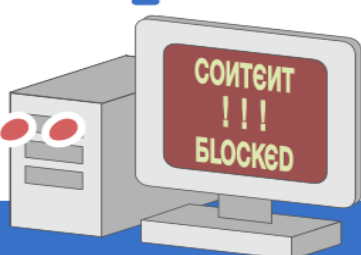


★ **YOU** ★

Can Help Protect

Freedom Of Speech

Online...



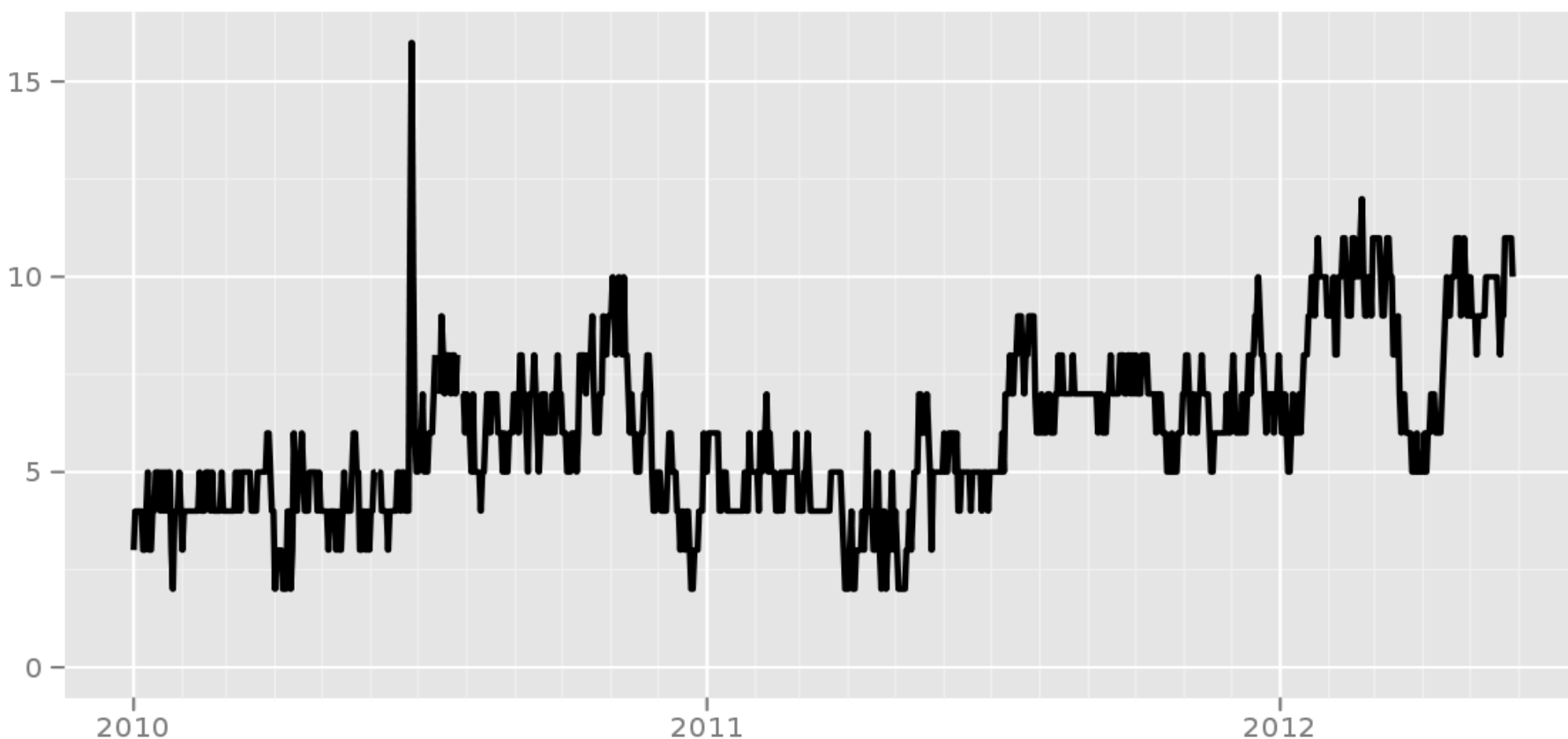
Run a
TOR RELAY
Today!

★★ **TorProject.org** ★★

Βοηθήστε το Tor!

Πληθυσμός: 10,787,690

Number of relays in Greece

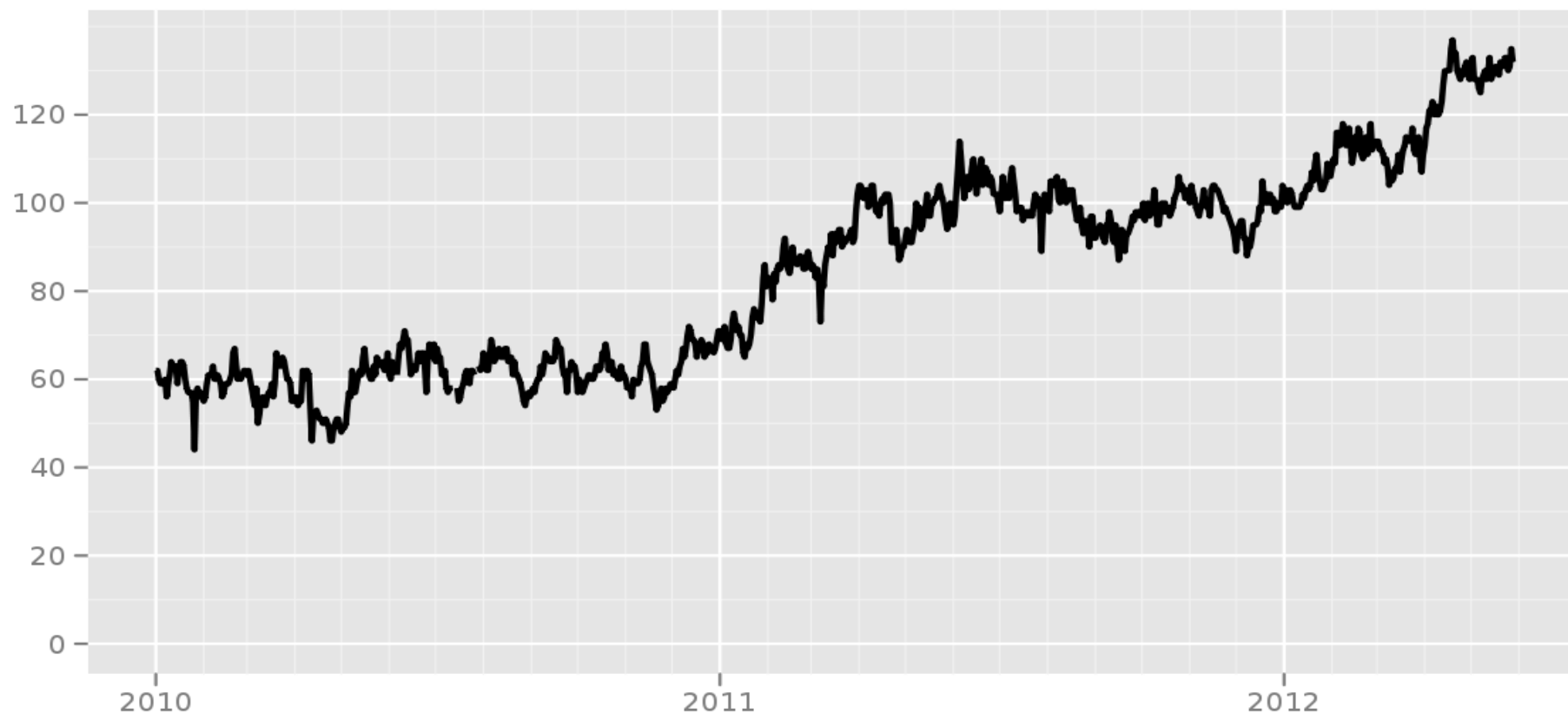


The Tor Project - <https://metrics.torproject.org/>

Βοηθήστε το Tor!

Πληθυσμός: 9,495,113

Number of relays in Sweden



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

Βοηθήστε το Tor!

- Τρέξτε ένα Relay / Bridge / Exit node!
 - Υπάρχει δυνατότητα για περιορισμούς σε bandwidth rate / όγκο δεδομένων
- Έρευνα σχετικά με κρυπτογραφία / p2p δίκτυα / ανωνυμία / κ.α
- Γράψτε κώδικα! Open Source!
 - C, Java, HTML, js, κ.α
- Βοηθήστε στις μεταφράσεις
 - [torproject on transifex](#)

Νομικά θέματα

- <https://www.torproject.org/eff/tor-legal-faq.html>
- <https://www.torproject.org/docs/faq-abuse>
- Tips for Running an Exit Node with Minimal Harassment

Ευχαριστίες

- Όσοι έστειλαν ιδέες
- Όσοι επικοινωνήσαν μαζί μου για να βοηθήσουν :)
- EFF
- Torproject.org

Freedom of Speech

Sites to visit

- 🍇 **Torproject.org**
- 🍇 **hackerspace.gr**
- 🍇 **dln.gr**
- 🍇 **The Hidden Wiki (ε...βρείτε το...)**

Freedom of Speech

Διαγωνισμός

Tor Relay/Bridge > 1Mbit για τουλάχιστον 15μέρες uptime

ή

Tor exit node > 512Kbit για τουλάχιστον 15μέρες uptime

ή

Μετάφραση του “The Short User Manual”

Στείλτε (μόνο) τα (απαραίτητα) στοιχεία στο kargig [at] void [dot] gr

Προφανώς κρυπτογραφημένα με GPG ☺

Ο πρώτος που θα κάνει όλα τα βήματα κερδίζει ένα T-Shirt του EFF

Freedom of Speech

Ερωτήσεις / Συζήτηση