4-4-6 DNS Rate Limiting
and UDP Attacks
a Hard Lesson

First Symptoms

- I was in a boring meeting and dealing with email

- Service to my email server was suddenly unusable

- The PoP in trouble also contained my MRTG and other measurement <blush>

- But I could log into the 'outside' IP address of one of the border routers
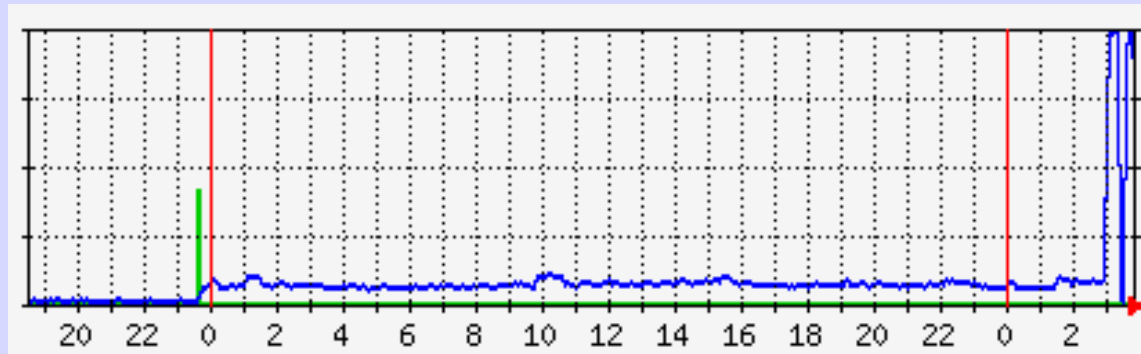
I am the Attacker?
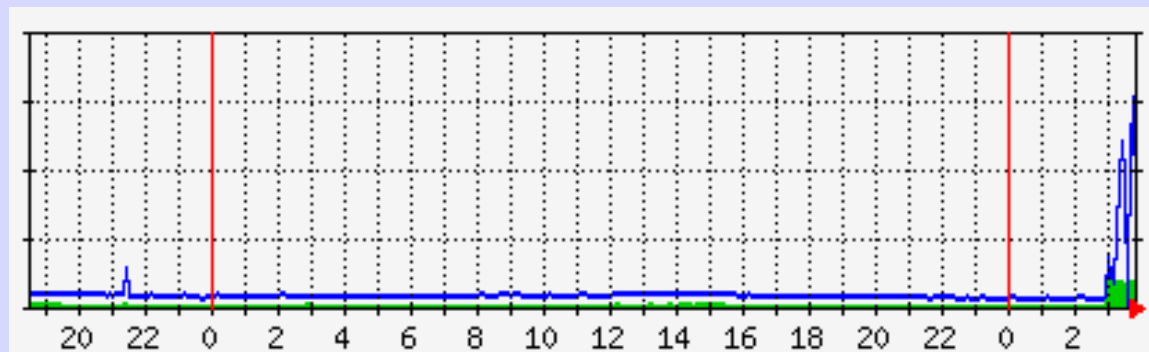
5 minute input rate 720000 bits/sec, 210 packets/sec

5 minute output rate **740230000** bits/sec, **72520** packets/sec

But it was Very Hard to reach MRTG and Other Tools

MRTG for Router

and a DNS Server

Really My Server?

- Managed to get to APC Power Bar which supplied server

- Shut the Server Down

- Problem Went Away!!!

- Powered Server Back Up

- OK for a Minute, but Then Back to Bad

SSH To Server -

Took Three Tries

Over 15 Minutes

tcpdump

```
06:28:26.448024  IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448026  IP rip.psg.com > 108.178.55.192: udp
06:28:26.448071  IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448072  IP rip.psg.com > 108.178.55.192: udp
06:28:26.448168  IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448171  IP rip.psg.com > 108.178.55.192: udp
06:28:26.448174  IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448176  IP rip.psg.com > 108.178.55.192: udp
06:28:26.448234  IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
06:28:26.448237  IP rip.psg.com > 108.178.55.192: udp
06:28:26.448247  IP rip.psg.com.domain > 108.178.55.192.9463: 54533*- 19/0/14 SOA,
RRSIG, RRSIG, Type51, RRSIG, RRSIG, RRSIG, RRSIG, RRSIG, DNSKEY[|domain]
```

So It Was a DNS Reflector Attack!

But the Server Was NOT a Recursive Resolver

Turned off DNS

- Used /etc/ipfw.conf, IP Firwall to

   ```
   add deny udp from any to any 53
   ```

- I Could Now Breathe and Think

- But the Server was Critical to DNS, serving 20 ccTLDs

- A Quick Mailing List Question Showed that this was a DNSsec-based Query Reflector Attack

With a Highly Signed CH ccTLD

One Byte of Query Produced > 1KB of DNSsec Response

Attacker Used Spoofed Source Address, the Address of the Victim, for UDP Query

The Solution Would Be Rate-Limiting

Throttle Queries From a Single Source

Upgraded BIND to 9.9.2 with Patch rl005.12-P1

```
Options {
  rate-limit {
    responses-per-second 5;
    window 5;
    };
  };
```
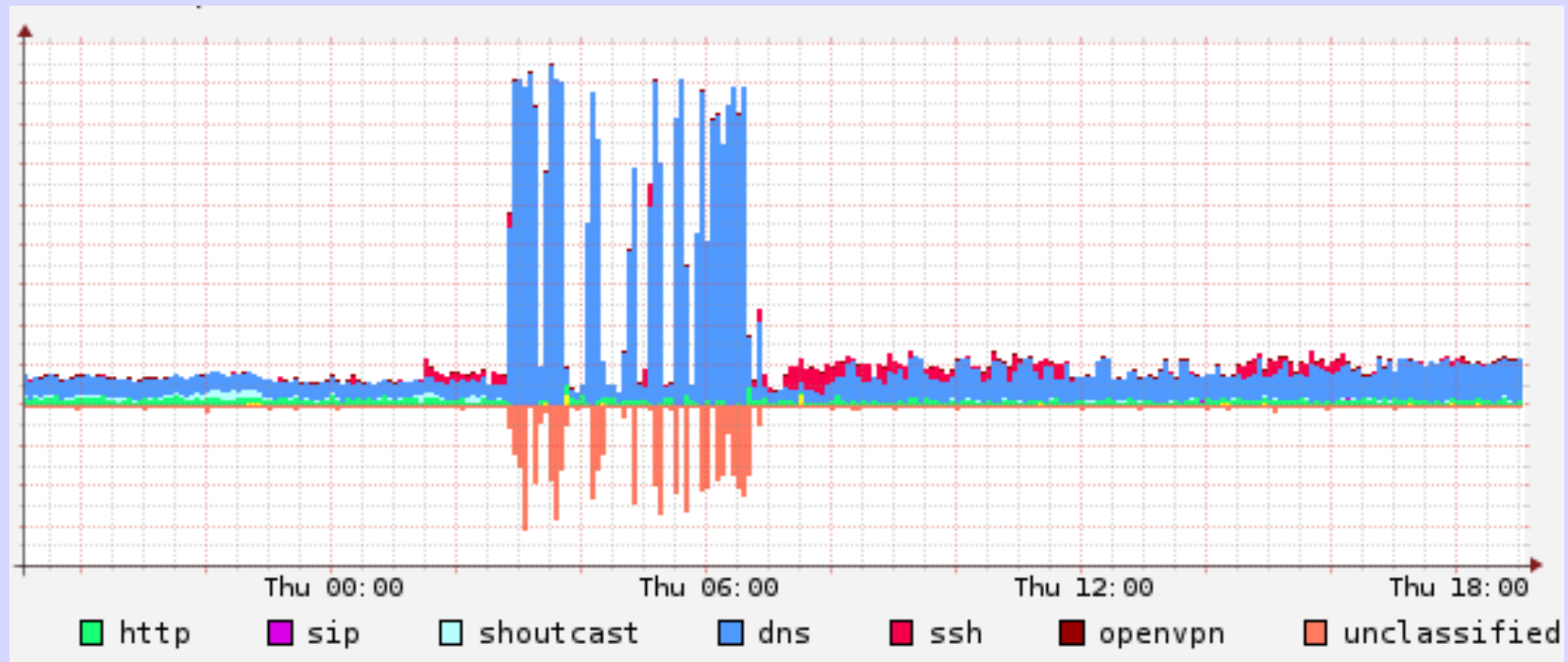
The Problem Was Solved!

From: CH ccTLD Admin

As you have seen today the CH-zone got hit
with a DNS ANY query storm. I assume the
traffic has been sent to most CH secondary
name-servers.

We saw the following kind of query towards
our name-servers which resulted in an
amplification factor of 75:

    dig +edns=0 +bufsize=9000 CH. ANY

Lessons

- OOB Access Really Needed to Be Out Of Band <blush>

- Set Up a Second Measurement System to Measure the First?

- Install and Configure DNS Flow-Limiting Before This Happens to You!!

Unbound

Rate Limiting is the Default

NSD

Use the configure script option

```
./configure —enable-ratelimit
```

The default parameters are a good start

Attacking Me

Bits/s: Thu Jan 9 23:05:00 2014 - Fri Jan 10 23:05:00 2014

Fri 00:00   Fri 06:00   Fri 12:00   Fri 18:00

■ http   ■ sip   □ shoutcast   ■ dns   ■ ssh   ■ openvpn   ■ tor   ■ unclassified
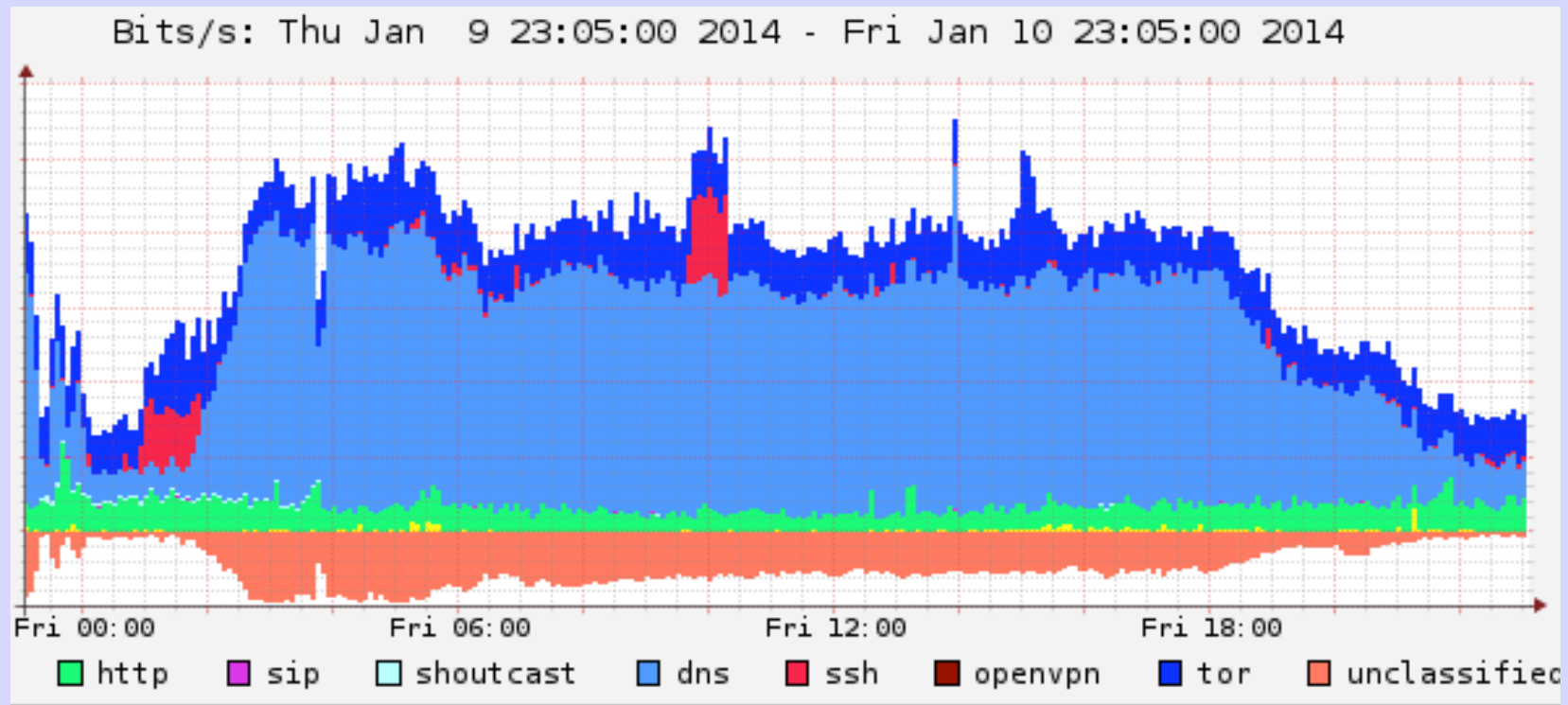
But ...

It is NOT Only DNS

DNS is One of Many UDP-Based Protocols Which Allow Amplification Attacks

NTP Has Amplification

```
$ ntpdc -c monlist tankgirl.kurtis.pp.s
remote address           port local address     count m ver rstr avgint lstint
===============================================================================
180.200.233.250         50820 194.15.141.69        13 7 2    0      8      0
v-209-98-138-61.ip.vis     80 194.15.141.69      1290 7 2    0      1      0
198.15.112.190          25565 194.15.141.69     10278 7 2    0      0      0
162.243.92.39              80 194.15.141.69       133 7 2    0      0      0
web.safe-node.com          80 194.15.141.69       271 7 2    0      0      0
lb03.us-west.hashfaste     80 194.15.141.69      5938 7 2    0      0      0
cpe-1-121-138-201.qwl9     80 194.15.141.69        61 7 2    0      4      0
162.218.54.28           29000 194.15.141.69     63108 7 2    0      0      0
joylynn.indoplanethost     80 194.15.141.69      5602 7 2    0      0      0
124-170-32-156.dyn.i in    80 194.15.141.69      1055 7 2    0      1      0
cpe-76-182-155-229.nat     80 194.15.141.69       460 7 2    0      0      0
c-50-158-5-167.hsd1.il     80 194.15.141.69        16 7 2    0      2      0
s0106001fcf507566.dr.s     53 194.15.141.69       652 7 2    0     10      0
198.50.129.50            3218 194.15.141.69      4522 7 2    0      1      0
178-32-59-1.kimsufi.co     80 194.15.141.69      2261 7 2    0      4      0
37.123.97.5                80 194.15.141.69       136 7 2    0      0      0
c80-216-31-118.bredban     80 194.15.141.69      1280 7 2    0      2      0
d206-116-203-41.bchsia   3074 194.15.141.69       131 7 2    0      1      0
198.50.180.205          29000 194.15.141.69    132865 7 2    0      0      1
cpe-74-76-232-195.nyca   1026 194.15.141.69      1369 7 2    0      3      1
70.38.71.244               80 194.15.141.69     12978 7 2    0      0      1
pool-71-122-77-191.tam     80 194.15.141.69       569 7 2    0      0      1
10554.kriter.com.tr      1905 194.15.141.69      7209 7 2    0      1      1
168.63.55.14               80 194.15.141.69      5528 7 2    0      0      1
136-14-12-198.static.d  25565 194.15.141.69       291 7 2    0      1      1
m5-240-220-121.cust.te     80 194.15.141.69      2407 7 2    0      1      1
46.105.254.28              80 194.15.141.69      2134 7 2    0      2      1
pool-108-13-78-10.lsan     80 194.15.141.69         7 7 2    0     15      1
148.197.184.211            80 194.15.141.69     97186 7 2    0      0      1
bas5-kingston08-1242 52    80 194.15.141.69       693 7 2    0      2      1
74-141-253-2.dhcp.insi   3074 194.15.141.69       683 7 2    0      5      1
mceu14.envioushost.com  25565 194.15.141.69      3817 7 2    0      1      1
192.184.13.233          25565 194.15.141.69      3698 7 2    0      0      1
172-13-170-159.lightsp     80 194.15.141.69       280 7 2    0      1      1
94.23.146.204              80 194.15.141.69      3588 7 2    0      1      1
cpe-24-167-18-198.rgv.   8080 194.15.141.69        18 7 2    0      7      2
bas1-montreal46-127937     80 194.15.141.69      4614 7 2    0      0      2
189.38.59.130.static.u  27017 194.15.141.69      8506 7 2    0      1      2
24-182-76-210.dhcp.hck     80 194.15.141.69      4102 7 2    0      1      2
c-50-183-97-88.hsd1.co     80 194.15.141.69        55 7 2    0      2      2
108.61.239.221.choopa.   3074 194.15.141.69        74 7 2    0     13      2
117.3.103.211              80 194.15.141.69       245 7 2    0    202      2
host-92-20-241-79.as13   3074 194.15.141.69         1 7 2    0      0      2
cpe-142-125-66.soc         80 194.15.141.69       105 7 2    0      6      2
c-69-250-180-142.hsd1.     80 194.15.141.69       221 7 2    0      6      2
199.58.147.81              80 194.15.141.69       174 7 2    0      1      3
ns4009551.ip-192-99-9.     22 194.15.141.69      1053 7 2    0      1      3
199.83.128.97.ip.incap     80 194.15.141.69       752 7 2    0      8      3
cpe-142-136-8-105.soca     80 194.15.141.69        24 7 2    0      3      3
cpe-72-228-146-57.buff   3074 194.15.141.69        27 7 2    0     15      3
176.57.141.243           2302 194.15.141.69       132 7 2    0     10      4
cpc14-hart10-2-0-cust9     80 194.15.141.69       122 7 2    0      3      4
204.static.sea.rackd.n  25565 194.15.141.69      4601 7 2    0      2      4
24-52-227-112.cable.te     80 194.15.141.69         5 7 2    0      0      5
adsl-75-46-30-7.dsl.sf     80 194.15.141.69       123 7 2    0      3      6
37.221.175.38.reserved     80 194.15.141.69       710 7 2    0      5      6
ool-44c0ea68.dyn.opton   3074 194.15.141.69        41 7 2    0     17      6
70.49.207.126              53 194.15.141.69       646 7 2    0      9      7
adsl-184-38-223-230.ms     80 194.15.141.69      1235 7 2    0      9      7
75-137-148-0.dhcp.gwnt     90 194.15.141.69       607 7 2    0     23      8
eagle715.startdedicate     80 194.15.141.69       226 7 2    0      7      8
cpc11-shep12-2-0-cust1     53 194.15.141.69       188 7 2    0      5      8
c12571h20597.vilayer.c   2302 194.15.141.69       156 7 2    0     13     10
cpe-192-136-252-78.tx.     80 194.15.141.69         7 7 2    0      7     10
c-50-151-74-71.hsd1.in   3074 194.15.141.69       240 7 2    0     14     14
c122-106-251-57.belrs3     80 194.15.141.69        74 7 2    0      6     14
lon036.multiplay.co.uk     80 194.15.141.69        33 7 2    0      8     15
107-212-125-251.lights     80 194.15.141.69        66 7 2    0      7     16
137.116.32.32              80 194.15.141.69      3371 7 2    0      0     19
cpe-74-69-109-238.roch   3070 194.15.141.69       112 7 2    0     42     25
140.101.123.37.salay.c     80 194.15.141.69      3411 7 2    0      1     27
70-56-146-208.bois.qwe     80 194.15.141.69       224 7 2    0      0     28
68-204-165-85.res.bhn.     80 194.15.141.69        16 7 2    0      1     30
cpe-24-193-145-48.nyc.   3074 194.15.141.69         5 7 2    0     18     33
c
-24-118-21-238.hsd1.m    3074 194.15.141.69        60 7 2    0      2     44
209-76-178-47.lightspe   3074 194.15.141.69        13 7 2    0     29     49
168.62.23.92               80 194.15.141.69         3 7 2    0     57     49
5e0f8613.bb.sky.com        80 194.15.141.69        66 7 2    0      1     50
70-56-151-99.bois.qwes     80 194.15.141.69      2659 7 2    0      0     65
pool-71-190-169-81.nyc     80 194.15.141.69       129 7 2    0      1     72
88.243.108.185.dynamic     80 194.15.141.69      2392 7 2    0      2     77
119-224-73-172.callplu     80 194.15.141.69        13 7 2    0     32     93
cpe-144-137-66-77.lnse   6500 194.15.141.69        40 7 2    0     21     98
94.23.184.100            6000 194.15.141.69        17 7 2    0      9    103
162.255.212.162.in-add  25565 194.15.141.69     38791 7 2    0      0    110
239.246.154.177.deltai     80 194.15.141.69        16 7 2    0      8    114
pool-173-71-75-209.cmd     80 194.15.141.69        19 7 2    0      2    115
201.171.243.177.dsl.dy     80 194.15.141.69         3 7 2    0     16    120
host86-174-38-212.rang   3074 194.15.141.69         1 7 2    0      0    124
cpe-172-251-214-27.soc   3074 194.15.141.69         1 7 2    0      0    125
cpe-72-182-50-237.aust     80 194.15.141.69         2 7 2    0     25    137
66-169-191-142.dhcp.ft     67 194.15.141.69       287 7 2    0      3    141
ip68-14-142-149.ri.ri.     80 194.15.141.69        13 7 2    0     42    163
affordable.high-perfor   9987 194.15.141.69        34 7 2    0     14    175
c-98-239-104-190.hsd1.   3074 194.15.141.69         4 7 2    0     27    176
cpc2-hari14-2-0-cust33     80 194.15.141.69      2206 7 2    0      5    190
ntp1.mmo.netnod.se        123 194.15.141.69     45196 4 4    0   1039    203
110-174-130-135.static   6500 194.15.141.69        17 7 2    0      6    204
c-24-3S-112-153.custom     80 194.15.141.69       136 7 2    0      5    209
c-50-149-194-70.hsd1.t     80 194.15.141.69         4 7 2    0      3    217
ntp1.sth.netnod.se        123 194.15.141.69     45022 4 4    0   1020    218
cpc2-perr13-2-0-cust93     80 194.15.141.69       152 7 2    0      1    223
101.167.22.79            6500 194.15.141.69        23 7 2    0      3    225
172-9-192-130.lightspe     80 194.15.141.69       166 7 2    0      0    231
108-222-193-172.lights   3074 194.15.141.69         6 7 2    0     16    247
v-74-91-123-196.unman-  27025 194.15.141.69        65 7 2    0      1    272
65.52.24.110               80 194.15.141.69      2108 7 2    0      0    280
198.24.187.41              80 194.15.141.69        30 7 2    0     39    287
pool-71-183-222-135.ny     80 194.15.141.69         5 7 2    0    104    303
94.23.184.200            6000 194.15.141.69         2 7 2    0      0    310
ns394890.ip-176-31-117     80 194.15.141.69       595 7 2    0      1    318
24-119-20-63.cpe.cable   3074 194.15.141.69         1 7 2    0      0    321
c-75-72-118-222.hsd1.m   3074 194.15.141.69         7 7 2    0     15    324
                        25565 194.15.141.69       618 7 2    0      2    325
88.247.203.8.static.tt     80 194.15.141.69      2509 7 2    0      0    343
wsip-70-184-76-130.t.c   3074 194.15.141.69         5 7 2    0     13   3667
76-220-29-27.lightspee     80 194.15.141.69        70 7 2    0      1   3687
142-196-165-57.res.bhn  40031 194.15.141.69         7 7 2    0      4   3688
c-24-22-71-132.hsd1.or   3074 194.15.141.69         2 7 2    0      0   3692
172.56.6.23              3074 194.15.141.69         4 7 2    0     14   3711
datacenter.lgvhost.com   9987 194.15.141.69        45 7 2    0     25   3713
c122-104-144-26.rochd6   6500 194.15.141.69        27 7 2    0      4   3747
122.sub-70-195-0.myvzw   3074 194.15.141.69        20 7 2    0     24   3752
50-89-149-133.res.bhn.     80 194.15.141.69       113 7 2    0      1   3756
99-72-206-4.lightspeed     80 194.15.141.69       209 7 2    0      1   3759
ip22-169-15-186.ct.co.     80 194.15.141.69       324 7 2    0      1   3761
97-86-112-243.dhcp.euc   3074 194.15.141.69        62 7 2    0      4   3767
172.56.15.46               80 194.15.141.69        78 7 2    0      1   3606
cpc4-leic15-2-0-cust14     80 194.15.141.69       173 7 2    0      2   3613
gamma.irc.socialgamer.     80 194.15.141.69      1445 7 2    0      0   3645
ip68-224-152-140.lv.lv   3074 194.15.141.69         4 7 2    0     14   3655
bom1-83-221-145-187.bo  29998 194.15.141.69         0 7 2    0      0   3657
252.190-155-29.uio.sat   3074 194.15.141.69        99 7 2    0      3   3667
ip68-100-248-179.dc.dc     53 194.15.141.69        16 7 2    0      2   3728
cmcustla-71.214.nulink     80 194.15.141.69       291 7 2    0      4   3728
aorleans-552-1-42-41.w   3074 194.15.141.69        15 7 2    0      4   3728
0279e267.bb.sky.com        80 194.15.141.69       793 7 2    0      0   3733
c-71-195-67-115.hsd1.p     80 194.15.141.69       144 7 2    0      1   3740
host-46-20-4-51.router   8040 194.15.141.69      3488 7 2    0      1   3743
69.171.233.113             80 194.15.141.69      3868 7 2    0      0   3785
pool-72-74-164-54.bstn     80 194.15.141.69        14 7 2    0      3   3790
host5-81-81-238.range5     80 194.15.141.69         9 7 2    0     10   3795
d58-106-36-74.rdl801.q   6500 194.15.141.69        29 7 2    0      3   3796
198.50.220.127           6010 194.15.141.69      2658 7 2    0      1   3801
99-182-17-46.lightspee     80 194.15.141.69         2 7 2    0     15   3801
93.174.95.41            25565 194.15.141.69         6 7 2    0     24   3805
host-184-167-144-23.cd   3074 194.15.141.69         2 7 2    0      0   3805
162.220.9.56               80 194.15.141.69      1408 7 2    0      2   3811
24-180-129-11.dhcp.ald     80 194.15.141.69       333 7 2    0      1   3812
68-202-176-195.res.bhn     80 194.15.141.69         7 7 2    0     14   3827
147-92-169-192.static.  28015 194.15.141.69      3213 7 2    0      0   3838
24.49.207.15               80 194.15.141.69      1035 7 2    0      1   3857
beach.ecgnetwork.co     27960 194.15.141.69     11498 7 7    0      0   3861
c95054ec.virtua.com.br  33592 194.15.141.69       715 7 2    0      1   3865
c-50-166-161-241.hsd1.     80 194.15.141.69       100 7 2    0     15   3870
66-55-129-154.constant  30365 194.15.141.69        13 7 2    0     15   3880
ns317118.ip-37-187-133   4101 194.15.141.69     20368 7 2    0      0   3881
23.235.23.228              53 194.15.141.69        22 7 2    0      2   3891
blk-212-116-184.eastli     80 194.15.141.69      3477 7 2    0      0   3891
adsl-76-202-133-1.dsl.   3074 194.15.141.69       131 7 2    0      3   3907
108.170.47.10           25565 194.15.141.69       325 7 2    0      0   3907
```
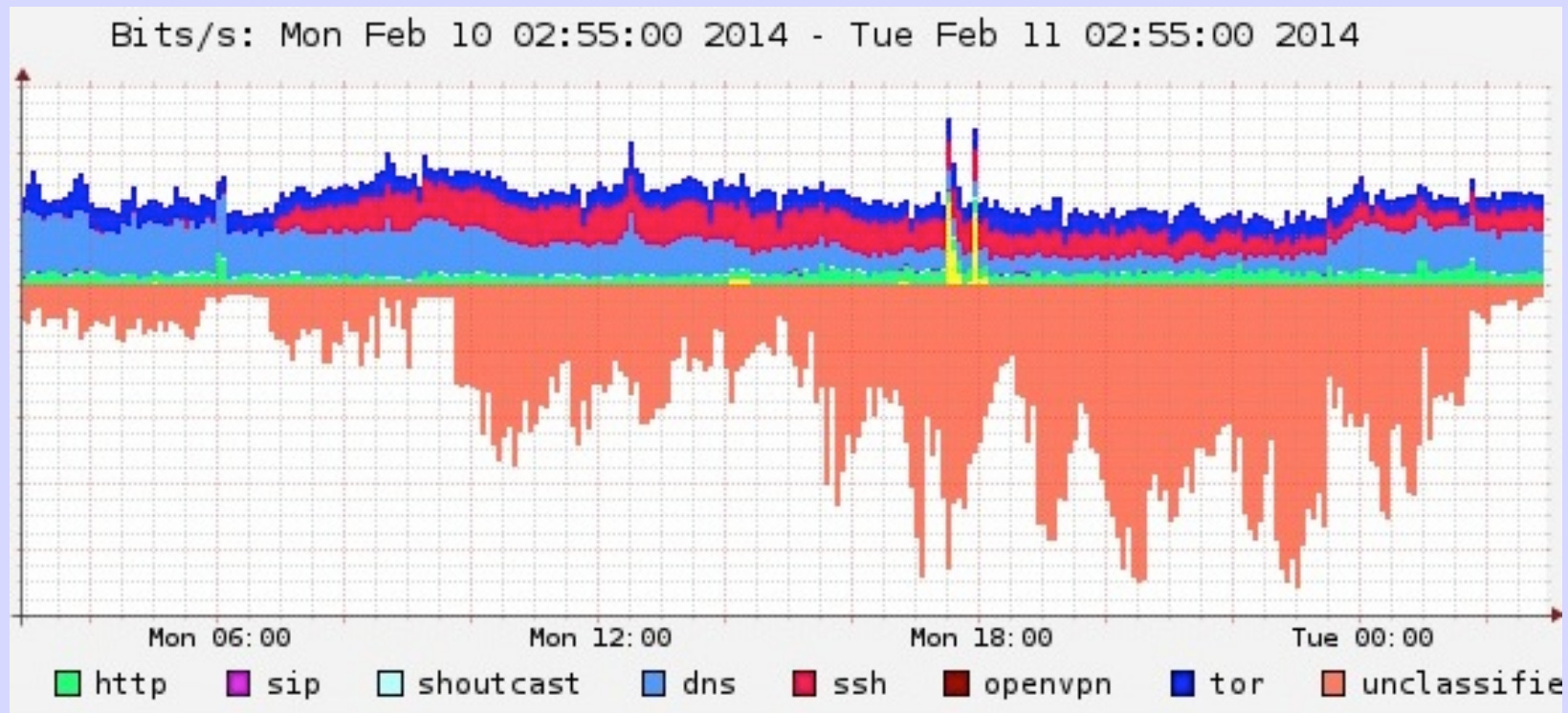
3 Vulnerable Servers

Bits/s: Mon Feb 10 02:55:00 2014 - Tue Feb 11 02:55:00 2014

Mon 06:00   Mon 12:00   Mon 18:00   Tue 00:00

■ http   ■ sip   □ shoutcast   ■ dns   ■ ssh   ■ openvpn   ■ tor   ■ unclassifie

Check Any Host

`ntpdc -c monlist` *hostname*

Block Bad NTP

```
# By default, exchange time with everybody, but don't
# allow configuration.
#
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery
#
# Local users may interrogate the ntp server closely.
restrict 127.0.0.1
restrict ::1
```

Cisco Router

```
! Core NTP configuration
ntp server 24.16.172.107                    ! ntp.psg.com
ntp server 147.28.0.36                      ! rip.psg.com
ntp server 147.28.0.62                      ! psg.com
!
access-list 46 remark utility ACL to block everything
access-list 46 deny any
!
access-list 47 remark NTP peers/servers we sync to/with
access-list 47 permit 24.16.172.107
access-list 47 permit 147.28.0.36
access-list 47 permit 147.28.0.62
access-list 47 deny any
!
! NTP access control
ntp access-group query-only 46   ! deny all NTP control queries
ntp access-group serve 46        ! deny all NTP time and control by default
ntp access-group peer 47         ! permit sync to configured peer(s)/server(s)
ntp access-group serve-only 46   ! deny NTP time sync requests
```
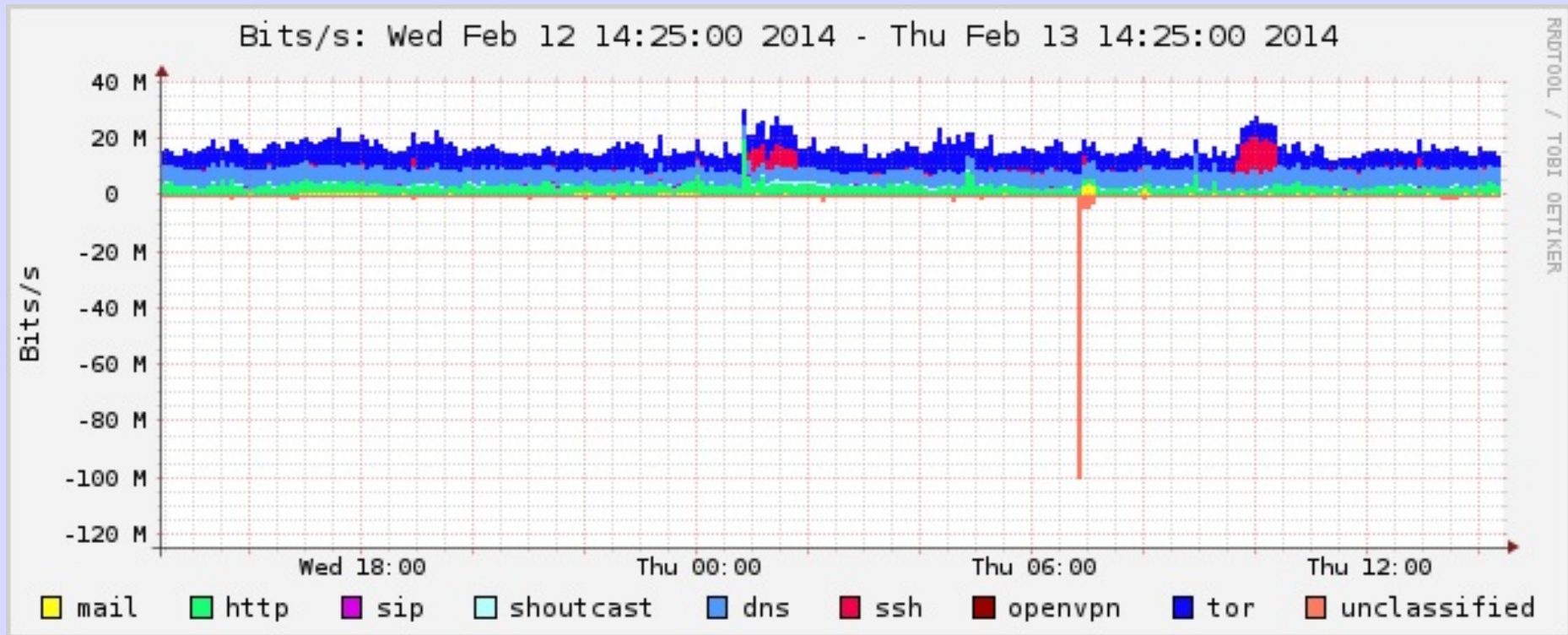
chargen is Vulnerable

Bits/s: Wed Feb 12 14:25:00 2014 - Thu Feb 13 14:25:00 2014

RRDTOOL / TOBI OETIKER

☐ mail   ☐ http   ☐ sip   ☐ shoutcast   ☐ dns   ☐ ssh   ☐ openvpn   ☐ tor   ☐ unclassified

NetFlow Told Me

Dst IP Addr	Bytes(%)	pps	bps	bpp
98.128.37.190	3.7 G(98.7)	3020	28.0 M	1157

Src IP Addr	Bytes(%)	pps	bps	bpp
124.158.127.250	26.0 M(0.7)	600	6.0 M	1241
111.1.20.239	21.1 M(0.6)	474	4.9 M	1277
218.75.208.104	20.6 M(0.5)	484	4.7 M	1222
198.180.150.9	18.3 M(0.5)	30	318398	1287
202.100.85.51	18.0 M(0.5)	418	4.1 M	1237
210.245.86.132	17.7 M(0.5)	416	4.1 M	1223
222.188.10.160	17.7 M(0.5)	407	4.1 M	1248
61.143.139.34	16.8 M(0.4)	391	3.9 M	1233
119.97.222.23	16.8 M(0.4)	390	3.9 M	1231
211.140.116.106	16.6 M(0.4)	377	3.8 M	1269

Src Port	Bytes(%)	pps	bps	bpp
0	2.2 G(58.9)	1588	13.9 M	1093
19	1.5 G(40.0)	1152	11.3 M	1228

Dst Port	Bytes(%)	pps	bps	bpp
0	2.2 G(58.8)	1152	11.3 M	1228

All UDP Services are Vulnerable

But
Do NOT Block
UDP

Look at Each Service Throttle, Manage, or Disable