Open Resolver Project

Results from ~3 months of active scans

http://www.openresolverproject.org

Background

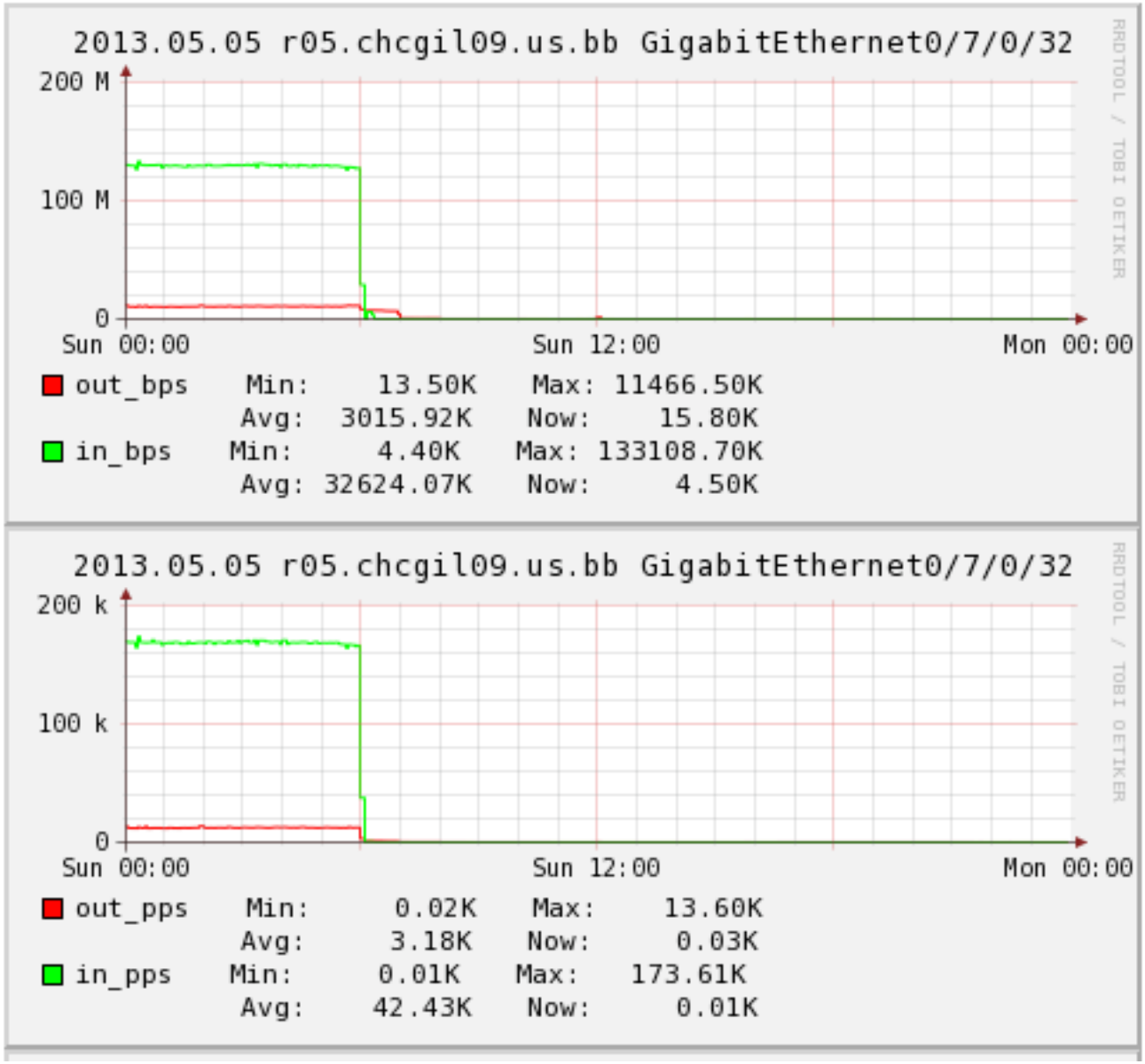
- Lack of BCP-38/anti-spoofing/uRPF means open resolvers can be used in DNS amplification attacks
- Small DNS packet can illicit large reply
- Lack of RRL means authority and recursive resolvers can be abused
- Historically defaults were more permissive in software (open relays, directed-broadcast, etc)
- No inventory available for teams to cross-reference with attack traffic

.


www.openresolverproject.org
Google
Open Resolver Project
Open Resolvers pose a significant threat to the global network infrastructure by answering recursive queries for hosts outside of its domain. They are utilized in DNS Amplification attacks and pose a similar threat as those from Smurf attacks commonly seen in the late 1990s.
We have collected a list of 33 million resolvers that respond to queries in some fashion. 28 million of these pose a significant threat (as of 26-MAY-2013). Detailed History and Breakdown
Check my IP space
Search my IP space (eg: 192.0.2.0/24 - searches "larger" than /22 will be rejected): 8.8.8.8
ipv4-heatmap of 20130519 data heatmap archive
What can I do?
If you operate a DNS server, please check the settings.
Recursive servers should be restricted to your enterprise or customer IP ranges to prevent abuse. Directions on securing BIND and Microsoft nameservers can be found on the Team CYMRU Website - If you operate BIND, you can deploy the TCP-ANY patch
Authoritative servers should not offer recursion, but can still be used in an attack. Configure your Authoritative DNS servers to use DNS RRL [Response Rate Limiting] Knot DNS and NLNetLabs NSD include this as a standard option now. BIND
If you are in the security community:
Please contact dns-scan /at/ puck.nether.net for access to raw data.
Additional Information
Informações em Português
We can provide you a List of Open Resolvers by ASN if you e-mail dns-scan /at/ puck.nether.net
Test your IP Now!

Methodology

- IPv4-only Scan runs weekly (0 UTC Sundays)
- Takes 6.5 hours
- One packet per IP (skips 10/8 127/8 192.168/16)
- Sends about 170kpps


2013.05.05 r05.chcgil09.us.bb GigabitEthernet0/7/0/32
200 M
100 M
0
Sun 00:00
Sun 12:00
Mon 00:00
RRDTOOL / TOBI OETIKER
out_bps Min: 13.50K Max: 11466.50K
Avg: 3015.92K Now: 15.80K
in_bps Min: 4.40K Max: 133108.70K
Avg: 32624.07K Now: 4.50K
2013.05.05 r05.chcgil09.us.bb GigabitEthernet0/7/0/32
200 k
100 k
0
Sun 00:00
Sun 12:00
Mon 00:00
RRDTOOL / TOBI OETIKER
out_pps Min: 0.02K Max: 13.60K
Avg: 3.18K Now: 0.03K
in_pps Min: 0.01K Max: 173.61K
Avg: 42.43K Now: 0.01K

More Methodology

- A.B.C.D
  - Walks IP space sparsely (1.0.0.0, 2.0.0.0 … 223, 1.1.0.0.. 223.1.0.0
  - First few weeks incremented linearly through space. New method catches more resolvers
- Single host doing Scanning and Data collection
  - Process waits just 60 seconds after last packet sent to capture last data.
  - Get responses for hours and days later from broken hosts
- DNS QNAME is unique per-IP
- Query-ID is last two octets of IPv4 address

Complaints?

- Get a few complaints each week, but have tapered off
- ISP Abuse Team was pre-informed of activities
- They have a template to auto-respond to people

Reply Template

Greetings,

X.X.X.X is part of a research project to map out open resolvers on the internet. The contact for

this research project is dns-scan@puck.nether.net. You can also read a bit more about this project at http://openresolverproject.org

Open Resolvers pose a security threat as they are used in DNS amplification attacks.

You can read about them here:

https://www.google.com/search?q=dns+open+resolver+amplification+attack

Let us know if you have additional questions or concerns.

Regards,

NTT Communications Global IP Network Security Team

Results

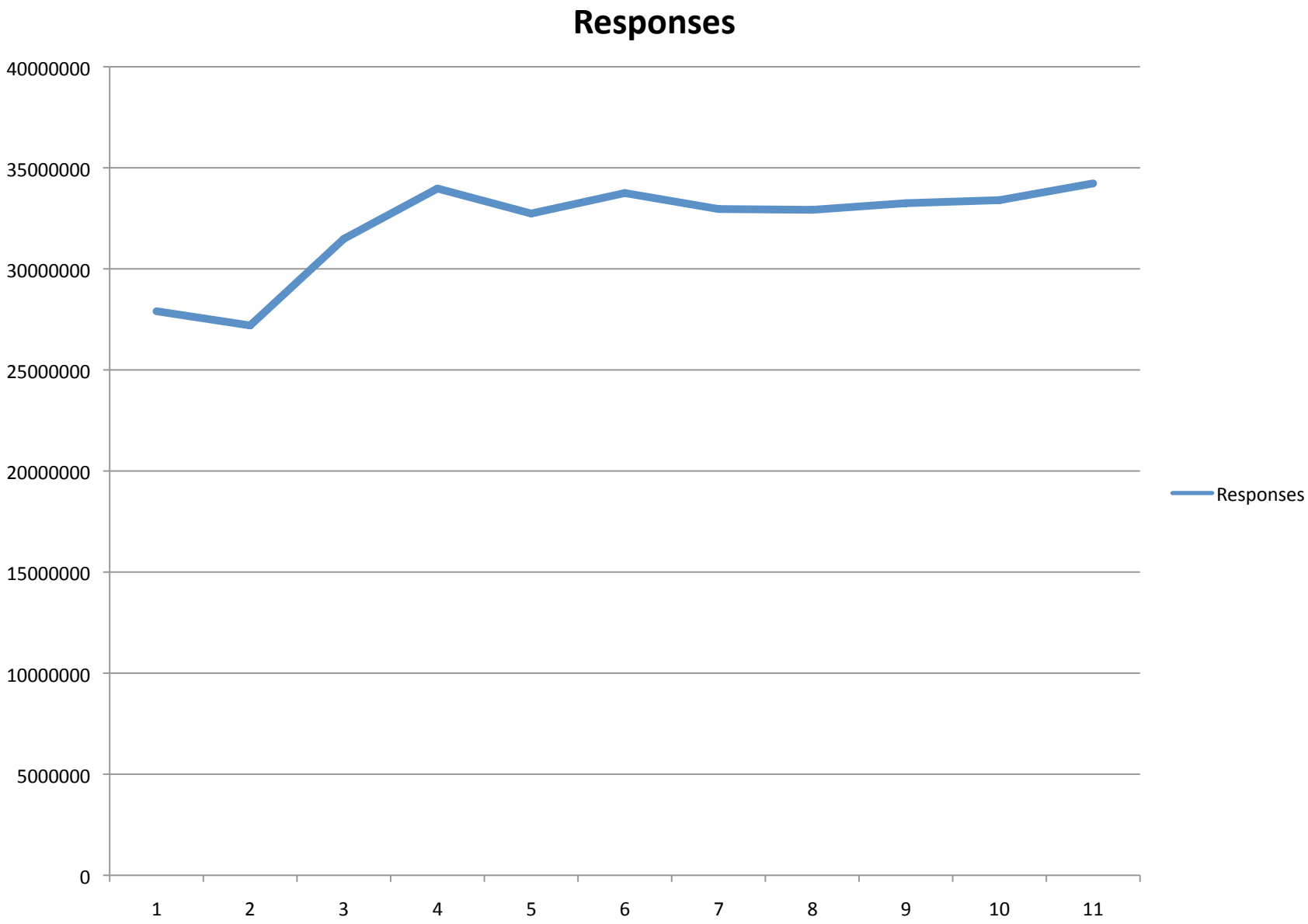
- Generates about 9.5GB of raw data per week
- Captures unix time_t, IP Address, Port and data packet

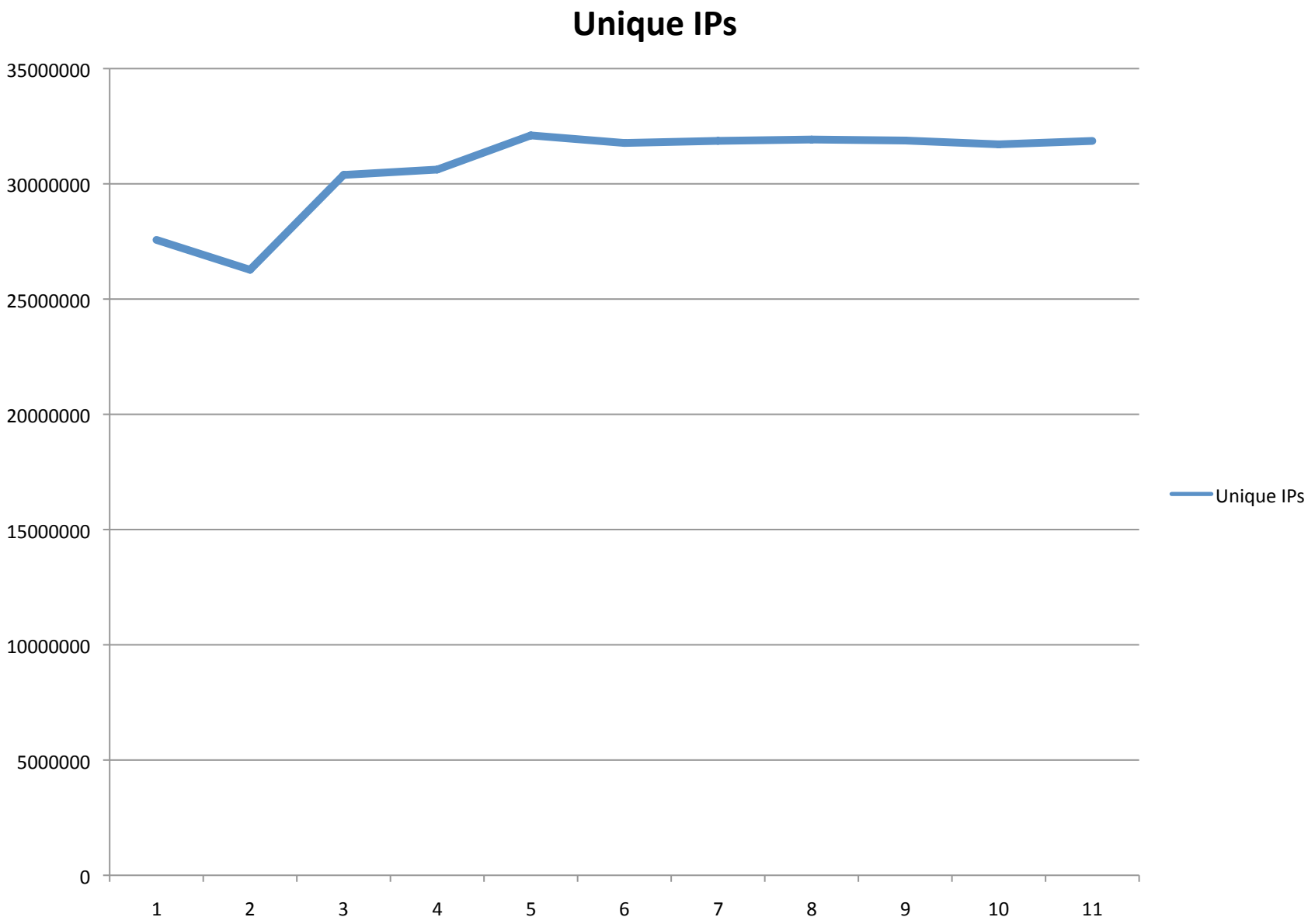
- 1367734028.41022:112.207.253.255:14432:fdff8180000100020003
0004083339383662346236136f70656e7265736f6c76657270726f6
a656374036f72670000010001c00c000500100000e100002c015c0
150001000100000ca50004cc2afe05**c01500020001000 00ca500120
574686f726e09626c61636b726f7365c029c01500020001000 00ca5
000f05616e796e730370636 8036e657400c01500020001000 00ca50
00e047075636b066e6574686572c084c095000100010 0013bf20004
cc2afe05c095001c000100013bf200102001041803f4000000000000
00000005c07a00010001000 1304c0004cc3dd804c05c00010001000
0fbad0004cc2afe07**

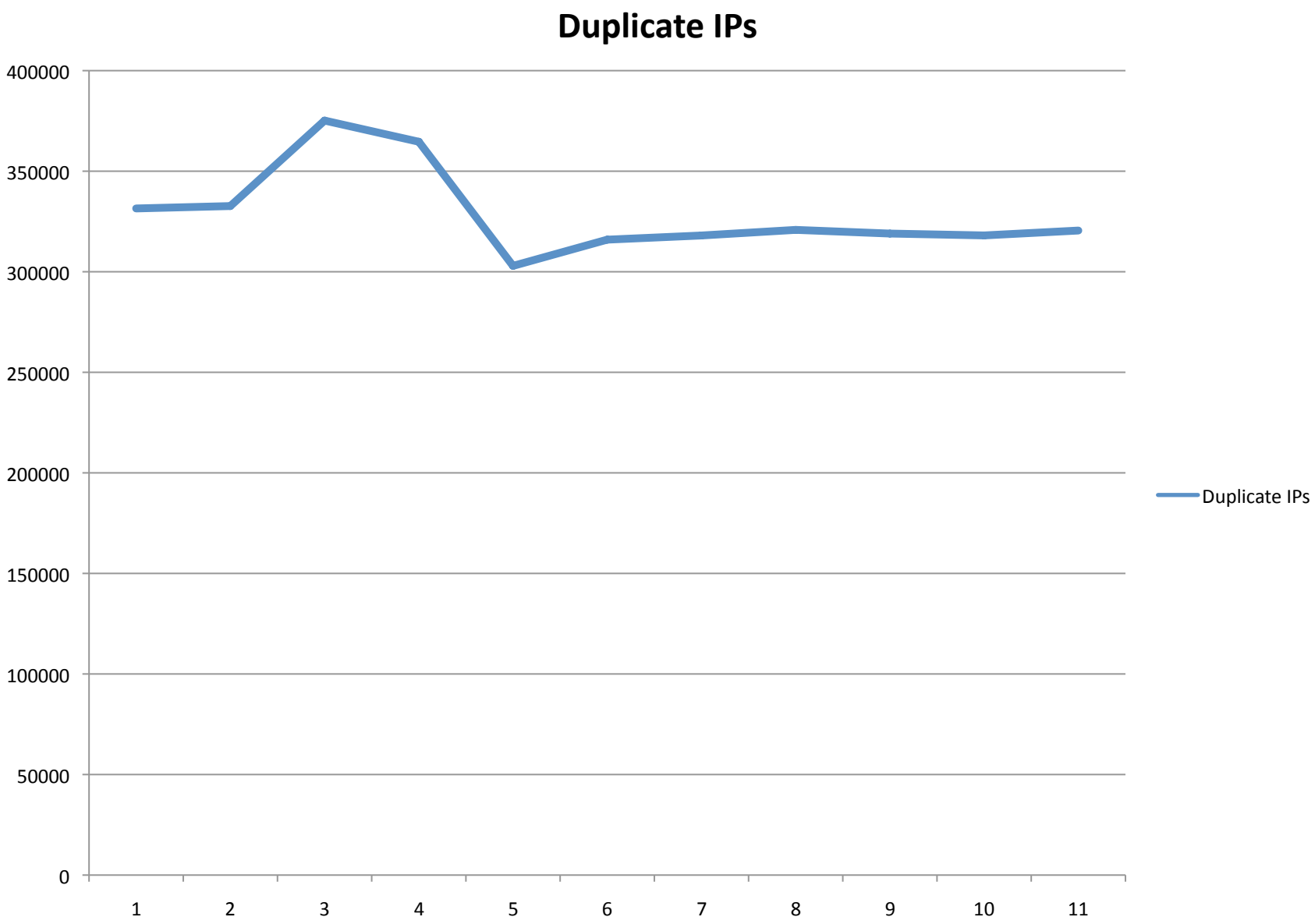
Weekly Statistics

2013-06-02 results

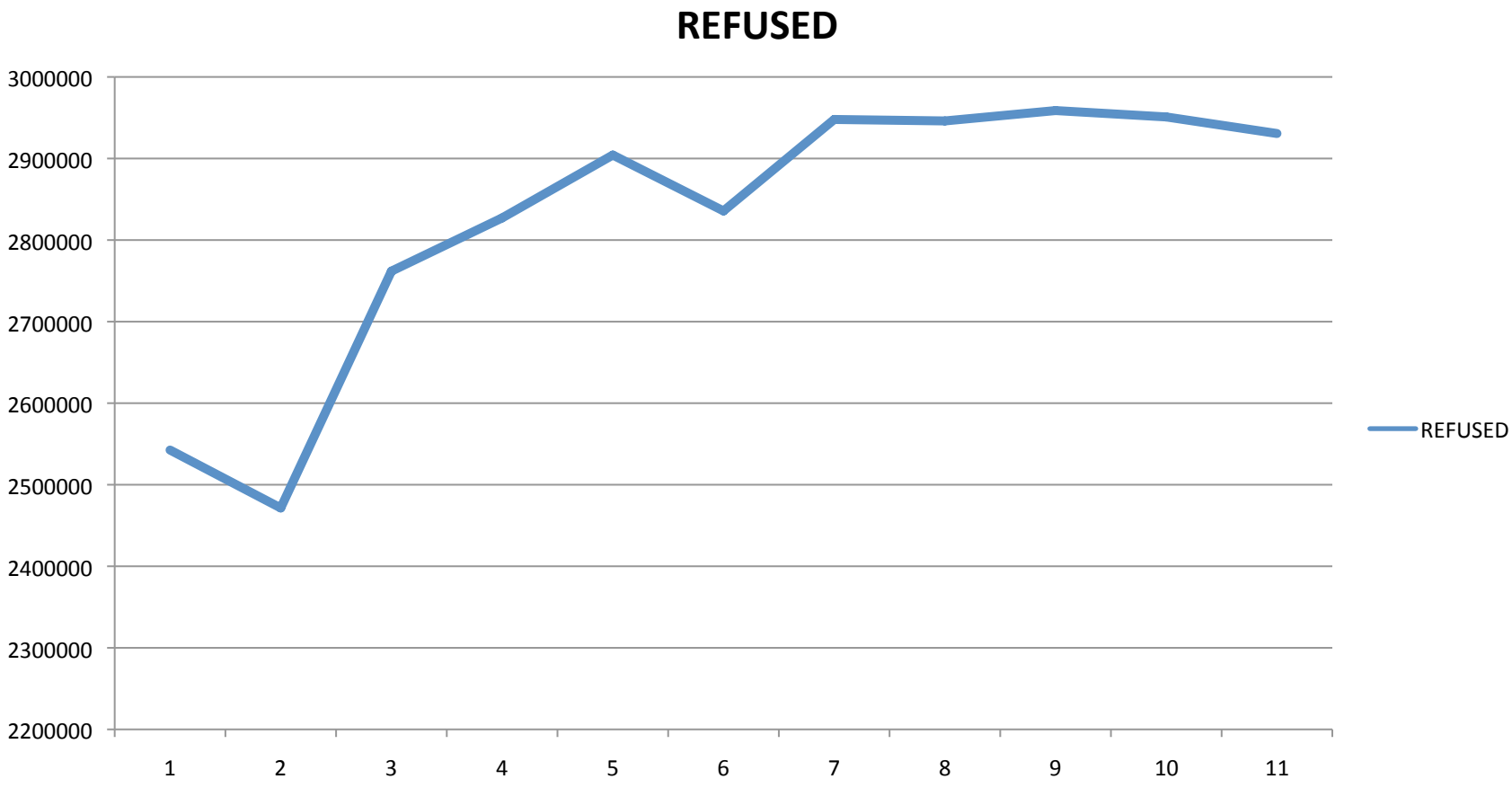
34,227,822 servers responded to udp/53 probe
31,860,982 unique IPs
320,493 IPs responded more than once
797,657 servers responded from a different IP than probed
29,207,283 gave the correct answer to the A? for the DNS name queried
14,951,390 responded from a source port other than udp/53
29,720,118 responses had recursion-available bit set
30,558,673 returned OK (RCODE=0)
5,654 returned FORMERR (RCODE=1)
548,423 returned SERVFAIL (RCODE=2)
183,022 returned NAMEFAIL (RCODE=3)
103 returned NOTIMP (RCODE=4)
2,930,646 returned REFUSED (RCODE=5)


Responses
40000000
35000000
30000000
25000000
20000000
15000000
10000000
5000000
0
1
2
3
4
5
6
7
8
9
10
11
Responses

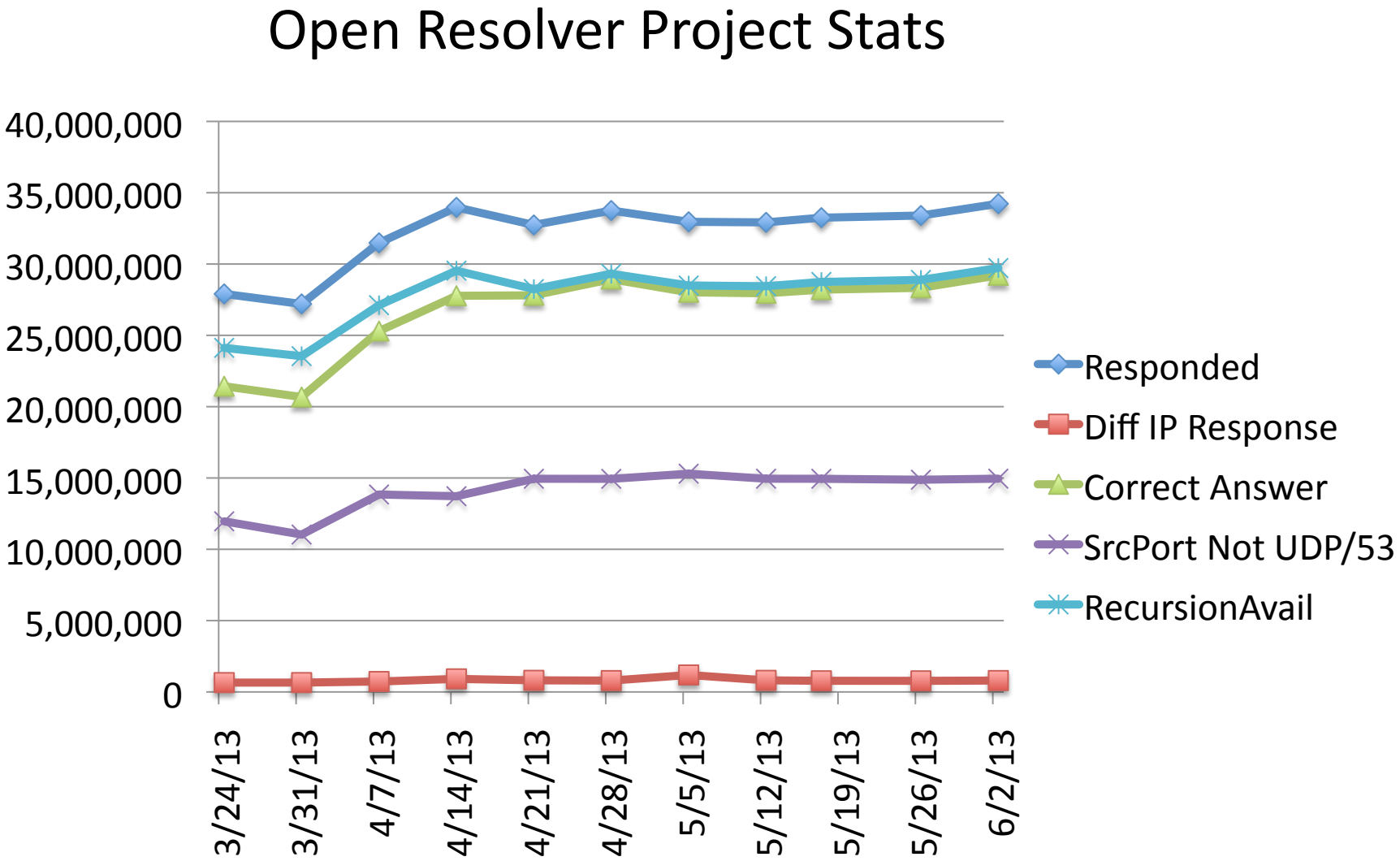

Unique IPs
35000000
30000000
25000000
20000000
15000000
10000000
5000000
0
1
2
3
4
5
6
7
8
9
10
11
Unique IPs


Duplicate IPs
400000
350000
300000
250000
200000
150000
100000
50000
0
1
2
3
4
5
6
7
8
9
10
11
Duplicate IPs

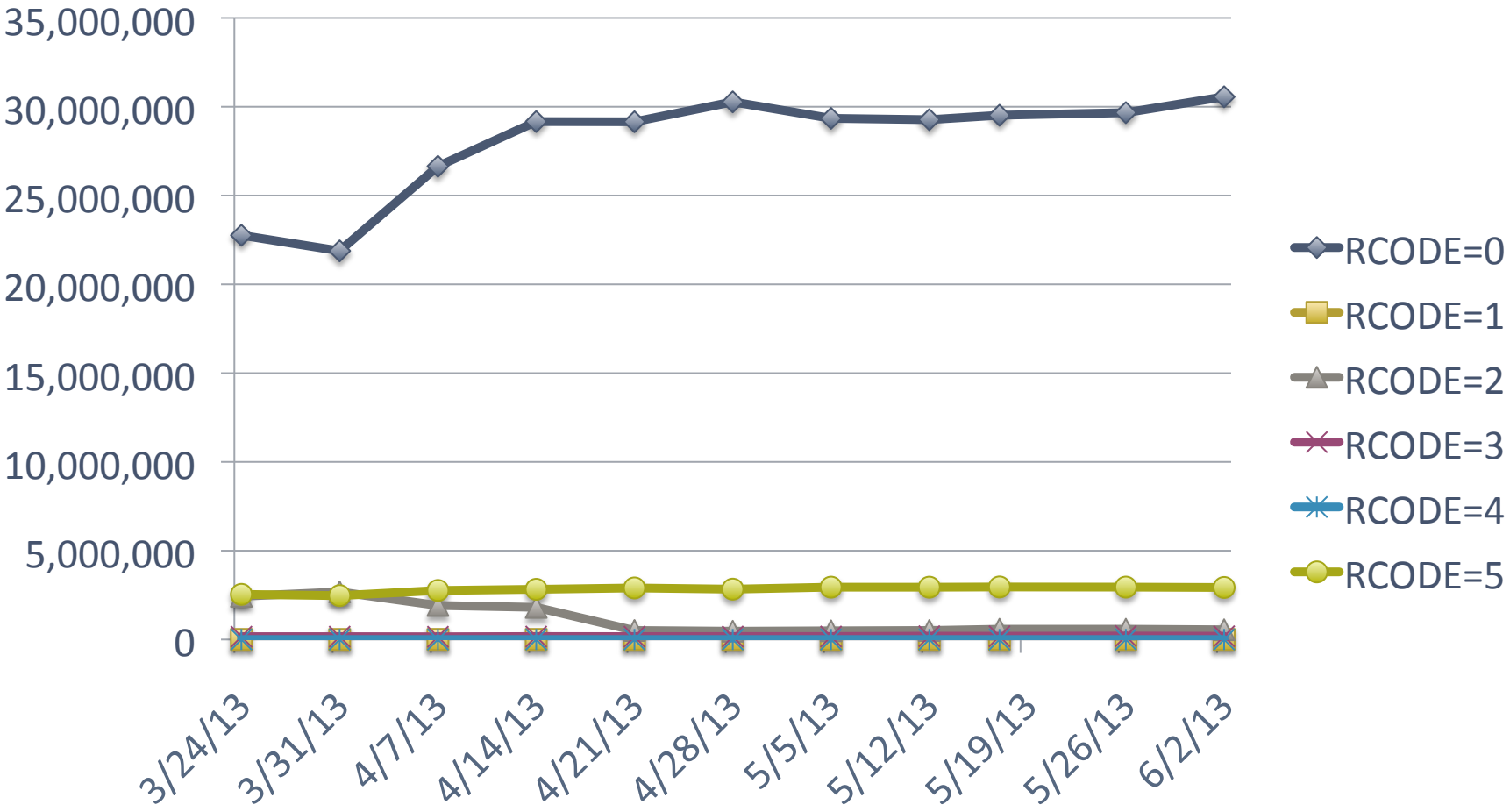
REFUSED trend



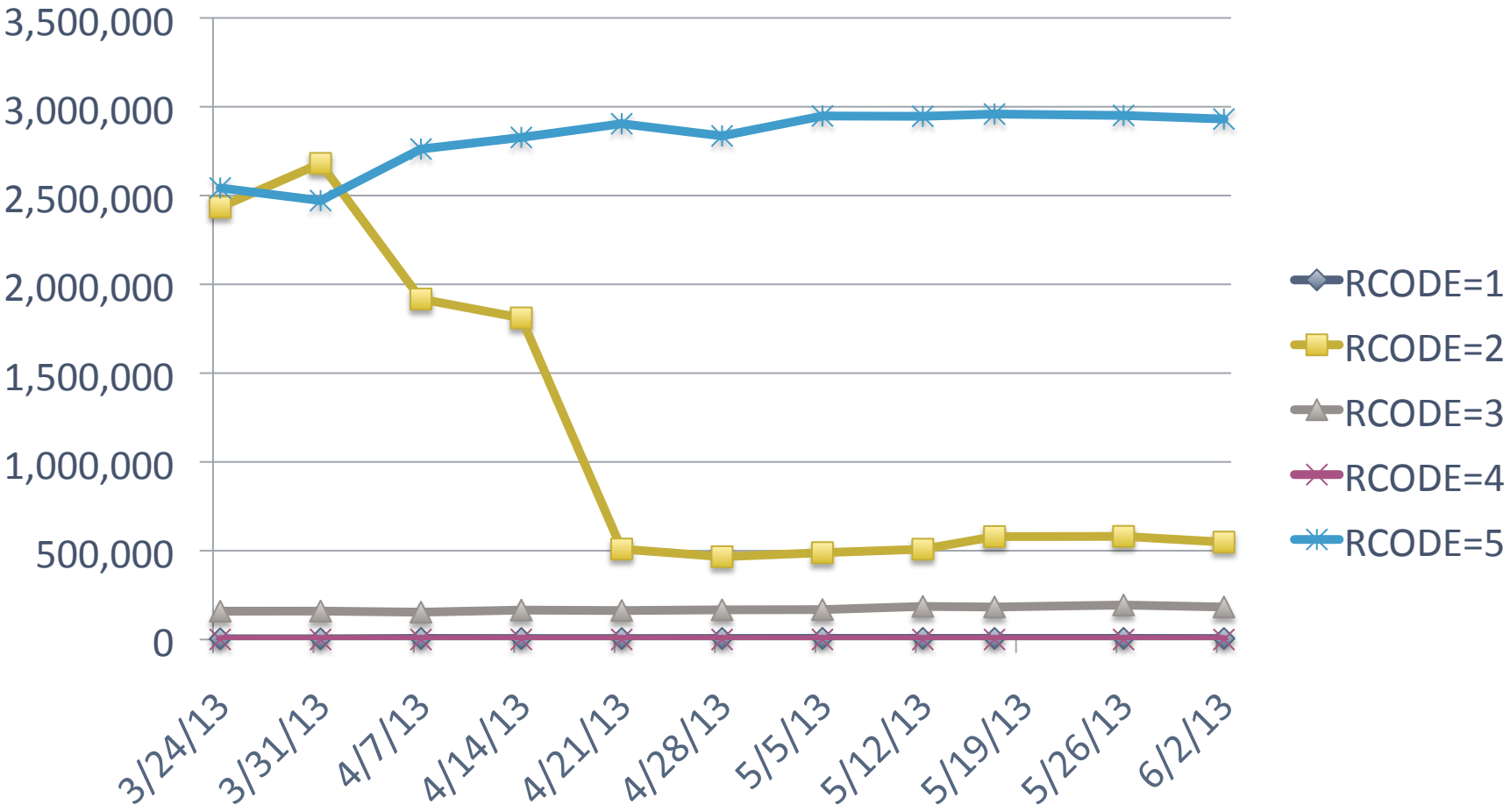
REFUSED	2542521	2471484	2761880	2827137	2904256	2835696	2947866
Responses	27904057	27200613	31485130	33974185	32737746	33750145	32959644
	9.11%	9.09%	8.77%	8.32%	8.87%	8.40%	8.94%


Open Resolver Project Stats
40,000,000
35,000,000
30,000,000
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
3/24/13
3/31/13
4/7/13
4/14/13
4/21/13
4/28/13
5/5/13
5/12/13
5/19/13
5/26/13
6/2/13
Responded
Diff IP Response
Correct Answer
SrcPort Not UDP/53
RecursionAvail

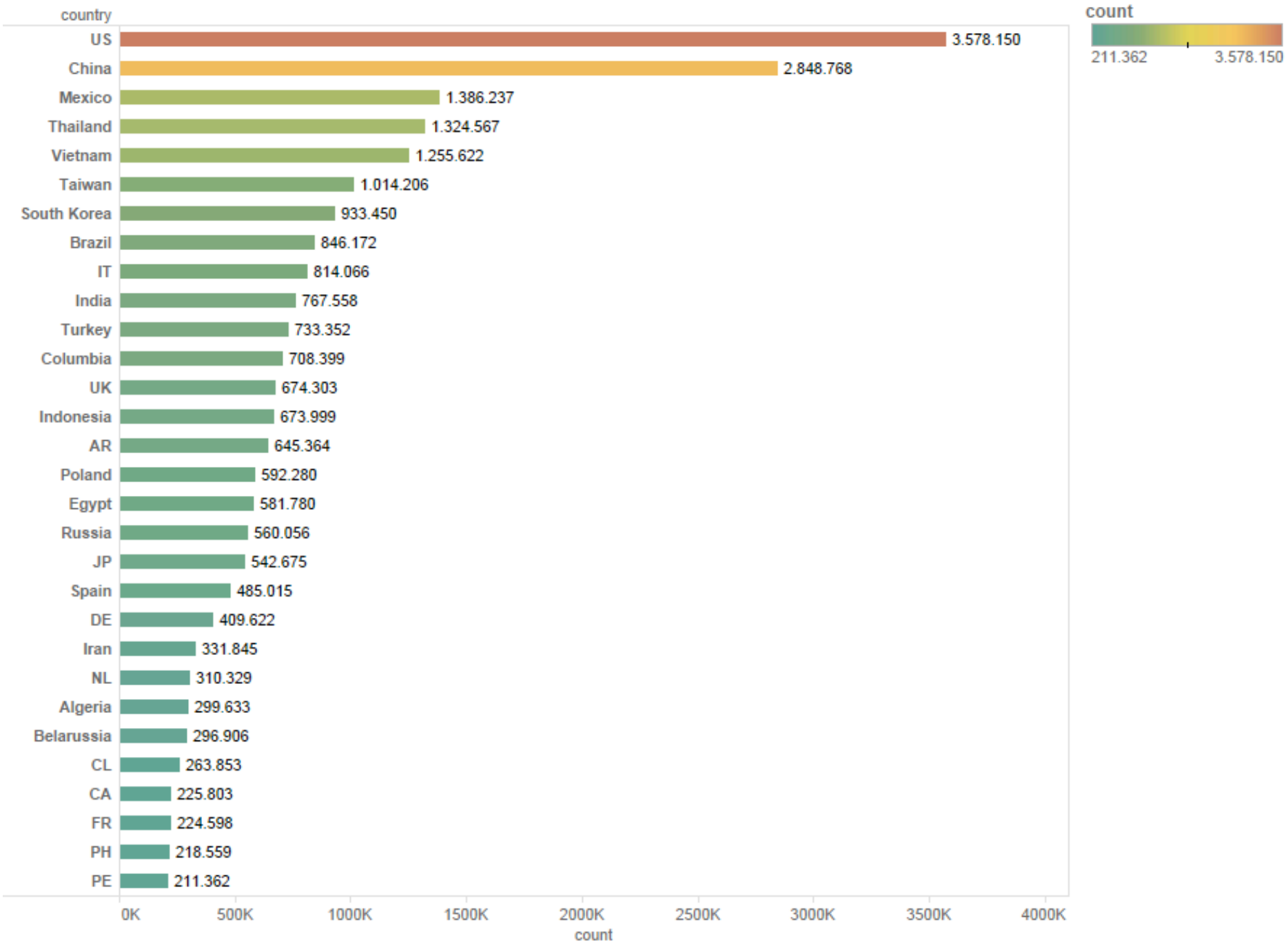
Open Resolver Project RCODE Stats



Open Resolver Project RCODE Stats(2)



Number of ORNs per country



Many devices do something odd..

- Many CPE devices listen on WAN interface
  - skbroadband is most common version.bind
- Android phones become open resolvers with tethering
- 0.18% respond with RA (recursion available) but wrong answer
- 46% of hosts respond from non port 53

UDP/53 is for DNS, right?

Sending a packet to UDP/53 gets a reply from another port

```
02:17:56.649949 IP x.x.x.x.45946 > 88.248.189.4.domain: 34307+ [1au]
TXT CHAOS? version.bind. (41)
    0x0000:  4500 0045 72ca 0000 4011 28b4 xxxx xxxx  E..Er...@.(..*..
    0x0010:  58f8 bd04 b37a 0035 0031 df6c 8603 0120  X....z.5.1.l....
    0x0020:  0001 0000 0000 0001 0776 6572 7369 6f6e  .........version
    0x0030:  0462 696e 6400 0010 0003 0000 2910 0000  .bind.......)...
    0x0040:  0000 0000 00                             .....
02:17:56.908332 IP 88.248.189.4.10002 > x.x.x.x.45946: UDP, length 62
    0x0000:  4500 005a 45a6 4000 f411 61c2 58f8 bd04  E..ZE.@...a.X...
    0x0010:  xxxx xxxx 2712 b37a 0046 85bb 8603 8500  .*..'..z.F......
    0x0020:  0001 0001 0000 0001 0776 6572 7369 6f6e  .........version
    0x0030:  0462 696e 6400 0010 0003 c00c 0010 0003  .bind...........
    0x0040:  0000 0000 0009 0839 2e38 2e31 2d50 3100  .......9.8.1-P1.
    0x0050:  0029 1000 0000 0000 0000                 .).........
```

Other hosts respond

- 3.6% of IPs probed had another IP respond back
- Typically CPE that did NAT on WAN interface
  - CPE respond to network and broadcast addresses
  - Host/CPE is allowed to spoof my IP
  - Provides small map of providers without BCP-38

Remediation Response

- Given out thousands of ASN reports
  - LINX contacting members
- Some providers have mitigated most resolvers
- Hosting providers contacting customers to disable open resolvers
  - http://status.ovh.net/?do=details&id=4802
- Continue to get more feedback
- Japan Telecom-ISAC started project to fix networks, including CPE
- E-Mailed reports to top-ASNs with open resolvers

Remediation Response

- NTT has restarted project to lock-down packet spoofing at network edge
  - First weeks of reports had more bogons that replied
  - Much better now
- Many folks reconfigured bind
- Even with recursion off you need:
  - additional-from-auth no;
  - additional-from-cache no;
- Hosting providers are changing defaults

Thank You & Questions?

- Thanks to:
  - NTT Communications
  - Merike Kaeo
  - Aaron Kaplan
  - Heather Schiller
- Please Visit www.openresolverproject.org
- RRL
  - http://www.redbarn.org/dns/ratelimits
- TCP ANY patch
  - http://puck.nether.net/~jared/bind-9.9.3rc2-tcp-any.patch
- QUESTIONS?