Thirteen Years of “Old J-Root”

DNS-OARC Fall 2015 Workshop, Montreal

Duane Wessels, Jason Castonguay, Piet Barber

October, 2015

Abstract

Thirteen years ago Verisign renumbered j.root-servers.net so that it could be anycasted. Since that time, we have been continuing to answer queries sent to the old IP address. We have also been collecting some data on queries to old J-root.

In this presentation we will explore such questions as: what do we know about the clients of old J-root? Do they overlap with clients of the real J-root? Are there noticeable differences in traffic characteristics (e.g., EDNS, DNSSEC, query types) between the two? Does old J-root traffic fluctuate in the same way as real traffic? When real J-root gets attacked, does old J-root also get attacked? If so, can this be used to identify attacks coming through recursive name servers?

Old J-Root -- 198.41.0.10

- January 1997
  - j.root-servers.net begins serving with address 198.41.0.10 [1]
  - same /24 as a.root-servers.net
- February 2002
  - j.root-servers.net renumbered to 192.58.128.30 [2]
  - in preparation for anycasting
- November 2002
  - root zone finally reflects new J-Root address [3]
- September 2015
  - 198.41.0.10 still receives and responds to queries
  - Can we turn it off yet?

[1] Postel to namedroppers 1997-01-23
[2] https://www.nanog.org/mailinglist/mailarchives/old_archive/2002-11/msg00035.html
[3] DNS-OARC Root Zone Archive

Root Server Renumberings

Date	Letter	Old IP	New IP
2002-11-05	J	198.41.0.10	192.58.128.30
2004-01-29	B	128.9.0.107	192.228.79.201
2007-11-01	L	198.32.64.12	199.7.83.42
2013-01-03	D	128.8.10.90	199.7.91.13
Upcoming:			
2015-12-01	H	128.63.2.53	198.97.190.53
2015-12-01	H	2001:500:1::803f:235	2001:500:1::53

Sources of Data

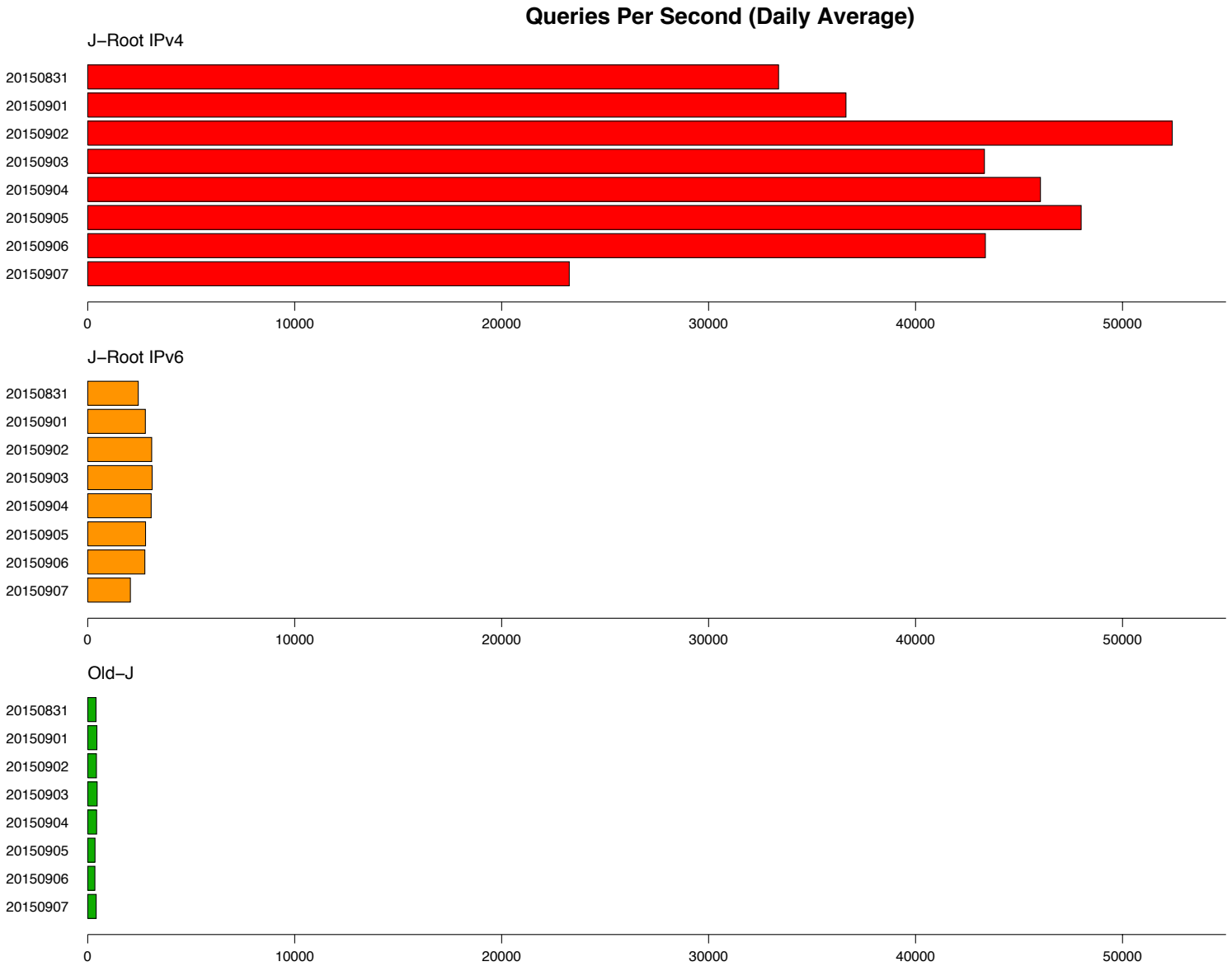
- Full pcaps for the week of Aug 31 - Sept 7, 2015
  - Approximately 12 Terabytes
  - 1,900,000 files
  - 87 datacenter sites (J-Root & Old J-Root)

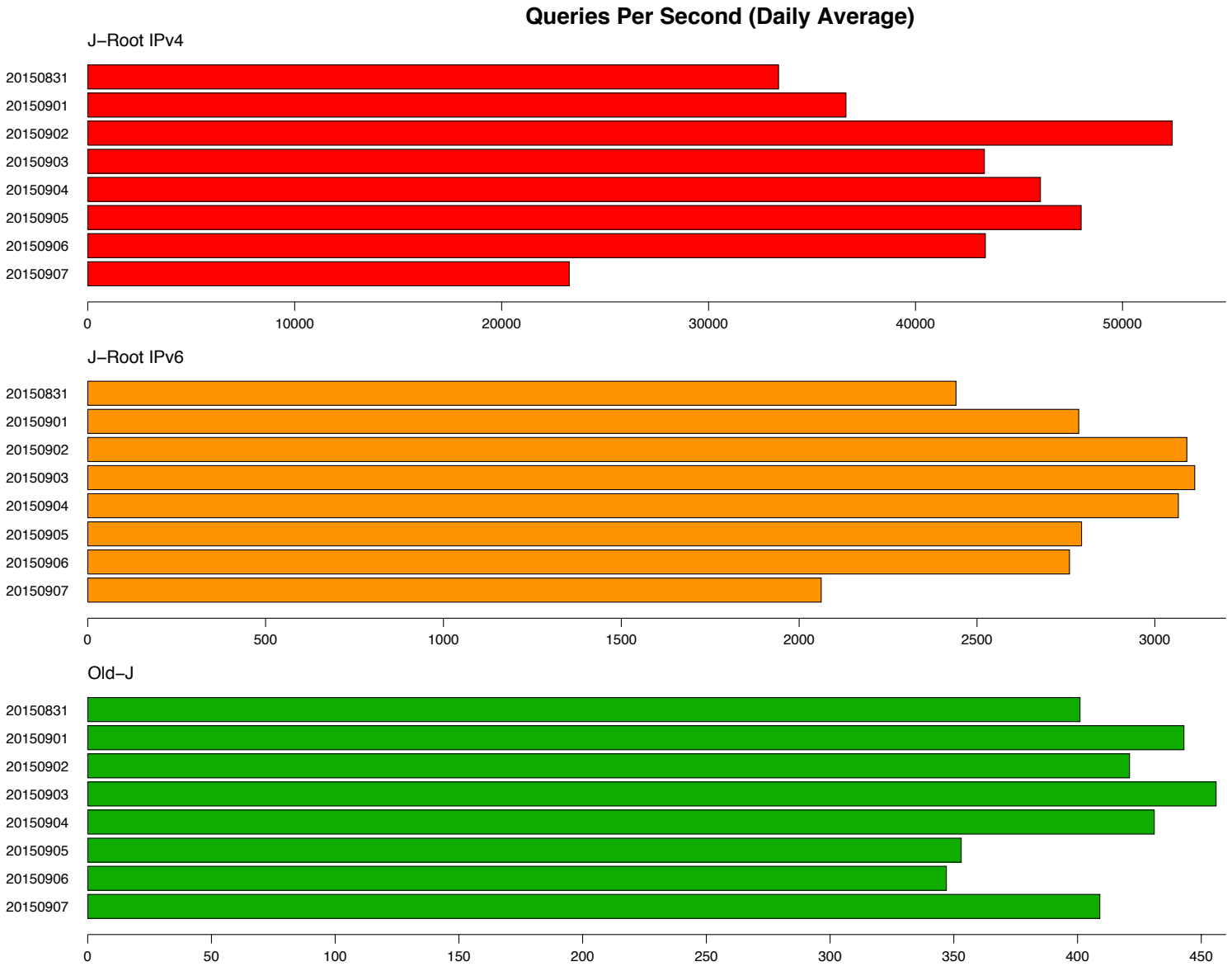
- Long term aggregated counts by protocol and query type back to the year 2000.
  - No IP addresses
  - Approximately 3,600,000,000 rows of data

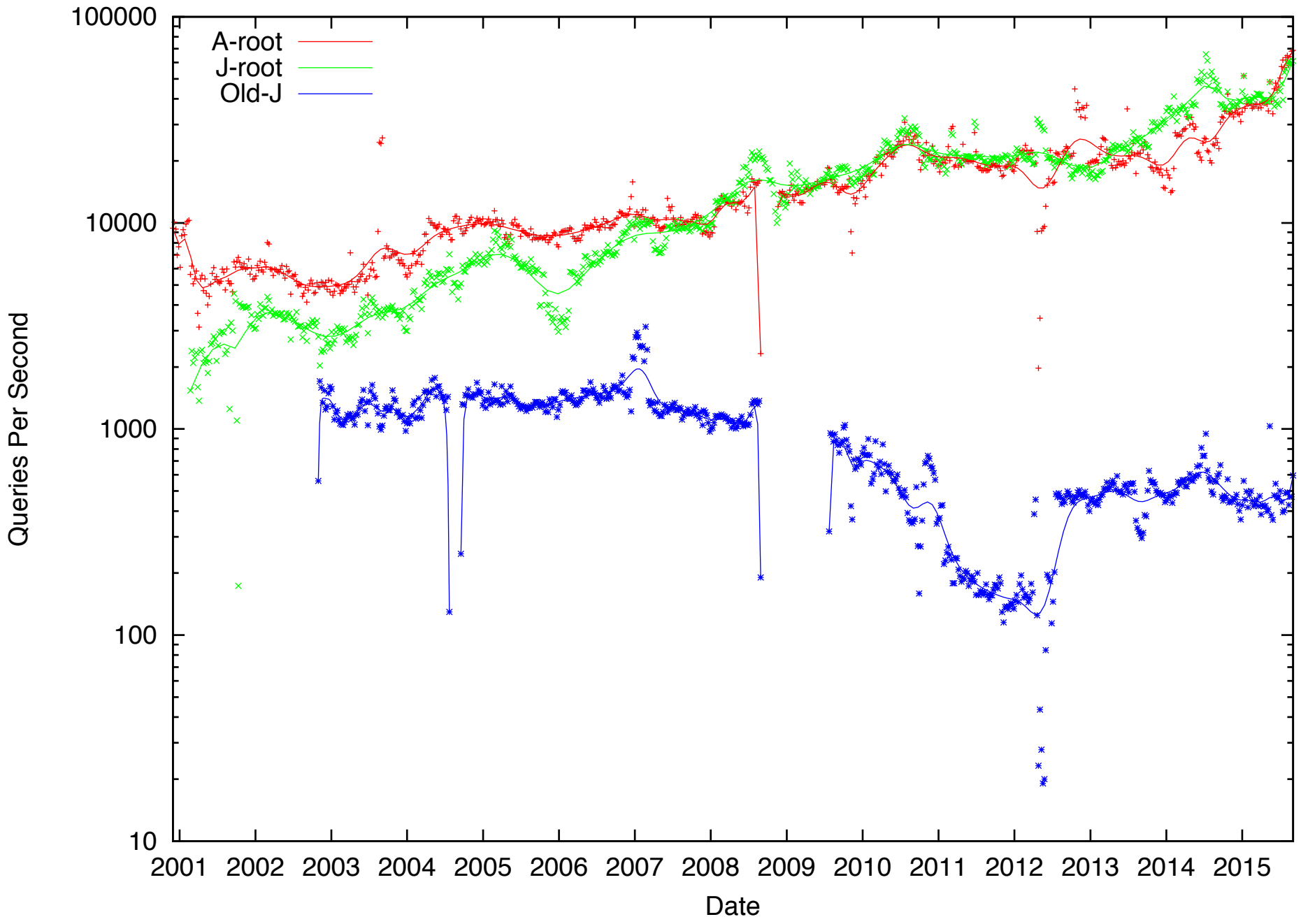
Traffic Volume Patterns

Short Term Average Queries Per Second

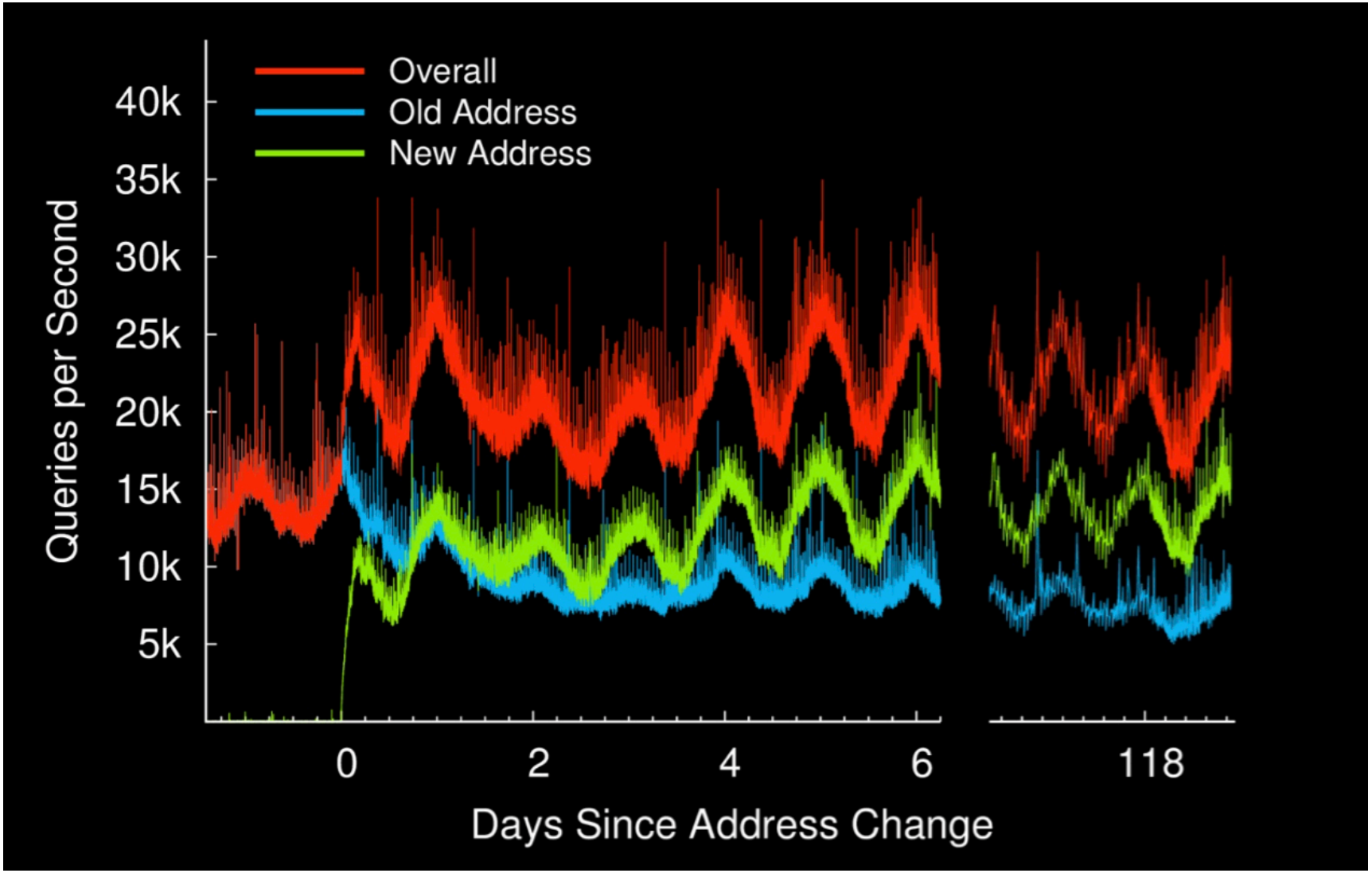
Date	J IPv4	J IPv6	Old J
2015-08-31 (Mo)	33,382	2,441	401
2015-09-01 (Tu)	36,637	2,786	443
2015-09-02 (We)	52,402	3,090	421
2015-09-03 (Th)	43,326	3,112	456
2015-09-04 (Fr)	46,034	3,066	431
2015-09-05 (Sa)	48,001	2,794	353
2015-09-06 (Su)	43,372	2,760	347
2015-09-07 (Mo)	23,267	2,062	409


Queries Per Second (Daily Average)
J–Root IPv4
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
0
10000
20000
30000
40000
50000
J–Root IPv6
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
0
10000
20000
30000
40000
50000
Old–J
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
0
10000
20000
30000
40000
50000


Queries Per Second (Daily Average)
J–Root IPv4
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
0
10000
20000
30000
40000
50000
J–Root IPv6
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
0
500
1000
1500
2000
2500
3000
Old–J
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
0
50
100
150
200
250
300
350
400
450


A-root
J-root
Old-J
100000
10000
1000
100
10
Queries Per Second
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
Date

Compare With D-Root



http://www.cs.umd.edu/projects/droot/droot_imc2013_slides.pdf

Clients

Who queries Old J-Root?

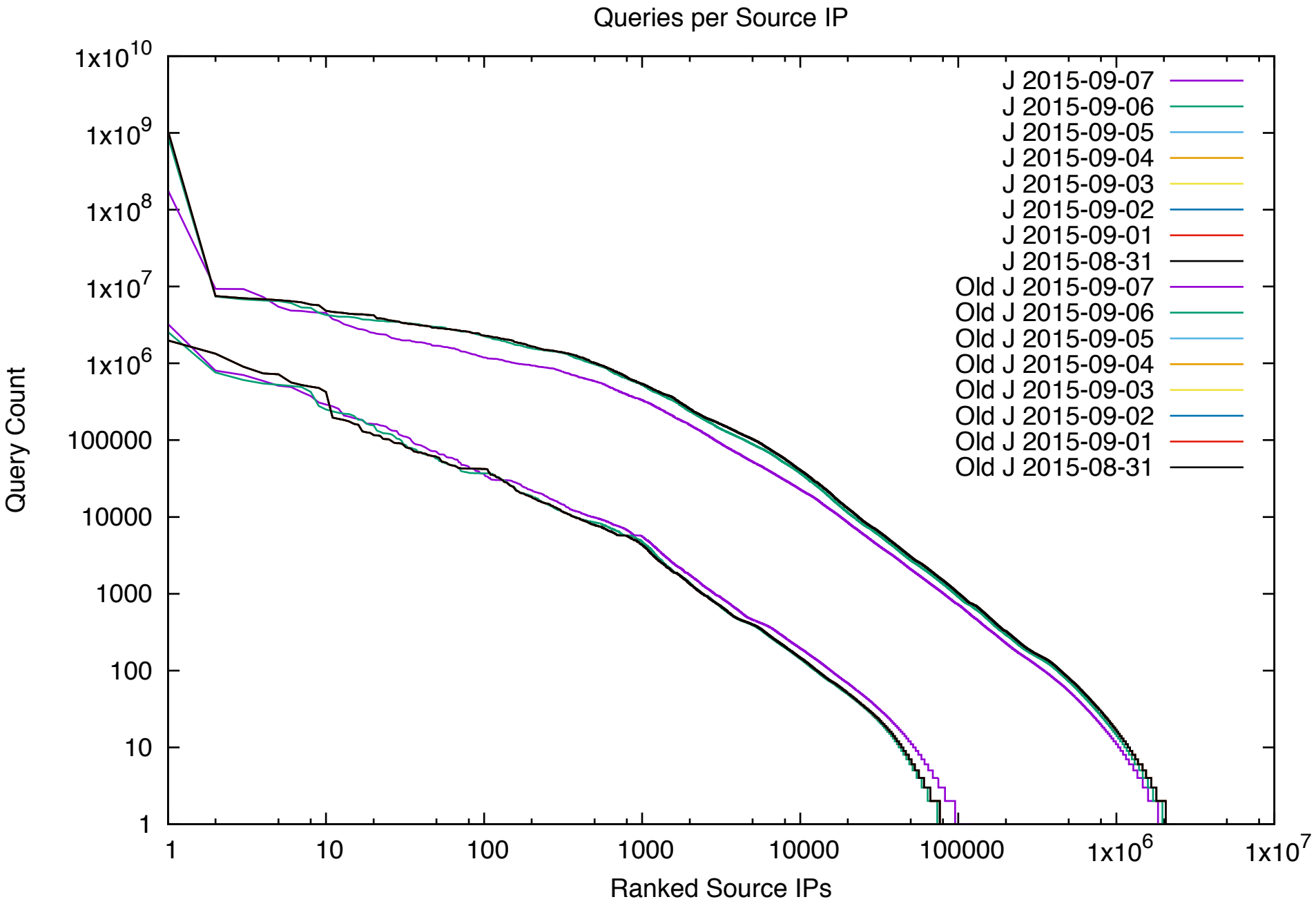
- Microsoft Windows NT4
  - Does not refresh server list with a priming query
- DJBDNS
  - Distributes old IP in dnsroots.global
  - Does update server list with priming query
- Others?

Fingerprinting Clients

Count	fpdns Fingerprint
838	TIMEOUT
87	ISC BIND 9.2.3rc1 -- 9.4.0a4 [Old Rules]
22	DJ Bernstein TinyDNS 1.05 [Old Rules]
10	No match found
8	Microsoft Windows DNS 2003 [New Rules]
7	Microsoft Windows DNS 2000 [New Rules]
7	ISC BIND 9.3.0 -- 9.3.6-P1 [New Rules]
5	ISC BIND 9.6.3 -- 9.7.3 [New Rules]
2	Microsoft Windows DNS NT4 [Old Rules]
2	Microsoft Windows DNS 2000 [Old Rules]
2	ISC BIND 9.2.3rc1 -- 9.4.0a4 [recursion enabled] [Old Rules]
2	ISC BIND 9.2.0 -- 9.2.2-P3 [New Rules]
1	bboy MyDNS [Old Rules]
1	Unlogic Eagle DNS 1.1.1 [New Rules]
1	NLnetLabs NSD 3.1.0 -- 3.2.8 [New Rules]
1	Mikrotik dsl/cable [Old Rules]
1	ISC BIND 9.7.2 [New Rules]
1	ISC BIND 9.6.0 OR 9.4.0 -- 9.5.1 [New Rules]
1	ISC BIND 9.5.2 -- 9.7.1 [New Rules]
1	ISC BIND 8.1-REL -- 8.2.1-T4B [recursion enabled] [Old Rules]

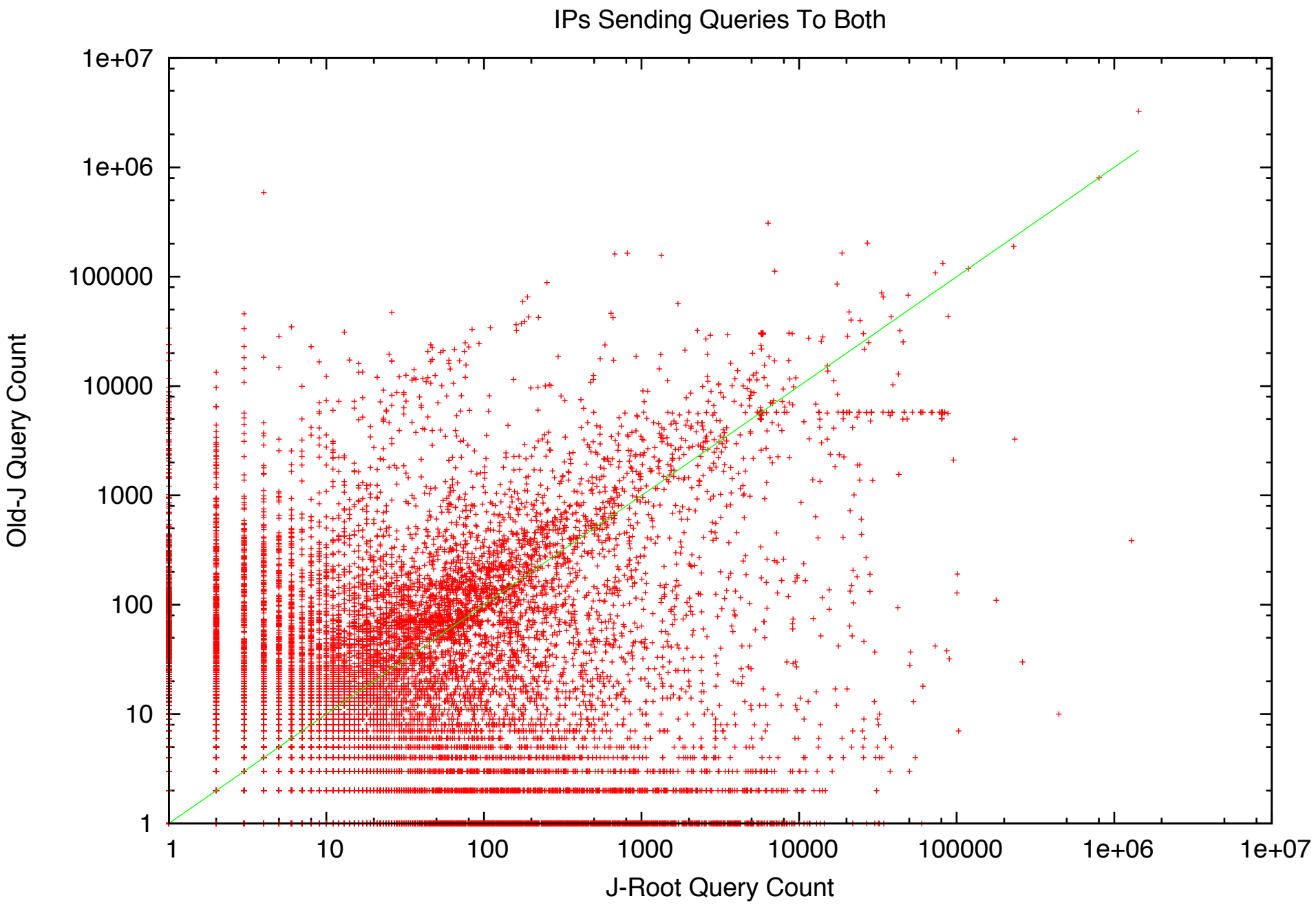
Number of Source IPs Seen Per Day

Date	J-Root	Old J-Root
2015-08-31 (Mo)	2,587,932	130,411
2015-09-01 (Tu)	2,670,339	129,597
2015-09-02 (We)	2,918,316	130,146
2015-09-03 (Th)	2,854,505	129,903
2015-09-04 (Fr)	2,780,233	125,819
2015-09-05 (Sa)	2,420,385	96,962
2015-09-06 (Su)	2,311,585	93,746
2015-09-07 (Mo)	2,195,234	122,649


Queries per Source IP
Query Count
Ranked Source IPs
1x10^10
1x10^9
1x10^8
1x10^7
1x10^6
100000
10000
1000
100
10
1
1
10
100
1000
10000
100000
1x10^6
1x10^7
J 2015-09-07
J 2015-09-06
J 2015-09-05
J 2015-09-04
J 2015-09-03
J 2015-09-02
J 2015-09-01
J 2015-08-31
Old J 2015-09-07
Old J 2015-09-06
Old J 2015-09-05
Old J 2015-09-04
Old J 2015-09-03
Old J 2015-09-02
Old J 2015-09-01
Old J 2015-08-31

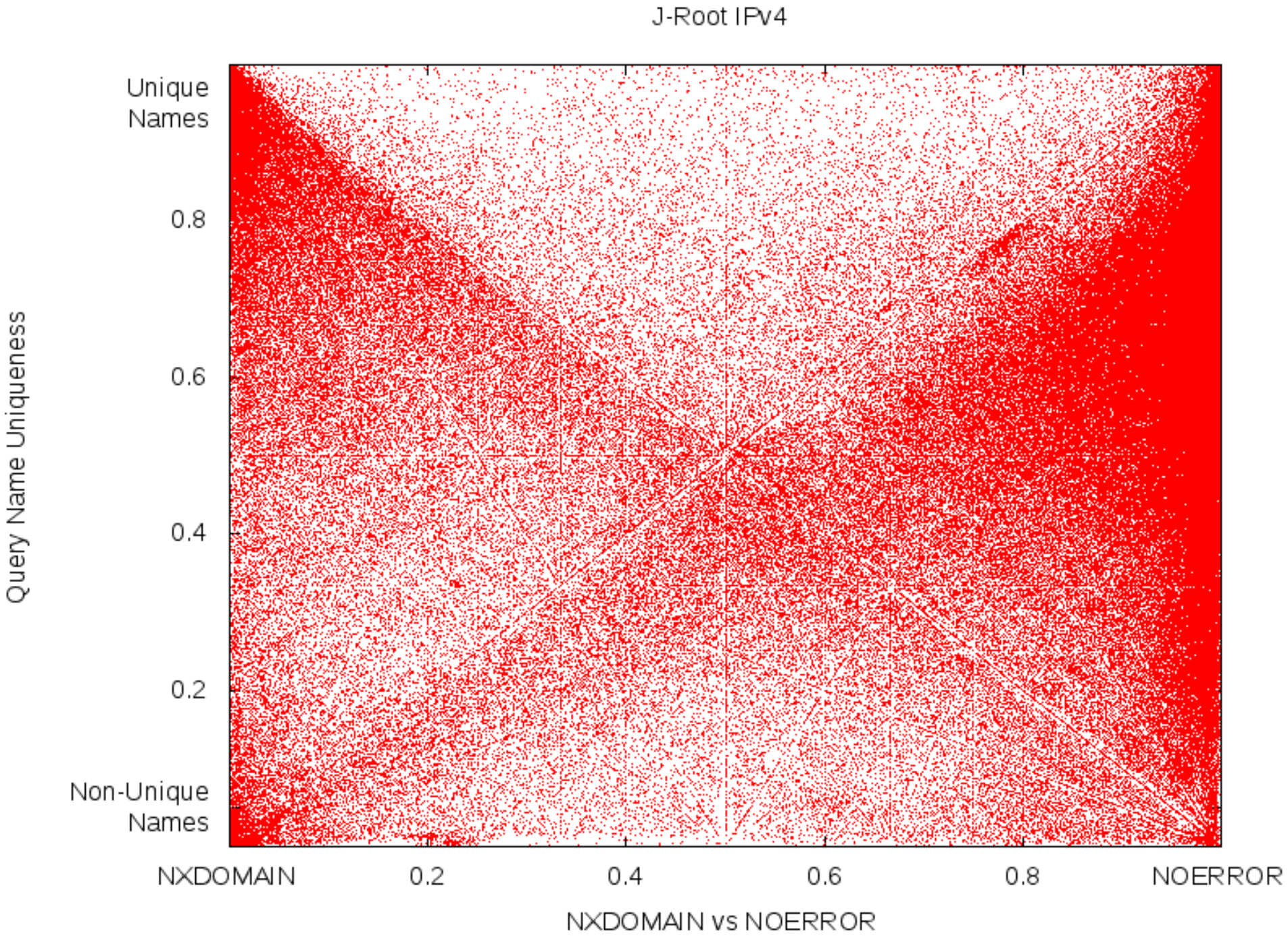
Number of Source IPs Seen at Both

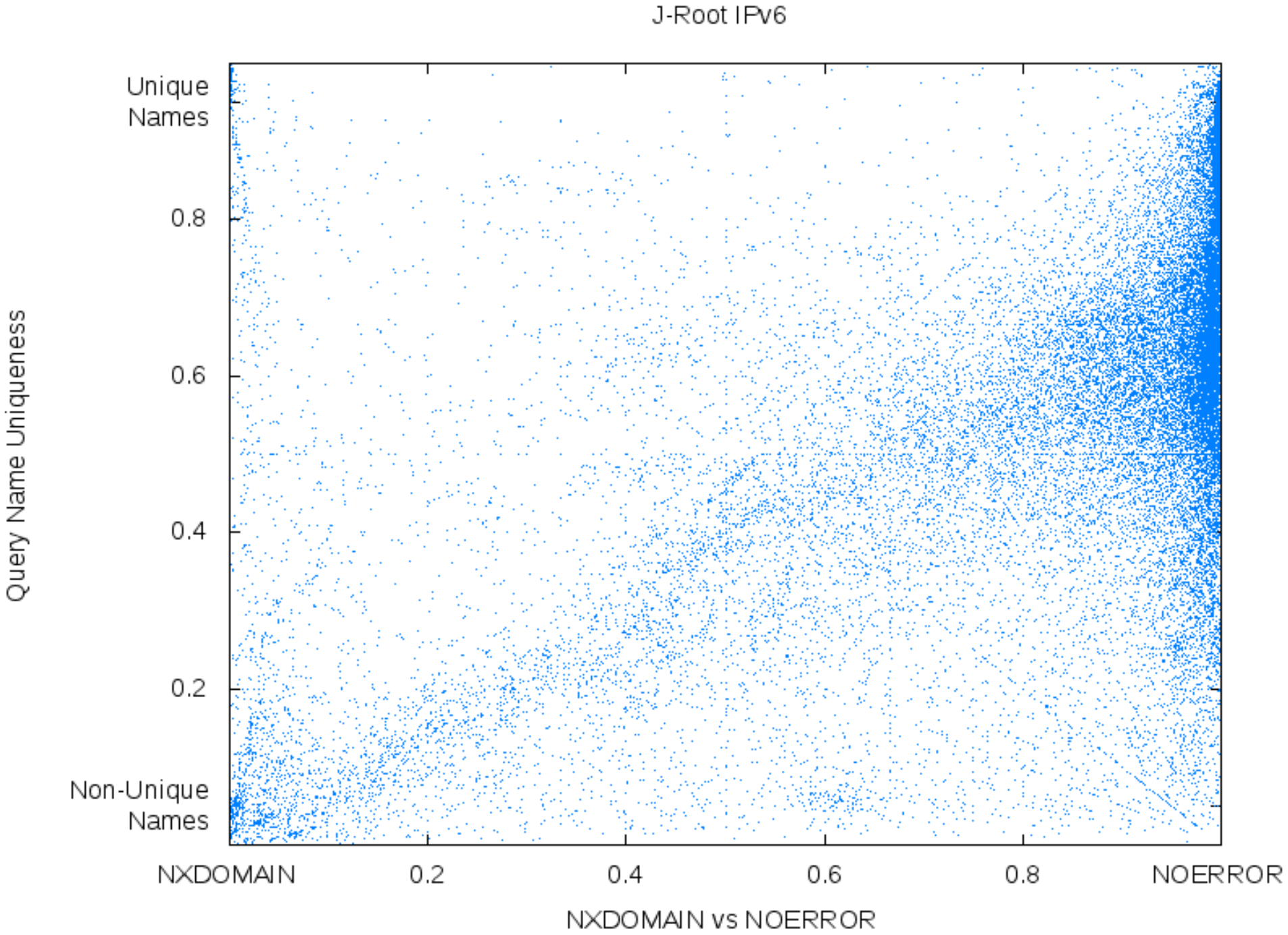
Date	J-Root & Old J-Root
2015-08-31 (Mo)	23,661
2015-09-01 (Tu)	24,990
2015-09-02 (We)	27,981
2015-09-03 (Th)	26,591
2015-09-04 (Fr)	25,718
2015-09-05 (Sa)	16,457
2015-09-06 (Su)	15,084
2015-09-07 (Mo)	18,836

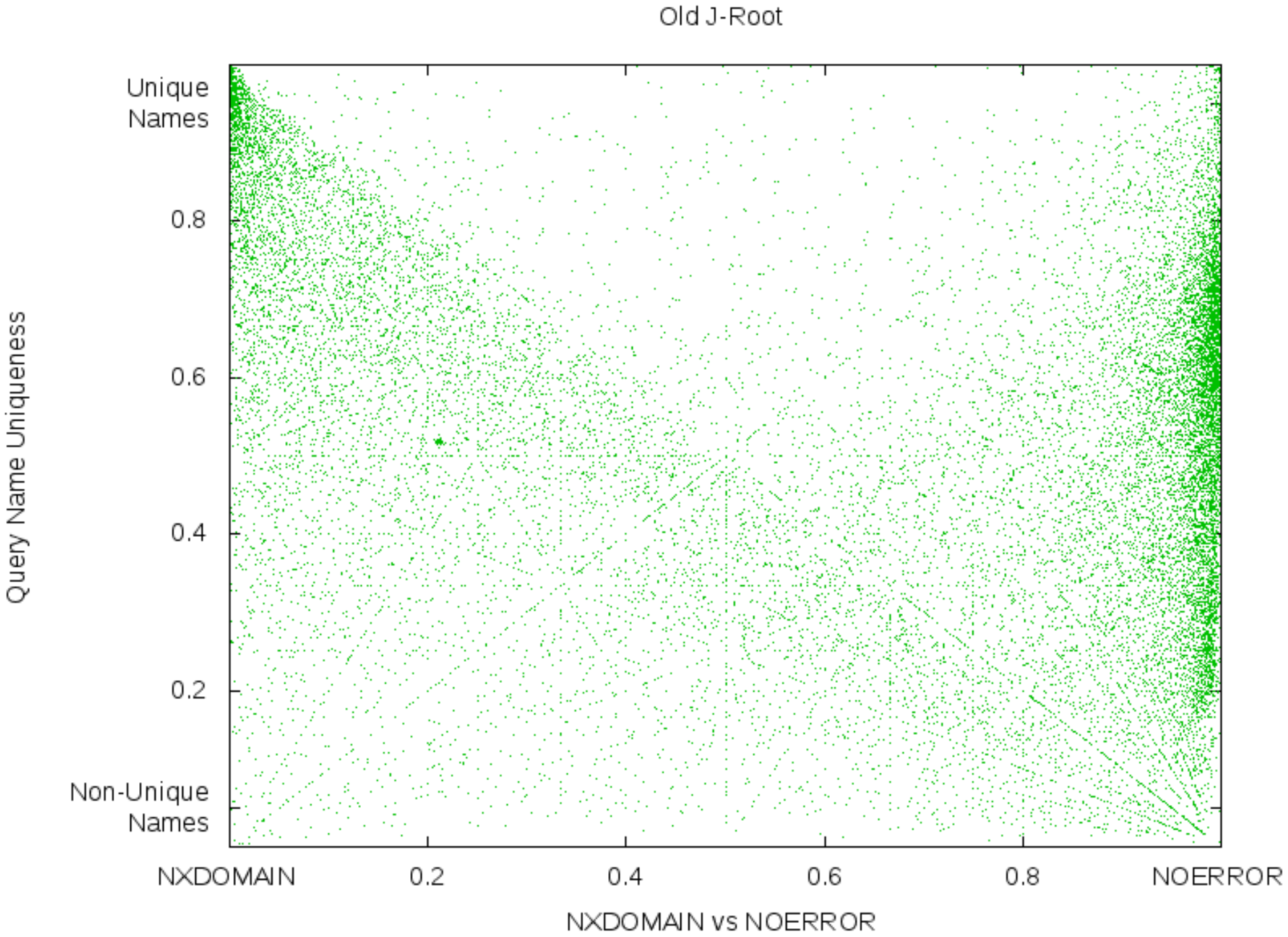

IPs Sending Queries To Both
Old-J Query Count
J-Root Query Count
1e+07
1e+06
100000
10000
1000
100
10
1
1
10
100
1000
10000
100000
1e+06
1e+07

Name Uniqueness vs Response Code

- Attempt to mimic University of Maryland analysis for D-Root
- X-axis: response code (NXDOMAIN vs NOERROR)
- Y-axis: query name uniqueness
  - low uniqueness -- all queries for same name
  - high uniqueness -- no repeated query names


J-Root IPv4
Unique Names
0.8
0.6
0.4
0.2
Non-Unique Names
Query Name Uniqueness
NXDOMAIN
0.2
0.4
0.6
0.8
NOERROR
NXDOMAIN vs NOERROR


J-Root IPv6
Unique Names
0.8
0.6
0.4
0.2
Non-Unique Names
Query Name Uniqueness
NXDOMAIN
0.2
0.4
0.6
0.8
NOERROR
NXDOMAIN vs NOERROR


Old J-Root
Unique Names
0.8
0.6
0.4
0.2
Non-Unique Names
Query Name Uniqueness
NXDOMAIN
0.2
0.4
0.6
0.8
NOERROR
NXDOMAIN vs NOERROR

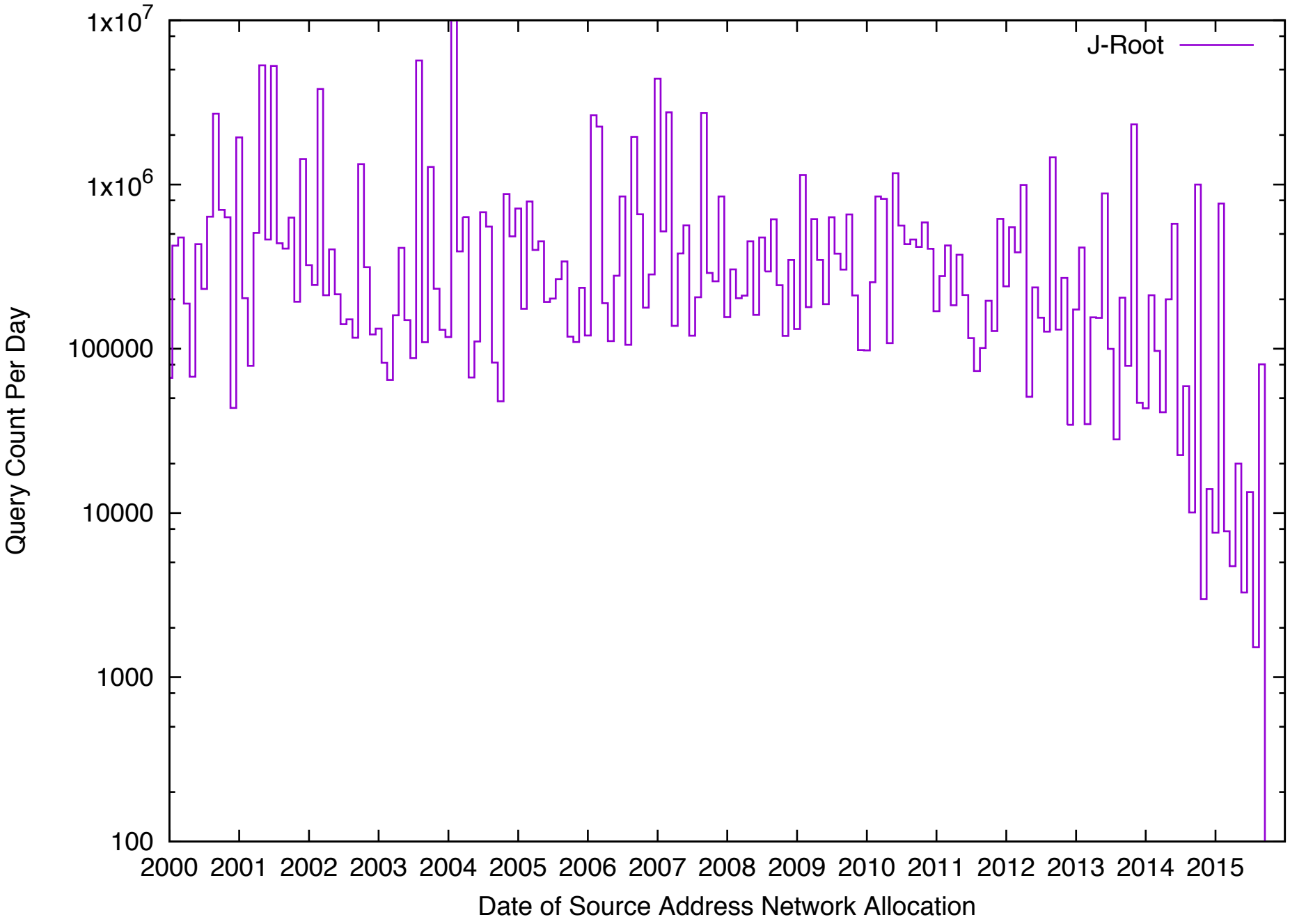
Old J-Root Top Talkers -- 2015-09-03

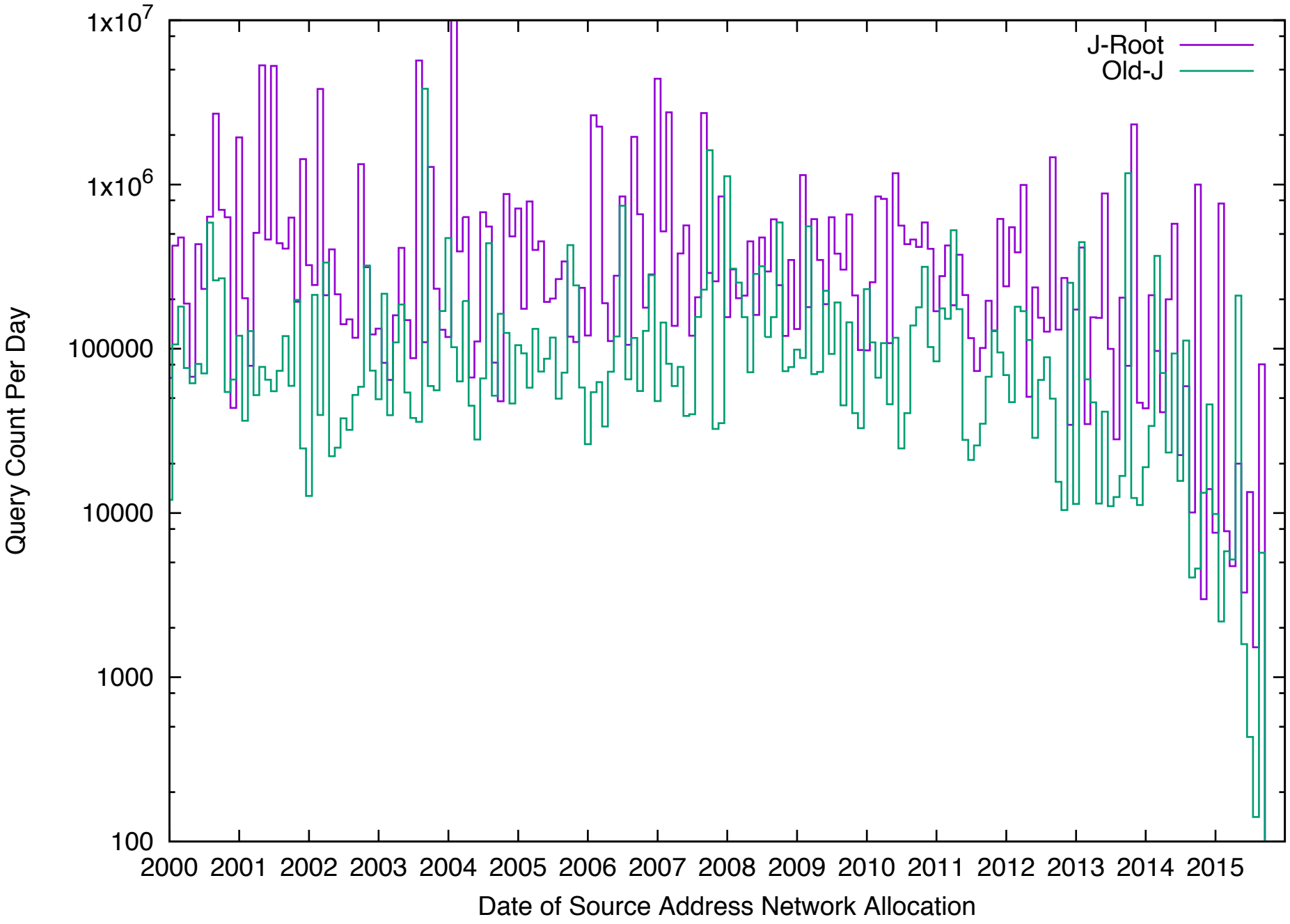
Query Count	ASN	Description
3,715,992	26454	HENRYSCHEIN - Henry Schein Inc,US
1,534,420	32081	DIGITALRIVER-DC2 - Digital River, Inc.,US
1,084,444	9008	AS9008 Visual Online S.A.,LU
1,056,367	20141	QUALITYTECH-SUW-300 - Quality ..., LLC.,US
721,805	8308	NASK-COMMERCIAL NAUKOWA I...,PL
698,575	16276	OVH OVH SAS,FR
572,081	5588	GTSCE T-Mobile Czech Republic a.s.,CZ
534,590	9318	HANARO-AS Hanaro Telecom Inc.,KR
527,674	11351	RR-NYSREGION-ASN-01 - Time Warner ...,US
521,618	37196	SUDATEL-SENEGAL,SN
517,498	17506	UCOM UCOM Corp.,JP
438,136	30729	TRANSFERTTK-AS Transfer ltd.,RU

Date of IP Network Allocation

- Does it matter when the source IP network was allocated by the RIR?
- Perhaps only “old” networks send queries to Old J-Root?
- Team Cymru ASN lookup provides date of allocation

- Old J-Root has ~130,000 source IPs on 2015-09-03
- Take random sample of 130,000 IPs from J-Root


J-Root
Query Count Per Day
1x10^7
1x10^6
100000
10000
1000
100
2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015
Date of Source Address Network Allocation

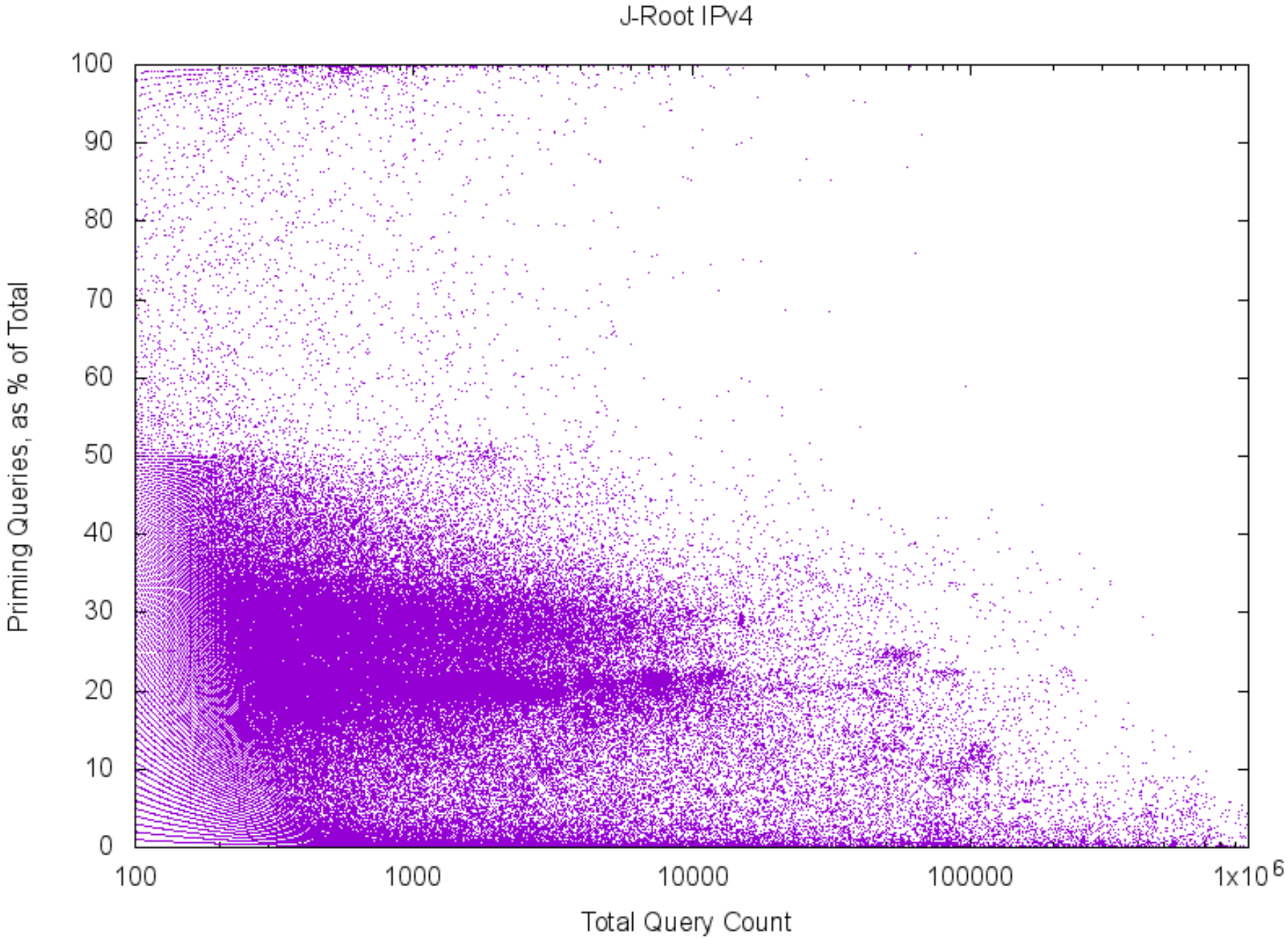

J-Root
Old-J
1x10^7
1x10^6
100000
10000
1000
100
Query Count Per Day
2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015
Date of Source Address Network Allocation

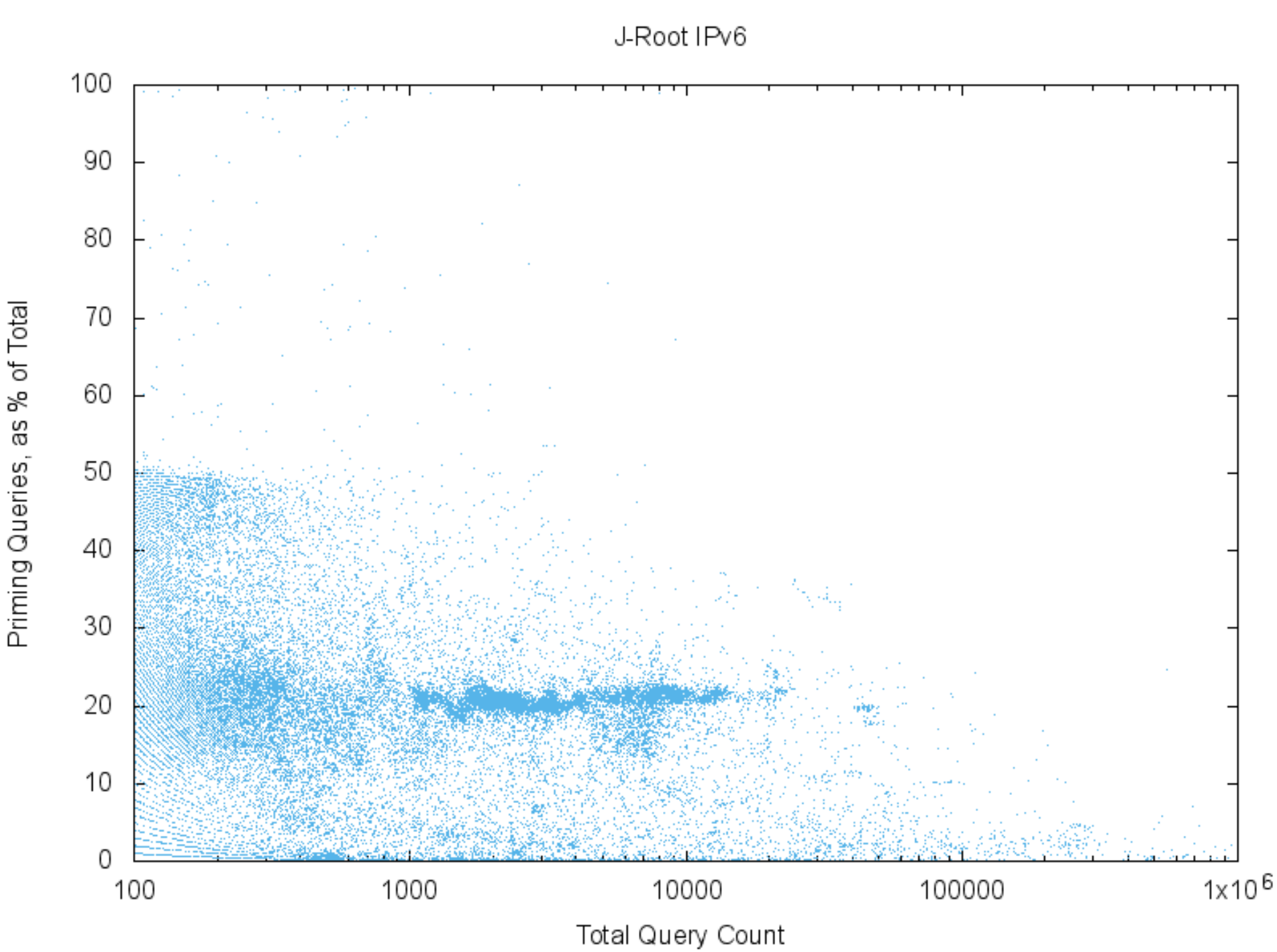
Priming Queries

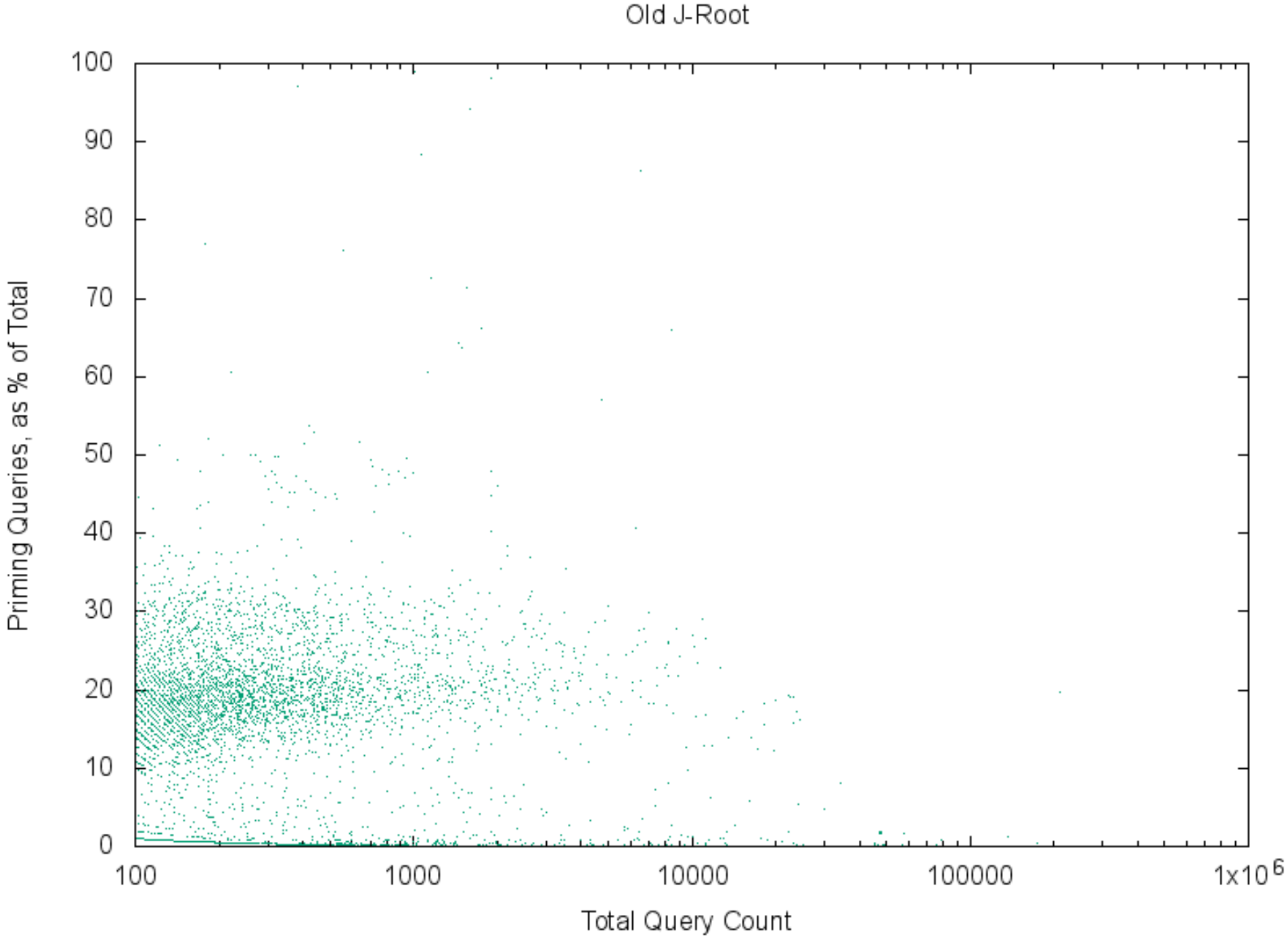
- Priming query is “. NS”
- At startup, and periodically thereafter, a recursive name server refreshes its list of roots with this priming query
- In theory: post-priming, a recursive name server should stop querying Old J-Root.

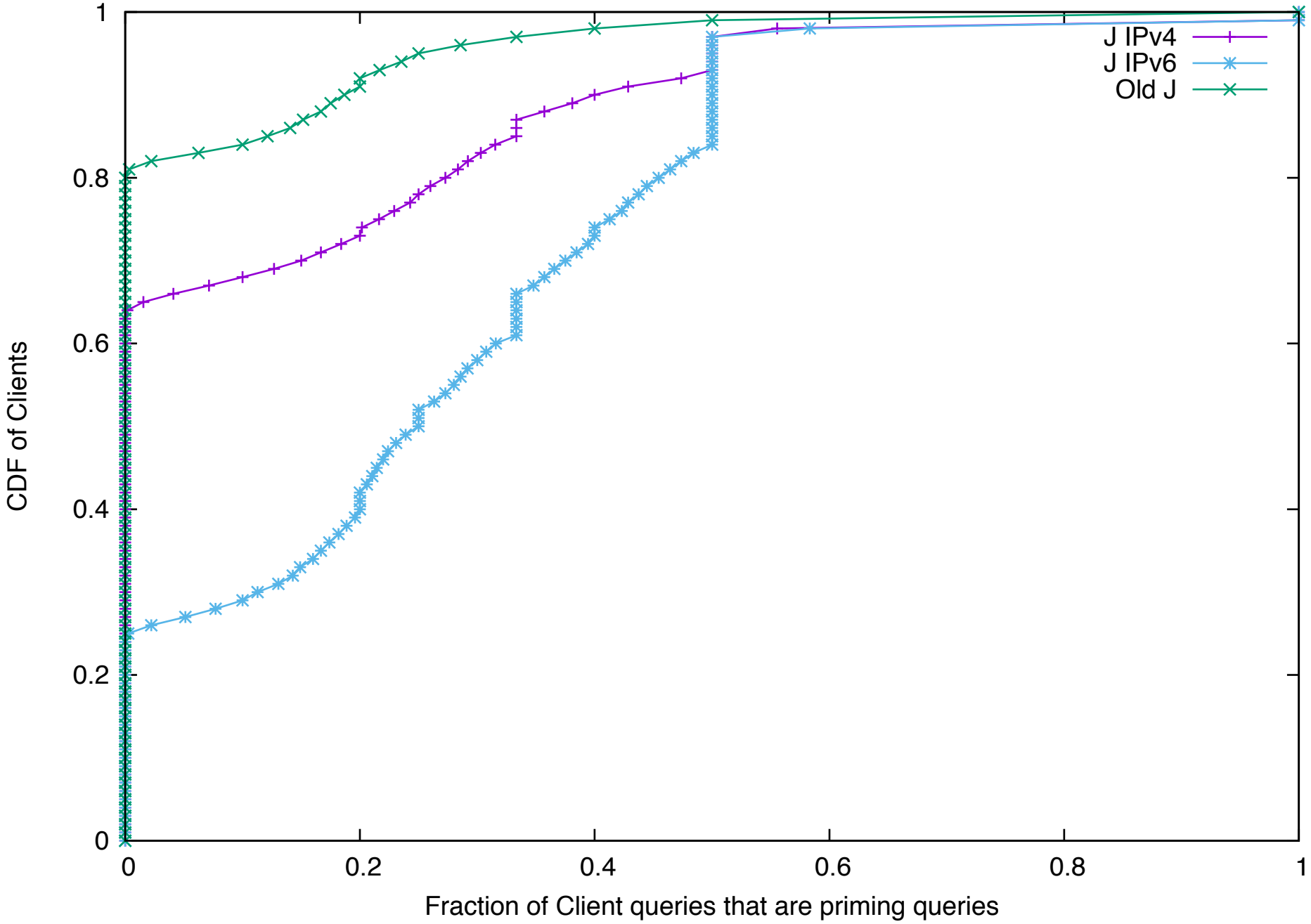
- What does the data indicate?

- Note: “. NS” is also the default query for dig, if no name and type are specified.


J-Root IPv4
Priming Queries, as % of Total
100
90
80
70
60
50
40
30
20
10
0
100
1000
10000
100000
1x10^6
Total Query Count


J-Root IPv6
Priming Queries, as % of Total
100
90
80
70
60
50
40
30
20
10
0
100
1000
10000
100000
1x10^6
Total Query Count

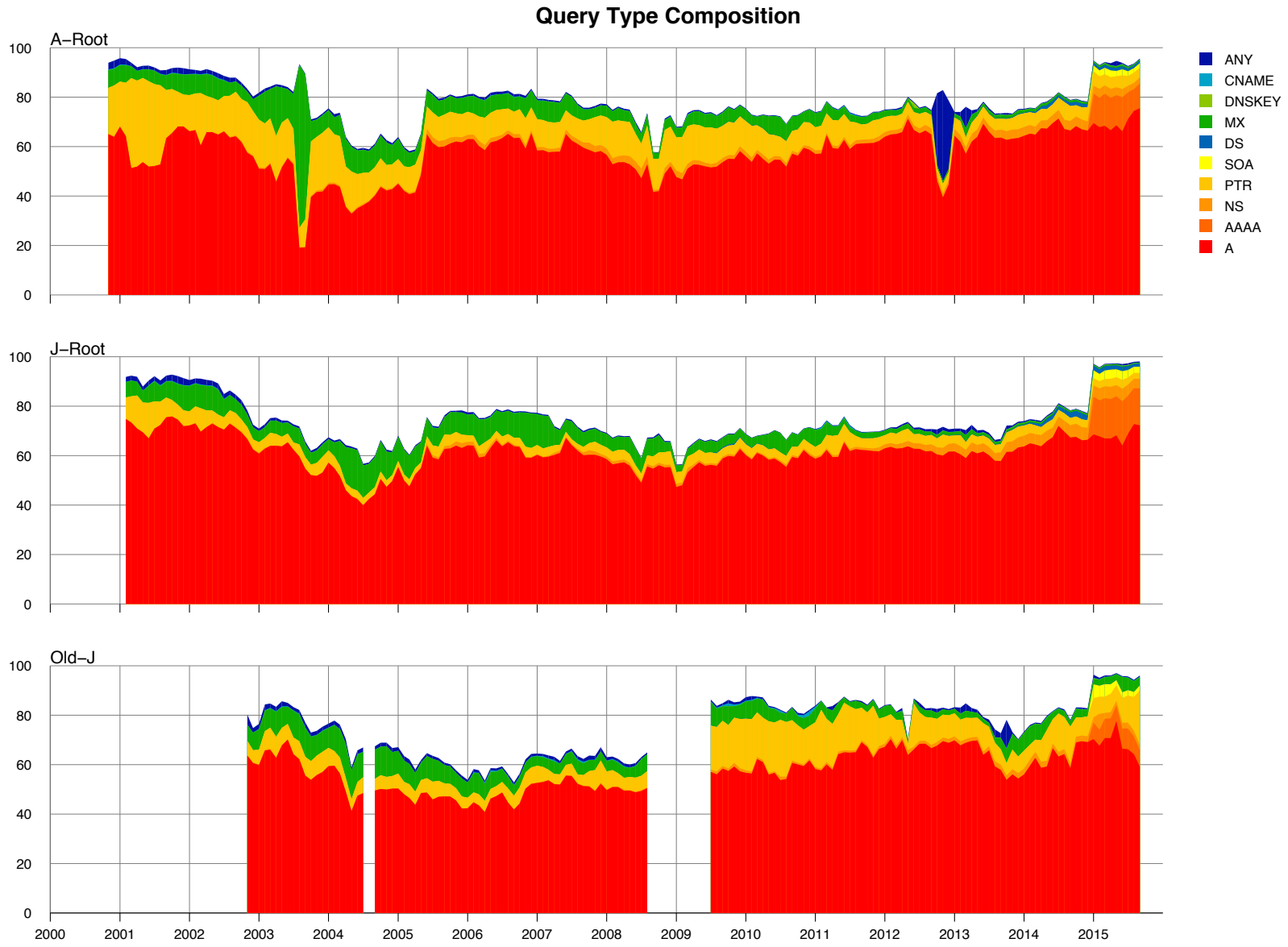

Old J-Root
Priming Queries, as % of Total
Total Query Count
100
90
80
70
60
50
40
30
20
10
0
100
1000
10000
100000
1x10^6


J IPv4
J IPv6
Old J
CDF of Clients
Fraction of Client queries that are priming queries
0
0.2
0.4
0.6
0.8
1

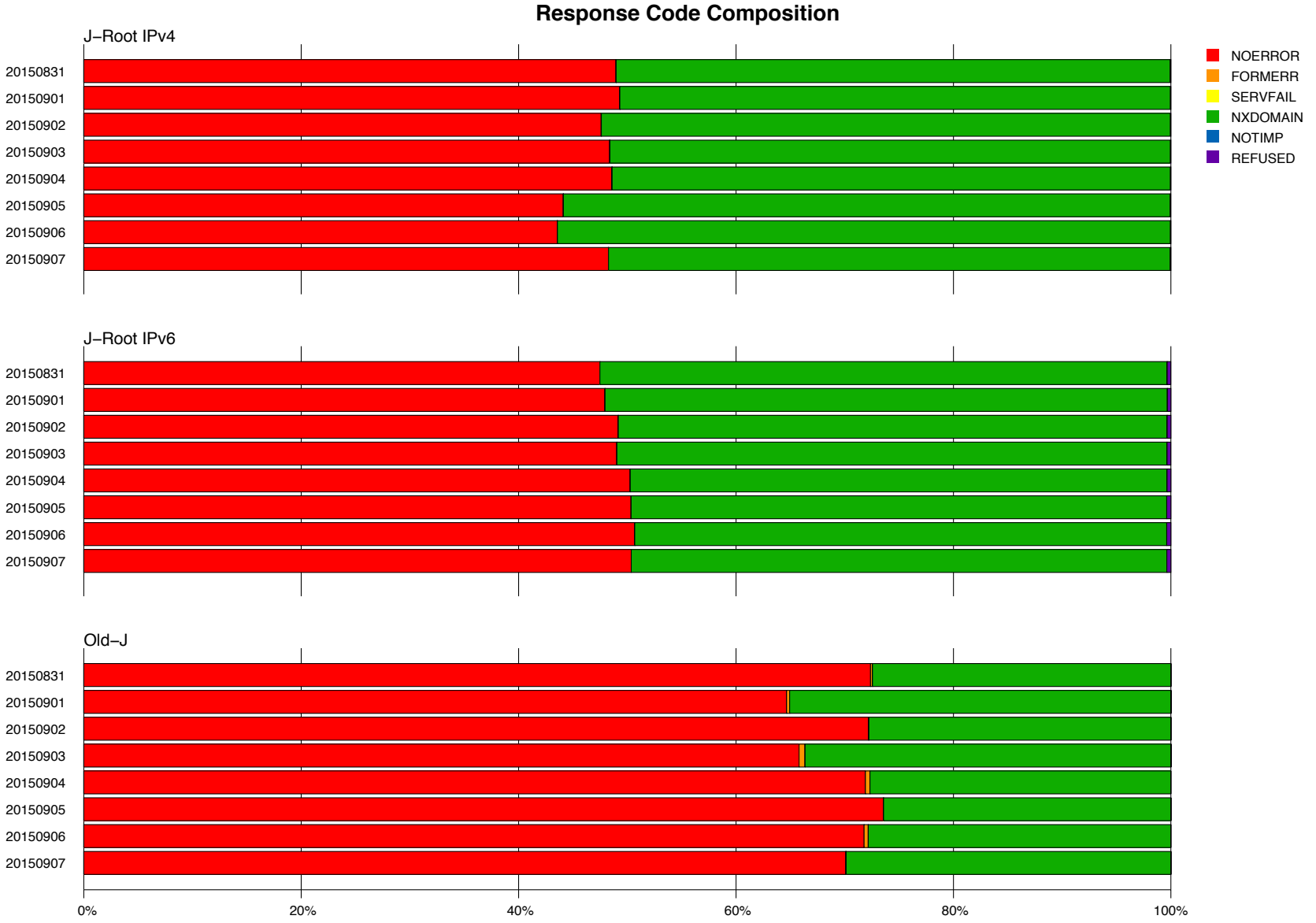
Types

Let’s compare distribution of query types on A-root, J-root and Old J-root.

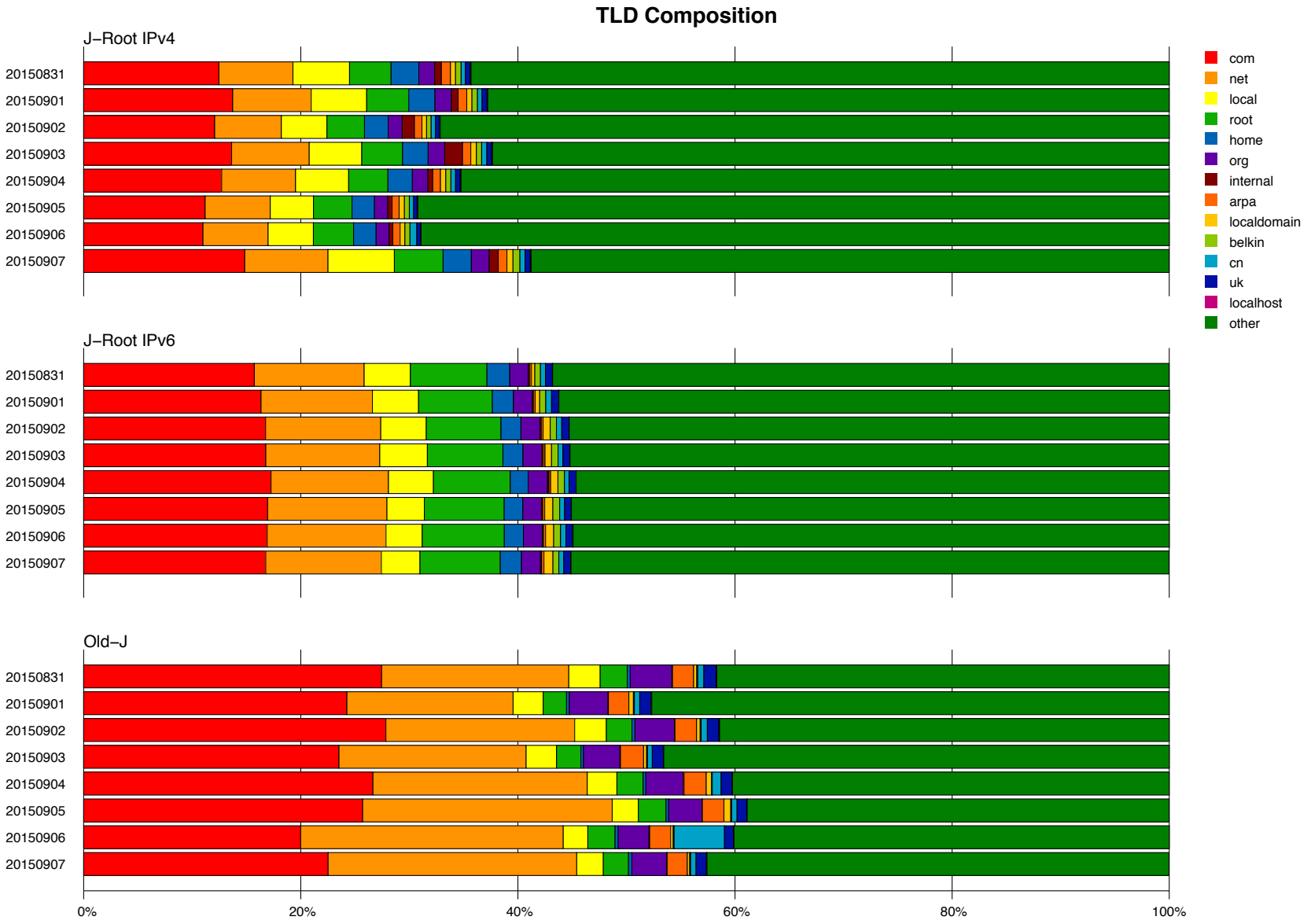

Query Type Composition
J–Root IPv4
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
J–Root IPv6
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
Old–J
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
0%
20%
40%
60%
80%
100%
A
AAAA
NS
PTR
SOA
SRV
MX
TXT
DS
DSNSKEY
ANY


Query Type Composition
A–Root
J–Root
Old–J
100
80
60
40
20
0
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
ANY
CNAME
DNSKEY
MX
DS
SOA
PTR
NS
AAAA
A

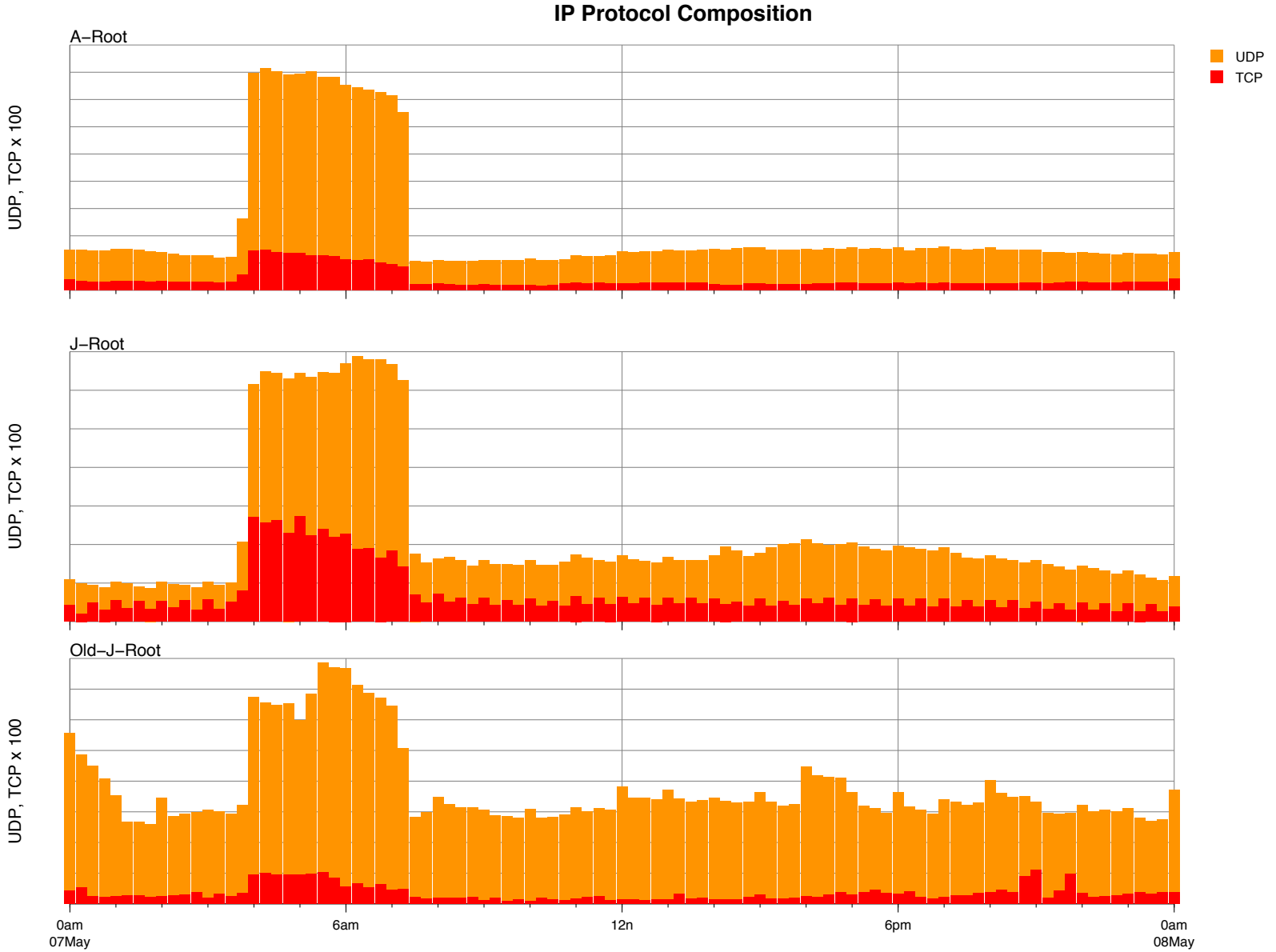
Response Codes

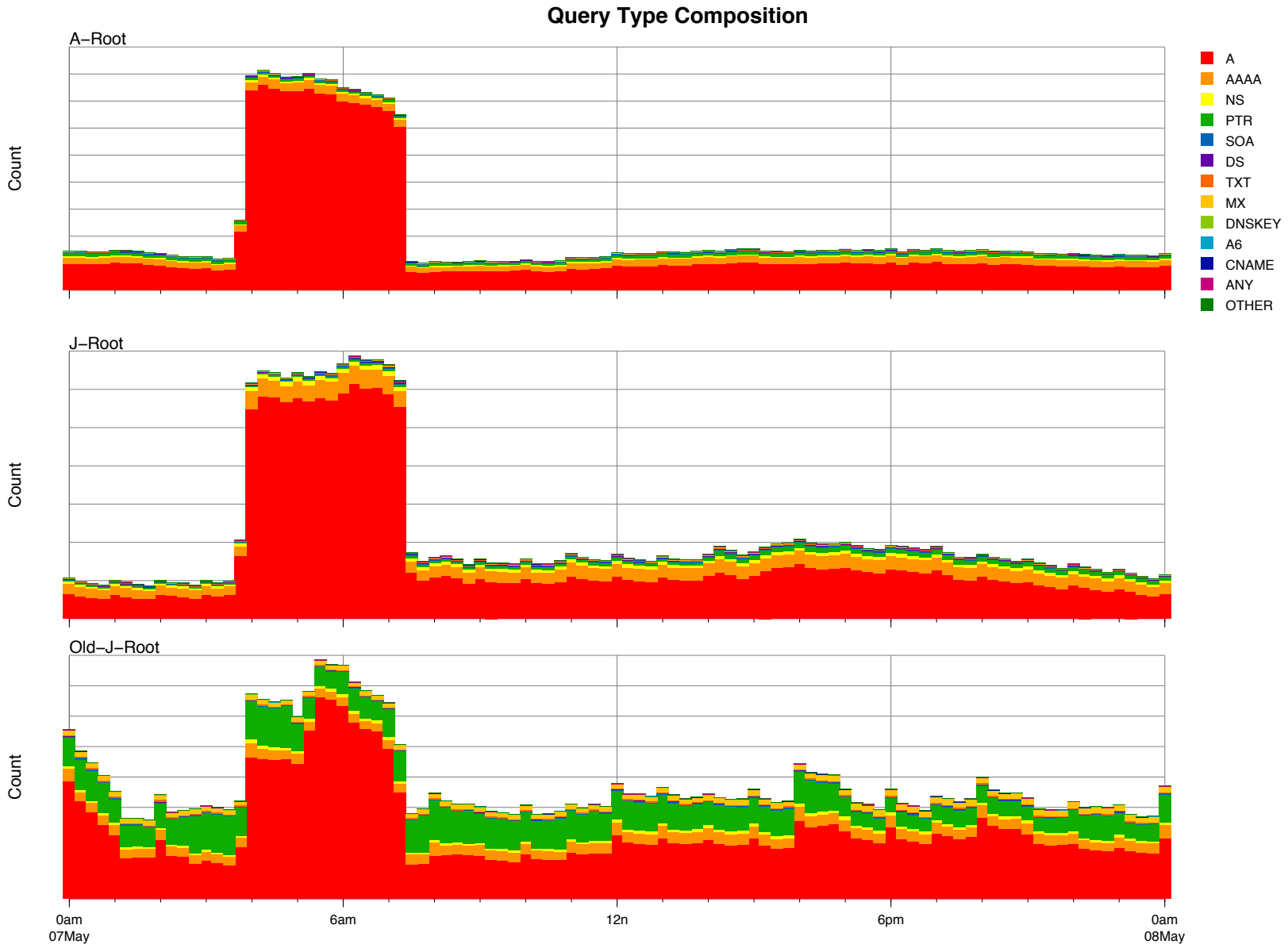

Response Code Composition
J–Root IPv4
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
J–Root IPv6
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
Old–J
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
0%
20%
40%
60%
80%
100%
NOERROR
FORMERR
SERVFAIL
NXDOMAIN
NOTIMP
REFUSED

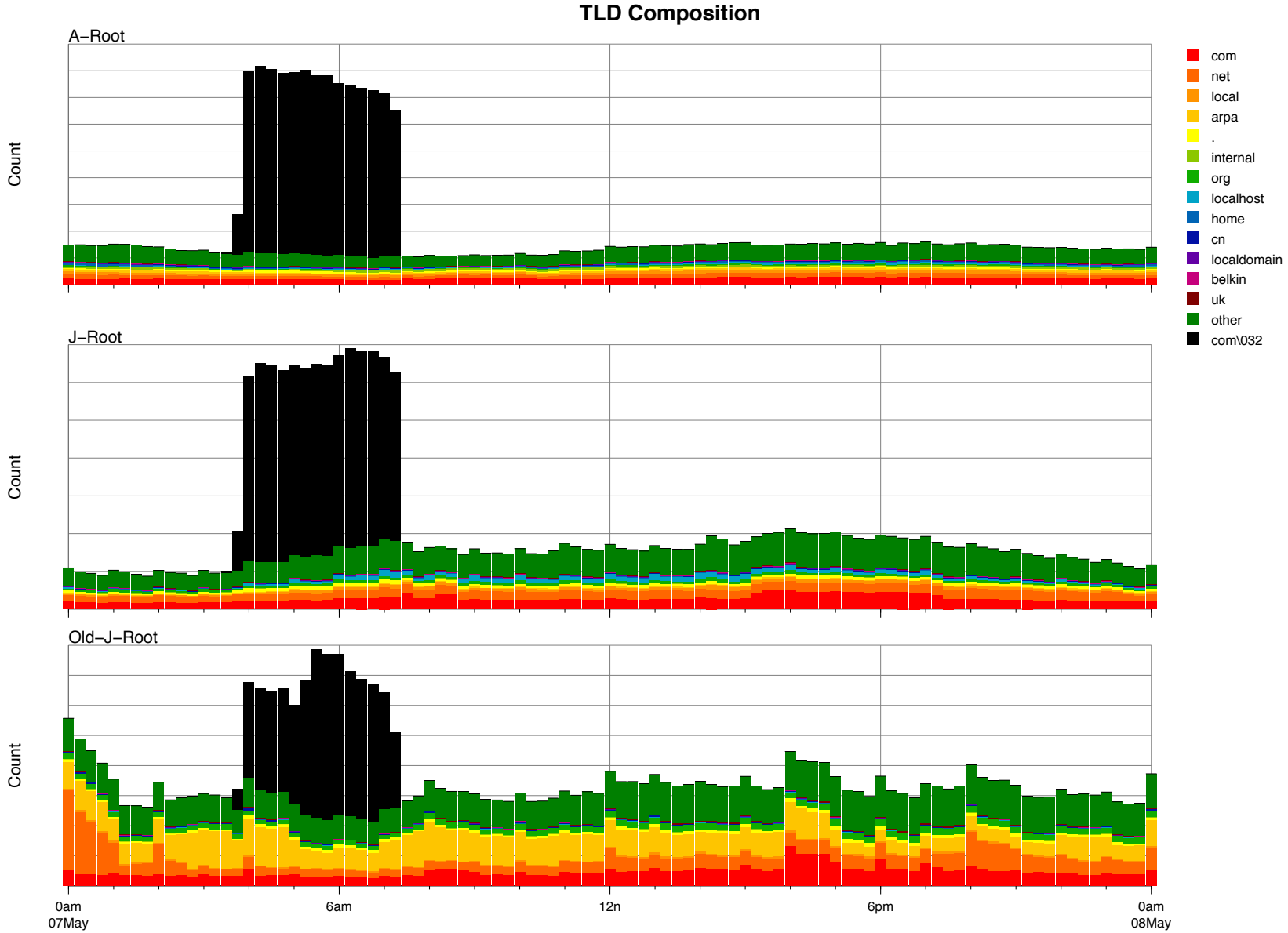
TLDs


TLD Composition
J–Root IPv4
J–Root IPv6
Old–J
20150831
20150901
20150902
20150903
20150904
20150905
20150906
20150907
0%
20%
40%
60%
80%
100%
com
net
local
root
home
org
internal
arpa
localdomain
belkin
cn
uk
localhost
other

An Attack Event


IP Protocol Composition
A–Root
J–Root
Old–J–Root
UDP, TCP x 100
UDP
TCP
0am
07May
6am
12n
6pm
0am
08May


Query Type Composition
A–Root
J–Root
Old–J–Root
Count
A
AAAA
NS
PTR
SOA
DS
TXT
MX
DNSKEY
A6
CNAME
ANY
OTHER
0am
07May
6am
12n
6pm
0am
08May


TLD Composition
A–Root
J–Root
Old–J–Root
Count
com
net
local
arpa
.
internal
org
localhost
home
cn
localdomain
belkin
uk
other
com\032
0am
07May
6am
12n
6pm
0am
08May

Open Resolvers

Ask All of IPv4 for j.root-servers.net?

Rank	Response	Count
1	192.58.128.30	12,033,768
2	reply, no answer records	4,502,621
3	11x.4x.19x.11x	185,100
4	7x.22x.19x.1x	8,573
5	192.168.2.1	3,500
6	192.168.1.1	1,801
7	7x.1x.5x.9x	1,332
8	7.0.0.0	1,289
9	20.20.20.20	1,112
10	192.168.1.254	735
11	198.41.0.10	686
12	192.168.128.1	505
13	5x.23x.15x.9x	470
14	10.0.0.1	453
15	127.0.0.1	415

Conclusions

- Old J-Root appears to still receive “legitimate” queries 13 years after it was removed from root hints.
- Significantly more MX, TXT, PTR queries at Old J-Root (as percentage).
- About two orders of magnitude less DNSKEY/DS at Old J-Root.
- Attack traffic observed at Old J-Root implies non-spoofed sources.

- Old Root Servers -- better to burn out, or fade away?

Questions?

powered by

VERISIGN™