Case Studies of DNS Server Abuse

Duane Wessels
The Measurement Factory, and
CAIDA
wessels@measurement-factory.com

March 2005

What is Abuse?

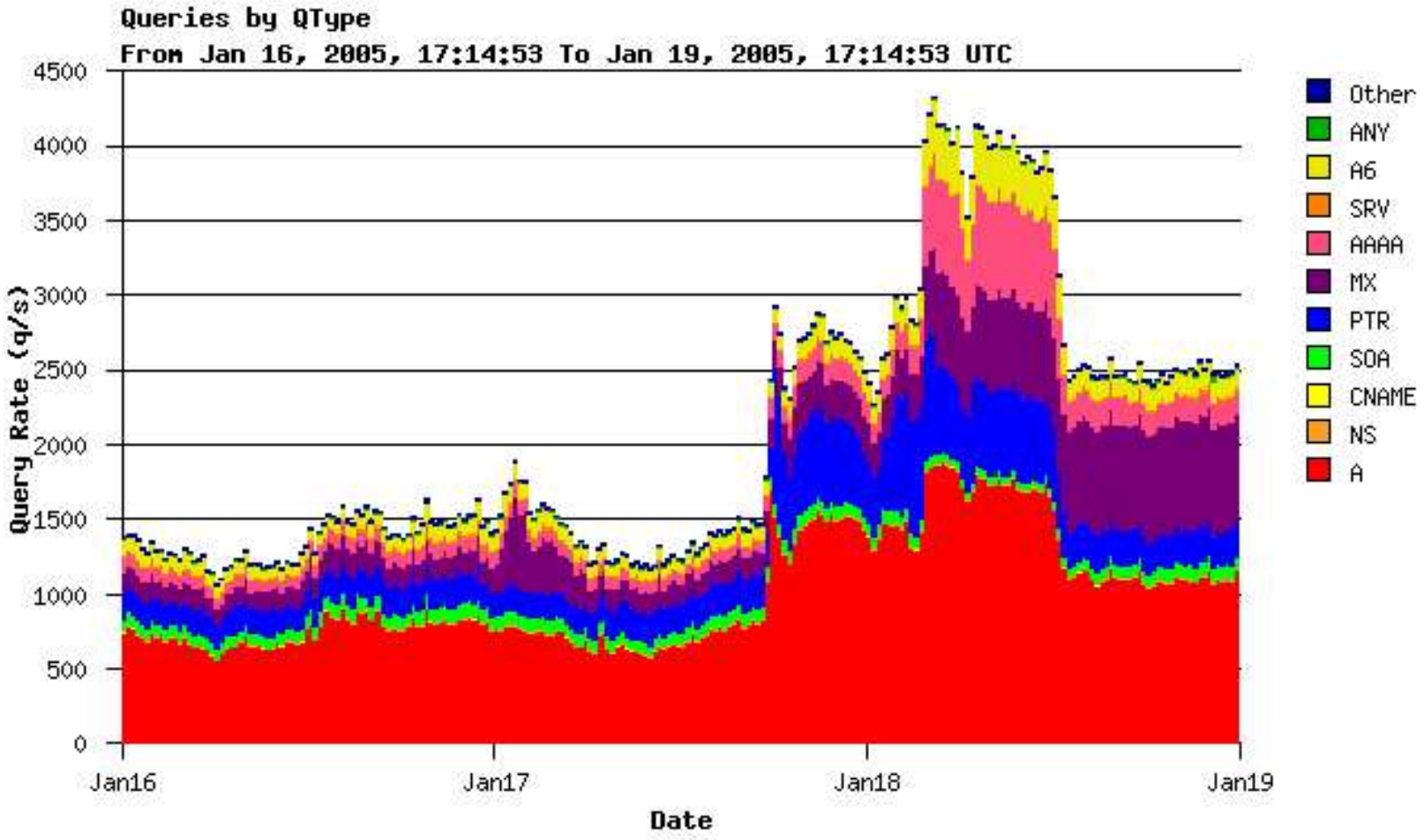
- An exessive number or rate of queries.
- Traffic that appears to be malicious or suspicous.

Where Are We Looking?

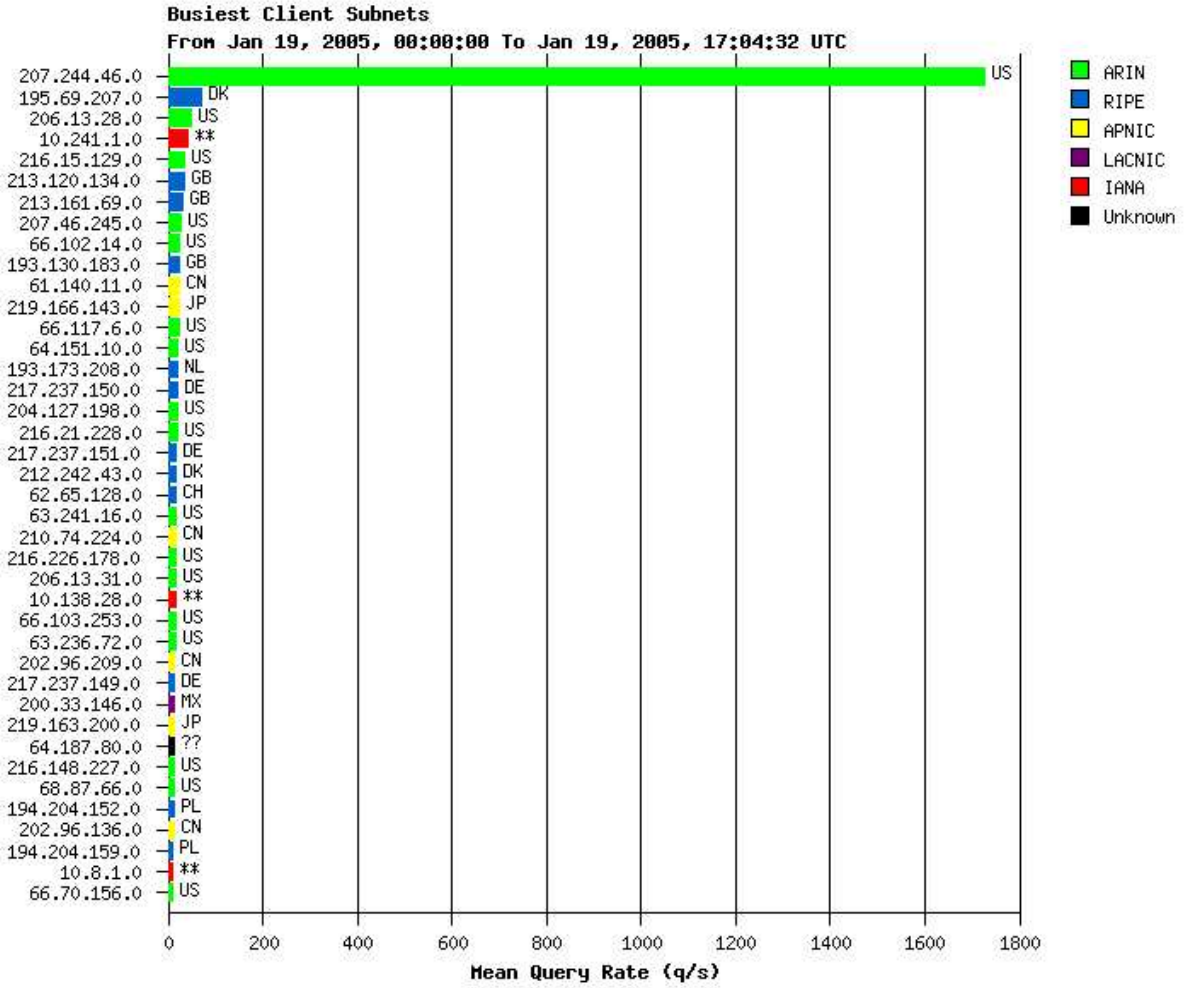
- f.root-servers.org
  - POA1
  - SFO2
- blackhole-[12].iana.org, aka AS112 project
  - as112.sql1.isc.org
- ns-ext.isc.org, authoritative for numerous TLDs

207.244.46.0/24

A large increase in total query rate



The Busy Clients List



How Many Sources?

```
> tcpdump -n -i em0 -c 100000 src net 207.244.46 \
  | awk '{print $2}' | sort | uniq
207.244.46.21.1024
207.244.46.22.1024
207.244.46.23.1024
207.244.46.24.1024
207.244.46.25.1024
...
207.244.46.113.2588
207.244.46.114.3565
207.244.46.115.4164
207.244.46.116.2112
207.244.46.117.3984
```

97 source IP addresses.

What do they have in in-addr.arpa?

```
> host 207.244.46.21
21.46.244.207.IN-ADDR.ARPA = 207-244-46-21.no-icmp-accepted.adsl.atl.ga.cdc.net
> host 207.244.46.22
22.46.244.207.IN-ADDR.ARPA = 207-244-46-22.no-icmp-accepted.adsl.atl.ga.cdc.net
> host 207.244.46.23
23.46.244.207.IN-ADDR.ARPA = 207-244-46-23.no-icmp-accepted.adsl.atl.ga.cdc.net
> host 207.244.46.24
24.46.244.207.IN-ADDR.ARPA = 207-244-46-24.no-icmp-accepted.adsl.atl.ga.cdc.net
> host 207.244.46.25
25.46.244.207.IN-ADDR.ARPA = 207-244-46-25.no-icmp-accepted.adsl.atl.ga.cdc.net
```

Not very encouraging....

ARIN whois?

```
> whois -a 207.244.46.0
Chattanooga Data Connection, Inc. CHATDATA (NET-207-244-0-0-1)
                                  207.244.0.0 - 207.244.63.255
Success Marketing Associates, LLC CDC-LEASED-IAG-40 (NET-207-244-40-0-1)
                                  207.244.40.0 - 207.244.47.255
```

Success Marketing??

```
OrgName:    Success Marketing Associates, LLC
OrgID:      SMAL-3
Address:    701 N. Green Valley Parkway
Address:    Suite 200
City:       Henderson
StateProv:  NV
PostalCode: 89074
Country:    US

NetRange:   207.244.40.0 - 207.244.47.255
CIDR:       207.244.40.0/21
NetName:    CDC-LEASED-IAG-40
NetHandle:  NET-207-244-40-0-1
Parent:     NET-207-244-0-0-1
NetType:    Reassigned
RegDate:    2005-01-10
Updated:    2005-01-10

OrgTechHandle: IPMAN10-ARIN
OrgTechName:   IP Manager
OrgTechPhone:  +1-800-477-1477
OrgTechEmail:  ipmanager@successmarketingassoc.com
```

Bouncy Bouncy

```
Hi. This is the qmail-send program at mail.smsonline.net.  I'm
afraid I wasn't able to deliver your message to the following
addresses.  This is a permanent error; I've given up. Sorry it
didn't work out.

<ipmanager@successmarketingassoc.com>:
This address no longer accepts mail.
```

Let's Try Their ISP

```
OrgName:    Chattanooga Data Connection, Inc.
OrgID:      CHAT
Address:    PO Box 5269, 2003 Amnicola Hwy.
City:       Chattanooga
StateProv:  TN
PostalCode: 37406
Country:    US

NetRange:   207.244.0.0 - 207.244.63.255
CIDR:       207.244.0.0/18
NetName:    CHATDATA
NetHandle:  NET-207-244-0-0-1
NetType:    Direct Allocation
NameServer: DNS1.CHATTANOOGA.CDC.NET
NameServer: DNS2.CHATTANOOGA.CDC.NET
RegDate:    1996-11-06
Updated:    2002-02-08

TechHandle: CNO2-ARIN
TechName:   Network Operations Center
TechPhone:  +1-423-266-3369
TechEmail:  noc@cdc.net
```

The Phone Call

- We phoned 423-266-3369
- An automated system gives us three choices: one for tech support, two for accounting information, three for sales. Choose tech support.
- The woman we spoke with insisted that I call back and speak with someone in sales, because they are "in the other building."
- Sigh.
- Sent email to noc@cdc.net, but did not get a reply.

Traceroute

At this point we wondered if Chattanooga Data Connection was indeed the ISP for Success Marketing Associates, LLC (or whoever is sourcing these packets). A traceroute reveals:

```
> traceroute -n 207.244.46.83
traceroute to 207.244.46.83 (207.244.46.83), 64 hops max, 40 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
^C
```

No route, really?

```
route-views.oregon-ix.net>show ip route 207.244.46.0
% Network not in table
```

Hm, I guess so.

What The ... ?

- Was the network previously in the routing table and then recently withdrawn?
- Was the address space hijacked?
- Why is someone allowing packets out **from** a network that does not have a return route?

We turn to Route Views archives for insight.

Route Views

```
2005-01-01-0000:*  207.244.46.0     64.200.151.12            0 7911 6389 6387 25817 21529 i
2005-01-02-0000:*  207.244.46.0     129.250.0.85       11    0 2914 209 25817 25817 25817 21529 i
2005-01-03-0000:*  207.244.46.0     129.250.0.85       11    0 2914 209 25817 25817 25817 21529 i
2005-01-04-0000:*  207.244.46.0     209.10.12.28        3    0 4513 701 6389 6387 25817 21529 i
2005-01-05-0000:*  207.244.46.0     209.10.12.28        3    0 4513 701 6389 6387 25817 21529 i
2005-01-06-0000:*  207.244.46.0     209.10.12.28        3    0 4513 701 6389 6387 25817 21529 i
2005-01-07-0000:*  207.244.46.0     216.218.252.152          0 6939 6389 6387 25817 21529 i
2005-01-08-0000:
2005-01-09-0000:
2005-01-10-0000:
2005-01-11-0000:
2005-01-12-0000:*  207.244.46.0/23  203.62.252.26            0 1221 4637 6461 30092 i
2005-01-13-0000:*  207.244.46.0/23  208.186.154.35      0     0 5650 6461 30092 i
2005-01-14-0000:*  207.244.46.0/23  208.186.154.35      0     0 5650 6461 30092 i
2005-01-15-0000:*  207.244.46.0/23  217.75.96.60        0     0 16150 15703 20495 6461 30092 i
2005-01-16-0000:*  207.244.46.0/23  129.250.0.11        6     0 2914 6461 30092 i
2005-01-17-0000:*  207.244.46.0/23  217.75.96.60        0     0 16150 15703 20495 6461 30092 i
2005-01-18-0000:*  207.244.46.0/23  196.7.106.245       0     0 2905 701 6461 30092 i
2005-01-19-0000:
```

Advertised by cdc.net (AS 21529) Jan 1–7, then withdrawn.

Reappeared via assertive.ca (AS 30092) Jan 12–18, then withdrawn again.

Let's Ask noc@assertive.ca

- Chris Phillips from assertive.ca explained that this was company who came to them recently for colo and turned out to be a spammer.
- Upon learning of the spamming, they withdrew the route, but left the customer connected.
- A few hours later the customer was entirely disconnected and the flood of queries stopped.

207.244.46.0/24

```
# tcpdump -n -i em0 port domain | grep aaaa
tcpdump: WARNING: em0: no IPv4 address assigned
tcpdump: listening on em0
00:08:47.621813 202.101.172.35.35205 > 204.152.184.64.53:  8629 [1au] A? aaaaaaaaaaaaaaaaaaaaaawj.edu.co.si.
00:08:48.936275 202.101.172.35.35205 > 204.152.184.64.53:  34479 [1au] A? aaaaxa.bz.ao.
00:08:49.449407 202.101.172.35.35205 > 204.152.184.64.53:  24146 [1au] A? aaaaxa.bz.co.ao.
00:08:49.872671 202.96.209.150.35215 > 204.152.184.64.53:  42903 [1au] A? aaaaaaaaaaaaaaaaaaxu.edu.hr.
00:08:51.571943 202.96.104.18.57713 > 204.152.184.64.53:  37051 A? aaaaaaaaaxb.com.co.hr.
00:08:53.471229 202.96.104.18.57713 > 204.152.184.64.53:  6966 A? aaaaaaaaaaxa.bz.aq.
00:08:54.230649 202.96.209.150.35215 > 204.152.184.64.53:  58011 [1au] A? aaaaaaaaaaaaaaaaaaaaaav6.org.ao.
00:08:54.749266 202.96.104.18.57713 > 204.152.184.64.53:  59337 A? aaaaaxa.org.cv.
00:08:55.283544 202.101.172.35.35205 > 204.152.184.64.53:  13223 [1au] A? aaaaaxa.org.co.cv.
00:08:55.982812 202.96.104.18.57713 > 204.152.184.64.53:  60961 A? aaaaaaaaaaxa.bz.co.aq.
00:08:56.949532 202.96.209.150.35215 > 204.152.184.64.53:  4630 [1au] A? aaaaaaaaaaaaaaaaaaaaaav6.org.co.ao.
00:08:57.176353 202.96.209.150.35215 > 204.152.184.64.53:  62041 [1au] A? aaaaaaxa.org.co.nl.
00:08:57.782361 202.96.209.150.35215 > 204.152.184.64.53:  30527 [1au] A? aaaaaaaaaaaaaaaaaaavn.net.co.hr.
00:08:59.734493 202.96.209.150.35215 > 204.152.184.64.53:  5119 [1au] A? aaaaaaaaaaaaaaaxt.bz.is.
00:09:02.928454 202.101.172.35.35205 > 204.152.184.64.53:  31615 [1au] A? aaaaaaaaaaaaaaaaaaaaaav6.org.aq.
00:09:03.462876 202.101.172.35.35205 > 204.152.184.64.53:  2507 [1au] A? aaaaaaaaaaaaaaaaaaaaaav6.org.co.aq.
```

Notes

- These queries are hitting authoritative TLD servers.
- The sources appear to be "legitimate" caching nameservers.
  - We can ping, traceroute, and DNS-fingerprint them.
  - We see other "normal" queries from them.
- Query rate is relatively low, perhaps 1–2 q/s per source

Group by Name Length

```
23:14:17.429383 202.101.172.35.35090 > 204.152.184.64.53: 39115 [1au] A? aaif.org.is.
23:14:31.875784 202.101.172.35.35090 > 204.152.184.64.53: 16994 [1au] A? aaif.org.ao.
23:14:32.207860 202.101.172.35.35090 > 204.152.184.64.53: 36322 [1au] A? aaif.org.co.ao.
23:15:12.952343 202.101.172.35.35090 > 204.152.184.64.53: 54201 [1au] A? aaif.org.nl.
23:15:13.316080 202.101.172.35.35090 > 204.152.184.64.53: 61457 [1au] A? aaif.org.co.nl.
23:16:26.022273 202.101.172.35.35090 > 204.152.184.64.53: 38192 [1au] A? aaif.org.bg.
23:16:35.257190 202.101.172.35.35090 > 204.152.184.85.53: 32498 [1au] A? aaif.org.fr.
23:16:35.636737 202.101.172.35.35090 > 204.152.184.85.53: 18025 [1au] A? aaif.org.co.fr.
23:17:37.869294 202.101.172.35.35090 > 204.152.184.70.53: 17524 [1au] A? aaif.org.co.br.
23:20:23.222867 202.101.172.35.35090 > 204.152.184.64.53: 19143 [1au] A? aaif.org.hr.
23:20:23.602669 202.101.172.35.35090 > 204.152.184.64.53: 58533 [1au] A? aaif.org.co.hr.
23:20:28.566850 202.101.172.35.35090 > 204.152.184.64.53: 19824 [1au] A? aaif.org.si.
23:20:28.958461 202.101.172.35.35090 > 204.152.184.64.53: 2693 [1au] A? aaif.org.co.si.
23:20:44.636916 202.101.172.35.35090 > 204.152.184.64.53: 26420 [1au] A? aaif.org.sk.
23:20:44.974471 202.101.172.35.35090 > 204.152.184.64.53: 40256 [1au] A? aaif.org.co.sk.
23:21:08.499066 202.101.172.35.35090 > 204.152.184.64.53: 39752 [1au] A? aaif.net.ae.
23:22:37.551458 202.101.172.35.35090 > 204.152.184.64.53: 41848 [1au] A? aaif.net.ao.
23:22:38.393458 202.101.172.35.35090 > 204.152.184.64.53: 45646 [1au] A? aaif.net.co.ao.
23:22:49.878092 202.101.172.35.35090 > 204.152.184.64.53: 27998 [1au] A? aaif.net.aq.
23:22:50.703233 202.101.172.35.35090 > 204.152.184.64.53: 62760 [1au] A? aaif.net.co.aq.
23:23:24.533399 202.101.172.35.35090 > 204.152.184.64.53: 51052 [1au] A? aaif.net.nl.
```

Domain Name Oddness

- The QNAME always has 3 or 4 components
- The second component is always one of: bz, info, com, cn, edu, org, gov
- Third component is always **co** for 4-component names.
- Why would someone search a bogus zone like **org.co.nl** when it is easy to verify that it does not exist?

Theory

- The originator of this traffic is trying to search for names in bz, info, com, cn, edu, org, and gov.
- ...is using gethostbyname() or similar
- ...on a box with an */etc/resolv.conf* like this:

```
nameserver 202.101.172.35
nameserver 202.101.172.36
search ae co.ae ao co.ao aq co.aq bg co.bg br co.br ca co.ca cs co.cs cv co.cv fj co.fj fr co.fr \
fx co.fx hr co.hr il co.il in co.in is co.is kp co.kp md co.md na co.na nl co.nl np co.np nr co.nr \
ph co.ph pn co.pn pt co.pt ro co.ro si co.si sk co.sk zr co.zr
```

- ccTLD operators see queries for names that don't exist in bz, info, com, cn, edu, org, and gov.
- Probably many more ccTLDs than this.
- The long search list is probably slowing their scan by two orders of magnitude.

Unresolved

- Is this traffic something to be really concerned about?
- Would be interesting to take traces from bz, info, com, cn, edu, org, or gov.
- Perhaps there are numerous other scanners, but we see the side-effects of one or two sources thanks to their long search list.

194.204.159.0/24

RFC 1918 Abuse

- About 50 q/s PTR queries
- Hitting as112.sql1.isc.org
- 10/8, 172.16/12, and 192.168/16

RIPE Whois

```
21:54:29.730972 IP 194.204.159.3.32890 > 192.175.48.42.53:  41950% [1au] PTR? 206.52.140.10.in-addr.arpa.
21:54:29.732164 IP 194.204.159.3.32890 > 192.175.48.42.53:  37996% [1au] PTR? 123.1.0.10.in-addr.arpa.
21:54:29.777007 IP 194.204.159.4.32851 > 192.175.48.42.53:  32943% [1au] PTR? 163.3.102.10.in-addr.arpa.
21:54:29.786721 IP 194.204.159.3.32890 > 192.175.48.42.53:  3384% [1au] PTR? 163.3.102.10.in-addr.arpa.
21:54:29.829095 IP 194.204.159.5.32915 > 192.175.48.6.53:  20876% [1au] PTR? 102.1.100.10.in-addr.arpa.
21:54:29.830278 IP 194.204.159.3.32890 > 192.175.48.6.53:  50130% [1au] PTR? 1.219.10.10.in-addr.arpa.
21:54:29.862932 IP 194.204.159.2.32854 > 192.175.48.6.53:  33726% [1au] PTR? 201.0.16.172.in-addr.arpa.
21:54:29.945602 IP 194.204.159.5.32915 > 192.175.48.6.53:  22135% [1au] PTR? 149.2.168.192.in-addr.arpa.
21:54:29.951493 IP 194.204.159.6.32955 > 192.175.48.42.53:  18646% [1au] PTR? 149.52.140.10.in-addr.arpa.
21:54:29.968998 IP 194.204.159.7.33303 > 192.175.48.42.53:  30082% [1au] PTR? 34.8.1.10.in-addr.arpa.
21:54:29.987390 IP 194.204.159.5.32915 > 192.175.48.6.53:  19997% [1au] PTR? 254.2.168.192.in-addr.arpa.
21:54:30.067860 IP 194.204.159.4.32851 > 192.175.48.6.53:  27912% [1au] PTR? 104.1.100.10.in-addr.arpa.
21:54:30.076532 IP 194.204.159.3.32890 > 192.175.48.6.53:  59769% [1au] PTR? 188.5.5.10.in-addr.arpa.
21:54:30.100076 IP 194.204.159.2.32854 > 192.175.48.42.53:  17146% [1au] PTR? 192.0.16.172.in-addr.arpa.
21:54:30.126555 IP 194.204.159.5.32915 > 192.175.48.6.53:  20582% [1au] PTR? 21.39.168.192.in-addr.arpa.
21:54:30.126854 IP 194.204.159.5.32915 > 192.175.48.6.53:  10291% [1au] PTR? 132.1.168.192.in-addr.arpa.
21:54:30.127884 IP 194.204.159.5.32915 > 192.175.48.6.53:  54878% [1au] PTR? 78.114.140.10.in-addr.arpa.
21:54:30.131556 IP 194.204.159.4.32851 > 192.175.48.6.53:  48435% [1au] PTR? 1.63.10.10.in-addr.arpa.
21:54:30.207024 IP 194.204.159.7.33303 > 192.175.48.6.53:  29509% [1au] PTR? 191.52.140.10.in-addr.arpa.
21:54:30.245716 IP 194.204.159.7.33303 > 192.175.48.6.53:  18238% [1au] PTR? 79.64.1.10.in-addr.arpa.
```

RIPE Whois

```
inetnum:      194.204.159.0 - 194.204.159.255
netname:      TPSA-ZT-PIOTRKOW
descr:        local network
country:      PL
admin-c:      KP21-RIPE
tech-c:       TK569-RIPE
tech-c:       KP21-RIPE
status:       ASSIGNED PA
mnt-by:       TPNET
changed:      konradpl@zt.piotrkow.tpsa.pl 19991202
source:       RIPE
```

Resolved?

- Wrote to Konrad on March 8
- No reply from Konrad
- Traffic "stopped" march 11
- Or maybe it moved?

64.124.43.0/24

```
21:50:46.381462 64.124.43.174.60201 > 192.5.5.241.53:  32381 A6? M.ROOT-SERVERS.NET.
21:50:46.381738 64.124.43.174.60201 > 192.5.5.241.53:  8689 AAAA? M.ROOT-SERVERS.NET.
21:50:46.382003 64.124.43.174.60201 > 192.5.5.241.53:  57393 A? M.ROOT-SERVERS.NET.
21:50:46.382212 64.124.43.174.60201 > 192.5.5.241.53:  7454 A6? L.ROOT-SERVERS.NET.
21:50:46.382462 64.124.43.174.60201 > 192.5.5.241.53:  50649 AAAA? L.ROOT-SERVERS.NET.
21:50:46.382836 64.124.43.174.60201 > 192.5.5.241.53:  22887 A? L.ROOT-SERVERS.NET.
21:50:46.383086 64.124.43.174.60201 > 192.5.5.241.53:  51870 A6? K.ROOT-SERVERS.NET.
21:50:46.383336 64.124.43.174.60201 > 192.5.5.241.53:  20171 AAAA? K.ROOT-SERVERS.NET.
21:50:46.383586 64.124.43.174.60201 > 192.5.5.241.53:  56246 A? K.ROOT-SERVERS.NET.
21:50:46.383873 64.124.43.174.60201 > 192.5.5.241.53:  16339 A6? J.ROOT-SERVERS.NET.
21:50:46.384101 64.124.43.174.60201 > 192.5.5.241.53:  29009 AAAA? J.ROOT-SERVERS.NET.
21:50:46.384371 64.124.43.174.60201 > 192.5.5.241.53:  22179 A? J.ROOT-SERVERS.NET.
21:50:46.384717 64.124.43.174.60201 > 192.5.5.241.53:  47357 A6? I.ROOT-SERVERS.NET.
21:50:46.384960 64.124.43.174.60201 > 192.5.5.241.53:  35724 AAAA? I.ROOT-SERVERS.NET.
21:50:46.385233 64.124.43.174.60201 > 192.5.5.241.53:  49742 A? I.ROOT-SERVERS.NET.
21:50:46.385479 64.124.43.174.60201 > 192.5.5.241.53:  51389 A6? H.ROOT-SERVERS.NET.
21:50:46.385719 64.124.43.174.60201 > 192.5.5.241.53:  31041 AAAA? H.ROOT-SERVERS.NET.
21:50:46.386001 64.124.43.174.60201 > 192.5.5.241.53:  28242 A? H.ROOT-SERVERS.NET.
21:50:46.386231 64.124.43.174.60201 > 192.5.5.241.53:  55560 A6? G.ROOT-SERVERS.NET.
21:50:46.386586 64.124.43.174.60201 > 192.5.5.241.53:  48631 AAAA? G.ROOT-SERVERS.NET.
21:50:46.386856 64.124.43.174.60201 > 192.5.5.241.53:  15939 A? G.ROOT-SERVERS.NET.
21:50:46.387085 64.124.43.174.60201 > 192.5.5.241.53:  59251 A6? F.ROOT-SERVERS.NET.
21:50:46.387336 64.124.43.174.60201 > 192.5.5.241.53:  30365 AAAA? F.ROOT-SERVERS.NET.
21:50:46.387584 64.124.43.174.60201 > 192.5.5.241.53:  49837 A? F.ROOT-SERVERS.NET.
21:50:46.387874 64.124.43.174.60201 > 192.5.5.241.53:  23024 A6? E.ROOT-SERVERS.NET.
```

```
21:53:40.024650 64.124.43.173.35658 > 192.5.5.241.53:  31887 [1au] A6? pdns4.register.com.
21:53:40.024841 64.124.43.173.35658 > 192.5.5.241.53:  23426 [1au] AAAA? pdns4.register.com.
21:53:40.024880 64.124.43.173.35658 > 192.5.5.241.53:  50072 [1au] A? pdns4.register.com.
21:53:40.024941 64.124.43.173.35658 > 192.5.5.241.53:  50777 [1au] A6? pdns3.register.com.
21:53:40.025003 64.124.43.173.35658 > 192.5.5.241.53:  3691 [1au] AAAA? pdns3.register.com.
21:53:40.025090 64.124.43.173.35658 > 192.5.5.241.53:  61737 [1au] A? pdns3.register.com.
21:53:40.380565 64.124.43.174.60201 > 192.5.5.241.53:  29921 [1au] A6? pdns4.register.com.
21:53:40.380776 64.124.43.174.60201 > 192.5.5.241.53:  47764 [1au] AAAA? pdns4.register.com.
21:53:40.381006 64.124.43.174.60201 > 192.5.5.241.53:  31898 [1au] A? pdns4.register.com.
21:53:40.381256 64.124.43.174.60201 > 192.5.5.241.53:  45035 [1au] A6? pdns3.register.com.
21:53:40.381466 64.124.43.174.60201 > 192.5.5.241.53:  47048 [1au] AAAA? pdns3.register.com.
21:53:40.381630 64.124.43.174.60201 > 192.5.5.241.53:  43905 [1au] A? pdns3.register.com.
21:53:41.373299 64.124.43.174.60201 > 192.5.5.241.53:  59808 [1au] A6? pdns2.register.com.
21:53:41.373549 64.124.43.174.60201 > 192.5.5.241.53:  5630 [1au] AAAA? pdns2.register.com.
21:53:41.373799 64.124.43.174.60201 > 192.5.5.241.53:  40685 [1au] A? pdns2.register.com.
21:53:41.374070 64.124.43.174.60201 > 192.5.5.241.53:  43936 [1au] A6? pdns1.register.com.
21:53:41.374299 64.124.43.174.60201 > 192.5.5.241.53:  20212 [1au] AAAA? pdns1.register.com.
21:53:41.374424 64.124.43.174.60201 > 192.5.5.241.53:  59230 [1au] A? pdns1.register.com.
```

whois -a 64.124.43.0

```
> whois -a NET-64-124-43-160-1

CustName:   REGISTER.COM
Address:    575 8'th Ave
City:       New York
StateProv:  NY
PostalCode: 10018
Country:    US
RegDate:    2003-01-27
Updated:    2003-01-27

NetRange:   64.124.43.160 - 64.124.43.175
CIDR:       64.124.43.160/28
NetName:    MFN-B580-64-124-43-160-28
NetHandle:  NET-64-124-43-160-1
Parent:     NET-64-124-0-0-1
NetType:    Reassigned
Comment:    Abuse issues should be sent to rgardos@register.com,rroberto@register.com
RegDate:    2003-01-27
Updated:    2003-01-27

TechHandle: NOC41-ORG-ARIN
TechName:   AboveNet NOC
TechPhone:  +1-877-479-7378
TechEmail:  noc@above.net
```

Let's try the abuse contact

```
This is the mail server at host mail89-ash-R.bigfish.com.

I wasn't able to deliver the message you sent to one or more
destinations.

<rgardos@register.com>: host smtpa.register.com[216.21.229.220] said: 550
    unknown user (in reply to RCPT TO command)

<rroberto@register.com>: host smtpa.register.com[216.21.229.220] said: 550
    unknown user (in reply to RCPT TO command)
```

whois register.com

```
Organization:
   Register.Com, Inc.
   Domain Registrar
   575 Eighth Avenue, 11th Floor
   New York, NY 10018
   US
   Phone: 212-798-9200
   Fax..: 212-629-9305
   Email: domainregistrar@register.com

Administrative Contact, Technical Contact, Zone Contact:
   Register.Com, Inc.
   Domain Registrar
   575 Eighth Avenue, 11th Floor
   New York, NY 10018
   US
   Phone: 212-798-9200
   Fax..: 212-629-9305
   Email: domainregistrar@register.com

DNS1.REGISTER.COM                          216.21.234.71
DNS2.REGISTER.COM                          216.21.226.71
DNS3.REGISTER.COM                          216.21.234.72
DNS4.REGISTER.COM                          216.21.226.72
```

whois -a 216.21.234.71

```
OrgName:    Register.com, Inc
OrgID:      REG
Address:    575 8th Avenue
City:       New York
StateProv:  NY
PostalCode: 10018
Country:    US

TechHandle: CK296-ARIN
TechName:   Kleban, Chris
TechPhone:  +1-212-798-9100
TechEmail:  chris@register.com

OrgAbuseHandle: CUSTO-ARIN
OrgAbuseName:   Customer Service
OrgAbusePhone:  +1-800-899-9724
OrgAbuseEmail:  support@register.com

OrgNOCHandle: NOC207-ARIN
OrgNOCName:   Network Operations Center
OrgNOCPhone:  +1-902-749-2488
OrgNOCEmail:  ops@register.com

OrgTechHandle: NETWO55-ARIN
OrgTechName:   Network Engineering
```

```
OrgTechPhone:  +1-212-798-9100
OrgTechEmail:  neteng@register.com
```

Unresolved

- Wrote to neteng@register.com March 8, 2005
  - no reply
- Wrote to chris@register.com March 9, 2005
  - no reply

Lessons

Stating the Obvious

- Getting people to fix problems is hard
- Whois contacts are usually wrong
- When correct, they usually don't reply

The End