Using DNS to Trace the Source of a DDoS Attack
Curon Davies, Jisc RSC Wales

https://www.flickr.com/photos/defenceimages/9393888616/
- 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
The Idea

https://www.flickr.com/photos/spine/1385104812
CAUTION

Legacy IP Only

This product does not support the current generation of Internet Protocol, IPv6.

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.
Using DNS to Trace the Source of a DDoS

https://www.flickr.com/photos/londonmatt/13937637187
Using DNS to Trace the Source of a DDoS

DNS Lookup for an Attack

DNS Request

Dynamic Response

Internet

Targeted Server(s)

softflowd

pfflowd

NefFlow Collector

Using DNS to Trace the Source of a DDoS

SYN Flood Attacks

http://commons.wikimedia.org/wiki/File:B1-B_Lancer_and_cluster_bombs.jpg
Using DNS to Trace the Source of a DDoS

### Graph: pfsense.localdomain - IFJANET :: Packets - 2 days - 5 minutes average

<table>
<thead>
<tr>
<th></th>
<th>maximum</th>
<th>average</th>
<th>current</th>
<th>period</th>
</tr>
</thead>
<tbody>
<tr>
<td>in-pass</td>
<td>13.60 kpps</td>
<td>2.53 kpps</td>
<td>1.54 kpps</td>
<td>372.14 M pkts</td>
</tr>
<tr>
<td>out-pass</td>
<td>7.48 kpps</td>
<td>1.55 kpps</td>
<td>0.96 kpps</td>
<td>227.24 M pkts</td>
</tr>
<tr>
<td>in-block</td>
<td>152.39 kpps</td>
<td>2.76 kpps</td>
<td>0.01 kpps</td>
<td>405.04 M pkts</td>
</tr>
<tr>
<td>out-block</td>
<td>77.59 kpps</td>
<td>1.31 kpps</td>
<td>0.75 kpps</td>
<td>192.00 k pkts</td>
</tr>
<tr>
<td>in-pass6</td>
<td>30.00 mpps</td>
<td>11.29 mpps</td>
<td>13.33 mpps</td>
<td>1.66 k pkts</td>
</tr>
<tr>
<td>out-pass6</td>
<td>0.00 pps</td>
<td>0.00 pps</td>
<td>0.00 pps</td>
<td>0.00 pkts</td>
</tr>
<tr>
<td>in-block6</td>
<td>10.00 mpps</td>
<td>0.09 mpps</td>
<td>0.00 mpps</td>
<td>12.99 pkts</td>
</tr>
<tr>
<td>out-pass6</td>
<td>0.00 pps</td>
<td>0.00 pps</td>
<td>0.00 pps</td>
<td>0.00 pkts</td>
</tr>
</tbody>
</table>

Mar 06 16:53:36 2014
### Similar attack 3 March 2014

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>IP Address</th>
<th>Country</th>
<th>Port</th>
<th>Target Host</th>
<th>Source Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 3, 2014</td>
<td>01:06:16</td>
<td>178.x.x.66</td>
<td>United Kingdom</td>
<td>5643</td>
<td>secure.colegsirgar.ac.uk</td>
<td>0x0001</td>
</tr>
<tr>
<td>Mar 3, 2014</td>
<td>01:10:29</td>
<td>178.x.x.66</td>
<td>United Kingdom</td>
<td>59440</td>
<td>secure.colegsirgar.ac.uk</td>
<td>0x001c</td>
</tr>
<tr>
<td>Mar 3, 2014</td>
<td>01:10:29</td>
<td>178.x.x.66</td>
<td>United Kingdom</td>
<td>59440</td>
<td>secure.colegsirgar.ac.uk</td>
<td>0x001c</td>
</tr>
<tr>
<td>Mar 3, 2014</td>
<td>08:00:17</td>
<td>178.x.x.66</td>
<td>United Kingdom</td>
<td>57217</td>
<td>secure.colegsirgar.ac.uk</td>
<td>0x0001</td>
</tr>
<tr>
<td>Mar 3, 2014</td>
<td>08:00:17</td>
<td>178.x.x.66</td>
<td>United Kingdom</td>
<td>57217</td>
<td>secure.colegsirgar.ac.uk</td>
<td>0x0001</td>
</tr>
<tr>
<td>Mar 3, 2014</td>
<td>08:04:19</td>
<td>178.x.x.66</td>
<td>United Kingdom</td>
<td>29399</td>
<td>secure.colegsirgar.ac.uk</td>
<td>0x0001</td>
</tr>
<tr>
<td>Mar 3, 2014</td>
<td>08:04:19</td>
<td>178.x.x.66</td>
<td>United Kingdom</td>
<td>29399</td>
<td>secure.colegsirgar.ac.uk</td>
<td>0x0001</td>
</tr>
</tbody>
</table>

Dedicated Server...
Using DNS to Trace the Source of a DDoS

World Map of Internet Addresses

This visualization shows the geographic location of IPv4/IPv6 address. The locations are grouped by city, district, state, and country group according to the total number of IP addresses belonging to a city. The categories are city/district (less than 10,000,000 IP), state/district (10,000,000 up to 100,000,000 IP), region (100,000,000 up to 1,000,000,000 IP) and country (over 1,000,000,000 IP). If addresses cannot be allocated to a city, even left out. The map is projected using the Albers equal area projection. The charts "Top 10 Countries" and "Top 10 Cities" are referring to the absolute number of IPs.

This visualisation is based on public data retrieved from MaxMind's available from https://maxmind.com/
See http://www.netriot/world-map-of-internet-addresses/for further details on how this map was created.

https://www.flickr.com/photos/53260176@N06/4917017613/
Most attacks from US and DE

- Or should that be Brussels
  - DE – 74.125.17.0/24
  - US – 74.125.181.0/24
GeoIP is biased – use last Octet instead
Using DNS to Trace the Source of a DDoS

EDNS Client Subnet

http://commons.wikimedia.org/wiki/File:Server-web.svg
Using DNS to Trace the Source of a DDoS
Using DNS to Trace the Source of a DDoS

![Graph showing packet traffic over time](image_url)

- **pfsense1.csg.ac.uk - IFJANET:** Packets - 1 hour - 1 minute average

- **Maximums:**
  - in-pass: 362.46 pps
  - out-pass: 331.68 pps
  - in-block: 160.72 k pps
  - out-block: 236.37 m pps
  - in-pass6: 51.40 m pps
  - out-pass6: 0.00 pps
  - in-block6: 0.00 pps
  - out-block6: 0.00 pps

- **Averages:**
  - in-pass: 151.80 pps
  - out-pass: 127.12 pps
  - in-block: 41.40 k pps
  - out-block: 104.23 m pps
  - in-pass6: 13.44 m pps
  - out-pass6: 0.00 pps
  - in-block6: 0.00 pps
  - out-block6: 0.00 pps

- **Currents:**
  - in-pass: 362.46 pps
  - out-pass: 331.68 pps
  - in-block: 0.00 k pps
  - out-block: 110.47 m pps
  - in-pass6: 3.80 m pps
  - out-pass6: 0.00 pps
  - in-block6: 0.00 pps
  - out-block6: 0.00 pps

- **Periods:**
  - in-pass: 273.24 k pkts
  - out-pass: 228.82 k pkts
  - in-block: 74.52 M pkts
  - out-block: 187.62 pkts
  - in-pass6: 24.19 pkts
  - out-pass6: 0.00 pkts
  - in-block6: 0.00 pkts
  - out-block6: 0.00 pkts

**Note:** Graph and data are from April 12, 2014.
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
Distributed HTTPS Flood Attack

The graph shows the utilization of a system over a period of 1 day, with a 1 minute average. The y-axis represents utilization, measured in number. The x-axis represents time, from 02:00 to 14:00.

The utilization data is categorized into user, nice, system, interrupt, and processes, with minimum, average, and maximum values provided:

- **User util.**
  - Minimum: 0.00
  - Average: 486.88 m
  - Maximum: 4.01
  - Current: 0.48

- **Nice util.**
  - Minimum: 0.00
  - Average: 1.53
  - Maximum: 43.17
  - Current: 871.93 m

- **System util.**
  - Minimum: 0.00
  - Average: 428.65 m
  - Maximum: 3.00
  - Current: 521.24 m

- **Interrupt**
  - Minimum: 0.00
  - Average: 1.52
  - Maximum: 8.31
  - Current: 975.35 m

- **Processes**
  - Minimum: 165.36
  - Average: 166.87
  - Maximum: 174.46
  - Current: 174.46

The data is dated Apr 17 17:20:44 2014.
Using DNS to Trace the Source of a DDoS

Minimal Bandwidth

---

**pfsense1.csg.ac.uk - IFJANET :: Traffic - 1 day - 1 minute average**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>In-pass</th>
<th>Out-pass</th>
<th>In-block</th>
<th>Out-block</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>66.22 Mb/s</td>
<td>7.85 Mb/s</td>
<td>4.73 Mb/s</td>
<td>0.92 Mb/s</td>
</tr>
<tr>
<td>IPv4</td>
<td>52.30 Mb/s</td>
<td>2.63 Mb/s</td>
<td>0.92 Mb/s</td>
<td>0.69 Mb/s</td>
</tr>
<tr>
<td>IPv4</td>
<td>47.17 kb/s</td>
<td>3.31 kb/s</td>
<td>0.79 kb/s</td>
<td>1.04 MB</td>
</tr>
<tr>
<td>IPv6</td>
<td>0.00 b/s</td>
<td>0.00 b/s</td>
<td>0.00 b/s</td>
<td>0.00 B</td>
</tr>
<tr>
<td>IPv6</td>
<td>0.00 b/s</td>
<td>0.00 b/s</td>
<td>0.00 b/s</td>
<td>0.00 B</td>
</tr>
<tr>
<td>IPv6</td>
<td>0.00 b/s</td>
<td>0.00 b/s</td>
<td>0.00 b/s</td>
<td>0.00 B</td>
</tr>
</tbody>
</table>

**95th percentile**

- IPv4: 16.41 Mb/s
- IPv6: 16.03 kB/s
Small number of packets
Using DNS to Trace the Source of a DDoS

Lots of states
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