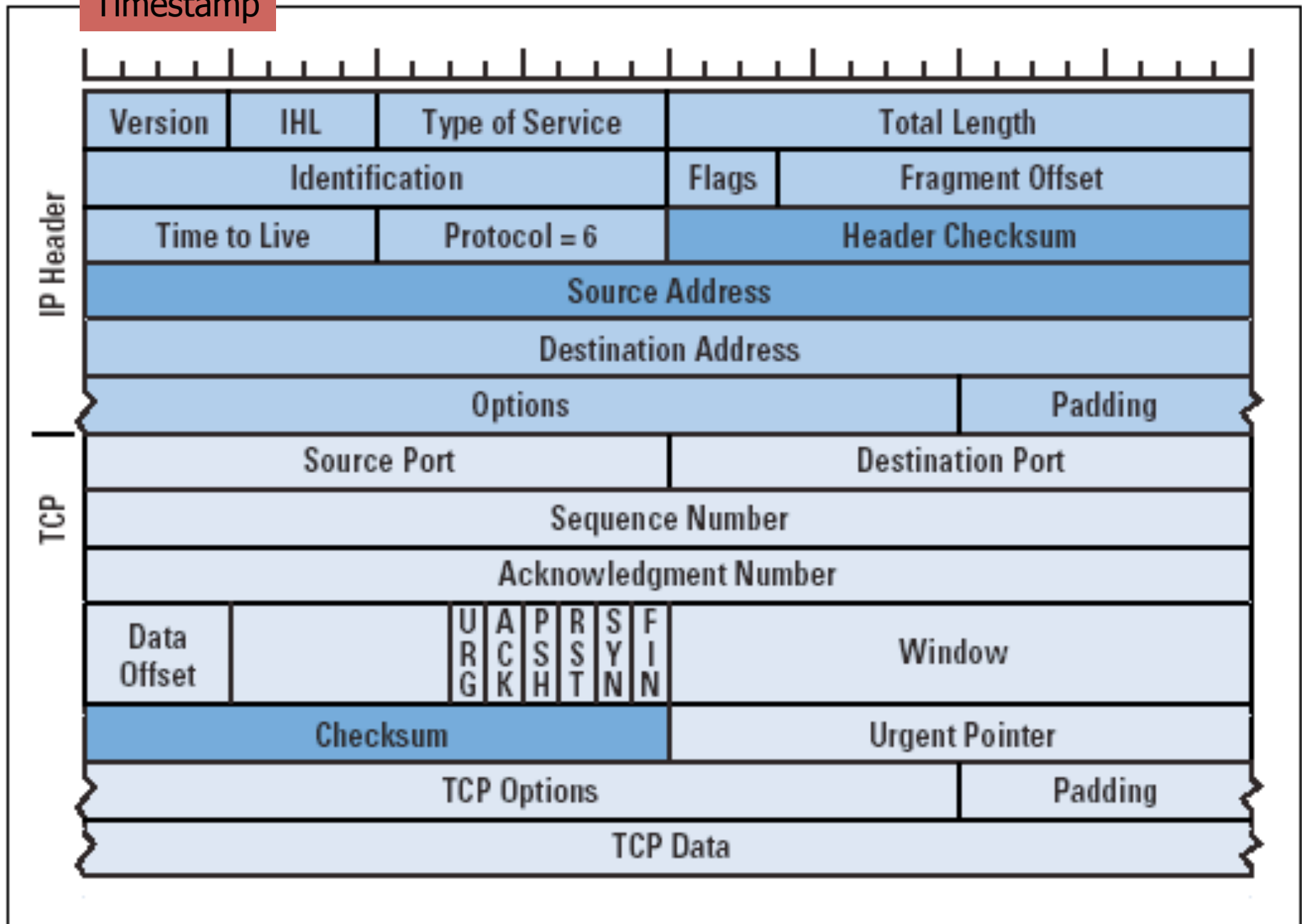
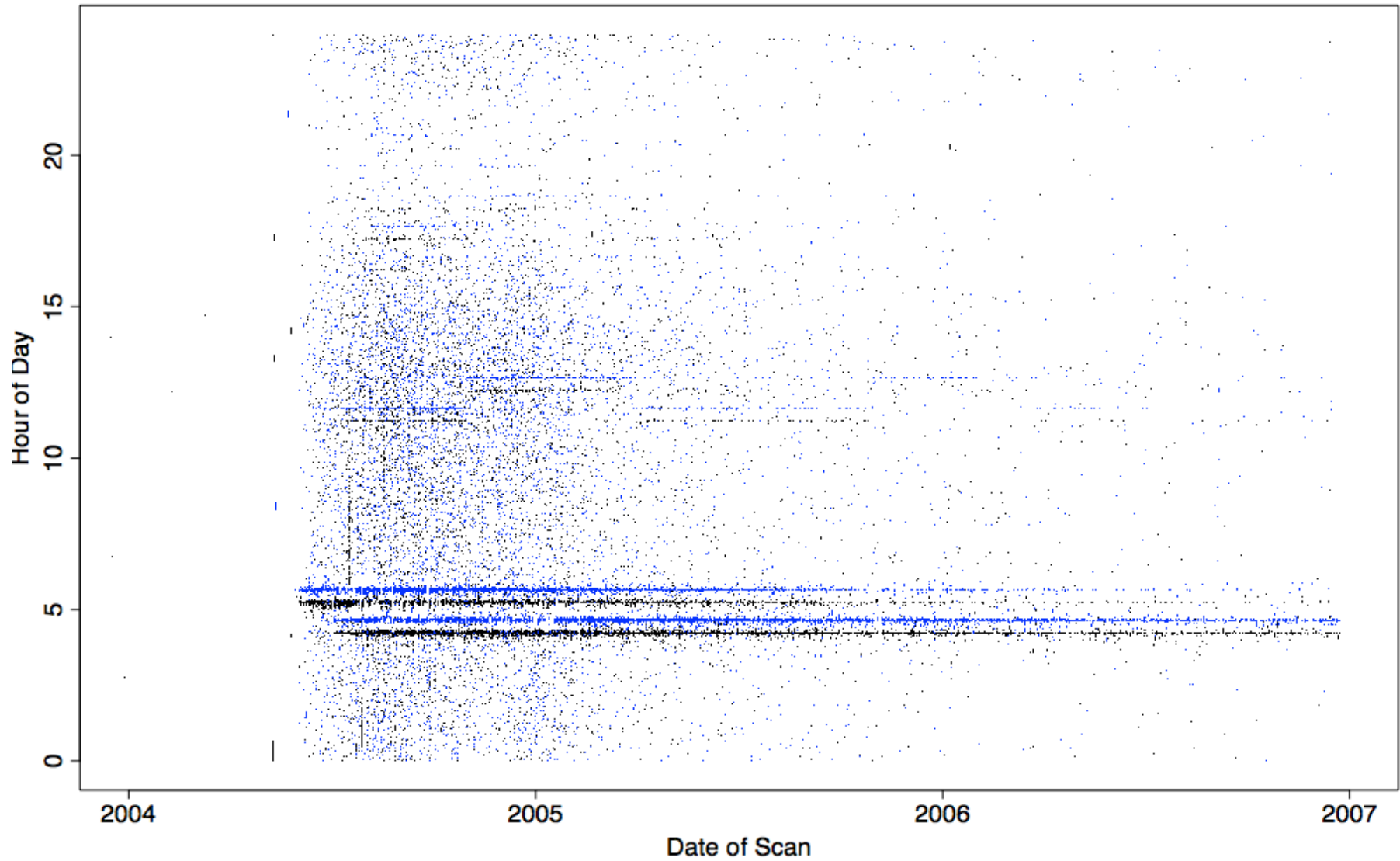


Timestamp

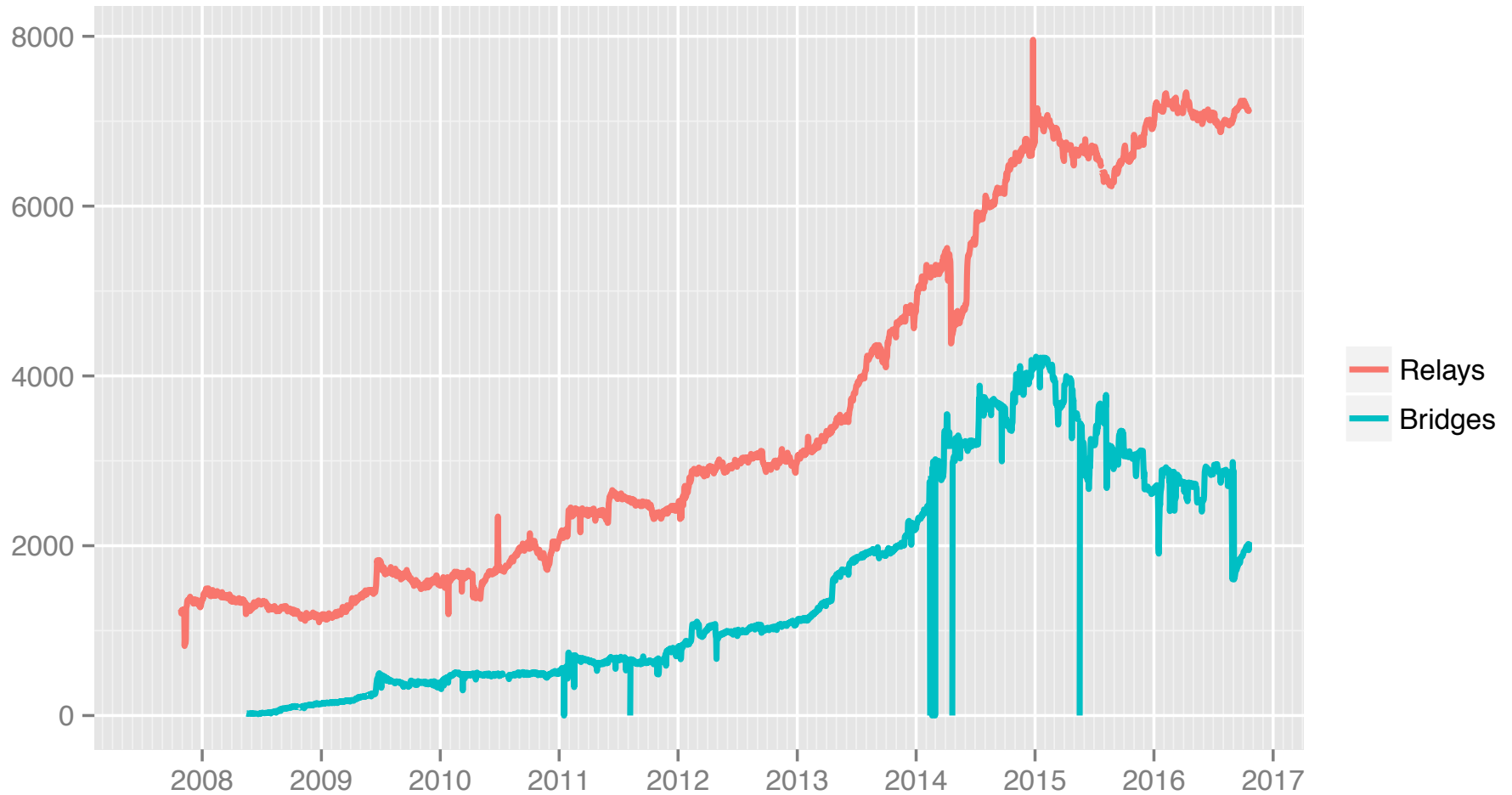


Daily Patterns Seen in 1023/TCP Scans



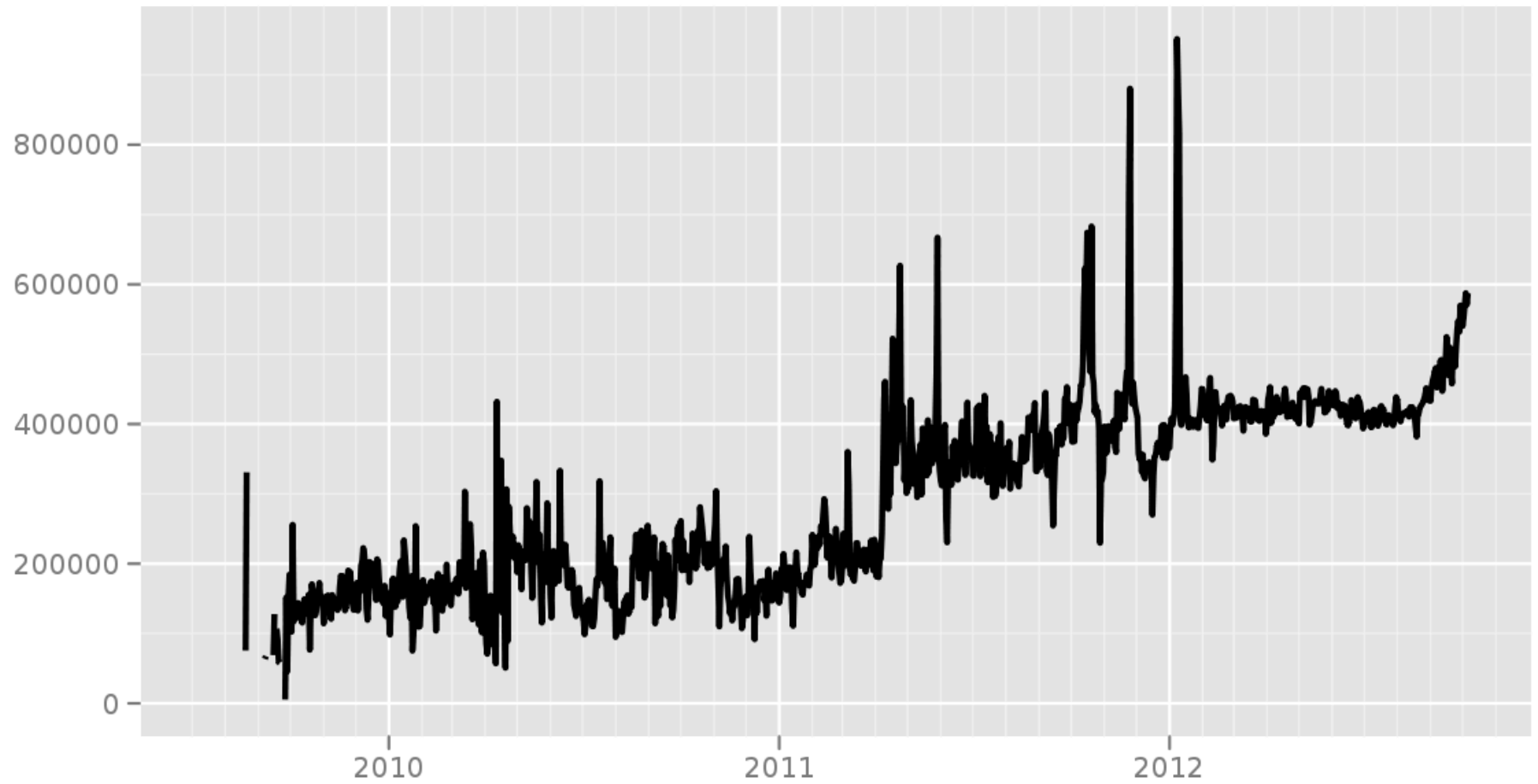
/16 at LBL, sampled 1-in-1K
2nd /16, sampled 1-in-1K

Number of relays



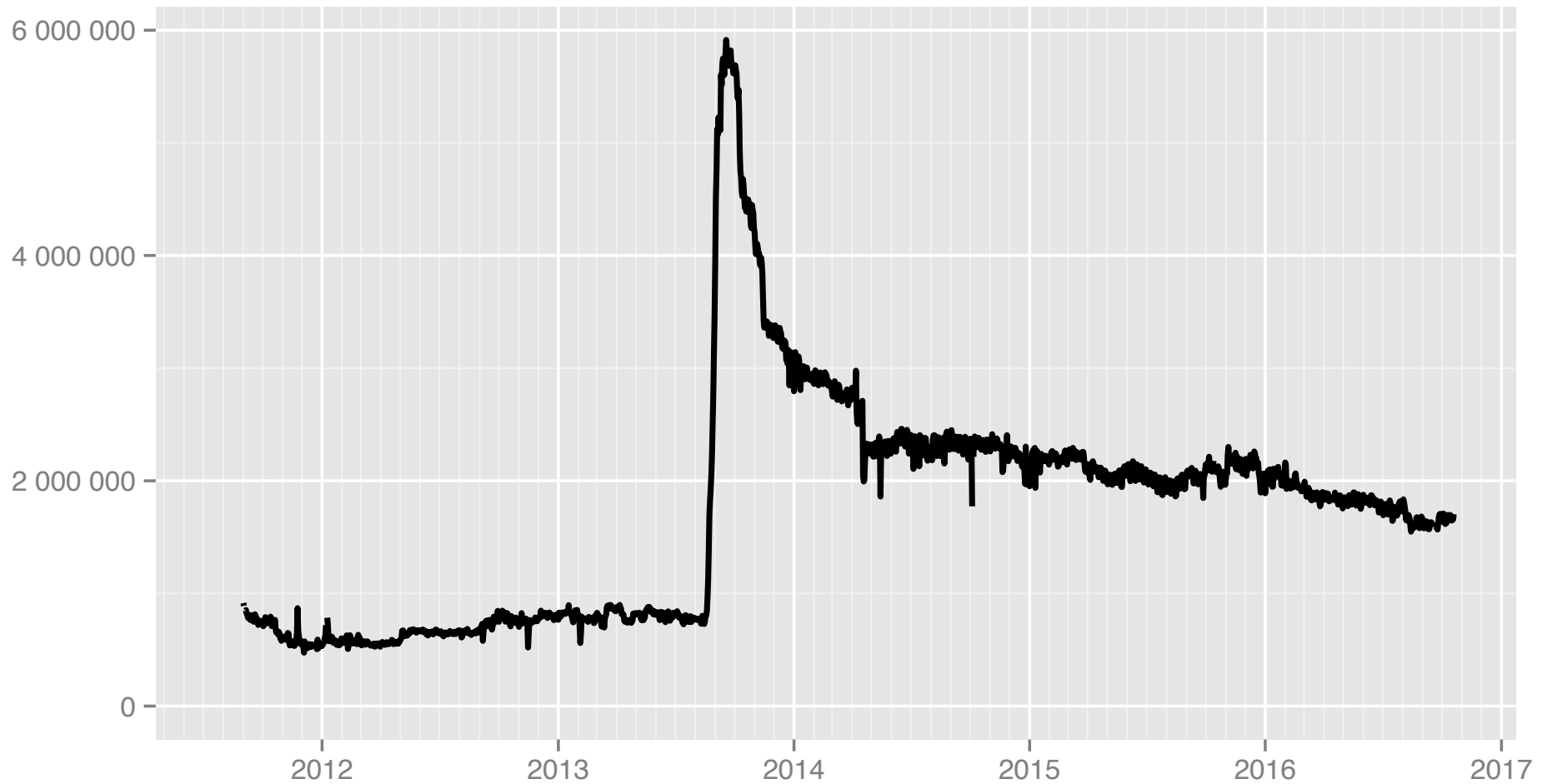
The Tor Project – <https://metrics.torproject.org/>

Directly connecting users from all countries



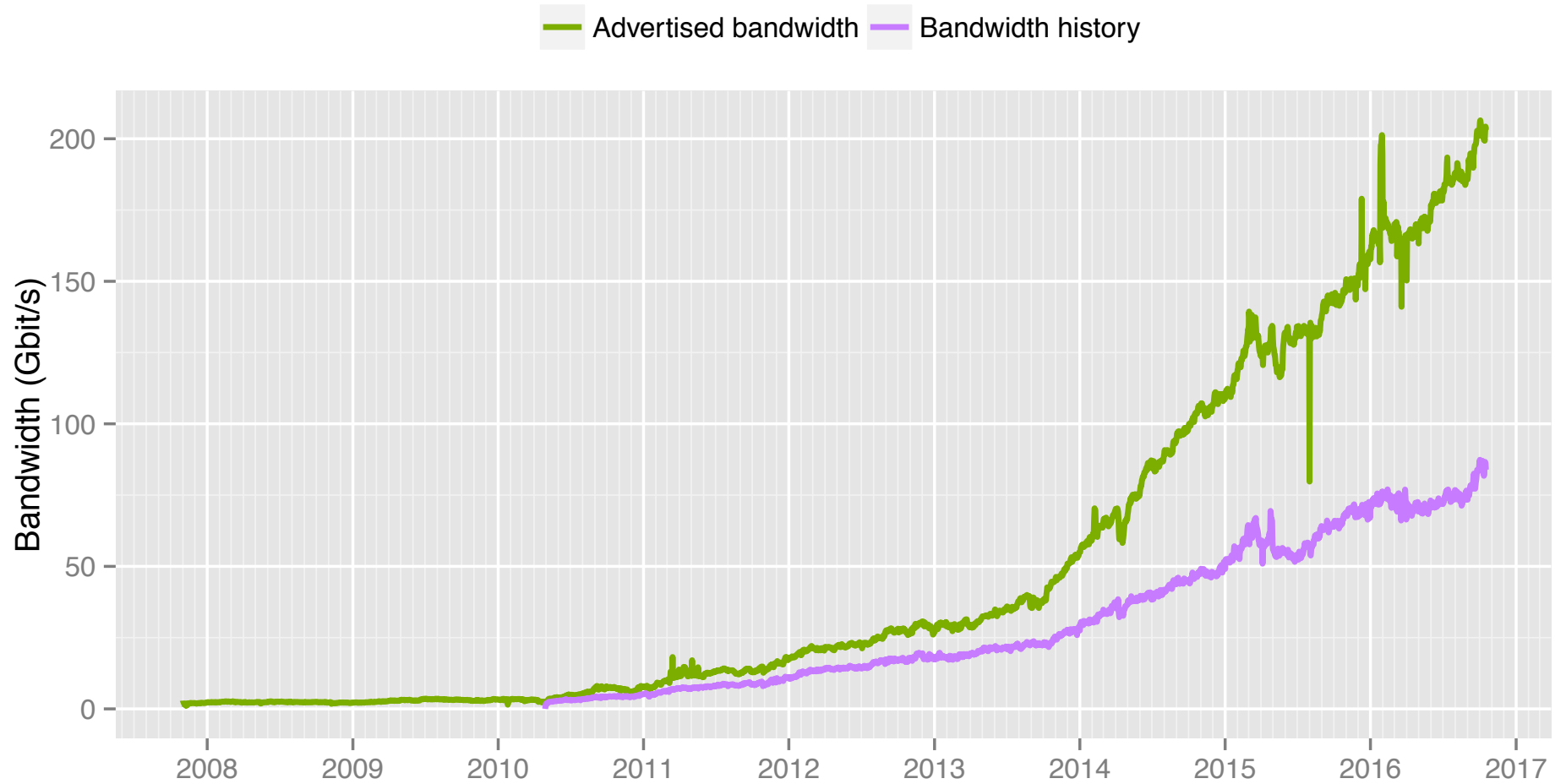
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users



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

Total relay bandwidth



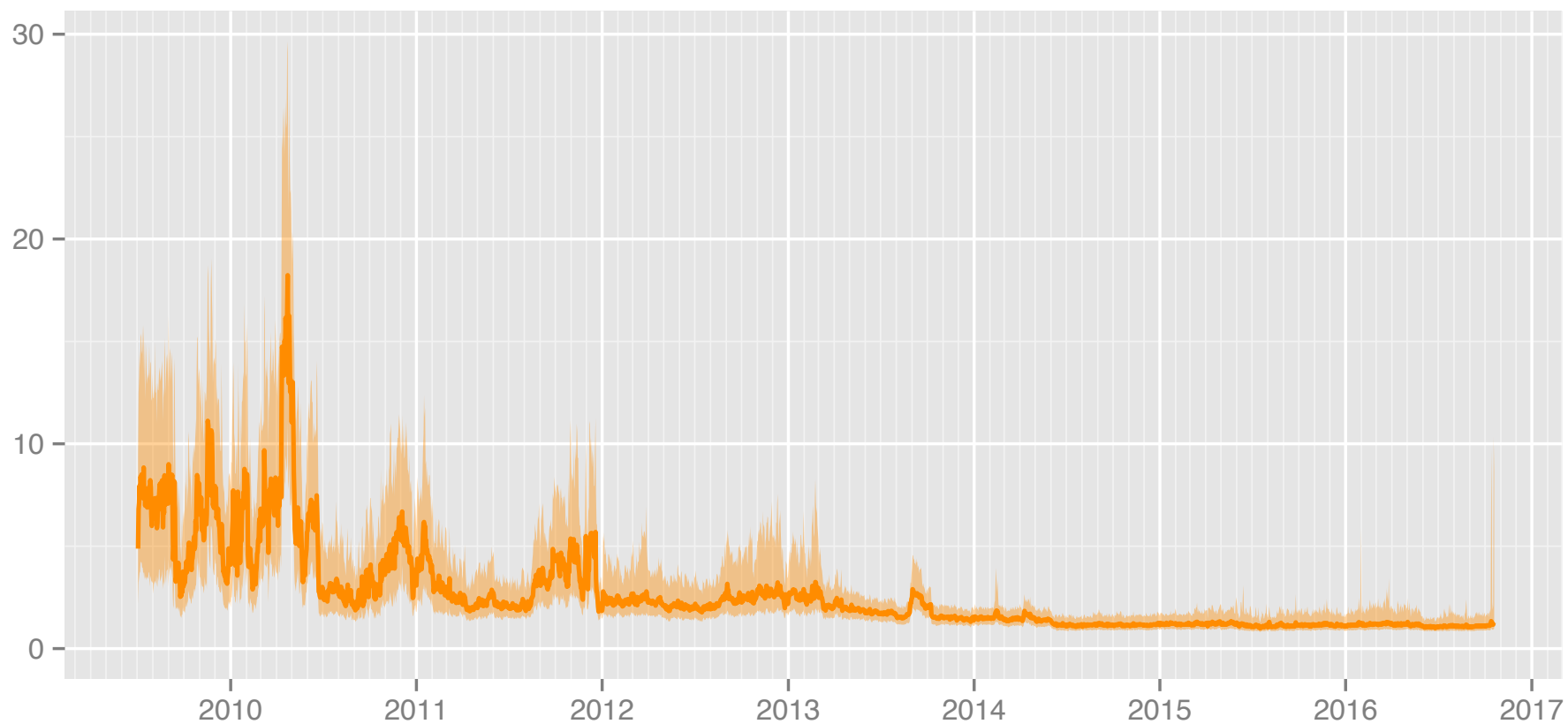
The Tor Project – <https://metrics.torproject.org/>

Time in seconds to complete 50 KiB request

Measured times on all sources per day

Median

1st to 3rd quartile



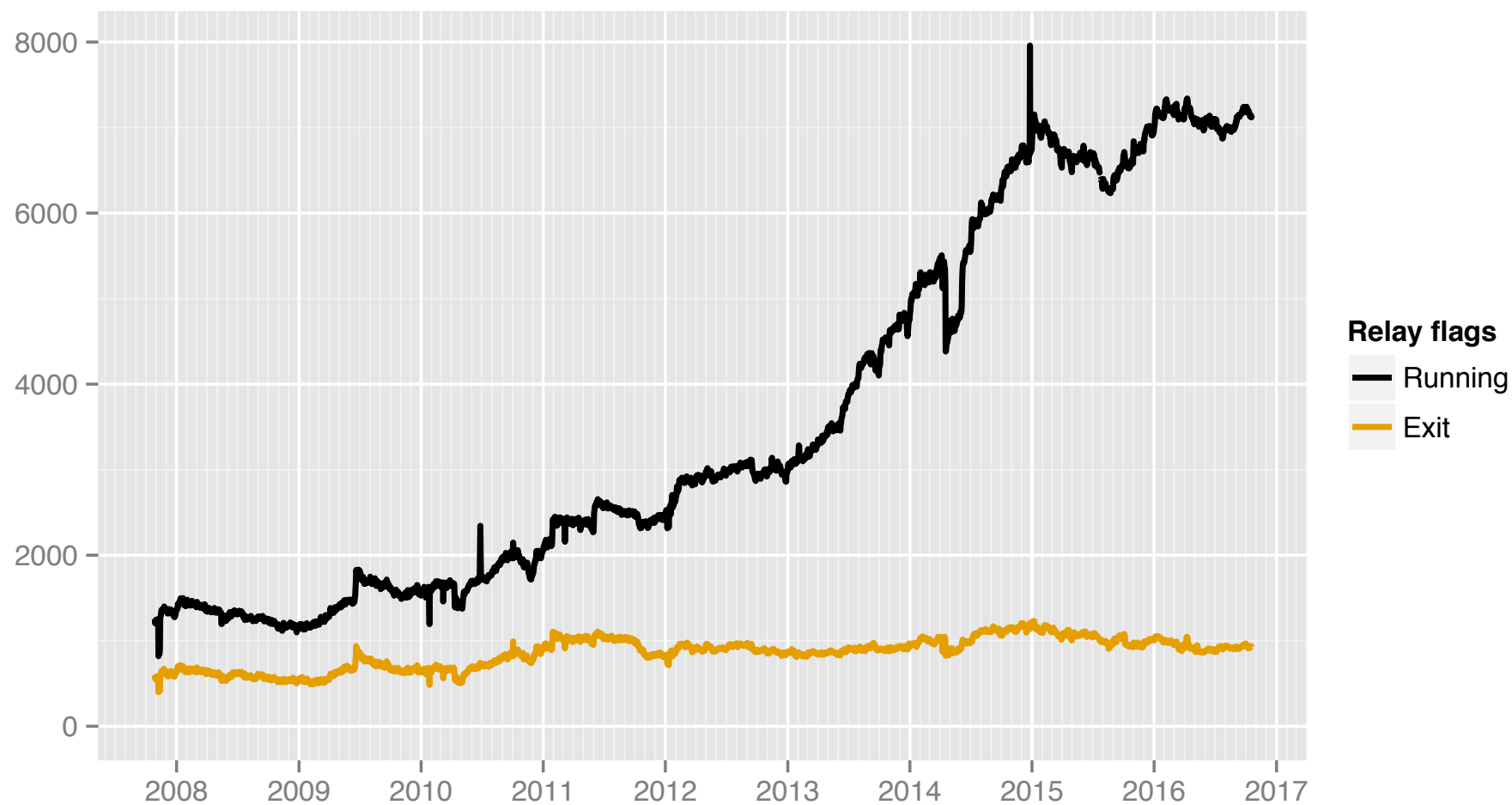
The Tor Project – <https://metrics.torproject.org/>

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)

Number of relays with relay flags assigned



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

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.

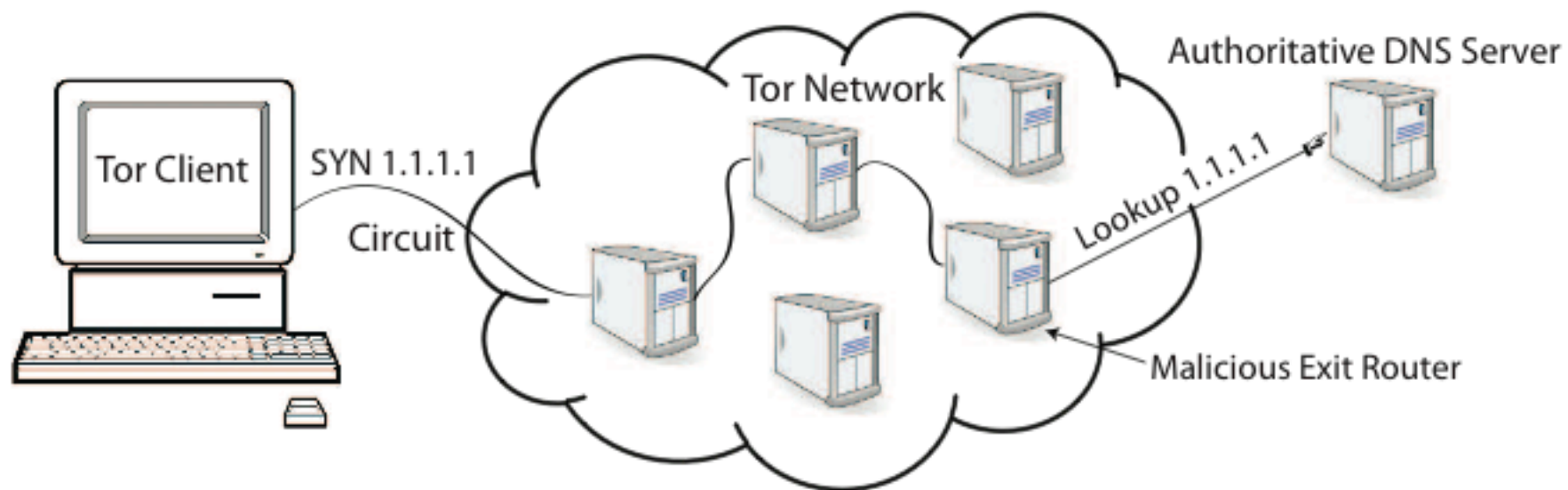


Fig. 1. Malicious exit router logging detection technique.

Nickname	Ban Type	IP	Port	Date	Reporter	Reason
⇒Unamed	BadExit	176.99.12.246	9001	7/12/13	phw	SSL MITM with CN as main authority
⇒Unamed	BadExit	109.68.190.231	9001	6/29/13	athena	SSL MITM with CN as main authority
⇒Unamed	BadExit	176.99.10.92	9001	4/10/13	-----	SSL MITM
⇒Unamed	BadExit	64.237.42.138	9001	3/1/13	-----	SSL MITM
⇒Unamed	BadExit	141.101.238.182	9001	1/8/13	Pierre Richard	SSL MITM
⇒Unamed	BadExit	46.30.42.154	9001	11/9/12	-----	SSL MITM with CN as main authority
⇒Unamed	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
⇒Unamed	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
⇒Unamed	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
⇒Unamed	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
⇒Unamed	BadExit	118.160.19.236	443	11/19/10	mikeperry	anti-virus filter is blocking sites (trend-micro)
⇒Unamed	BadExit	---	---	11/19/10	mikeperry	anti-virus filter is blocking sites (trend-micro)
⇒Unamed	BadExit	---	---	11/19/10	mikeperry	anti-virus filter is blocking sites (trend-micro)
⇒Unamed	BadExit	---	---	11/19/10	mikeperry	anti-virus filter is blocking sites (trend-micro)
⇒Unamed	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

Diffie-Hellman Exchange

Well-known: g, p

Secret: x, y

$A \rightarrow E \rightarrow B: g^x \bmod p$

$B \rightarrow E \rightarrow A: g^y \bmod p$

Derived key: g^{xy}

Tor DHE

Well-known: g, p

Secret: x, y

$A \rightarrow M \rightarrow B$: $E_B(g^x \bmod p)$

$B \rightarrow M \rightarrow A$: $g^y \bmod p, \text{Hash}(K=g^{xy})$

Derived key: g^{xy}

Tor DHE: Mallory Attacks?

Well-known: g, p

Secret: x, y

$A \rightarrow M: E_B(g^x \bmod p)$

$M \rightarrow B: E_B(g^{x'} \bmod p)$

$B \rightarrow M: g^y \bmod p, \text{Hash}(K=g^{x'y})$

$M \rightarrow A: g^{y'} \bmod p, \text{Hash}(K=g^{?})$

Derived key: $g^{xy} ? g^{x'y} ? g^{xy'} ? g^{x'y'} ?$

Tor DHE: Mallory Attacks!

Well-known: g, p

Secret: x, y ; $x' = y' = 0$

$A \rightarrow M$: $E_B(g^x \bmod p)$

$M \rightarrow B$: $E_B(g^{x'} \bmod p) = E_B(g^0 \bmod p) = E_B(1 \bmod p)$

$B \rightarrow M$: $g^y \bmod p$, $\text{Hash}(K = g^{x'y}) = \text{Hash}(g^0) = \text{Hash}(1)$

$M \rightarrow A$: $g^{y'} \bmod p = 1 \bmod p$, $\text{Hash}(K = 1)$

Derived key: g^{xy} ? $g^{x'y} = g^{xy'} = g^{x'y'} = 1$

Tor DHE Fixed

Well-known: g, p

Secret: x, y

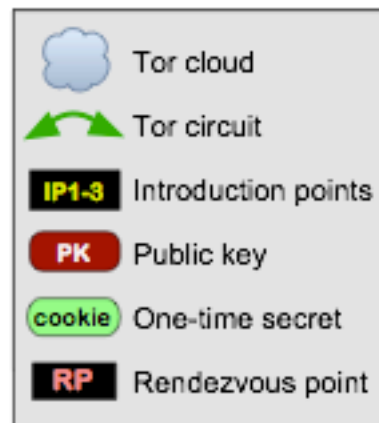
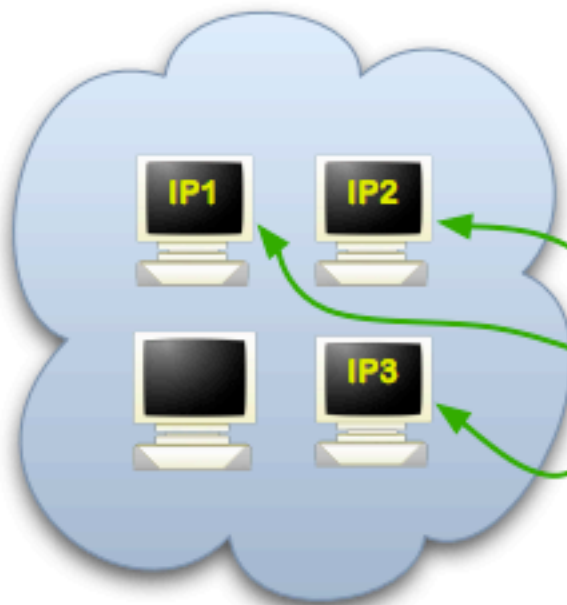
$A \rightarrow M \rightarrow B$: $E_B(g^x \bmod p)$

$B \rightarrow M \rightarrow A$: $g^y \bmod p$, $\text{Hash}(g^x \parallel g^y \parallel K = g^{xy})$

Derived key: g^{xy}

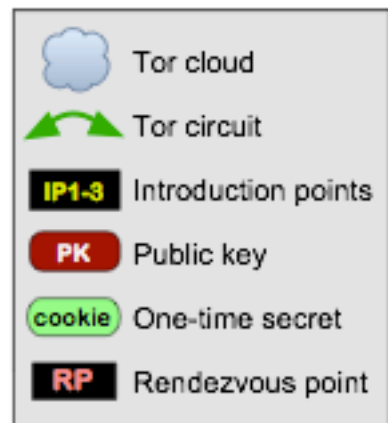
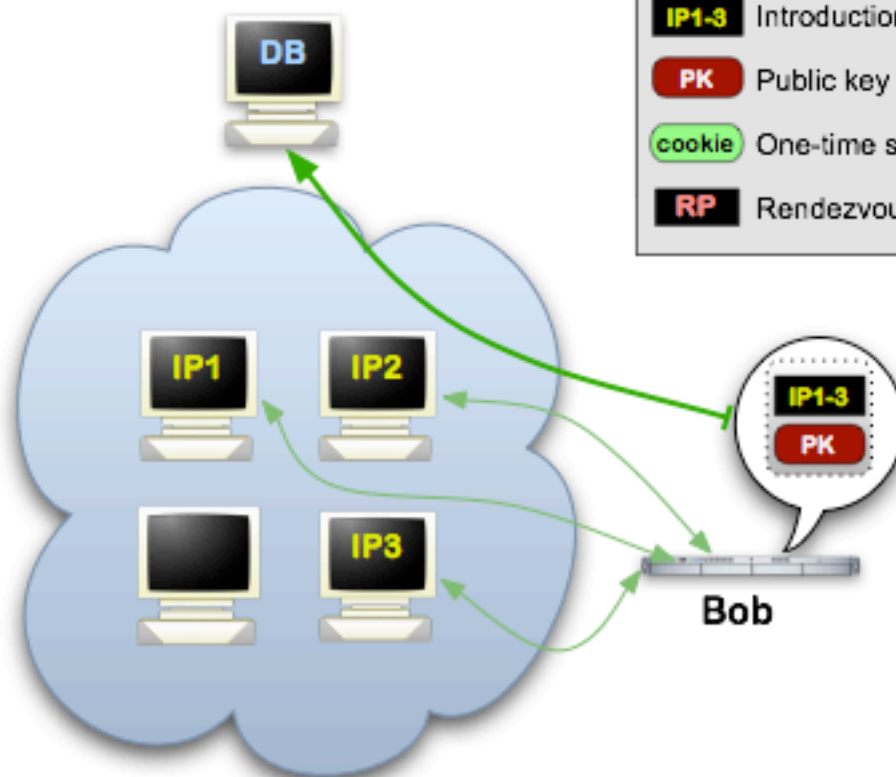
Tor Hidden Services: 1

Step 1: Bob picks some introduction points and builds circuits to them.



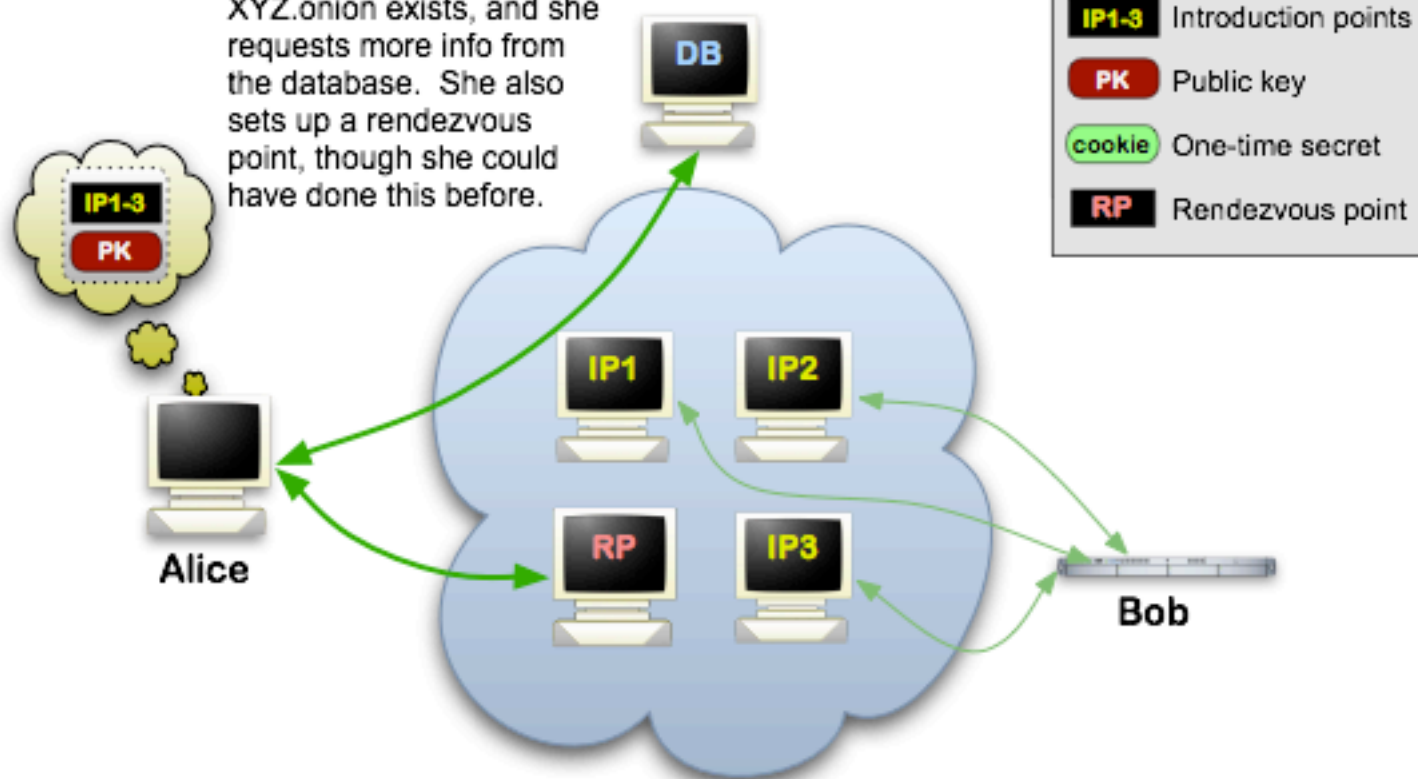
Tor Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



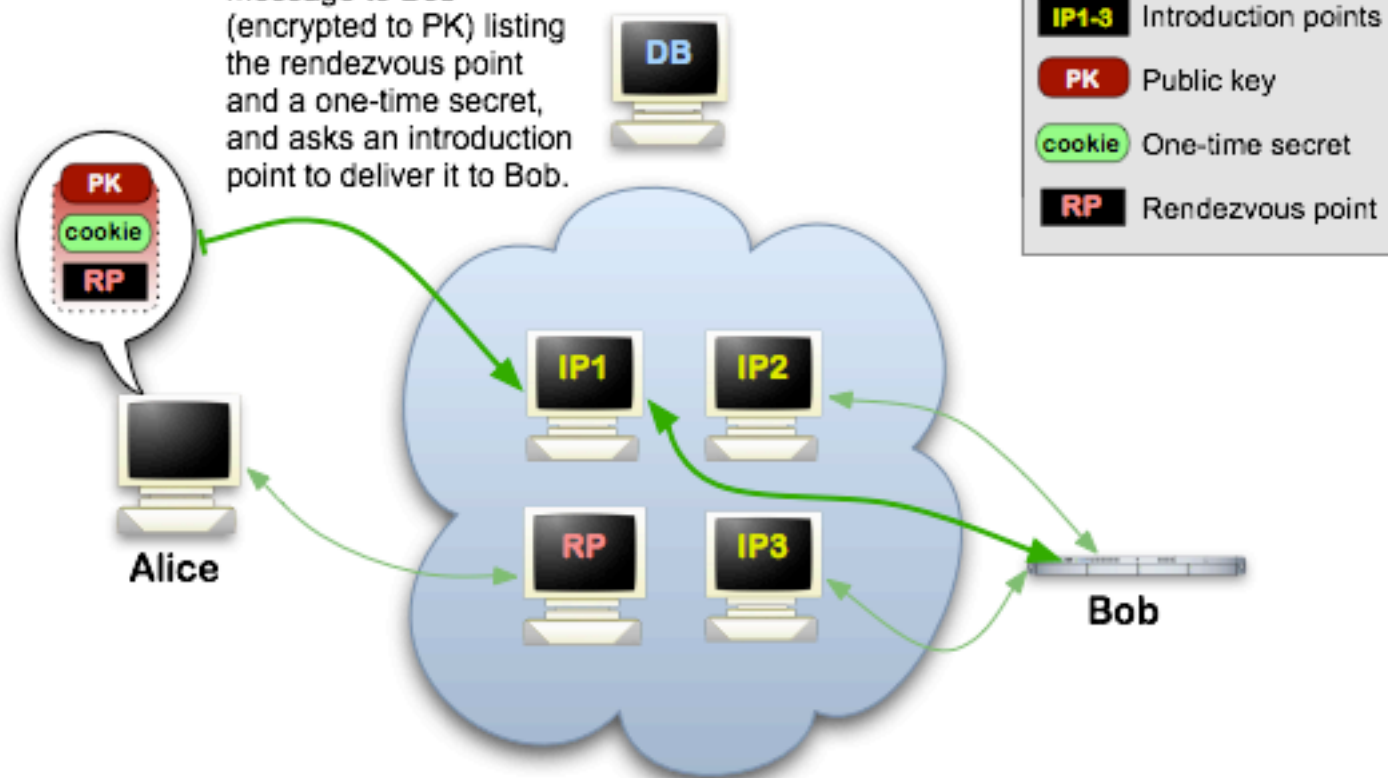
Tor Hidden Services: 3

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



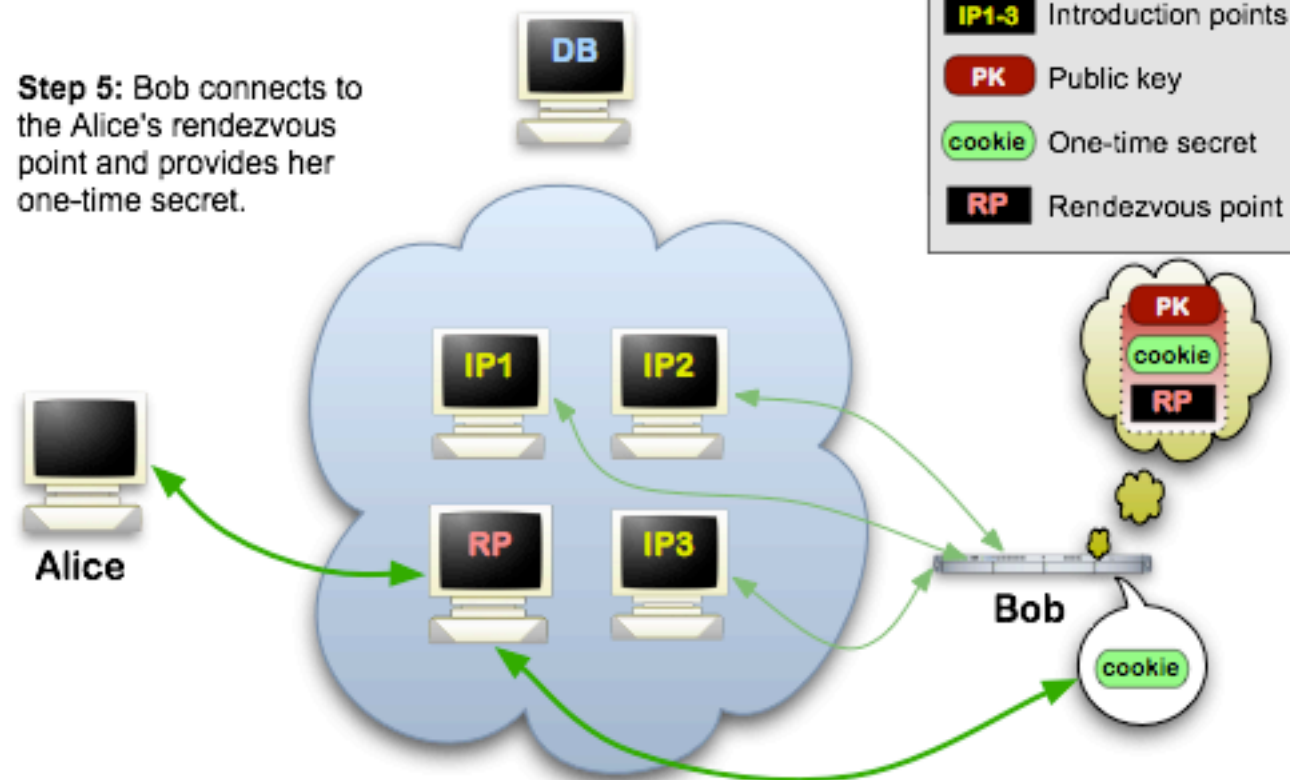
Tor Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Tor Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.

