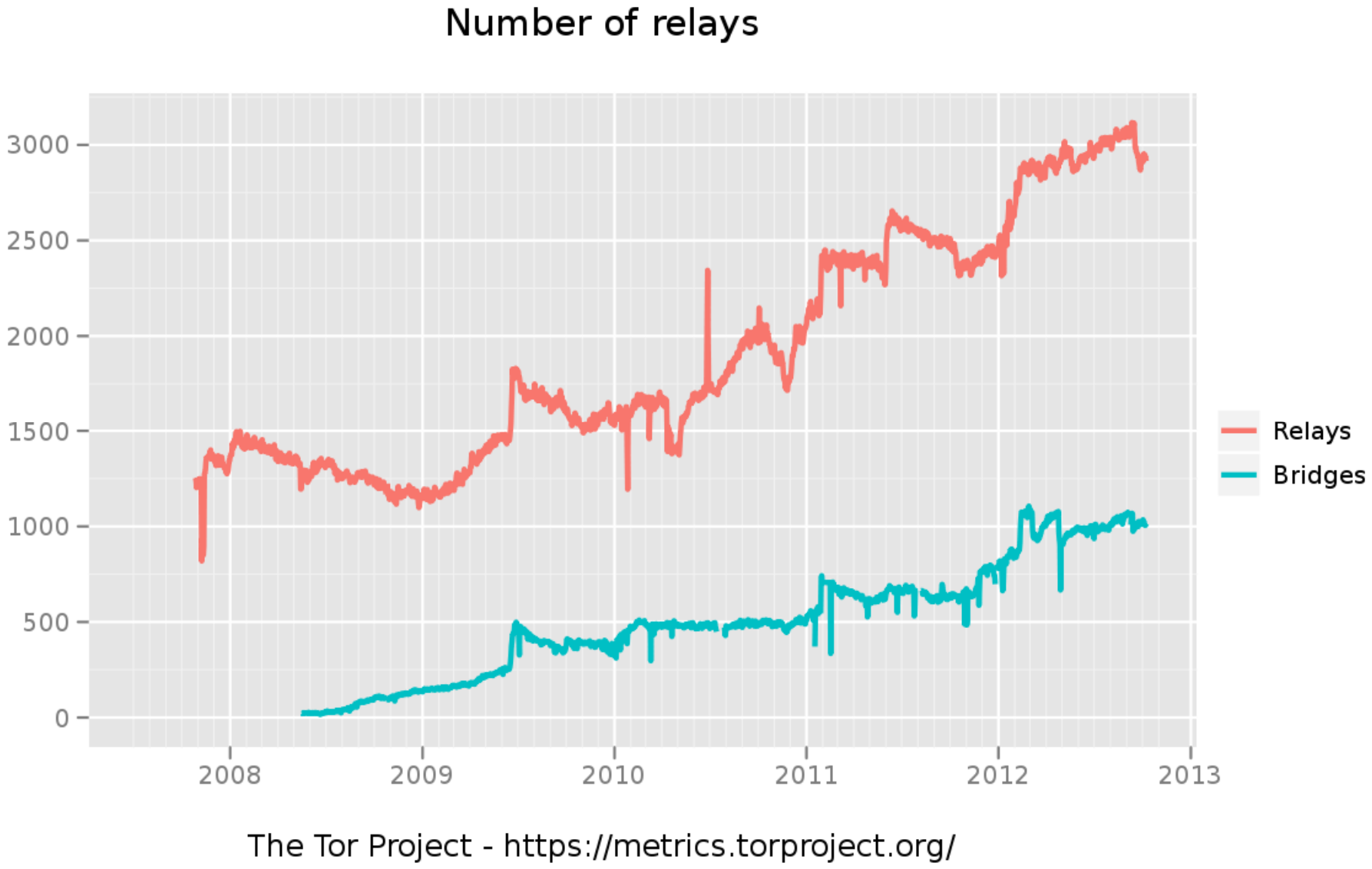
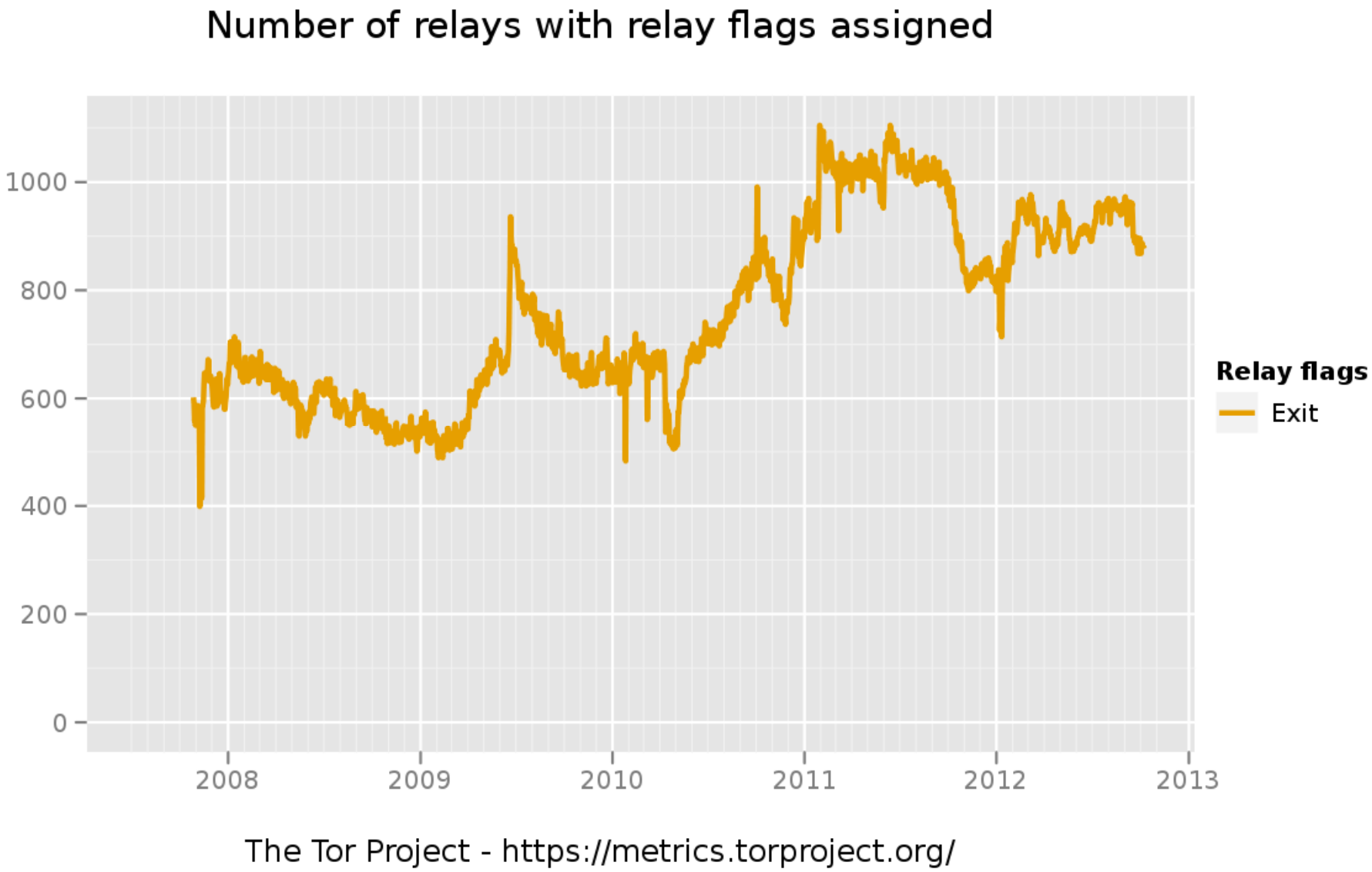
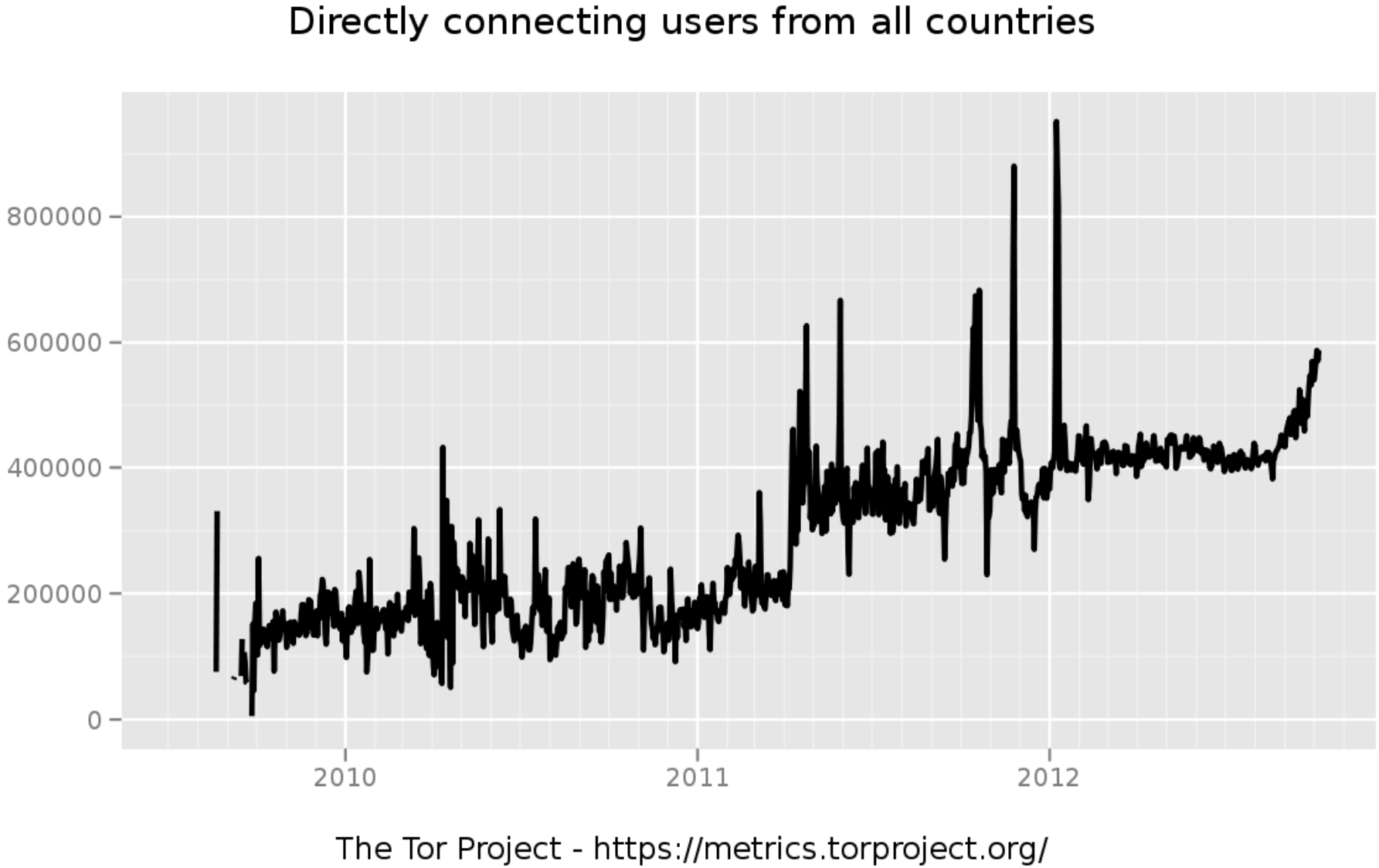
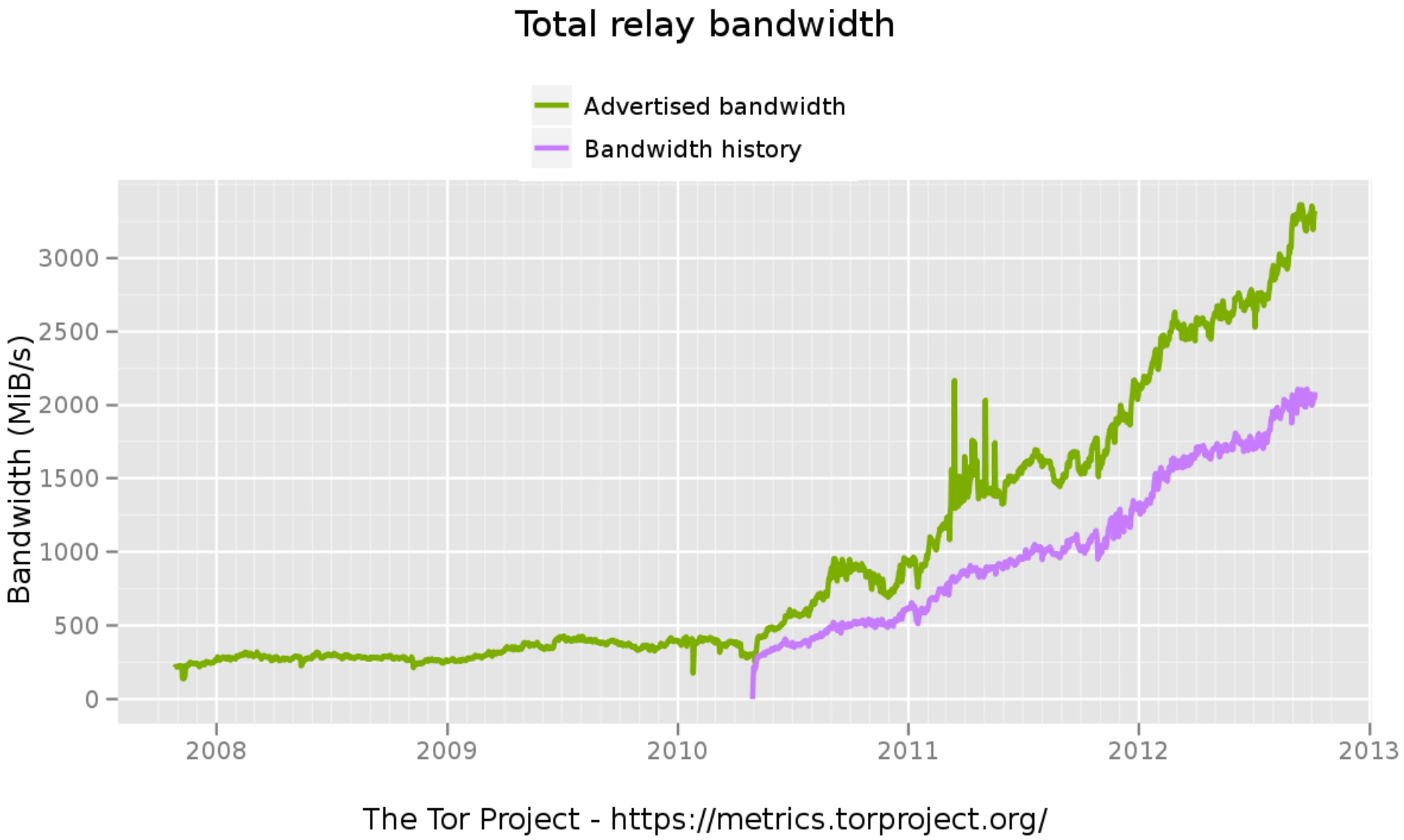
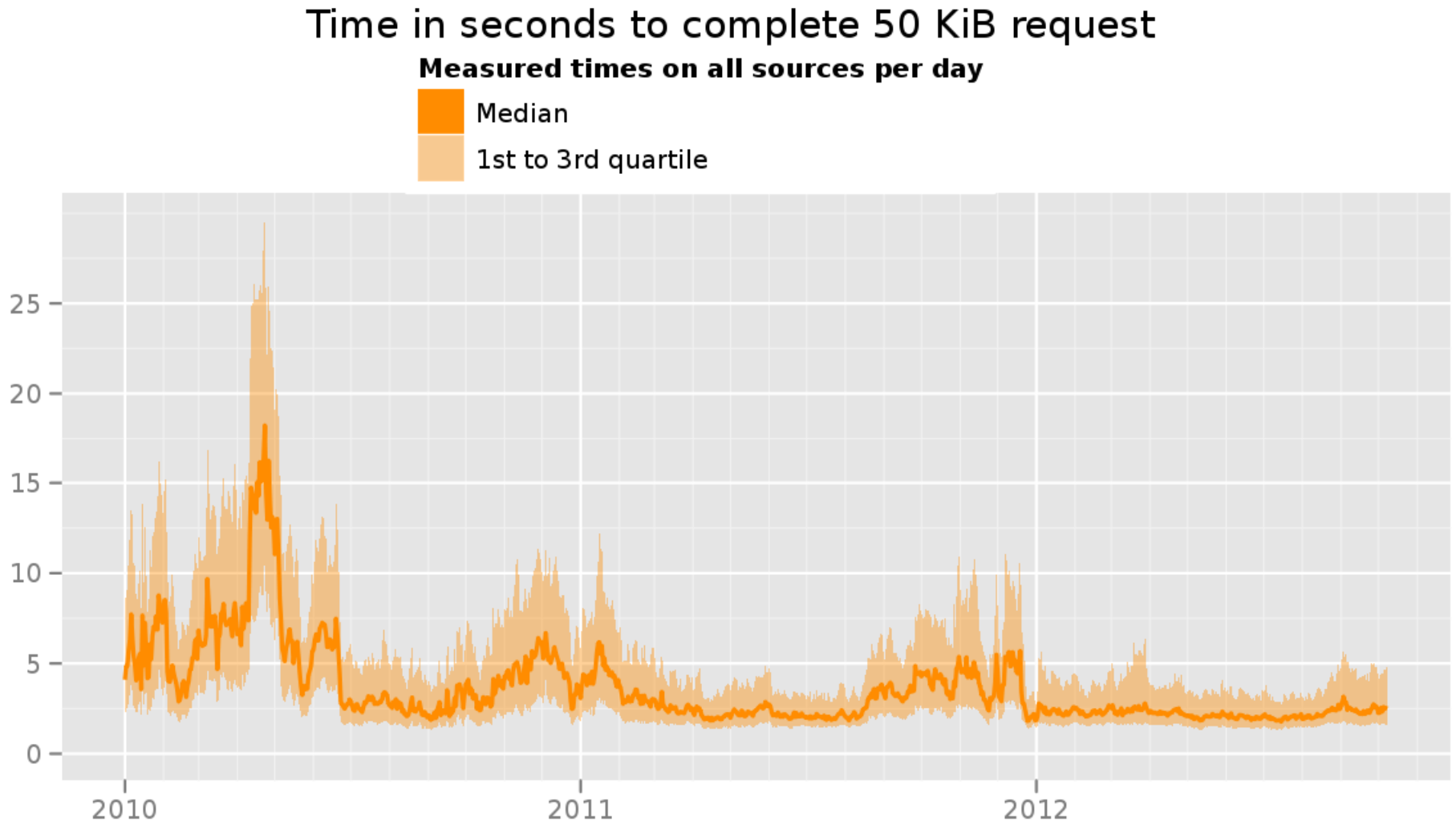

Number of relays
3000
2500
2000
1500
1000
500
0
2008
2009
2010
2011
2012
2013
Relays
Bridges
The Tor Project - https://metrics.torproject.org/


Number of relays with relay flags assigned
1000
800
600
400
200
0
2008
2009
2010
2011
2012
2013
Relay flags
Exit
The Tor Project - https://metrics.torproject.org/


Directly connecting users from all countries
800000
600000
400000
200000
0
2010
2011
2012
The Tor Project - https://metrics.torproject.org/


Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
3000
2500
2000
1500
1000
500
0
2008
2009
2010
2011
2012
2013
The Tor Project - https://metrics.torproject.org/


Time in seconds to complete 50 KiB request
Measured times on all sources per day
Median
1st to 3rd quartile
25
20
15
10
5
0
2010
2011
2012
The Tor Project - https://metrics.torproject.org/

Port	Number of Exit Nodes
22	211
53	216
80	226
110	210
143	208
443	238
5190	184
6667	172

Port	Number of Exit Nodes
25	4
119	25
135–139	6
445	6
465	12
587	13
1214	7
4661–4666	5
6699	9

(from 2006)

Table 1. Exit traffic protocol distribution by number of TCP connections, size, and number of unique destination hosts.

Protocol	Connections	Bytes	Destinations
HTTP	12,160,437 (92.45%)	411 GB (57.97%)	173,701 (46.01%)
SSL	534,666 (4.06%)	11 GB (1.55%)	7,247 (1.91%)
BitTorrent	438,395 (3.33%)	285 GB (40.20%)	194,675 (51.58%)
Instant Messaging	10,506 (0.08%)	735 MB (0.10%)	880 (0.23%)
E-Mail	7,611 (0.06%)	291 MB (0.04%)	389 (0.10%)
FTP	1,338 (0.01%)	792 MB (0.11%)	395 (0.10%)
Telnet	1,045 (0.01%)	110 MB (0.02%)	162 (0.04%)
Total	13,154,115	709 GB	377,449

(from 2008)

Passion and dalliance

Tch! What's the World coming to?

« Let's try this one

More Tor! »

Why you need balls of steel to operate a Tor exit node

By calumog

I became interested in Tor in the spring of 2007 after reading about the situation in Burma and felt that I would like to do something, anything, to help. As a geek and lover of the internet it seemed the best thing I could do was to run Tor as an exit node to allow those under jurisdictions that censor the internet free access to the information they need. I had a lot of unused bandwidth and it seemed like a philanthropic use of it to donate that to Tor.

POLITICS : SECURITY

Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise

By Kim Zetter 09.10.07

A security researcher intercepted thousands of private e-mail messages sent by foreign embassies and human rights groups around the world by turning portions of the Tor internet anonymity service into his own private listening post.

A little over a week ago, Swedish computer security consultant Dan Egerstad posted the user names and passwords for 100 e-mail accounts used by the victims, but didn't say how he obtained them. He revealed Friday that he intercepted the information by hosting five Tor exit nodes placed in different locations on the internet as a research project.

But Egerstad says that many who use Tor mistakenly believe it is an end-to-end encryption tool. As a result, they aren't taking the precautions they need to take to protect their web activity.

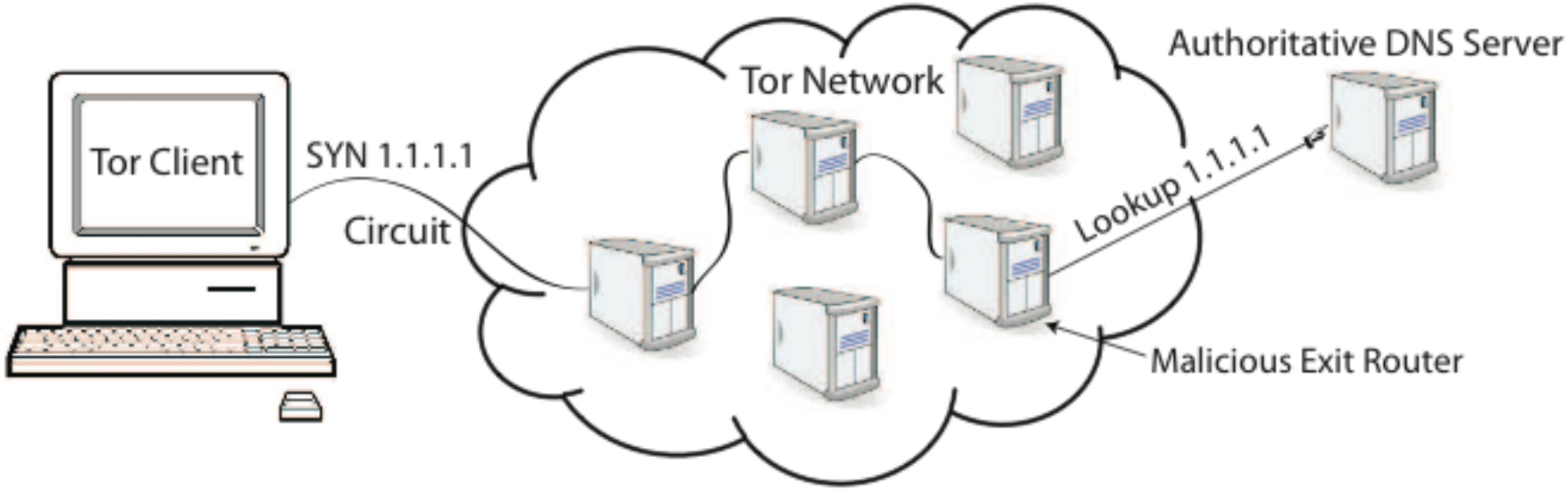
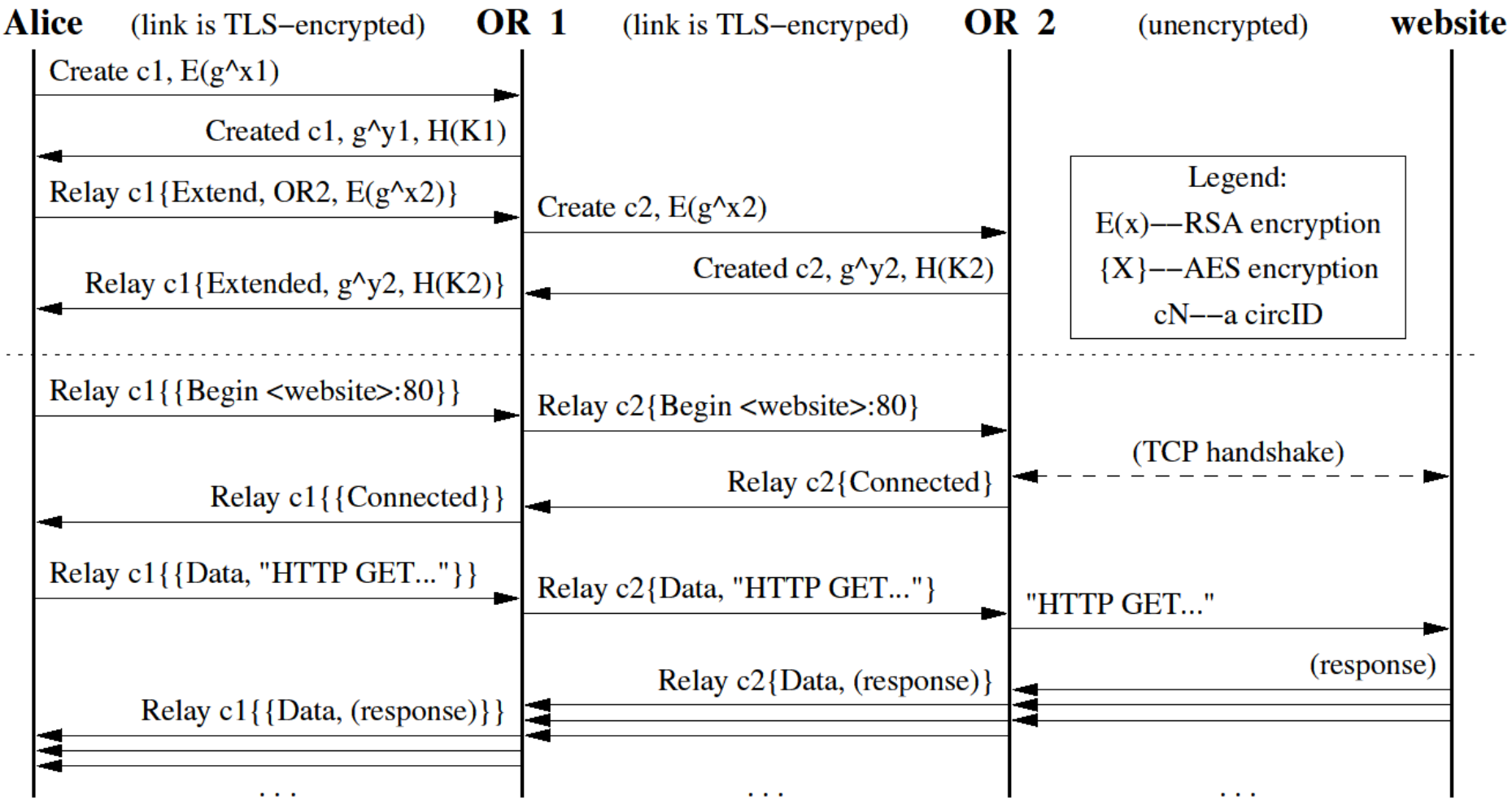
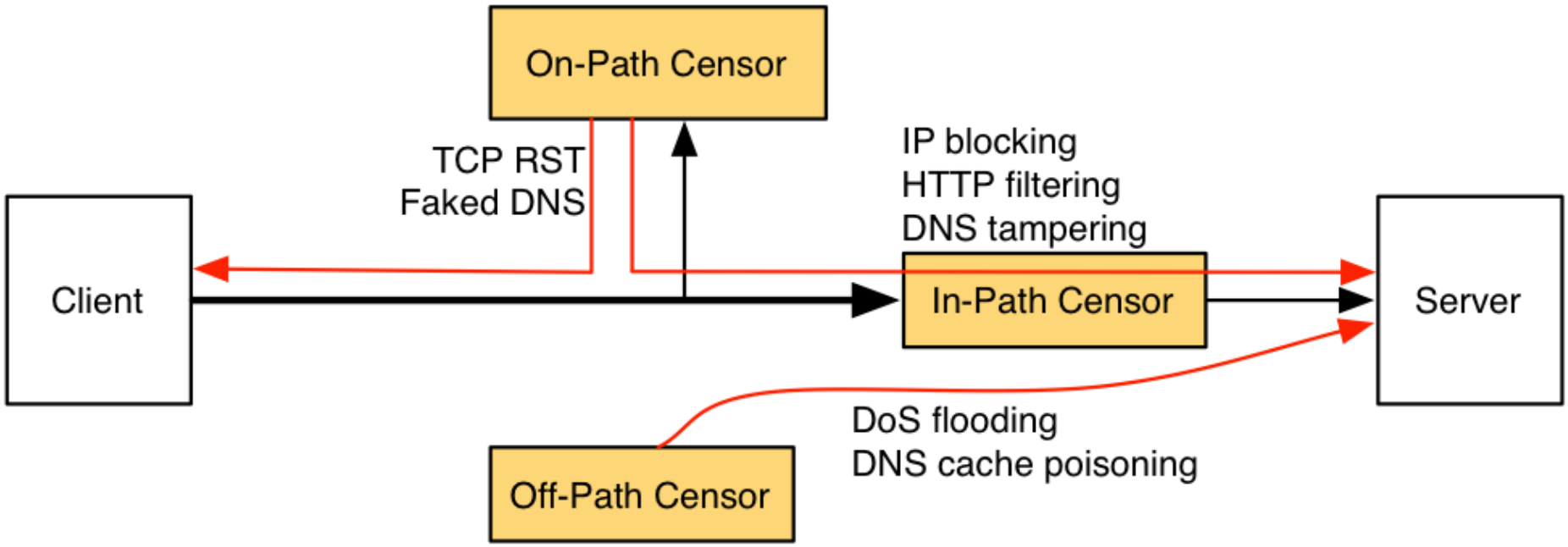


Fig. 1. Malicious exit router logging detection technique.

Individual Bans

Nickname	Ban Type	IP	Port	Date	Reporter	Reason
HumaniTOR	BadExit	212.80.35.73	9001	5/11/12	arma	connection refused for ports 80 and 443
Unnamed	BadExit	219.90.126.61	443	5/1/12	James Hooker	running sslstrip
ididedittheconfig	BadExit	94.185.81.130	9001	4/3/12	James Hooker	running sslstrip
UnFilTerD	BadExit	82.95.57.4	8888	4/3/12	James Hooker	running sslstrip
default	BadExit	66.165.177.139	443	3/5/12	---	sniffing traffic
100mbitTOR	BadExit	109.87.69.138	---	11/6/11	Sebastian	MITM of SSL
Secureroute	BadExit	---	---	11/4/11	mikeperry	MITM of SSL with self-signed cert
Unnamed	BadExit	164.41.103.153	443	9/30/11	aagbsn	MITM of SSL with a fortinet cert
QuantumSevero	BadExit	84.19.176.56	443	1/30/11	mikeperry	plaintext-only exit policy + no reachable contact
ElzaTorServer	BadExit	109.202.66.4	9001	1/30/11	mikeperry	plaintext-only exit policy + no reachable contact
agitator	BadExit	188.40.77.107	9001	1/15/11	---	sniffing traffic
PrivacyPT	BadExit	84.90.72.186	---	1/5/11	mikeperry	running sslstrip
KnightVison	BadExit	213.247.98.204	---	1/5/11	mikeperry	403 responses for arbitrary URLs
Unnamed	BadExit	84.46.20.223	---	1/5/11	mikeperry	SSL MITM with Kaspersky AV certs
newworld	BadExit	98.126.68.58	443	12/22/10	mikeperry	running sslstrip
Unnamed	BadExit	118.160.19.236	443	11/19/10	mikeperry	anti-virus filter is blocking sites (trend-micro)
Unnamed	BadExit	---	---	11/19/10	mikeperry	anti-virus filter is blocking sites (trend-micro)
Unnamed	BadExit	---	---	11/19/10	mikeperry	anti-virus filter is blocking sites (trend-micro)
Unnamed	BadExit	---	---	11/19/10	mikeperry	anti-virus filter is blocking sites (trend-micro)
Unnamed	BadExit	---	---	11/19/10	mikeperry	anti-virus filter is blocking sites (trend-micro)
703server	BadExit	173.49.70.62	---	11/19/10	mikeperry	several issues including possible SSL downgrade attack
Tark69	BadExit	66.169.160.200	443	10/28/10	mikeperry	anti-virus filter is blocking sites
Unnamed	BadExit	90.22.200.39	---	10/24/10	mikeperry	dropping TLS connections for multiple sites
ArsenalGear	BadExit	88.207.18.230	---	7/27/10	susurrusus	running sslstrip
FluideGlacial	BadExit	78.229.212.4	9001	7/14/10	mikeperry	spurious RST packets
capoteATWO	BadExit	148.88.190.145	9001	4/28/10	phobos, xiando	misconfigured
PrivacyNow	BadExit	83.91.86.29	9001	4/14/10	Scott Bennett	misconfigured DNS
romainaForever	BadExit	64.191.73.149	9001	---	---	---
netwroke421d2a	BadExit	64.191.22.197	9001	---	---	---


Alice
(link is TLS−encrypted)
OR 1
(link is TLS−encryped)
OR 2
(unencrypted)
website
Create c1, E(g^x1)
Created c1, g^y1, H(K1)
Relay c1{Extend, OR2, E(g^x2)}
Create c2, E(g^x2)
Created c2, g^y2, H(K2)
Relay c1{Extended, g^y2, H(K2)}
Legend:
E(x)−−RSA encryption
{X}−−AES encryption
cN−−a circID
Relay c1{{Begin <website>:80}}
Relay c2{Begin <website>:80}
(TCP handshake)
Relay c2{Connected}
Relay c1{{Connected}}
Relay c1{{Data, "HTTP GET..."}}
Relay c2{Data, "HTTP GET..."}
"HTTP GET..."
(response)
Relay c2{Data, (response)}
Relay c1{{Data, (response)}}
. . .
. . .
. . .


On-Path Censor
TCP RST
Faked DNS
IP blocking
HTTP filtering
DNS tampering
Client
In-Path Censor
Server
DoS flooding
DNS cache poisoning
Off-Path Censor