Running Tor exits and handling abuse@

Johan Nilsson

DFRI - Föreningen för digitala fri- och rättigheter

sec-heads, Linköping 2013-02-12

Outline

What is a Tor exit node?

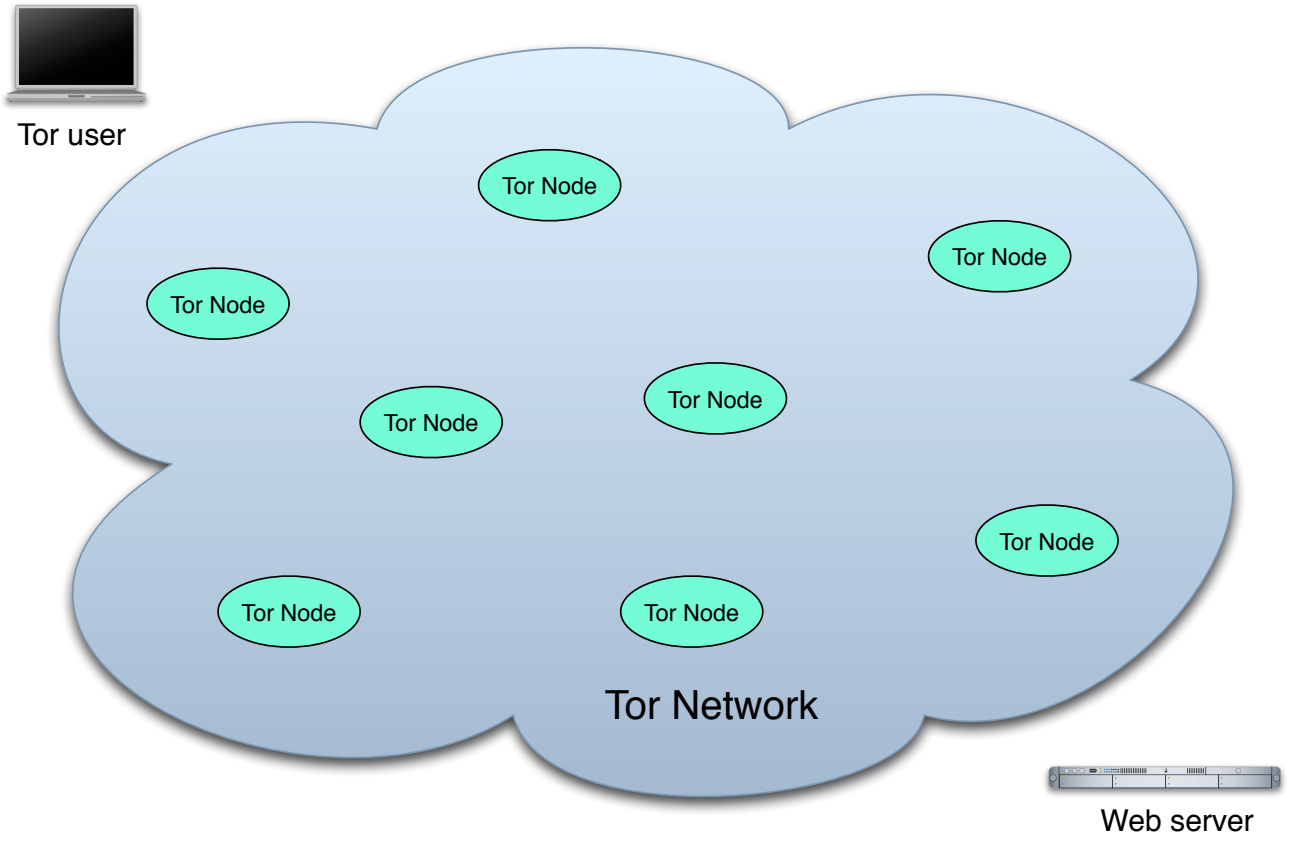


Diagram: Robert Watson

What is a Tor exit node?

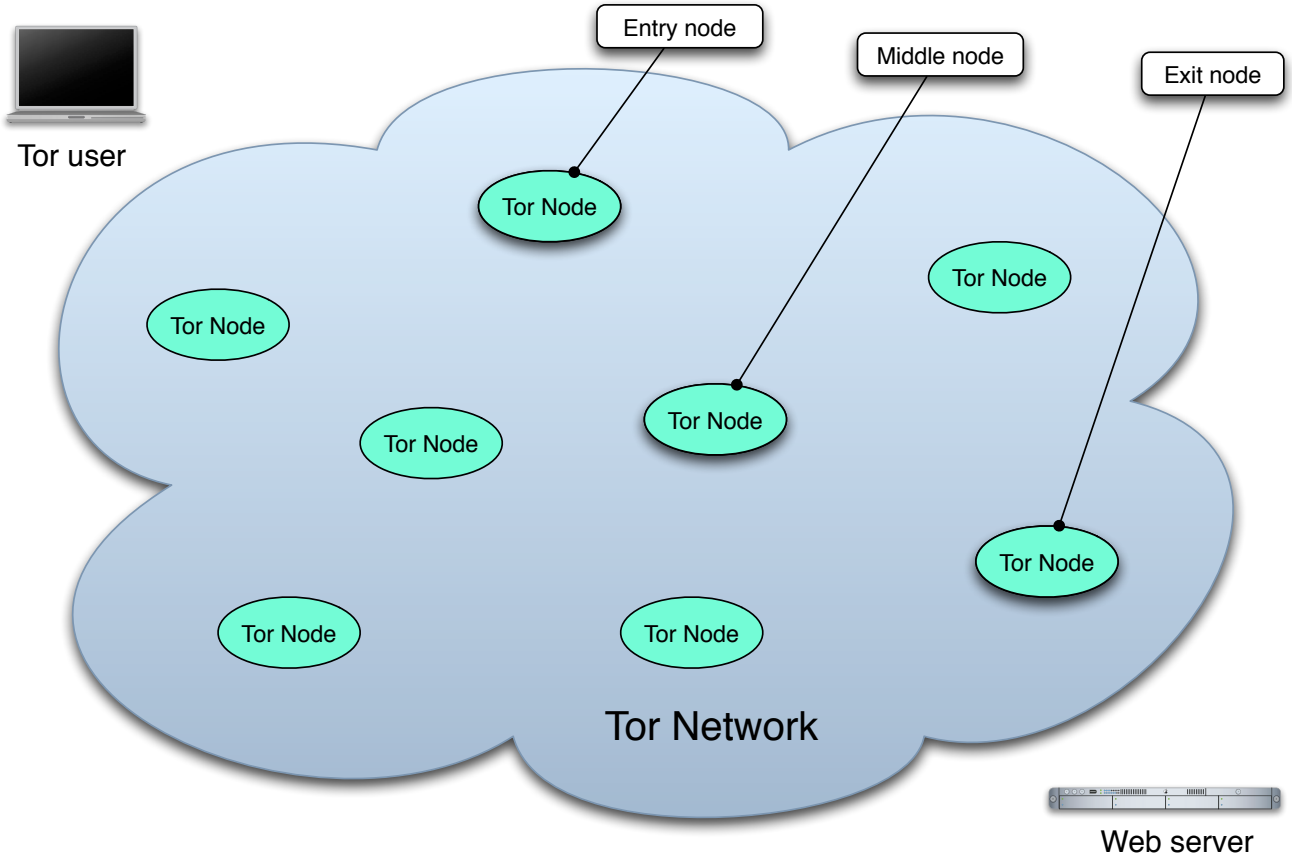


Diagram: Robert Watson

What is a Tor exit node?

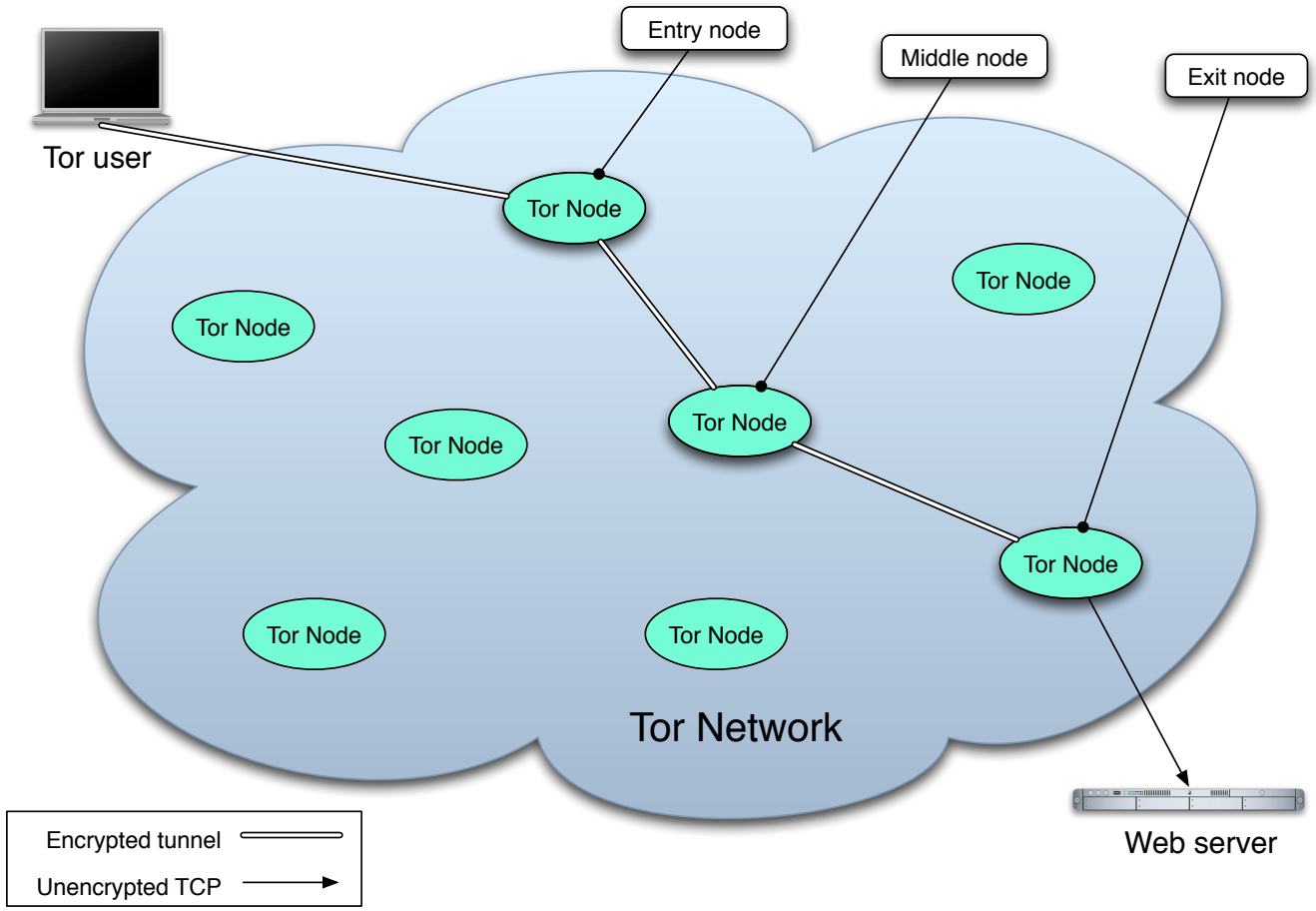


Diagram: Robert Watson

My history as an exit operator

- 200X - Rented servers outside Sweden.
- May 2010 - Helped starting torservers.net
- July 2011 - DFRI founded to run a Tor exit

Tips for Running an Exit Node
with Minimal Harassment (1/2)

- Inform your potential ISP(s)
  - or create a new. ASN 198093
- Get a separate IP for the node. Do not route your own traffic via this IP
- Get recognizable Reverse DNS for this IP
  - 171.25.193.20 resolves to tor-exit0-readme.dfri.se.
- Set up a Tor Exit Notice
  - `http://171.25.193.20/`
- Get RIPE/ARIN/... registration (if possible)
  - whois 171.25.193.0/24

:DFRI

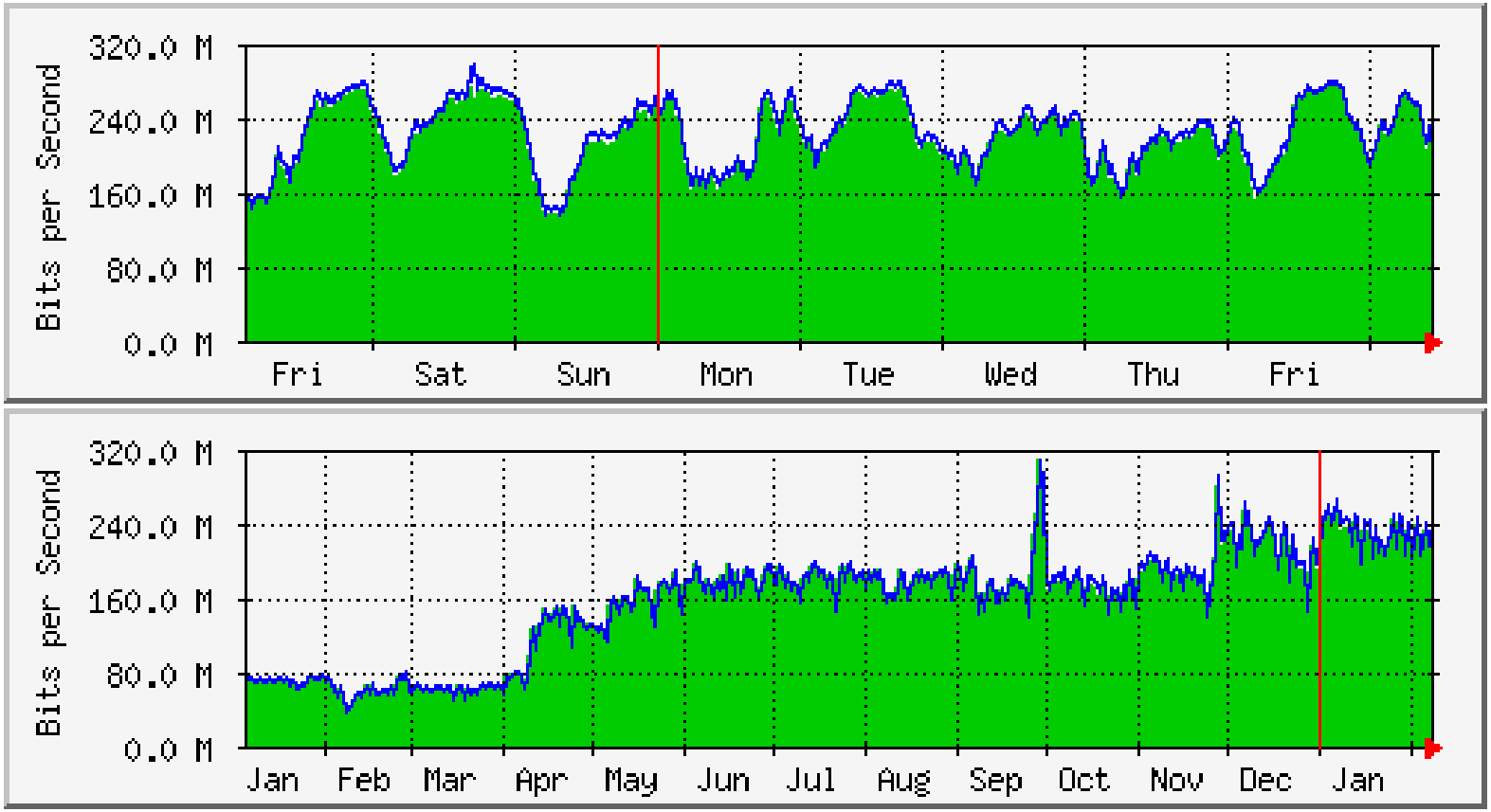
Tips for Running an Exit Node
with Minimal Harassment (2/2)

- Consider a Reduced Exit Policy
  - https://trac.torproject.org/projects/tor/wiki/doc/ReducedExitPolicy
- Consider creating a corporate entity to run your node
  - Föreningen för digitala fri- och rättigheter, 802461-0852
- https://blog.torproject.org/running-exit-node

:DFRI

DFRI Tor exit traffic

Now and the past year



Abuse complaints 2013

- Mail sent to abuse@dfri.net is read by the NOC of DFRI

Only three complaints and 16 spam so far this year

- 2013-01-09 Spam complaint from UOL
- 2013-01-11 2x Compromised IP address

Types of abuse complaints since 2011

- spam
- web scraping
- DOS/DDOS
- hacking/cracking/scans

web mail/blog spam/USENET/forums

Spam sent by web mail.

- Received: from 171.25.193.20 ([171.25.193.20]) by mail.inbox.lv with HTTP;

```
Hey,

It's the holiday season and I want to give
something special to you...

Click Here Now
```

Abuse from Yahoo mail

Last 20 days I have been receiving some abondoned mails from a yahoo mail account. When I check the details of IP traffic, I realized that he/she were using TOR in order to give wrong IP address details in mail logs. This case is very serious and urgent for me and for my family. I would like to get actual IP numbers to find who is doing this and why..

USENET spam from Google groups

Subject: Ongoing, repetitive, flooding and abuse on Usenet newsgroup ba.broadcast from your site

> *This is some voluminous, off-topic flooding and harassment on the ba.broadcast Usenet newsgroup...*

Honeypot and other reports

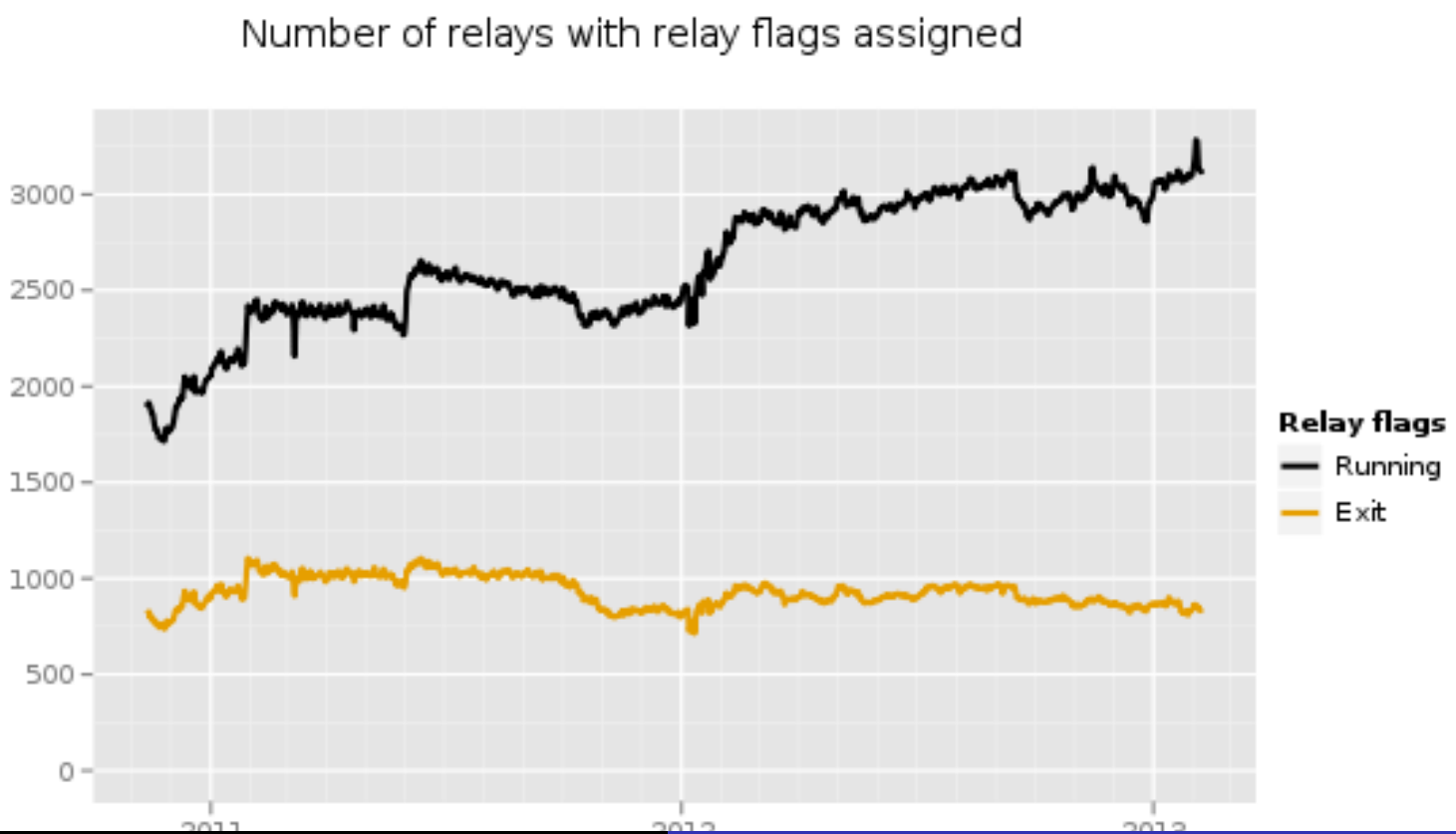
- Lots of mail reports about spam on forums and blogs from `https://www.blocklist.de`.
- BUT they started to keep track of Tor exits.
- Opererators can now opt-out.

Web scraping report

We noticed something that resembles a RIP attempt from one of your IP addresses. Our system temporarily blocked the IP address. Please, contact the respective user. In case that there is a need for Icecat content download, they can register and make use of our legal (xml) download interface http://icecat.biz/en/menu/services/index.htm. In case that the IP is used for search engine crawling, the user can inform us to whitelist the respective IP addresss. 100 requests during period...

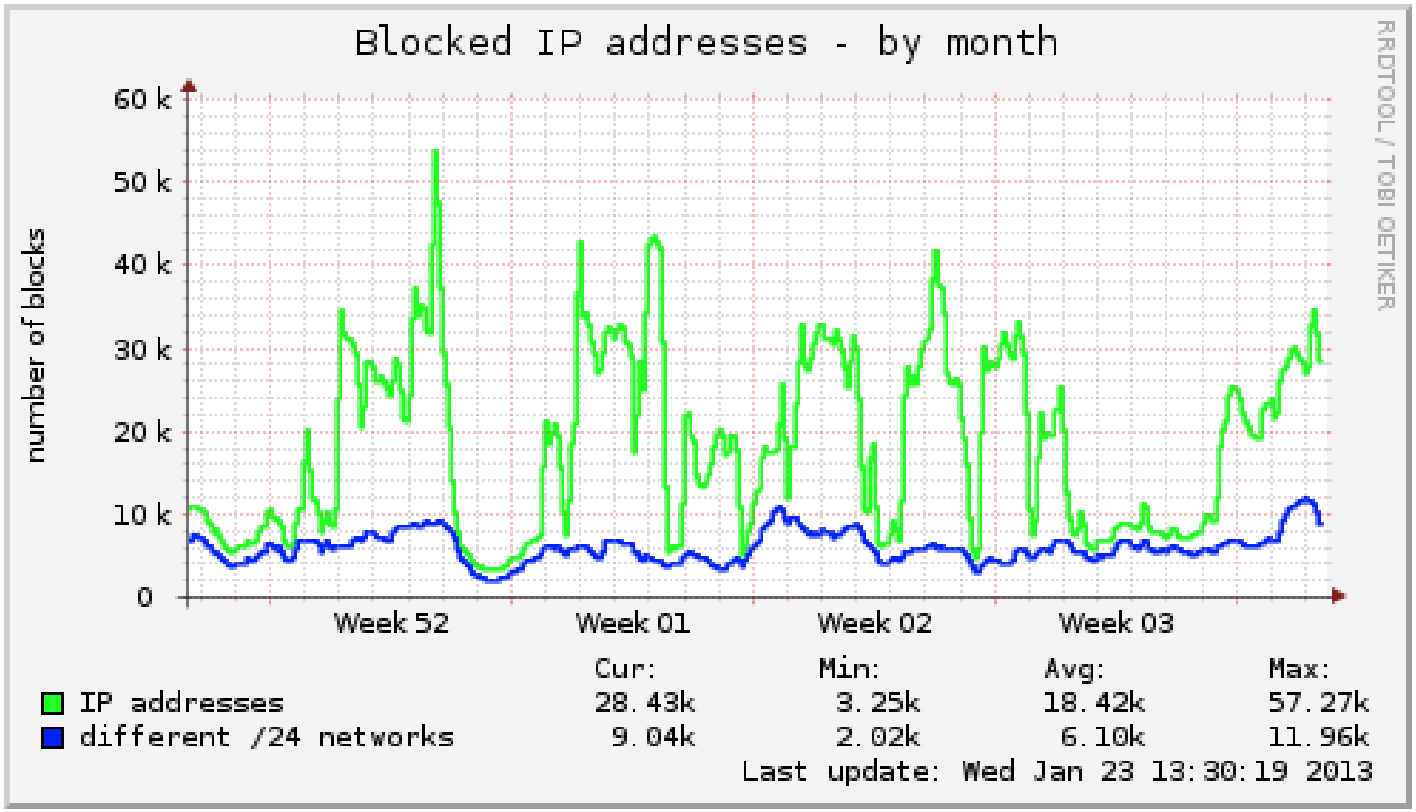
Web scraping from Tor?

- Small number of well know IP-addresses -> easy to handle
- curl https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=171.25.193.19



Web scraping of some sites

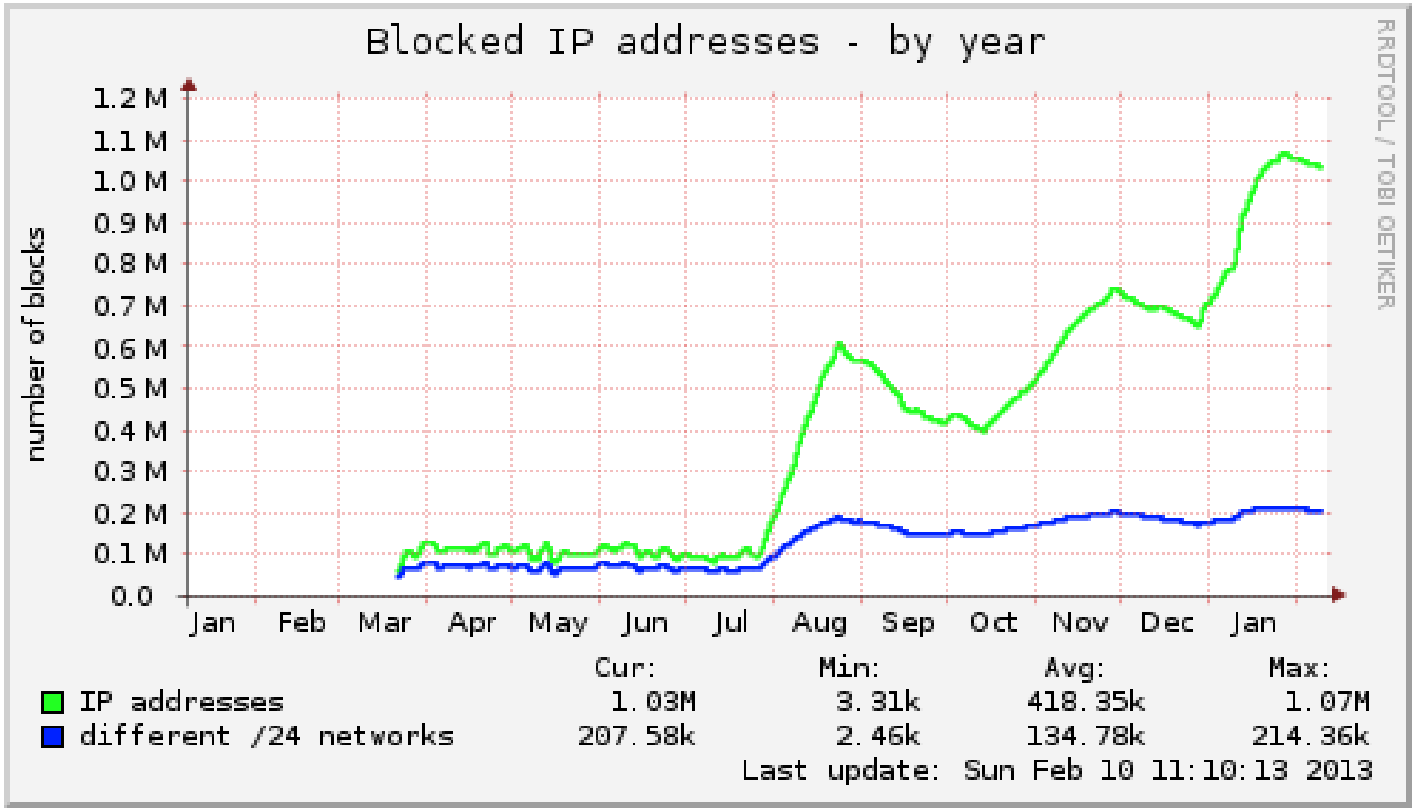
Tor is not the problem



Web scraping of some sites

Tor is not the problem

No shortage in IPv4 addresses for scraping.



Legal cease and desist letter

- Asked us to stop the DOS/DDOS of a specific site.
- Was not sent to abuse@dfri.net but to an individual.
- Referenced laws that did not apply for us in Sweden .

Anonymous FTP and port scans

one of our customers has been the target of an attack by the group "anonymous". During this attack, one ip-address that belongs to your network seems to be involved. <logs from a FTP login> Please check your system as it also may have been compromised. If you find anything which could be helpful in this case, please let us know. Thank you.

We are receiving port scans or other abusive behavior from an IP in your network, 171.25.193.235 Please stop sending these attacks, secure your systems and terminate your customer(s) involved.

Complete loss

Subject: URGENT - Criminal action notice this is to inform you that a Customer of ours had an attack from internet that caused the entire deletion of their virtual infrastructure with the complete loss of all corporate data. Tracking down all the connection we got evidence that the attacker was using Tor and the connection was coming from this IP: 171.25.193.20 that is belonging to your IP range. As this is a criminal action, we ask you to explain us the proper ocedure in order to have more information about the real IP that was connecting to your systems and to be able to identify the real source IP of the attack.

:DFRI

Open source tools

- DirBuster
- "HEAD /open-source/ HTTP/1.1" 404 0 "-" "DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP-DirBuster-Project)"
- Sqlmap
- SQL Injection Scan reports from celepar.pr.gov.br to several exit operators.

Few answers

One thanks so far.

- Subject: RE: DDoS Attack from IP:171.25.193.235

  Excellent, thank you for the information.

Summary

- Less abuse reports than expected.
- The reports decrease over time.
- https://dfri.se/