Relay statuses

Relay locations

| Client Distribution		Router Distribution			Relative Tor Usage	
Country	Total	Country	Total		Country	Ratio
Germany	2,304	Germany	374		Germany	7.73
China	988	United States	326		Turkey	2.47
United States	864	France	69		Italy	1.37
Italy	254	China	40		Russia	0.89
Turkey	221	Italy	36		China	0.84
United Kingdom	170	Netherlands	35		France	0.77
Japan	155	Sweden	35		United Kingdom	0.75
France	150	Finland	25		United States	0.62
Russia	146	Austria	24		Brazil	0.56
Brazil	134	United Kingdom	24		Japan	0.32
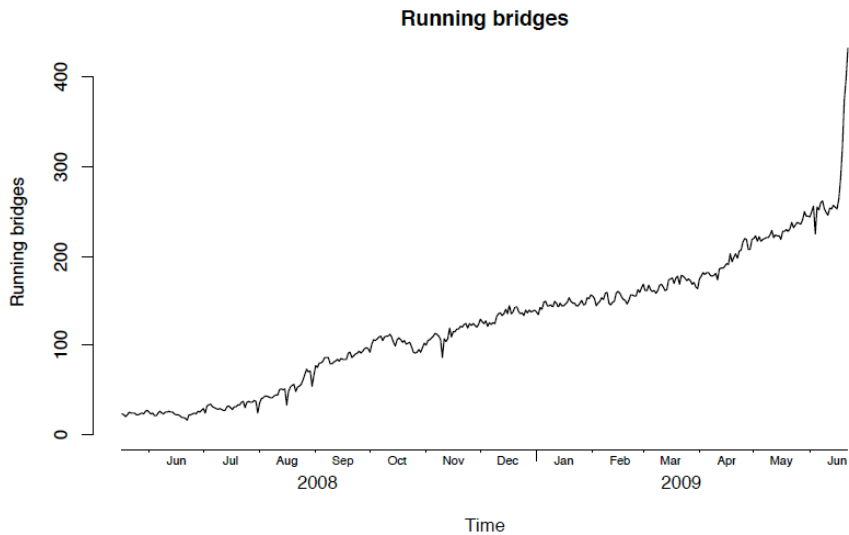
Figure 1: Running bridges between May 16, 2009 and June 21, 2009. The graph shows clearly that the number of bridges increases continuously over time with a significant increase in June 2009, probably as a result of the Iranian elections.

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.

WIRED   SUBSCRIBE »   SECTIONS »   BLOGS »   REVIEWS »   VIDEO »   HO

Sign In | RSS F

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.

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

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

509 bytes

2	1	
CircID	CMD	DATA

2	1	2	6	2	1	498
CircID	Relay	StreamID	Digest	Len	CMD	DATA

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)

Relay c1{Extended, g^y2, H(K2)}   Created c2, 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 c1{{Connected}}   Relay c2{Connected}

Relay c1{{Data, "HTTP GET..."}}   Relay c2{Data, "HTTP GET..."}   "HTTP GET..."

(response)

Relay c2{Data, (response)}

Relay c1{{Data, (response)}}

. . .   .