

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/269111944>

Using DNS to Trace the Source of a DDoS Attack

Conference Paper · May 2014

DOI: 10.13140/2.1.2524.3209

CITATIONS

0

READS

127

1 author:



Curon Wyn Davies

Swansea University

1 PUBLICATION 0 CITATIONS

SEE PROFILE

14/05/14

Using DNS to Trace the Source of a DDoS Attack

Curon Davies, Jisc RSC Wales



- Further Education (FE) 14+
- Higher Education (HE)
- 5 sites, ~10,000 students, ~850 staff
- 1Gbps Internet at HQ site
- 1Gbps Internet at DR site
- 1Gbps private circuit between sites





<https://www.flickr.com/photos/n3pb/8765646099/in/set-72157634324914351/>

```
=====
|| CONTROLLING LOIC FROM IRC ||
=====
```

As an OP, Admin or Owner, set the channel topic or send a message like the following:

```
!lazor targetip=127.0.0.1 message=test_test port=80 method=tcp wait=false random=true
```

To start an attack, type:

```
!lazor start
```

Or just append "start" to the END of the topic:

```
!lazor targetip=127.0.0.1 message=test_test port=80 method=tcp wait=false random=true start
```

To reset loic's options back to its defaults:

```
!lazor default
```

To stop an attack:

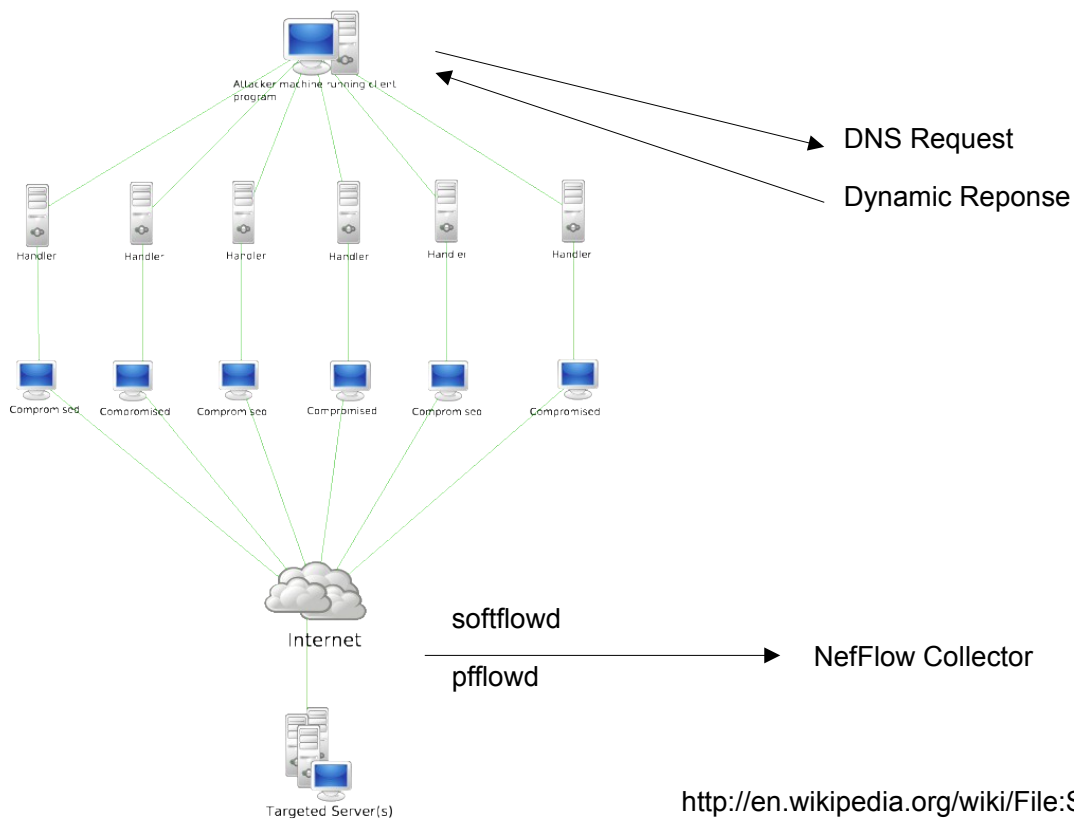
```
!lazor stop
```

and be sure to remove "start" from the END of the topic, if it exists, too.

Take a look at source code for more details.



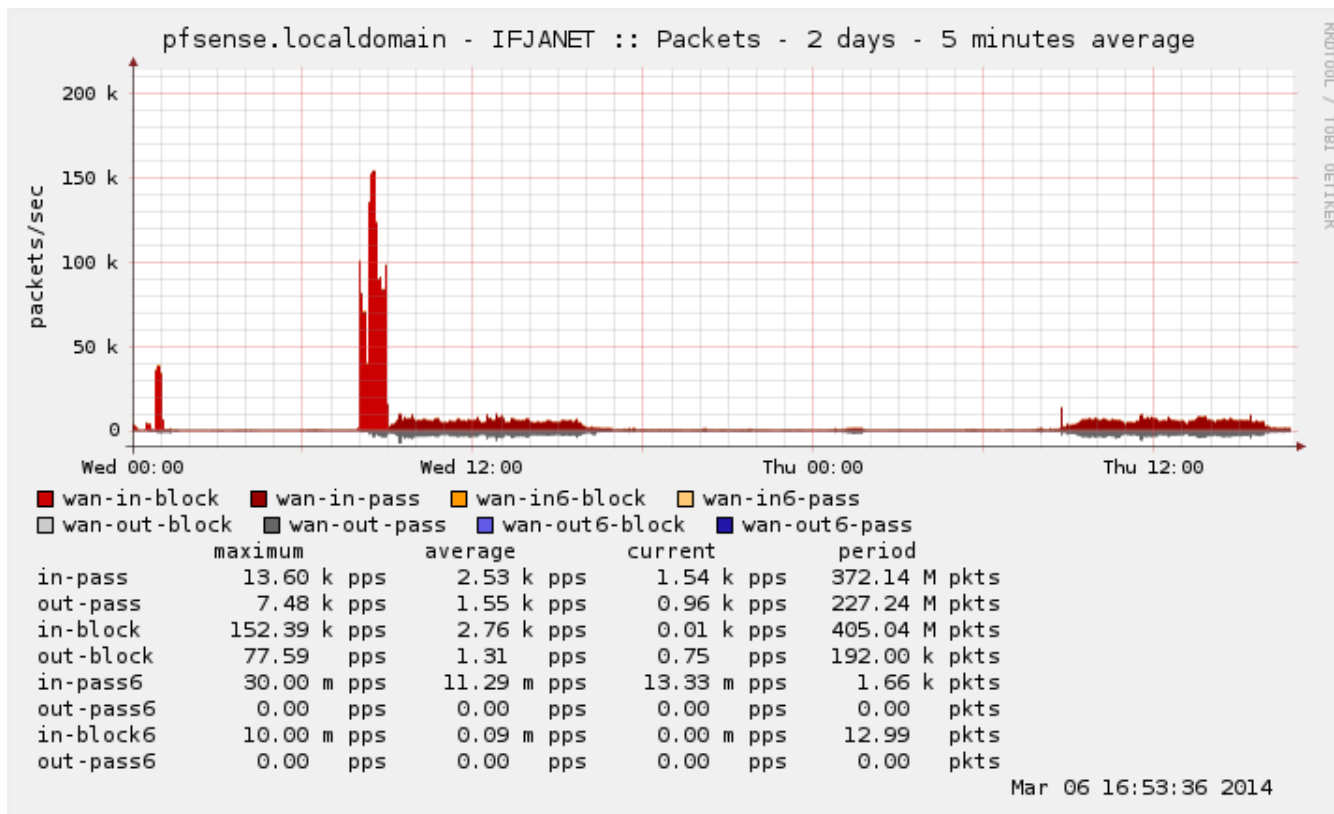
<https://www.flickr.com/photos/londonmatt/13937637187>

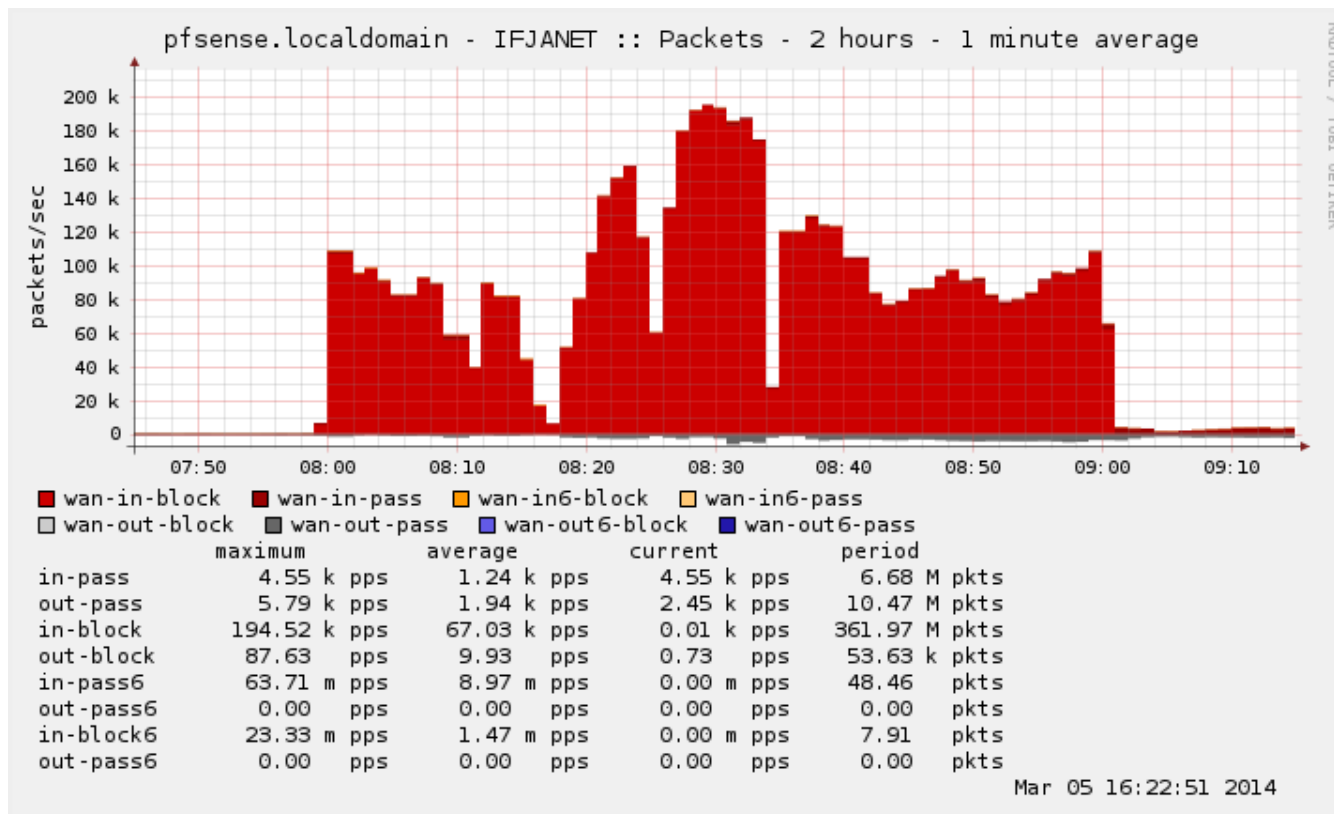


http://en.wikipedia.org/wiki/File:Stachledraht_DDoS_Attack.svg

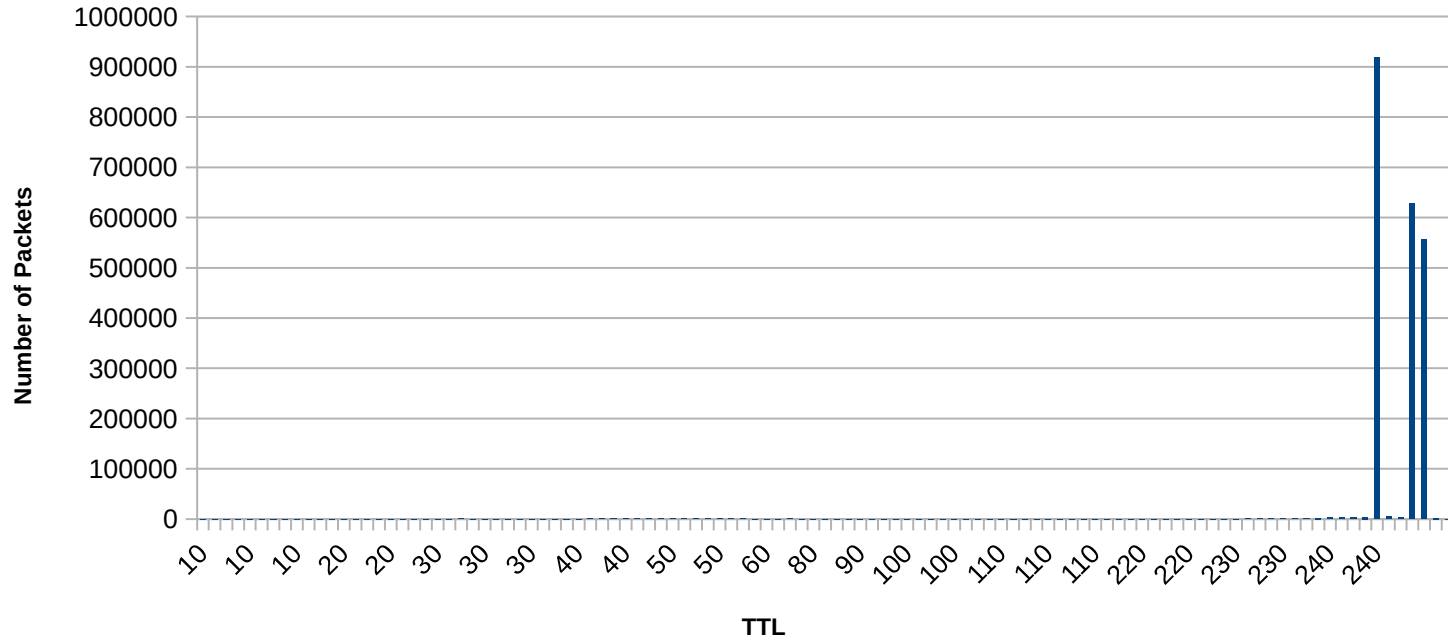


http://commons.wikimedia.org/wiki/File:B1-B_Lancer_and_cluster_bombs.jpg

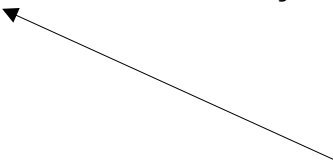




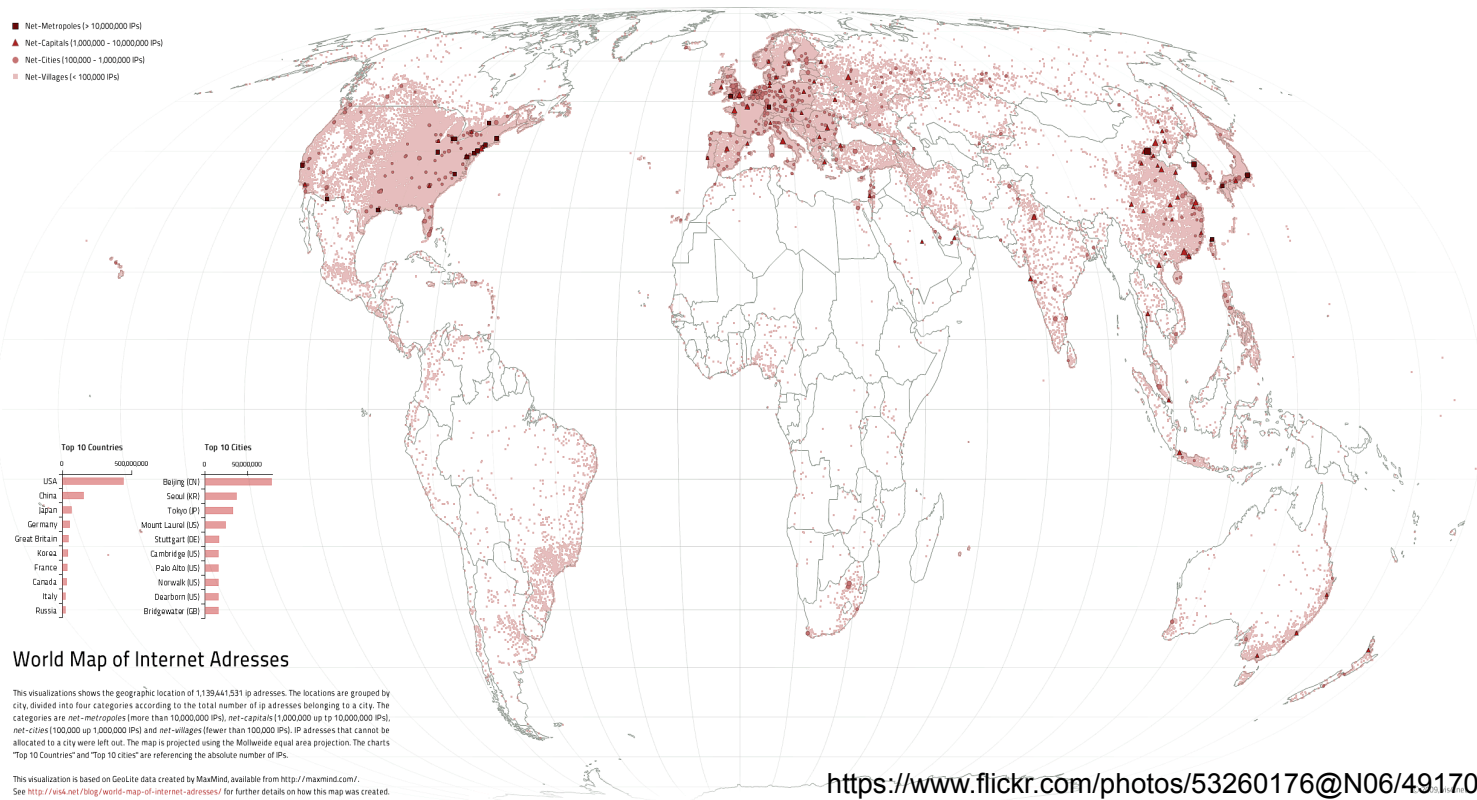
Number of Packets by TTL



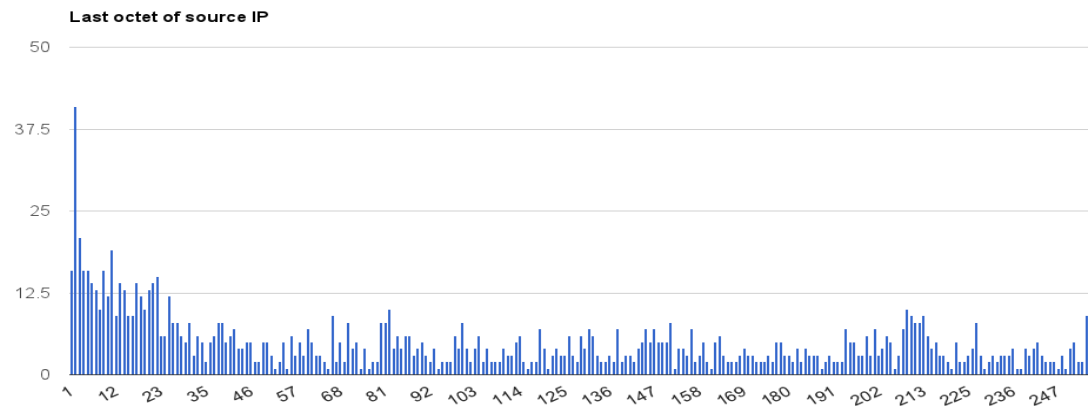
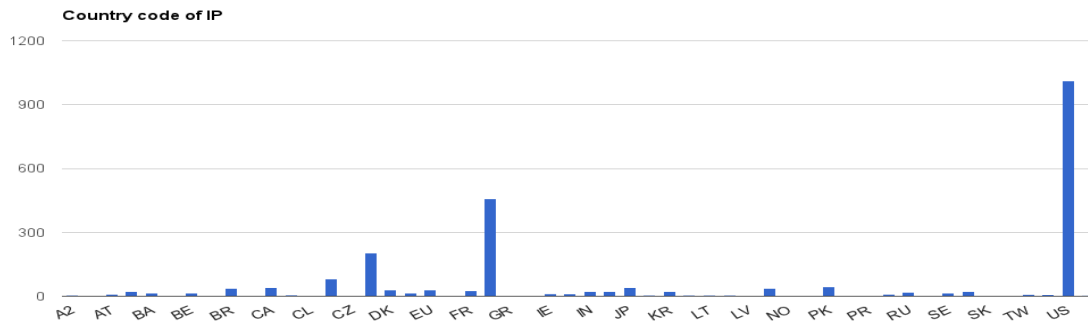
Mar 3, 2014 01:06:16.814944000	178.x.x.66	United Kingdom	5643	secure.colegsirgar.ac.uk	0x0001
Mar 3, 2014 01:10:29.281929000	178.x.x.66	United Kingdom	59440	secure.colegsirgar.ac.uk	0x001c
Mar 3, 2014 01:10:29.281933000	178.x.x.66	United Kingdom	59440	secure.colegsirgar.ac.uk	0x001c
Mar 3, 2014 08:00:17.999137000	178.x.x.66	United Kingdom	57217	secure.colegsirgar.ac.uk	0x0001
Mar 3, 2014 08:00:17.999145000	178.x.x.66	United Kingdom	57217	secure.colegsirgar.ac.uk	0x0001
Mar 3, 2014 08:04:19.773735000	178.x.x.66	United Kingdom	29399	secure.colegsirgar.ac.uk	0x0001
Mar 3, 2014 08:04:19.773737000	178.x.x.66	United Kingdom	29399	secure.colegsirgar.ac.uk	0x0001

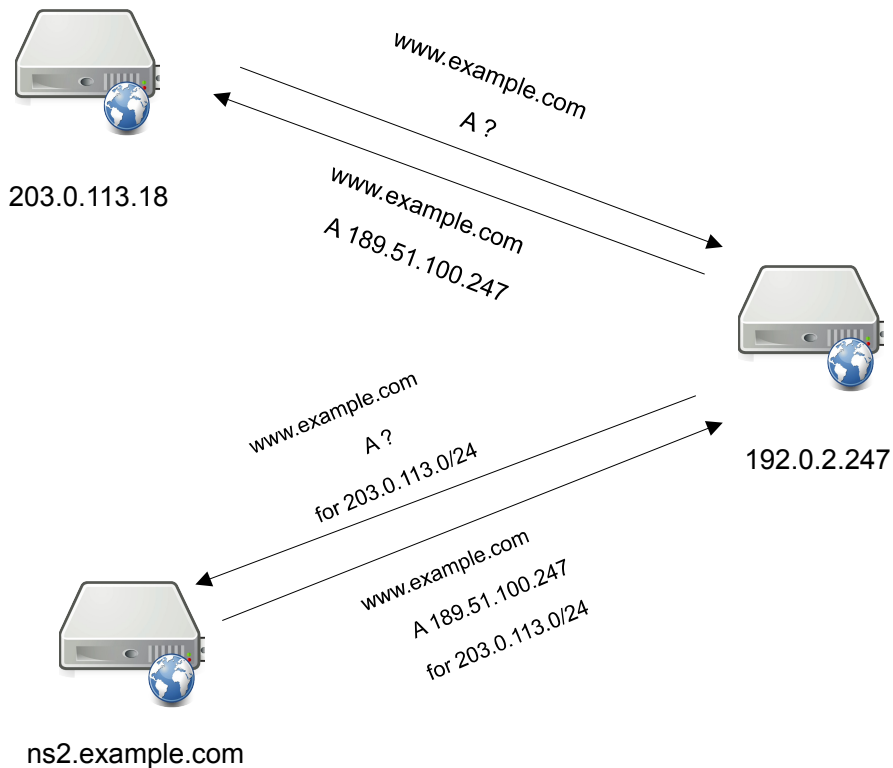


Dedicated Server...



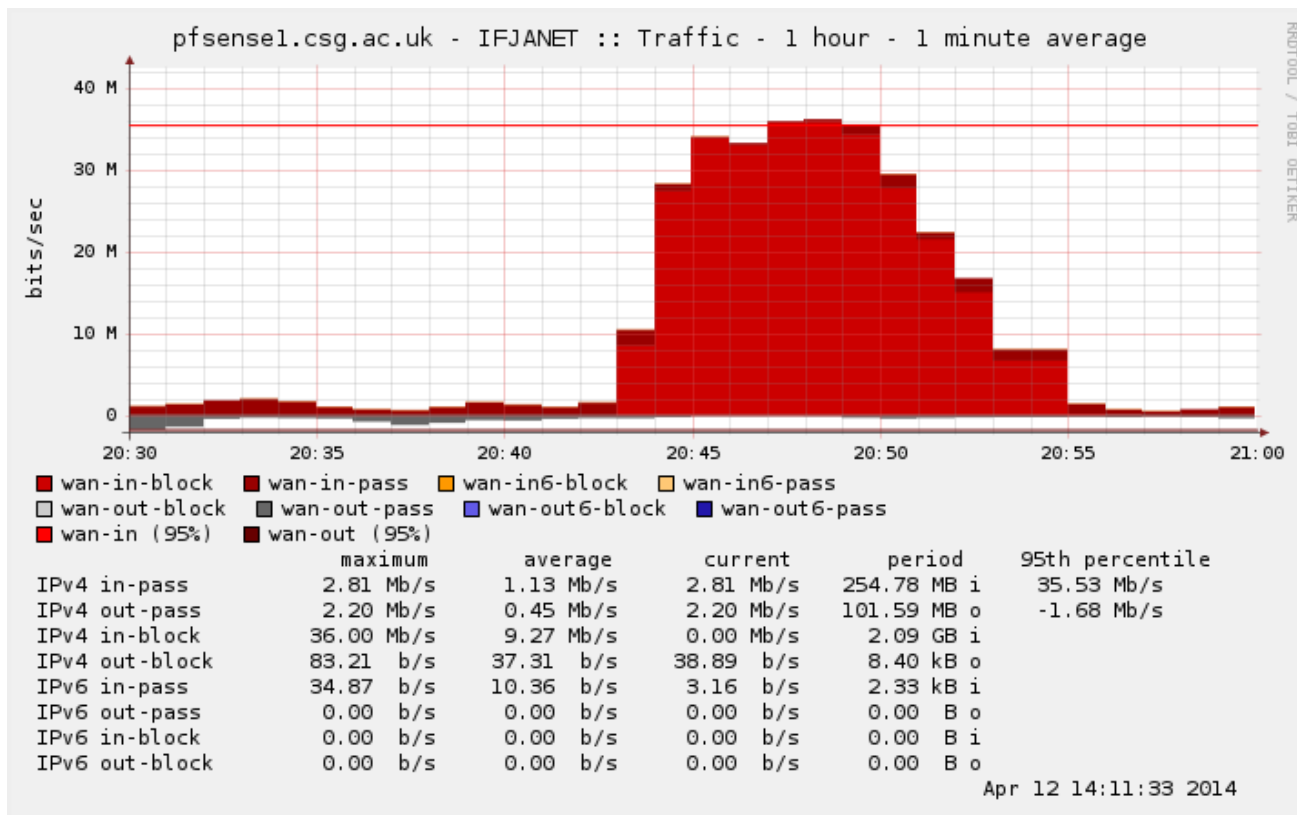
- Or should that be Brussels
 - DE – 74.125.17.0/24
 - US – 74.125.181.0/24

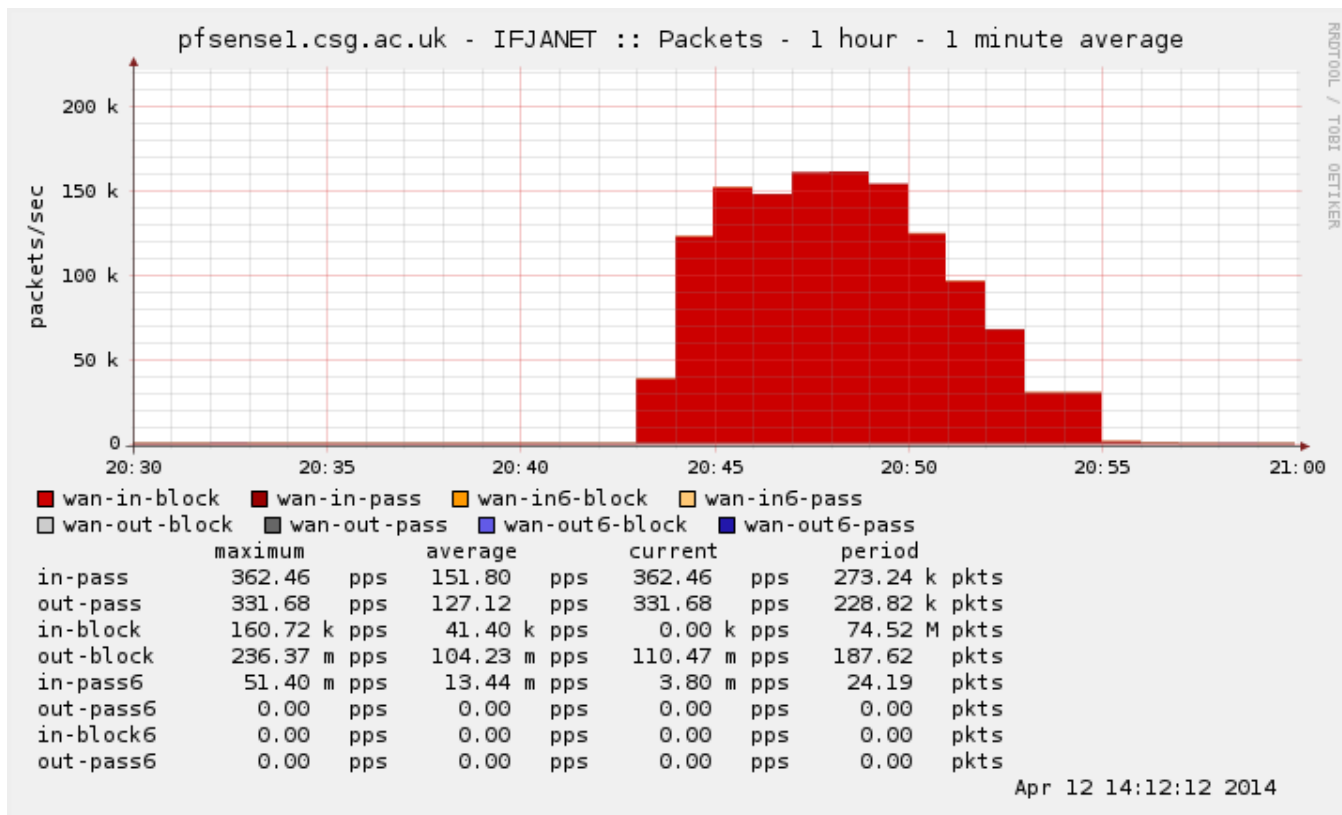




<http://commons.wikimedia.org/wiki/File:Server-web.svg>







Apr 11 12:57:45 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147

Apr 11 20:20:12 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147

Apr 11 20:43:51 dns1 pdns[14695]: Coprocess: DDOS Query from 198.51.100.0/24 via 74.125.17.147; returned 212.219.193.147

Apr 11 22:02:20 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.x.147; returned 212.219.193.147

Apr 12 05:00:22 dns3 pdns[31799]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147

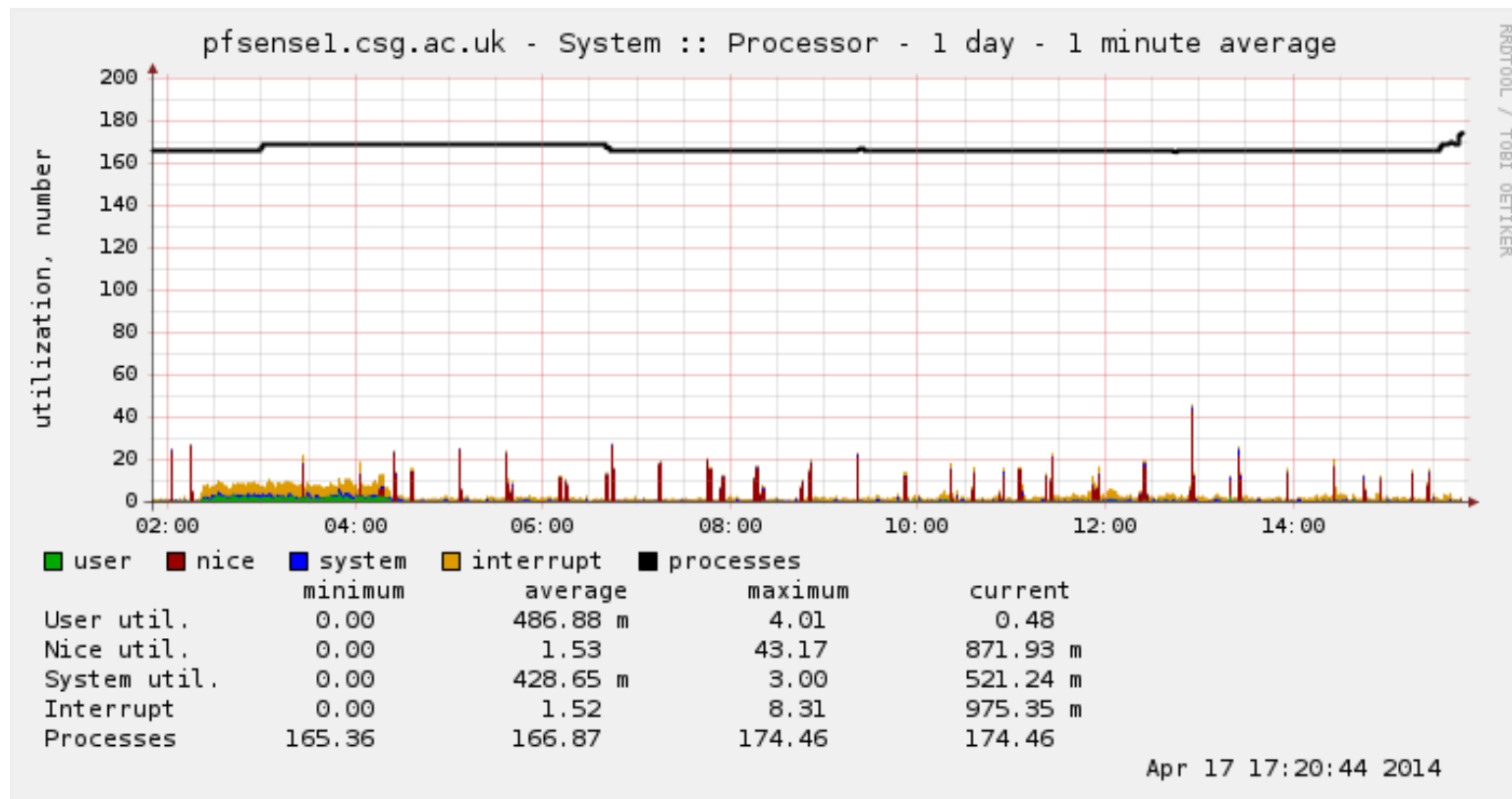
Apr 12 05:44:06 dns1 pdns[14695]: Coprocess: DDOS Query from 203.0.113.147; returned 212.219.193.147

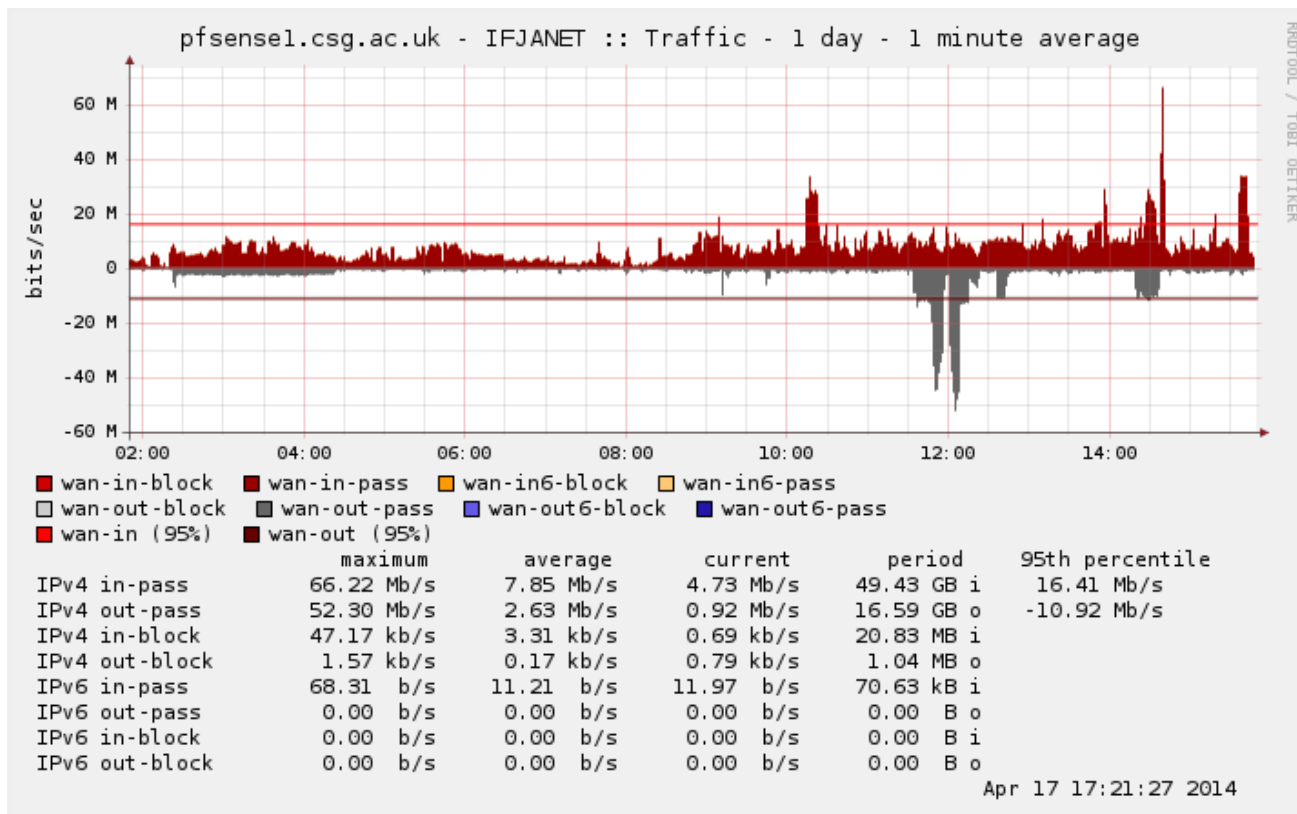
UK VPS provider

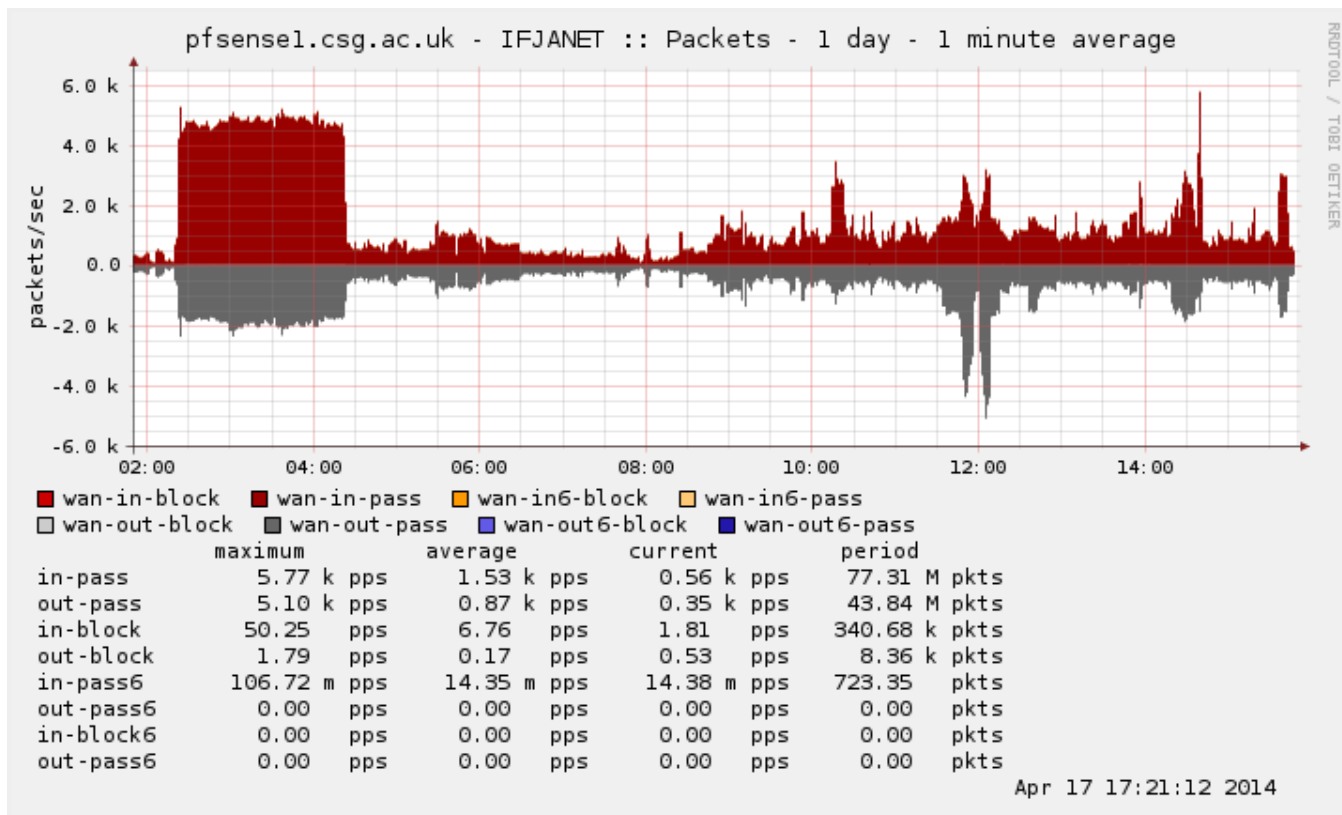
2014-04-11 20:43:51.651423000 - DNS request made from Google to dns1

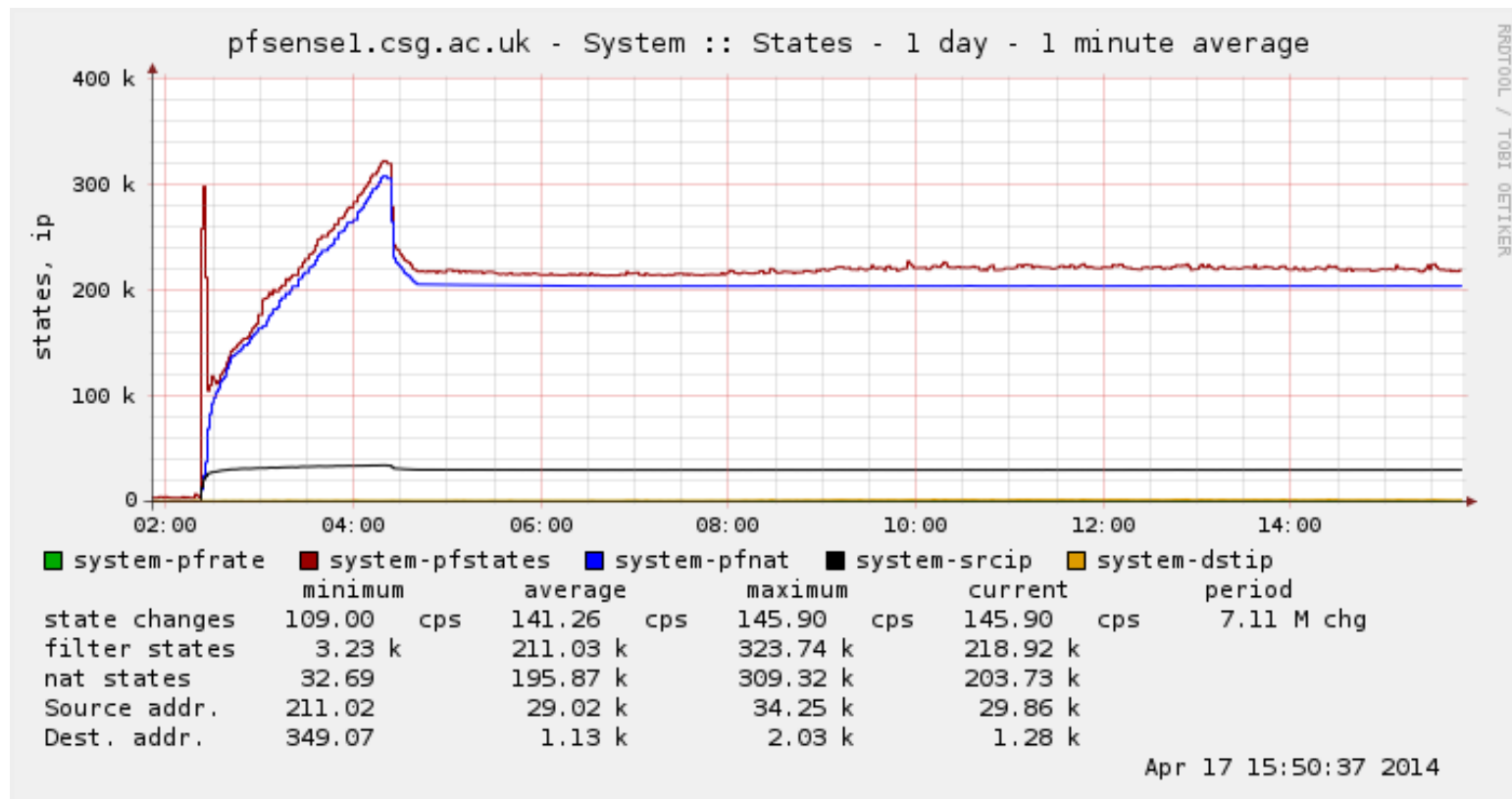
2014-04-11 20:43:51 - response sent to Google DNS

2014-04-11 20:43:58.996 - UDP dst port 80, random src port attack started









- Stateful Attack
- Data logged in NetFlow (pfflowd)
- States still in memory – dumped via pfctl
- Some 100,000 queries per hour for `secure.colegsirgar.ac.uk`
- Some 36,000 compromised/infected hosts
- Mostly hosting providers

2001:0DB8:AC10:FE01:0000:0000:0000:0000



Network Prefix



Interface Identifier

~~secure.colegsirgar.ac.uk~~

s-2049dkk3saf87.colegsirgar.ac.uk

s-4598sal4dof40.colegsirgar.ac.uk

s-3553sge4ive29.colegsirgar.ac.uk

s-3294skd2ifw83.colegsirgar.ac.uk

s-1208oud3lih78.colegsirgar.ac.uk

s-9720dig4kud39.colegsirgar.ac.uk

Curon Wyn Davies
Elearning Advisor (Technical Infrastructure)

curon.w.davies@swansea.ac.uk
jiscrsc.ac.uk/wales



Except where otherwise noted, this work is licensed under CC-BY-NC-ND