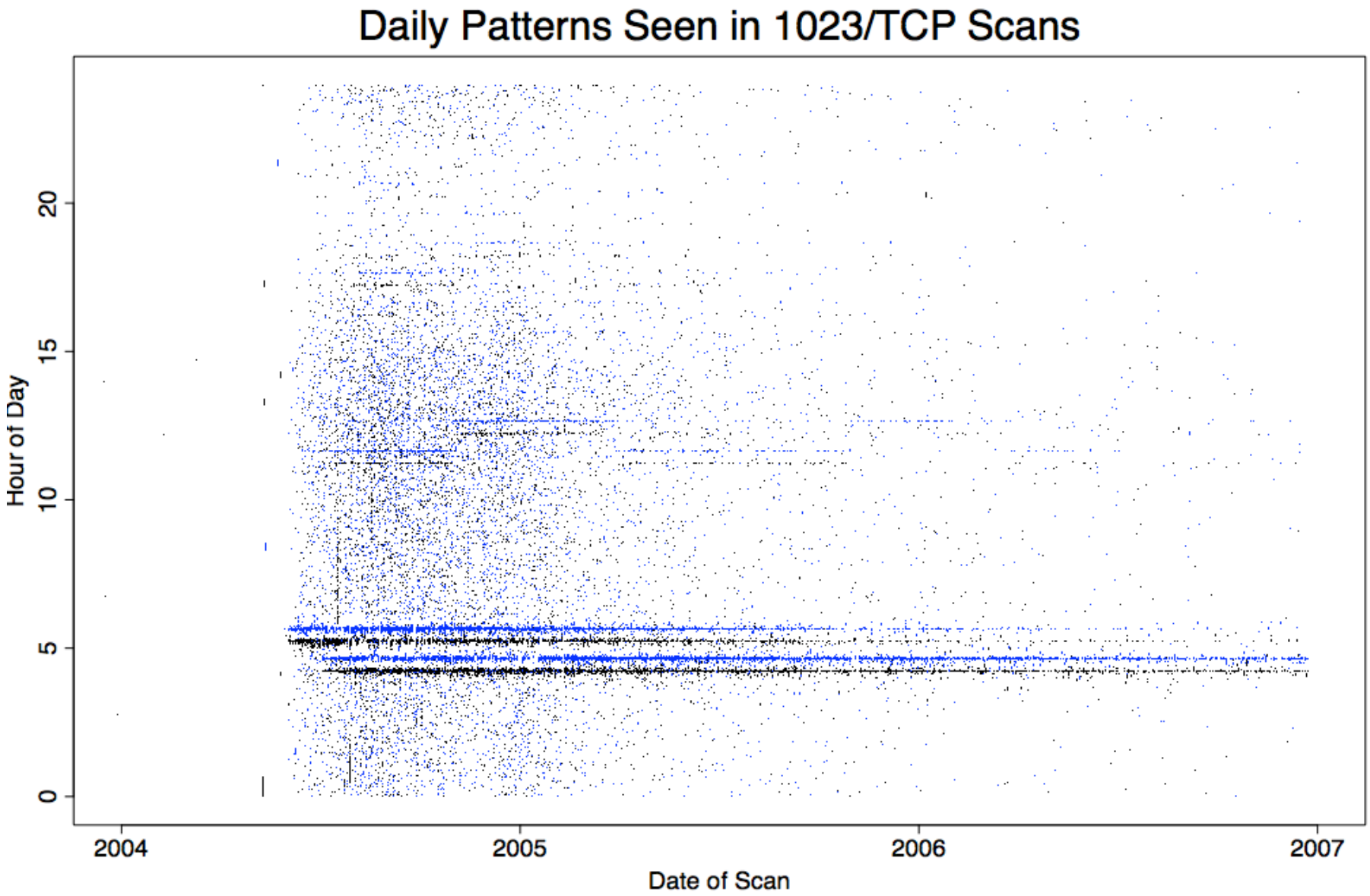
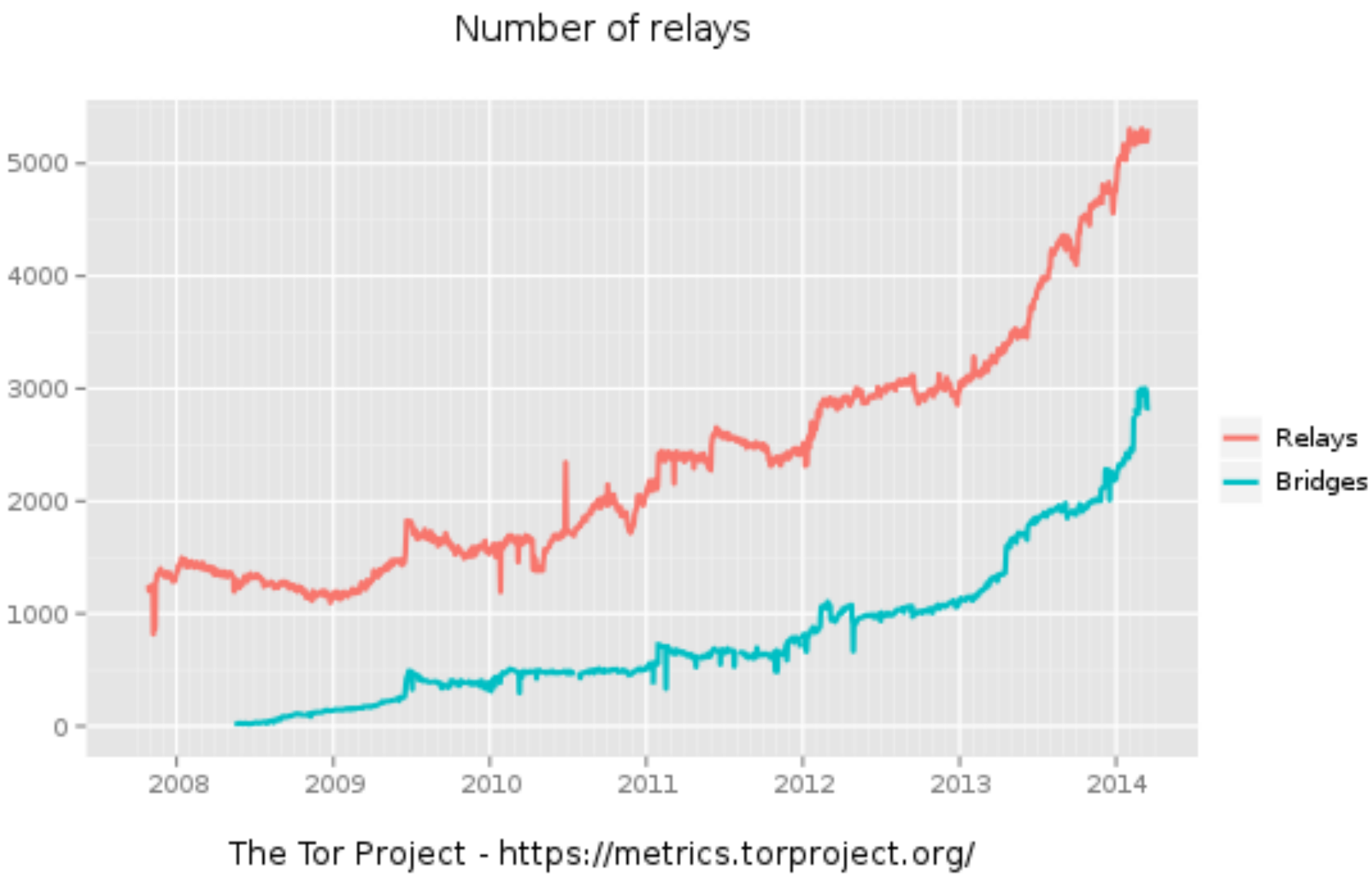
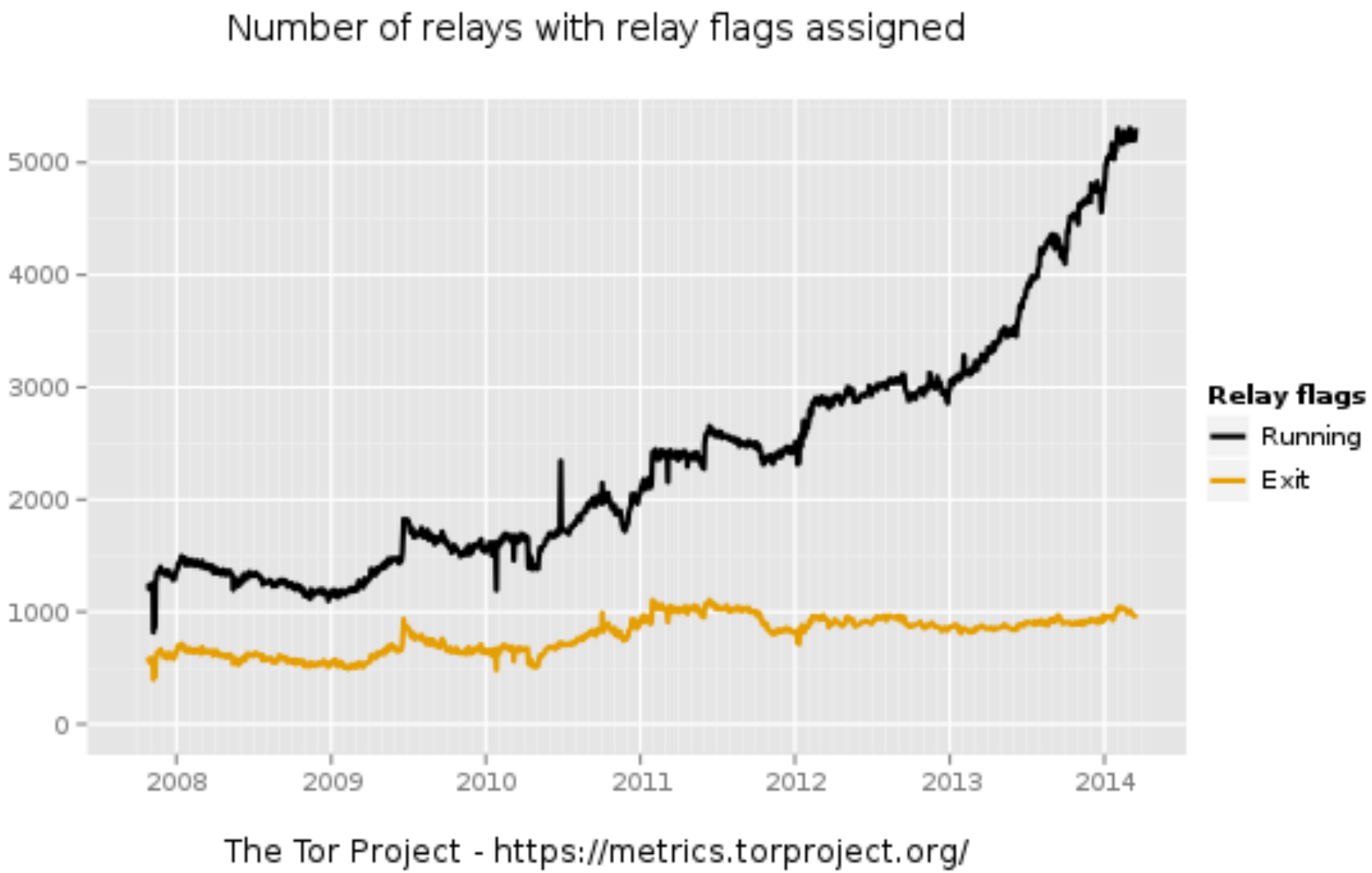
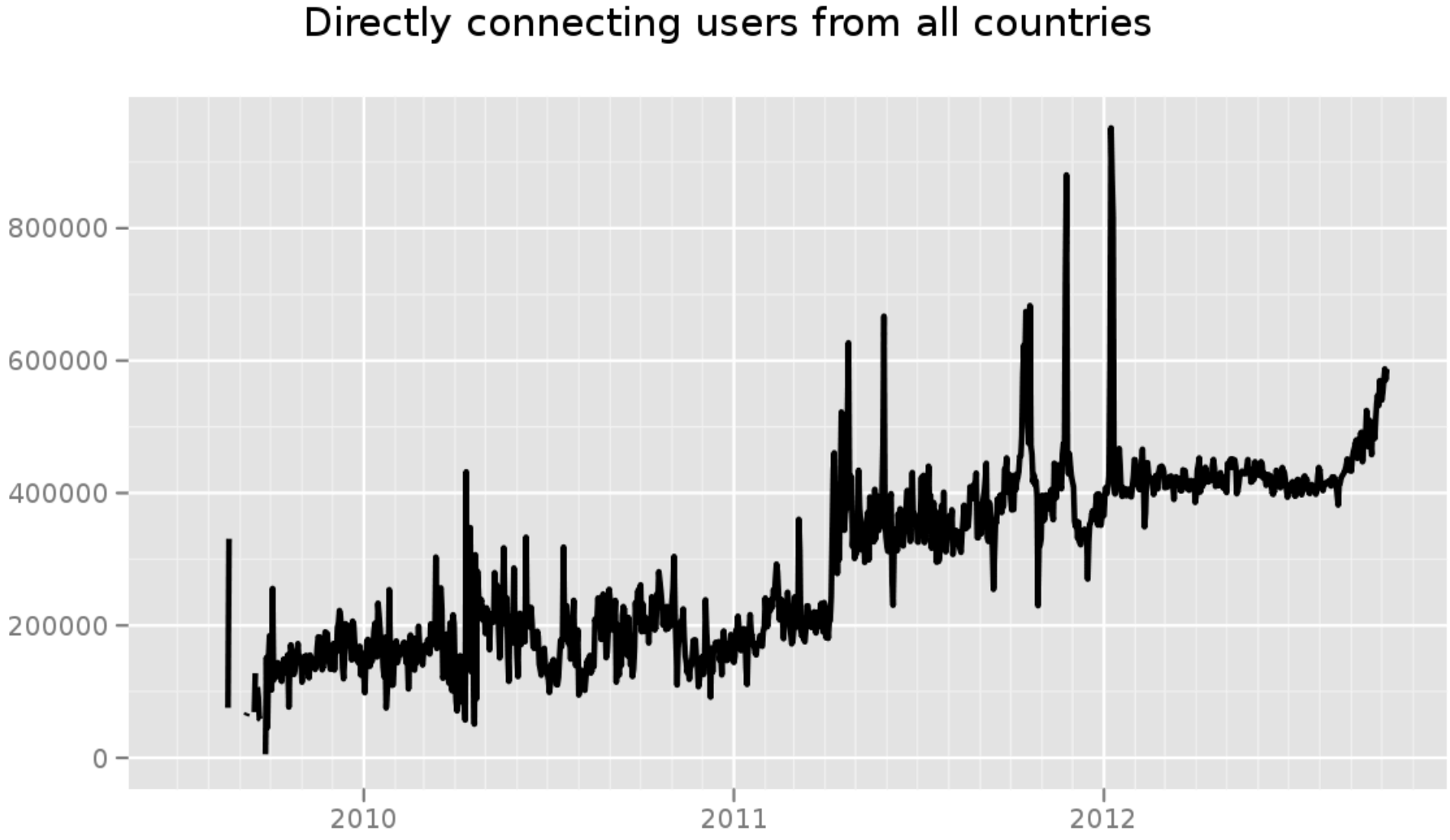
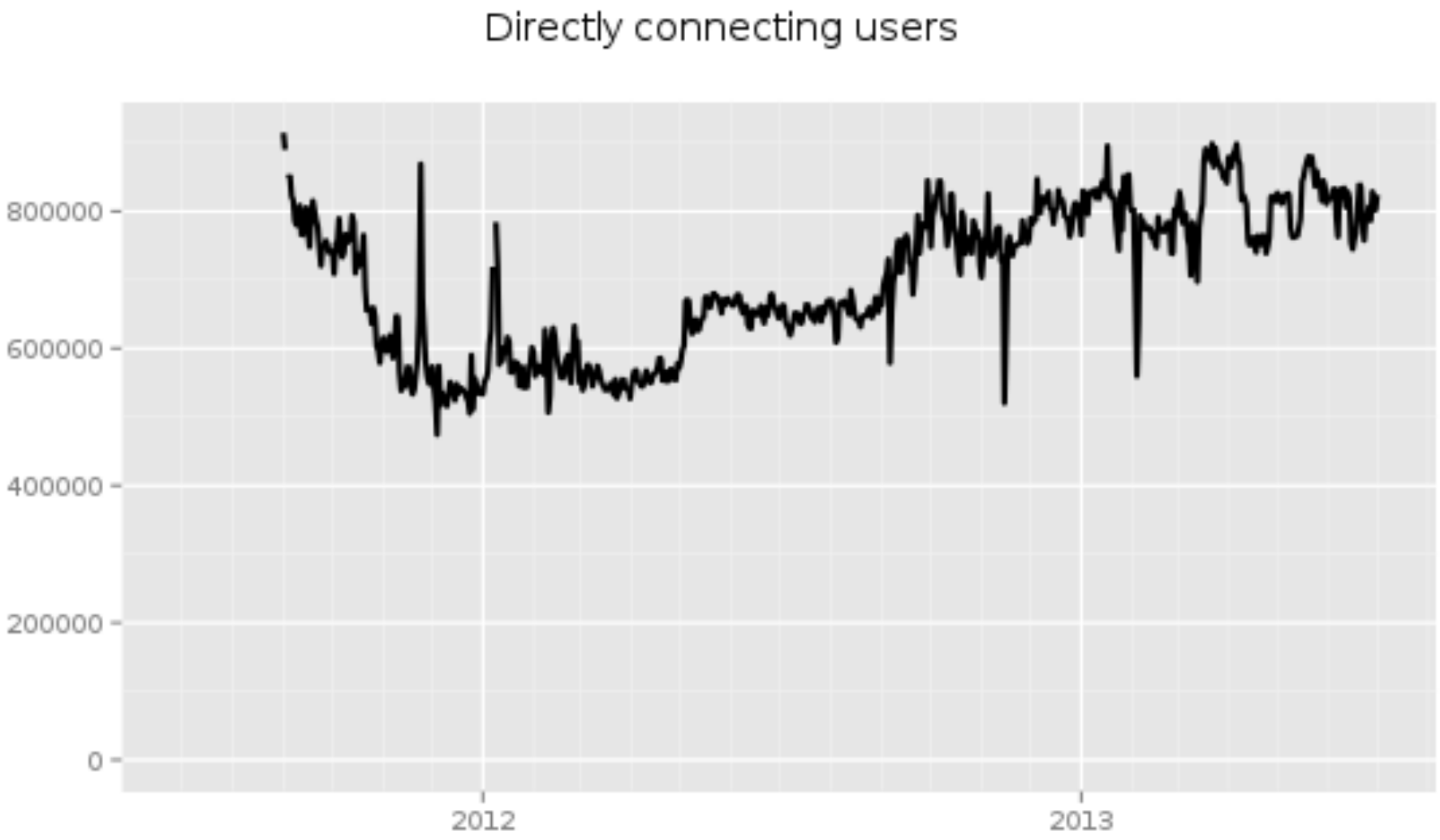
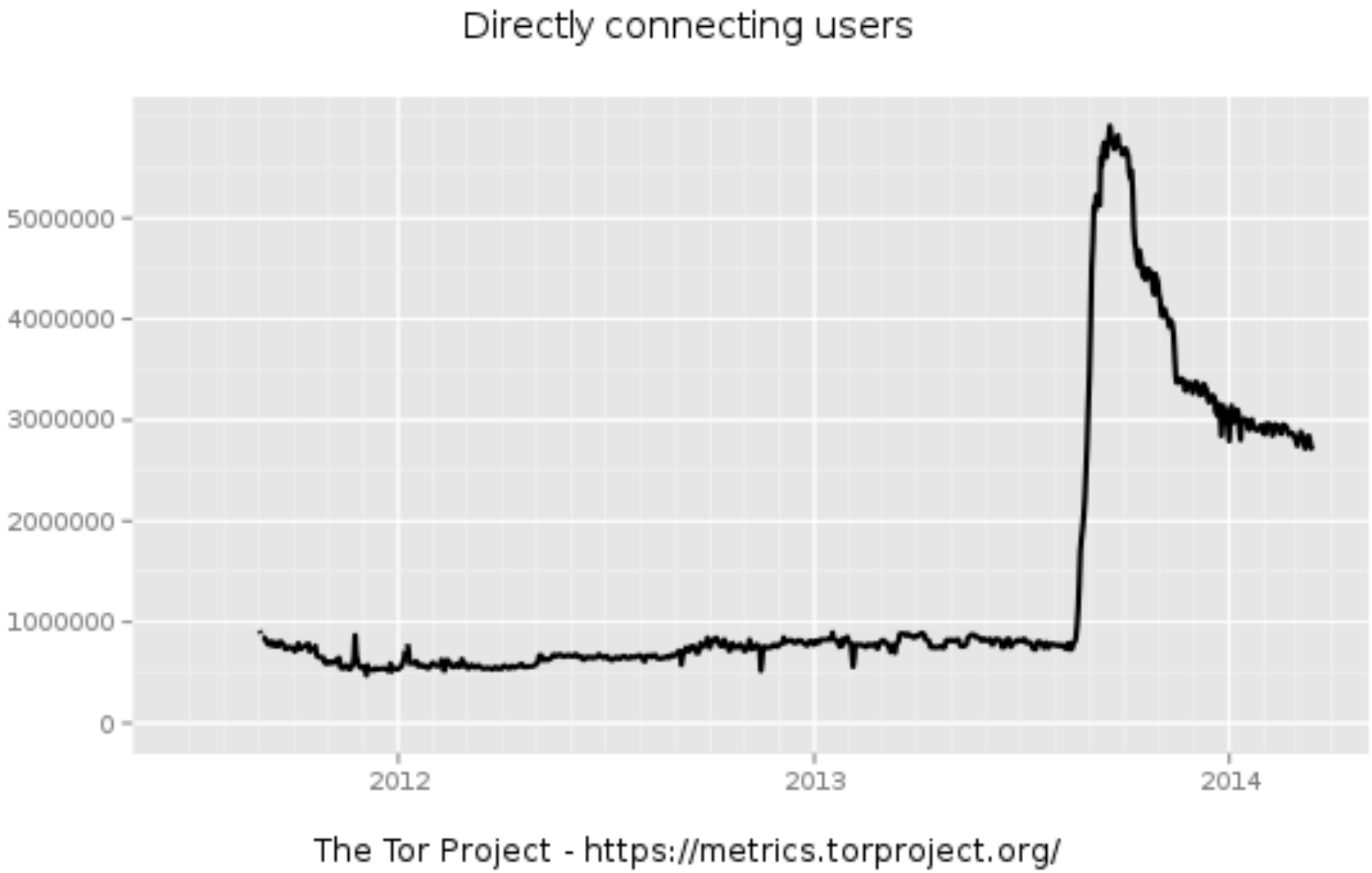

Daily Patterns Seen in 1023/TCP Scans
Hour of Day
0
5
10
15
20
2004
2005
2006
2007
Date of Scan
/16 at LBL, sampled 1-in-1K
2nd /16, sampled 1-in-1K

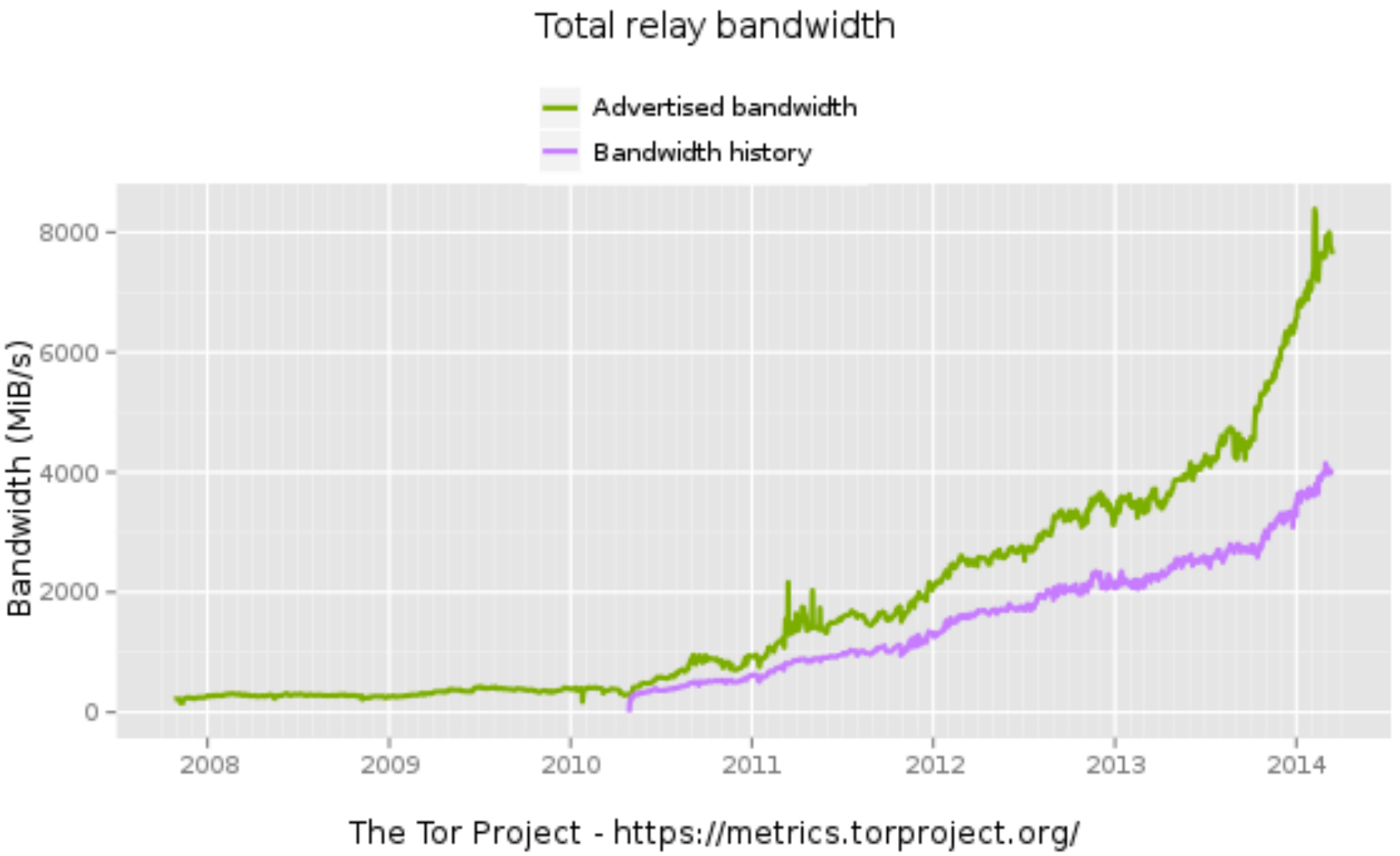

Number of relays
5000
4000
3000
2000
1000
0
2008
2009
2010
2011
2012
2013
2014
Relays
Bridges
The Tor Project - https://metrics.torproject.org/

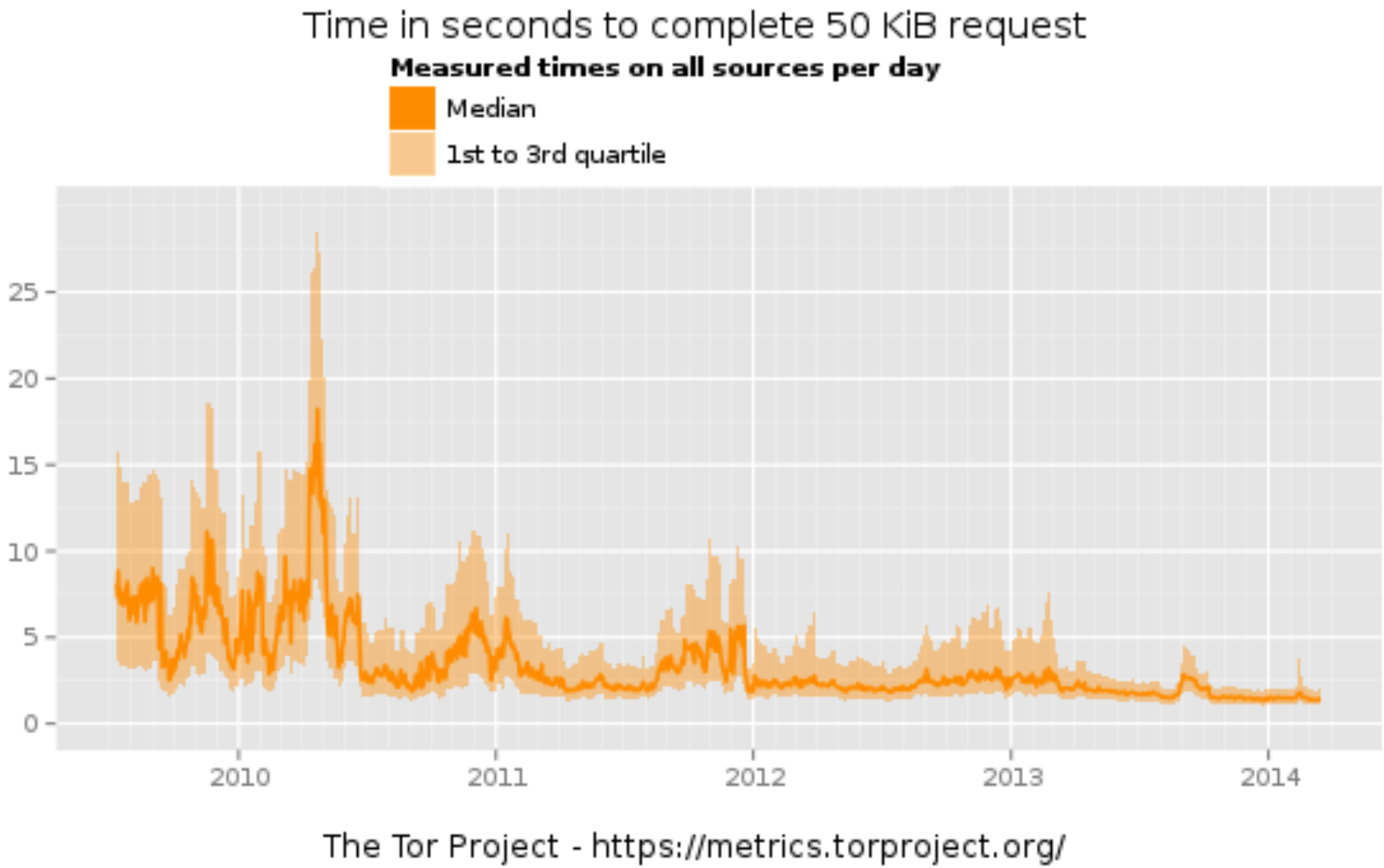

Number of relays with relay flags assigned
5000
4000
3000
2000
1000
0
2008
2009
2010
2011
2012
2013
2014
Relay flags
Running
Exit
The Tor Project - https://metrics.torproject.org/


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


Directly connecting users
800000
600000
400000
200000
0
2012
2013
The Tor Project - https://metrics.torproject.org/


Directly connecting users
5000000
4000000
3000000
2000000
1000000
0
2012
2013
2014
The Tor Project - https://metrics.torproject.org/


Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
8000
6000
4000
2000
0
2008
2009
2010
2011
2012
2013
2014
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
2013
2014
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.

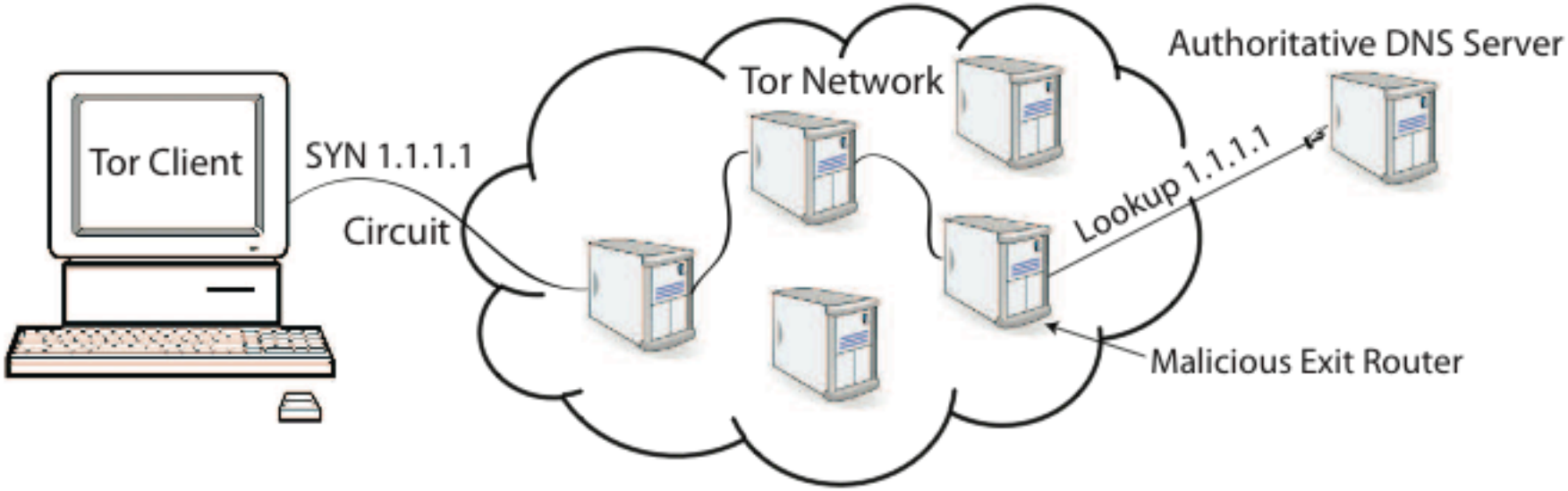
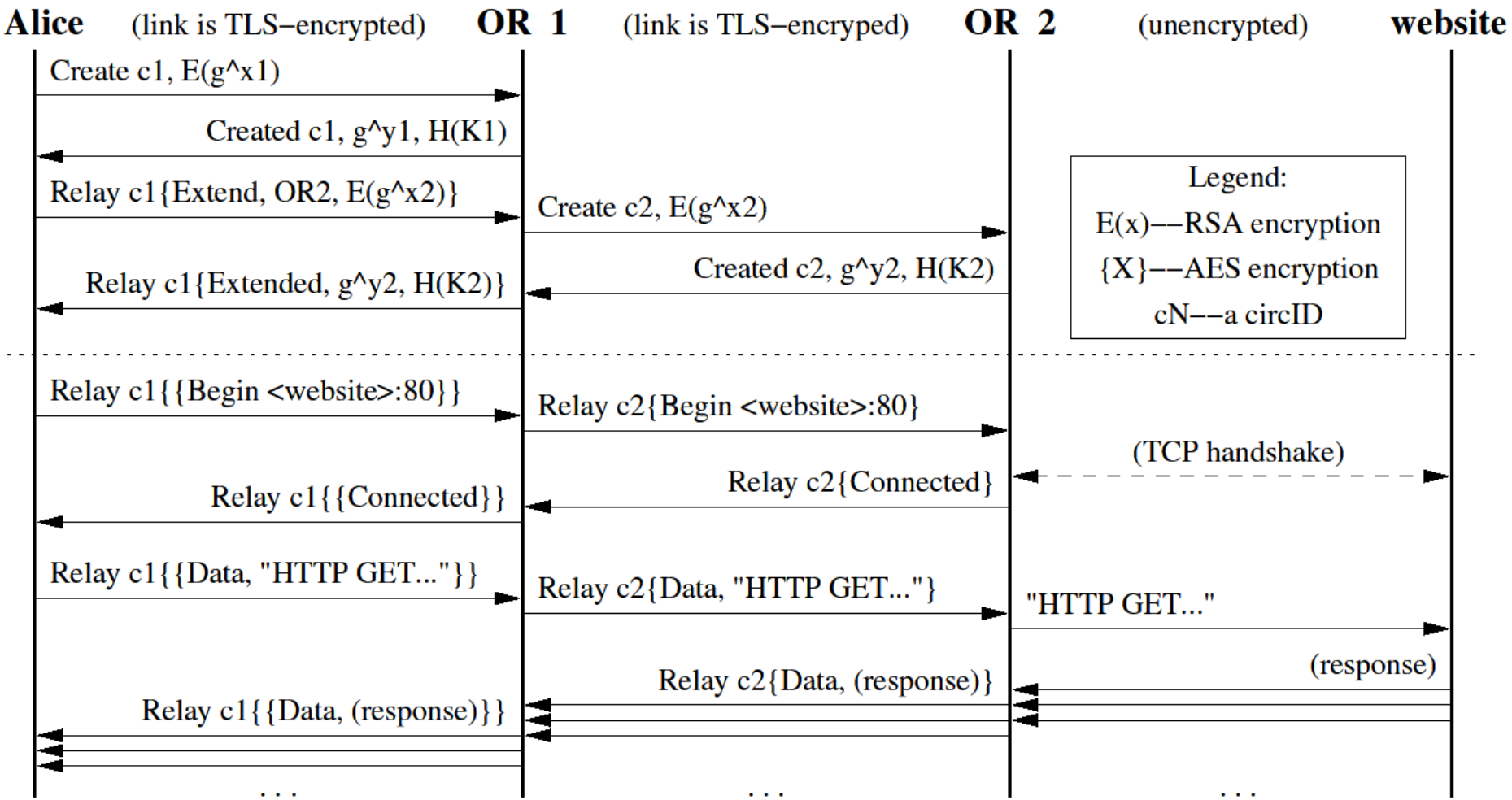
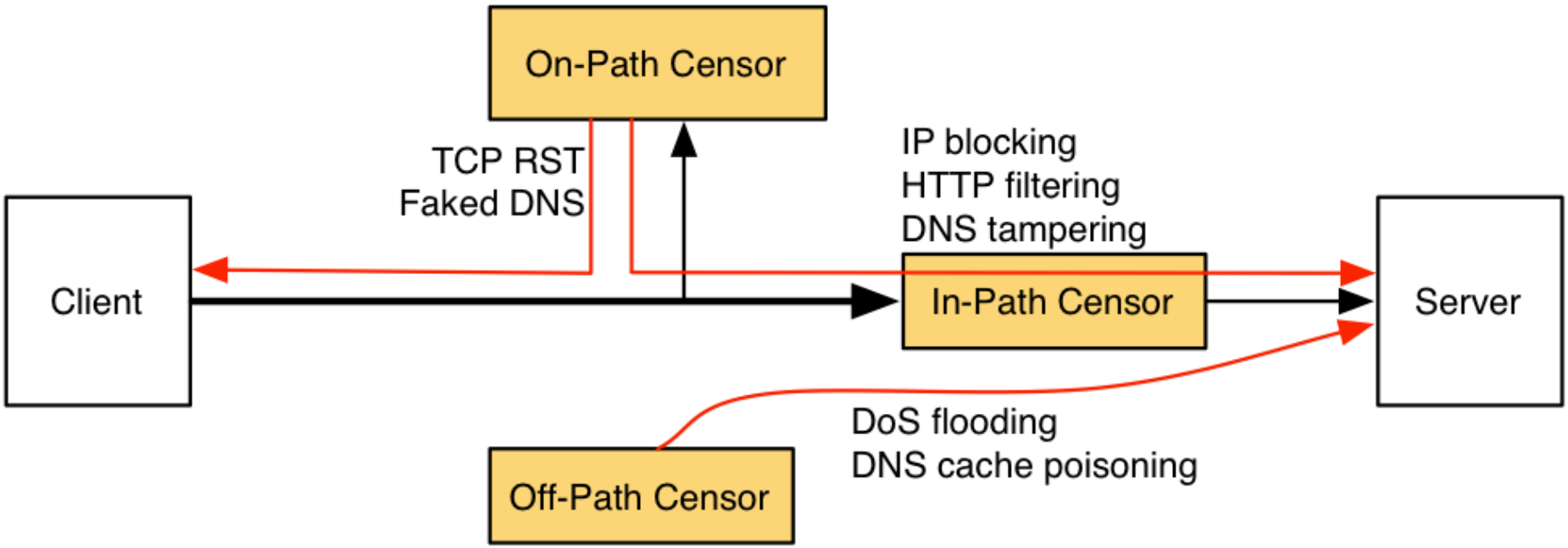


Fig. 1. Malicious exit router logging detection technique.

Nickname	Ban Type	IP	Port	Date	Reporter	Reason
⇉Unnamed	BadExit	176.99.12.246	9001	7/12/13	phw	SSL MITM with CN as main authority
⇉Unnamed	BadExit	109.68.190.231	9001	6/29/13	athena	SSL MITM with CN as main authority
⇉Unnamed	BadExit	176.99.10.92	9001	4/10/13	-----	SSL MITM
⇉Unnamed	BadExit	64.237.42.138	9001	3/1/13	-----	SSL MITM
⇉Unnamed	BadExit	141.101.238.182	9001	1/8/13	Pierre Richard	SSL MITM
⇉Unnamed	BadExit	46.30.42.154	9001	11/9/12	-----	SSL MITM with CN as main authority
⇉Unnamed	BadExit	46.30.42.153	9001	11/9/12	-----	SSL MITM with CN as main authority
⇉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


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

Identified Source	Signature
Identified Injector	
Sandvine	Multipacket: First Packet IPID += 4, second packet SEQ + 12503, IPID += 5
Bezeqint	Multipacket: Constant sequence, RST_ACK_CHANGE, IPID = 16448
Yournet	SYN_RST: Only on SMTP, TTL usually +3 to +5, unrelated IPID
Victoria	Multipacket: Sequence Increment 1500, IPID = 305, TTL += 38
IPID 256	Single packet: Usually less TTL, IPID = 256
IPID 64	Multipacket: IPID = 64, often sequence increment of 1460
IPID -26	Multipacket: First IPID -= 26, often sequence increment of 1460
SEQ 1460	Multipacket: Sequence increment always 1460
RAE	Single packet: Sets RST, ACK and ECN nonce sum (control bit 8)
Go Away	Single packet: Payload on RST of "Go Away, We're Not Home"
Optonline	Multipacket: No fingerprint, all activity from a single ISP
Identified Non-Injected Source	
SYN/RST 128	SYN_RST with RST TTL += 128
SYN/RST 65259	SYN_RST with RST IPID = 65259
0-Seq RST	Reset with SEQ = 0
IPID 0	IPID = 0, multiple RSTs, limited range
IPID 0 Solo	IPID = 0, spurious RST (often ignored)
Stale RST	RST belonging to a previous connection (port reuse)
Spambot SR	Spam source sending payload packets with SYN and RST flags
DNS SYN_RST	Normal DNS servers aborting connections at initiation

Table 1. Features for both identified RST injectors and identified non-injected sources.

Test	Evasion Class	Description	Circumvention Opportunities	Fixing Cost	Receiver Dependent?
IP1	Ambiguity	$_{IP(TTL=<low>)}p(Bad) \implies reset$	Insertion	High	
IP2	Reassembly	Overlapping fragment processing	Insertion	High	✓
TCP1	TCB creation	$_{IP(TTL=<low>)}p_i^S,\ p_{i+1}^S,\ p_{i+2}(Bad) \wedge (tuple(p_i) = tuple(p_{i+1})) \wedge (seq(p_i) \neq seq(p_{i+1})) \implies \neg\, reset$	Insertion-Evasion	Low	
TCP2	Incompleteness	$_{IP(ack=<bad>)}p(Bad) \implies reset$	Insertion	Low	
TCP3	Incompleteness	$_{IP(chksum=<bad>)}p(Bad) \implies reset$	Insertion	Low	
TCP4	Incompleteness	$p^{\neg A}(Bad) \implies reset$	Insertion	Low	
TCP5	Reassembly	Overlapping segment processing	Insertion	High	✓
TCP6[a]	TCB Teardown	$_{IP(TTL=<low>)}p_i^{R(A)}, p_{i+1}(Bad) \implies \neg\, reset$	Insertion-Evasion	High	
TCP6[b]	TCB Teardown	$_{IP(TTL=<low>)}\ p_i^F, p_{i+1}(Bad) \implies \neg\, reset$	Insertion-Evasion	Low	
TCP7	State Management	$\tau(\leq\ \approx 10\text{ hr}), p_i(Bad) \implies reset$	State exhaust.	High	
TCP8	State Management	$(p_i(Good)^+ \wedge \delta(Good) \leq\ \approx 1\text{ GB}), p_{i+1}(Bad) \implies reset$	State exhaust.	High	
TCP9	State Management	$hole,\ (p_i(Good)^+ \wedge \delta(Good) \geq 1\ \text{KB} \wedge abovehole(p_i)), p_{i+1}(Bad) \implies \neg reset$	State exhaust.	High	✓
TCP10	State Management	$hole, \tau(y) \geq 60\text{ min}, (p_i(Bad) \wedge abovehole(p_i)) \implies \neg reset$	State exhaust.	High	✓
HTTP1	Ambiguity	GET with >1 space between method and URI $\implies \neg\, reset$	Evasion	Low	
HTTP2	Incompleteness	GET with keyword at location $>2048 \implies \neg\, reset$	Evasion	Low	
HTTP3	Incompleteness	GET with keyword in $\geq$ 2nd of multiple requests in single segment $\implies \neg\, reset$	Evasion	Low	
HTTP4	Incompleteness	GET with URL encoded (except %-encoding) $\implies \neg\, reset$	Evasion	Low	✓

Table 1: Evasion opportunities in GFW's analysis of network traffic.