Source port vulnerabilities in .JP
- static source port issue -

24 SEP 2008
2008 OARC Workshop in Ottawa

Izuru Shirai
Japan Registry Services Co., Ltd.

Contents

- Introduction
  - About JPRS and .JP
  - JP DNS
- General statistics
- DNS vulnerability issue
  - JPRS's work
  - Progress report
- Characteristics of source port usage
- Discussion

INTRODUCTION

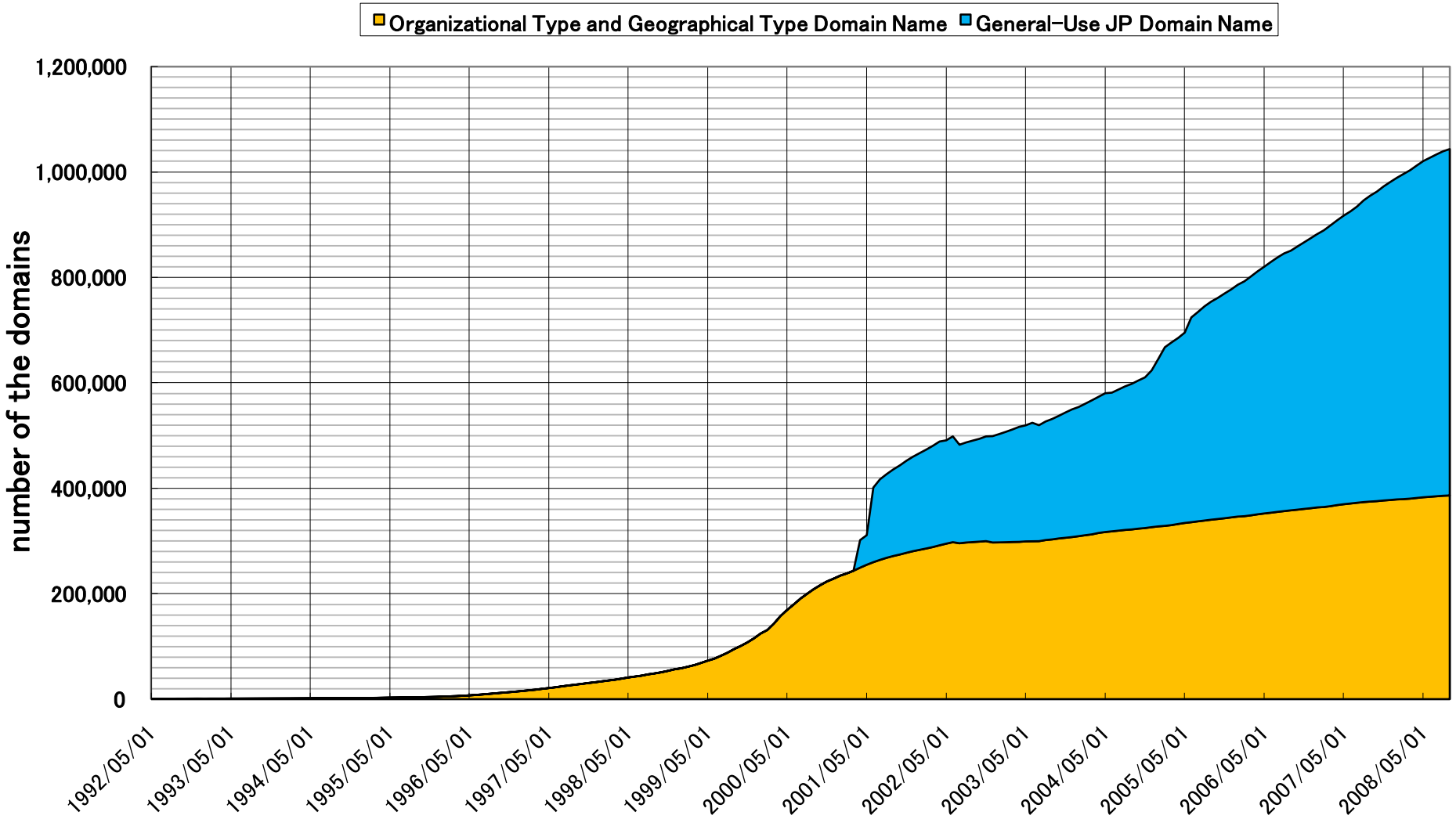
About JPRS and .JP

- history
  - Aug, 1986: JP domain name was delegated to Jun MURAI
  - Dec, 1991: JNIC established.
  - Apr, 1993: JNIC reorganized as JPNIC.
  - Dec, 1993: JPNIC delegated by InterNIC to manage reverse DNS name server for JPNIC-assigned address block.
  - Jun, 1995: Application fees for IP addresses and JP domain names introduced.
  - Dec, 2000: JPRS established to succeed management and administration of JP domain names.
  - Feb, 2002: “ccTLD Sponsorship Agreement(.JP)” executed.
- Role
  - .JP registration
  - .JP DNS operation

Outline of JP domain

- Registered JP Domain Names (@2008/09/01)
  - 1,043,513 domains
  - .JP has two levels of name space
    - 3rd and more level domain
      - → Organizational Type and Geographic Type JP Domain Name
      - Judgment required
      - sub total: 386,447 domains
      - Ex) jprs.co.jp, nic.ad.jp, metro.tokyo.jp, city.yokohama.jp…
    - 2nd level domain
      - → General-Use JP Domain Name
      - sub total: 657,066 domains
      - Ex) jprs.jp
- Local presence required

Time-Series Data of .JP



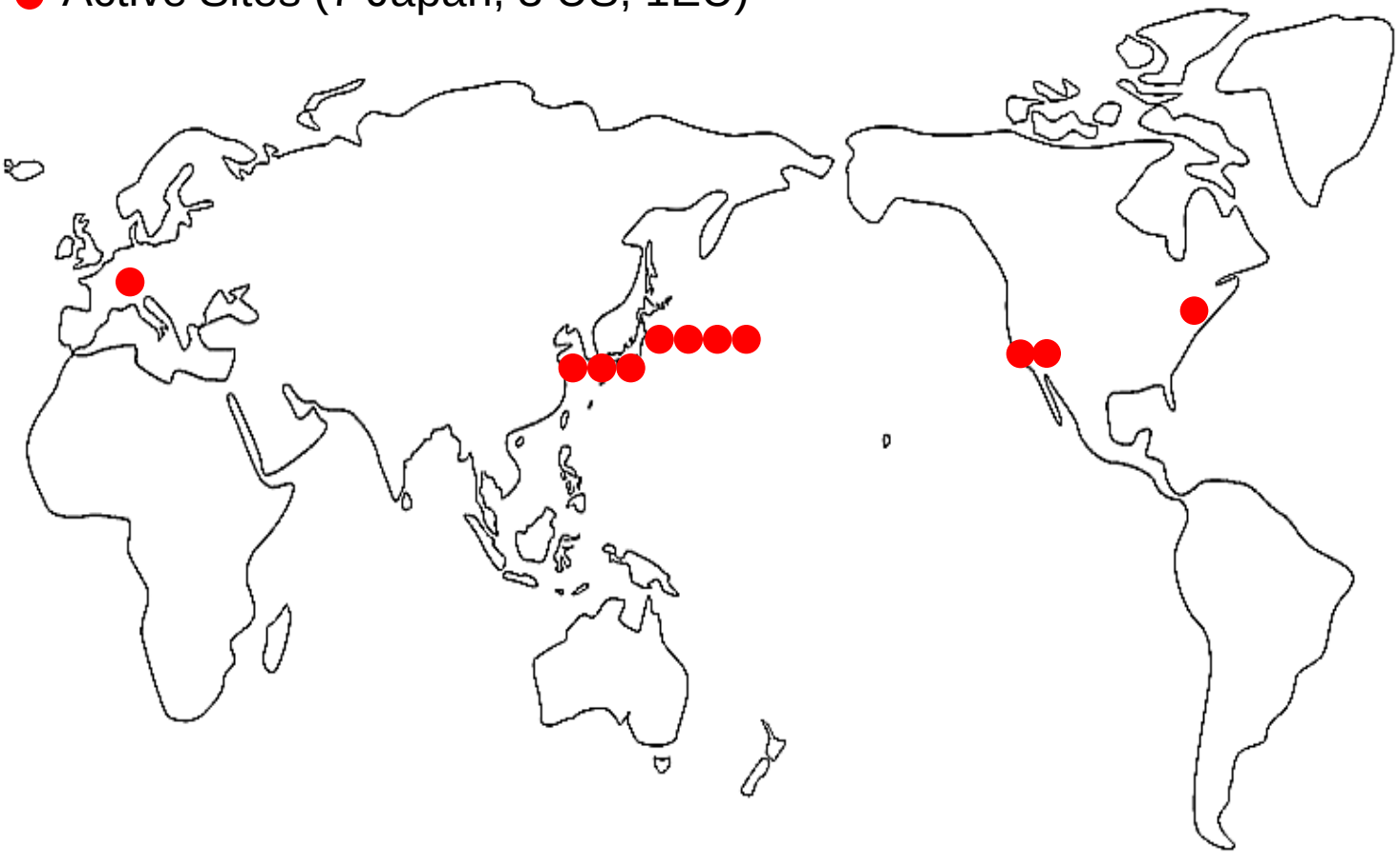
JP DNS

- JP DNS servers are managed by JPRS and operated by the following organizations.
  - 2 more NS will be added.

NS	IPv4	IPv6	Organization	Anycast
a.dns.jp	203.119.1.1	2001:dc4::1	JPRS	BGP anycast
b.dns.jp	202.12.30.131	-	JPNIC	N/A
d.dns.jp	210.138.175.244	2001:240::53	IIJ	IGP anycast
e.dns.jp	192.50.43.53	2001:200:c000::35	WIDE	BGP anycast
f.dns.jp	150.100.2.3	2001:2f8:0:100::153	SINET	N/A

JP DNS Server Locations

- Active Sites (7 Japan, 3 US, 1EU)

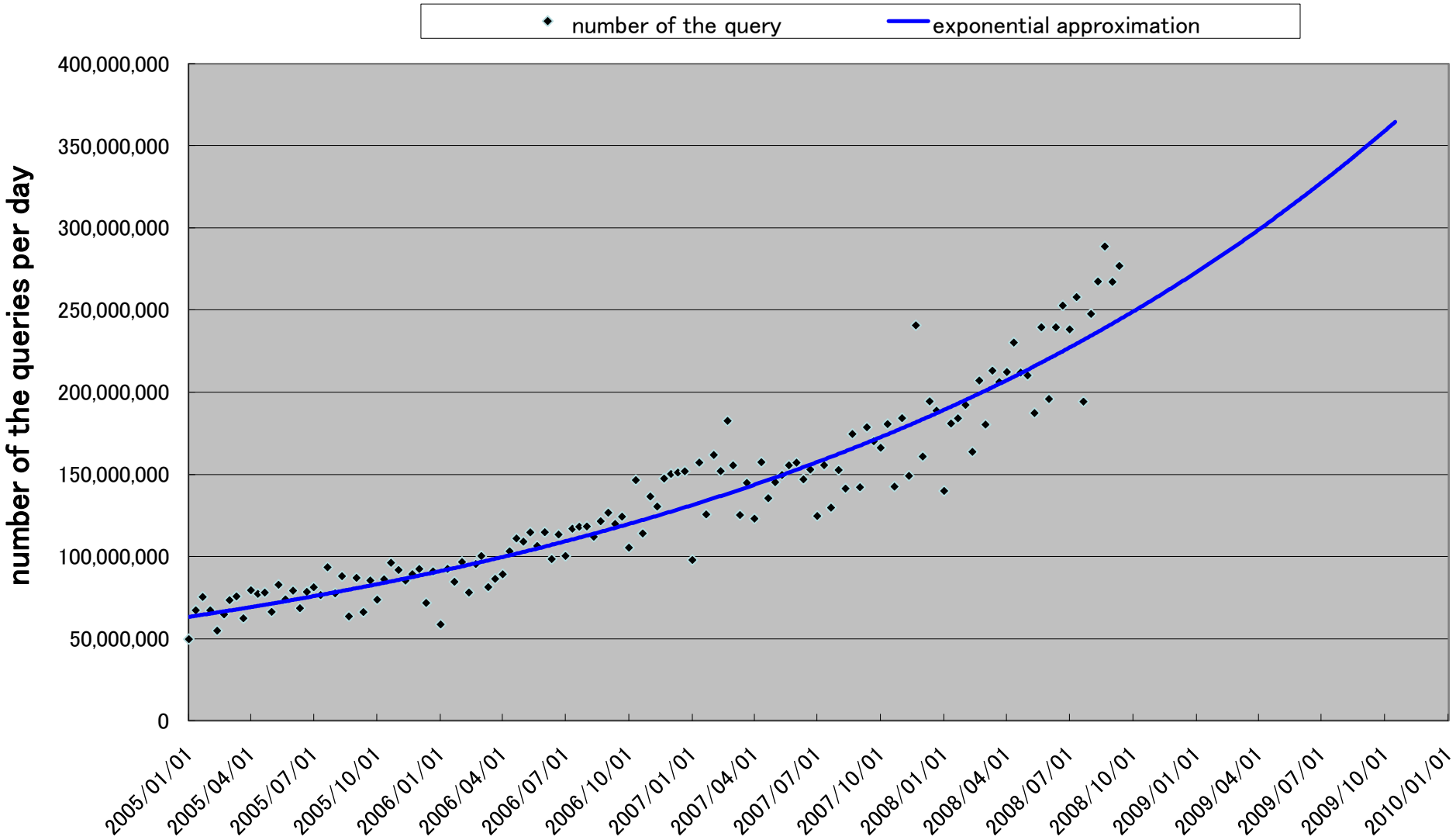


GENERAL STATISTICS

Statistics for a.dns.jp

- Why a.dns.jp?
  - We have whole query log at a.dns.jp from Jan,2004.
    - Time-series analysis is easily.
  - Various feature has been supported.
    - BGP anycast ready
    - IPv6 ready

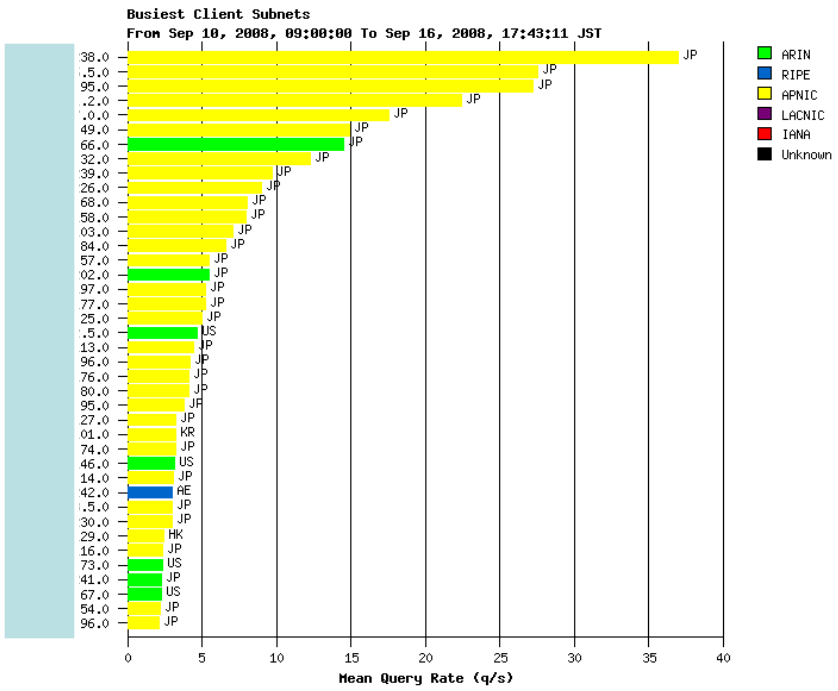
Time-series data for number of the queries at A.DNS.JP



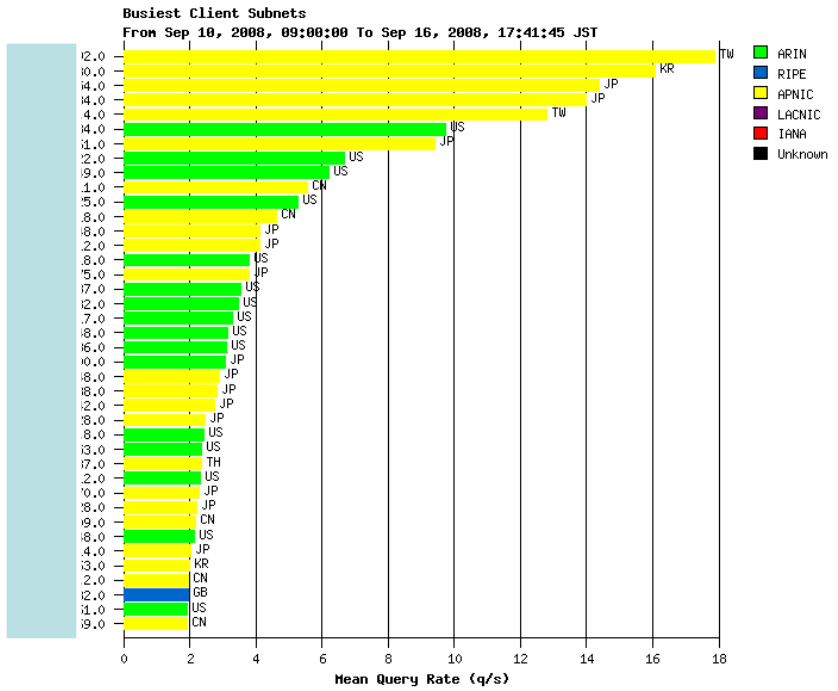
DSC: Client Geography

APNIC and ARIN blocks are dominant.

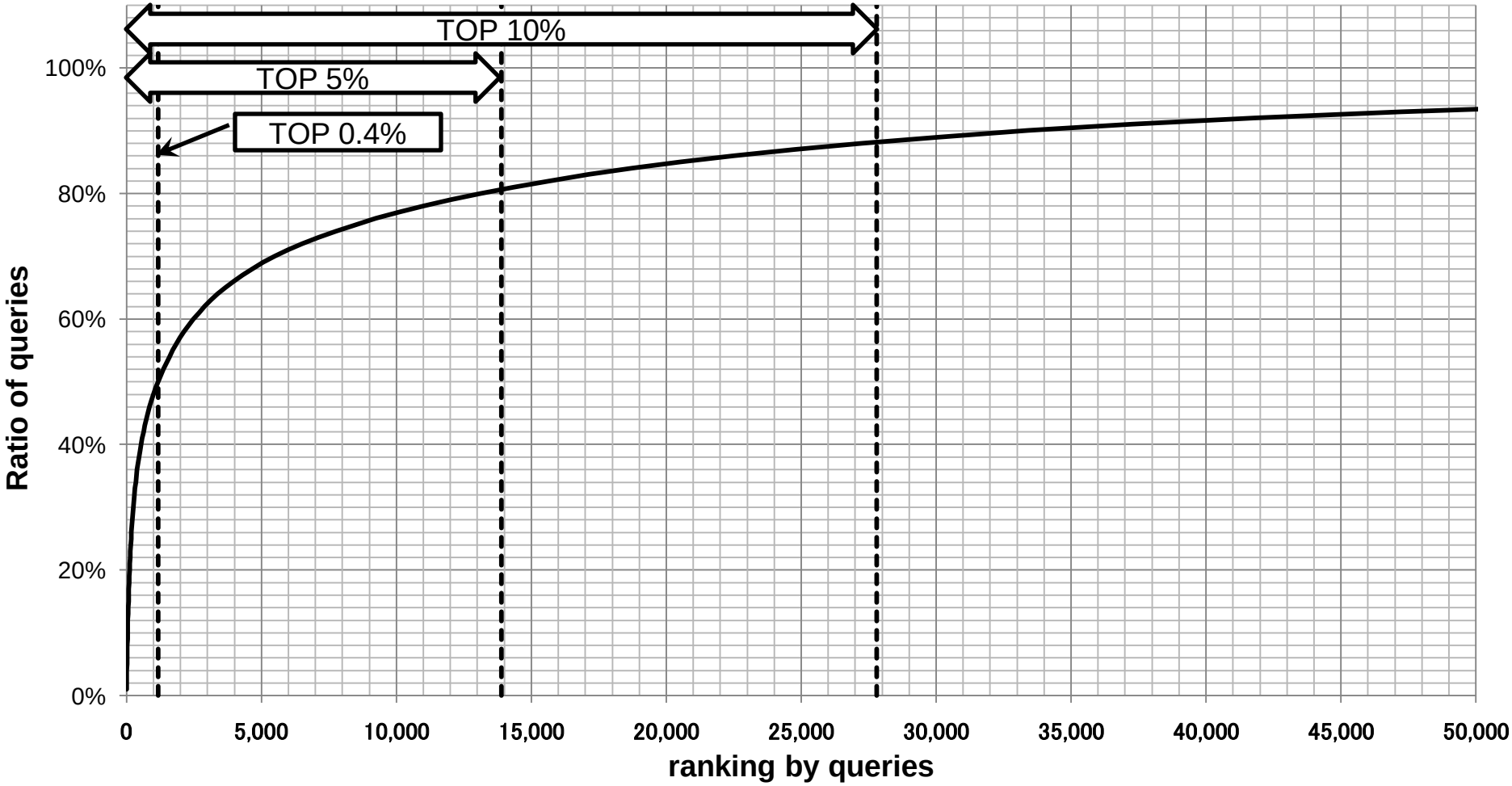
Some node



Another node



Heavy user (Heavy hitter?)



DNS VULNERABILITY ISSUE

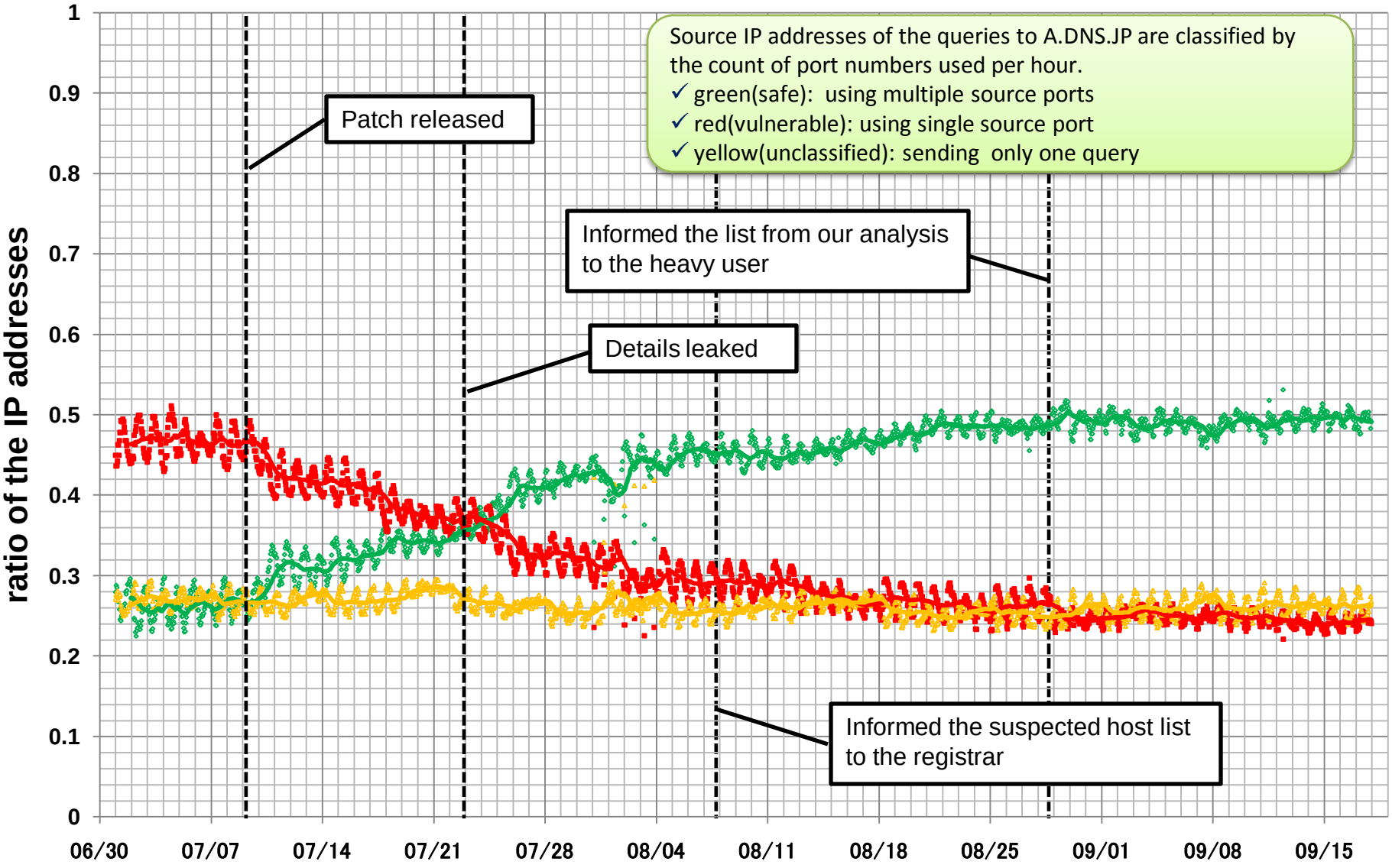
What has JPRS done?

- Co-operated with JPCERT/CC and JPNIC for disclosure on the issue
  - The suspected host list has been informed via the .JP registrar
  - Reported technical details in Japanese
- Making analysis of the queries at a.dns.jp
  - Progress report of applying patches
  - Suspected host list (who are heavy user)
    - Call direct attention to some heavy user

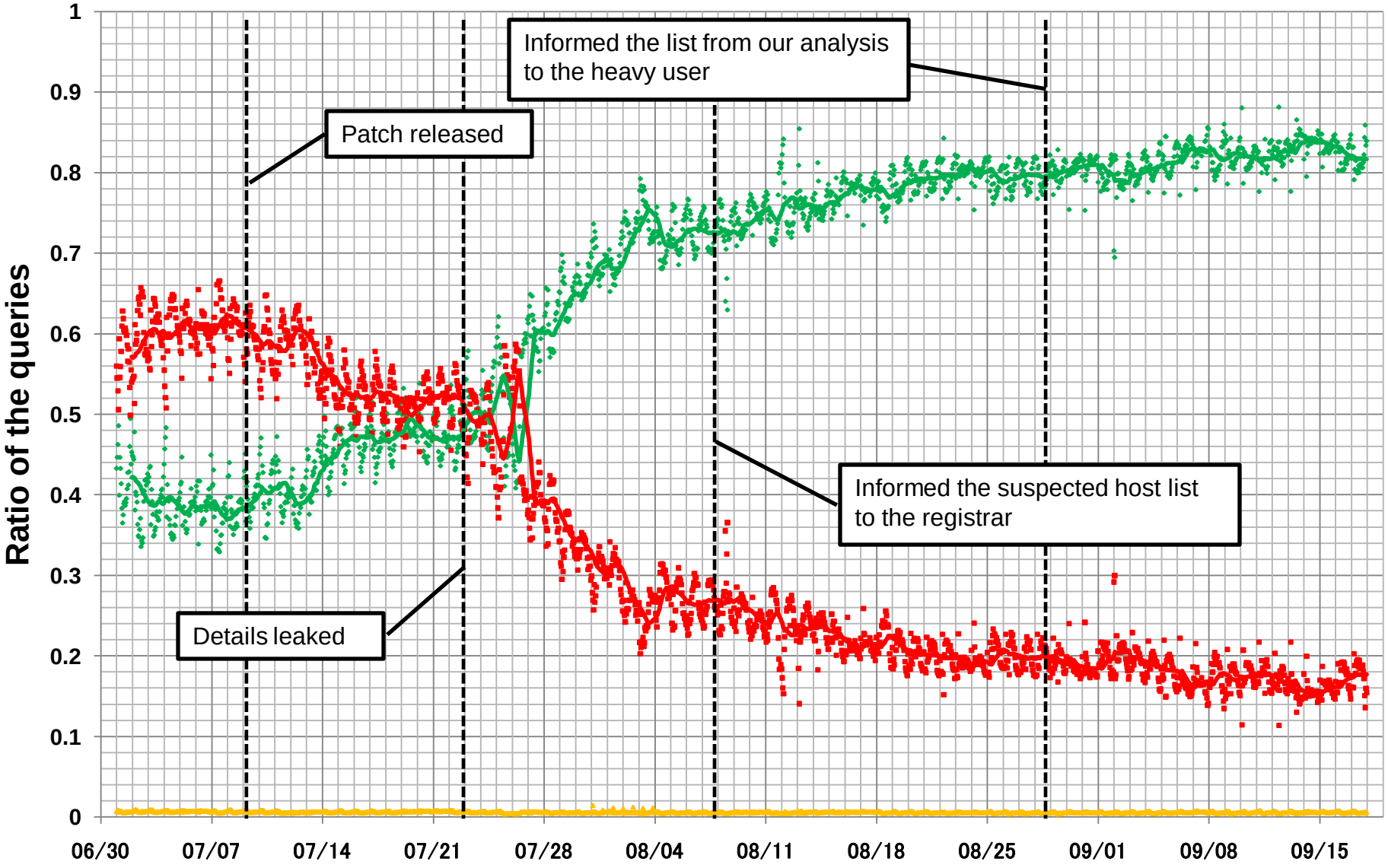
Progress report in .JP

- Making classification
  - Analyzed the queries per hour
    - Green means the clients are probably safe.
      - They use multiple source ports.
    - Red means the clients are vulnerable.
      - They use only one source ports.
    - Yellow means the clients are not classified.
      - They send only one query per hour.

detected Safe/Vulnerable/Unclassified clients



detected queries from the Safe/Vulnerable/Unclassified clients



Overview of the graph

- Current status
  - Reached equilibrium in ratio of the clients
  - Slightly making progress in ratio of the queries
    - Watching the behavior of heavy user
- Discussion
  - randomness in their query source ports
    - Not checked in this graph
  - necessity of infrequent user in making statistics
    - Shown by later discussion

CHARACTERISTIC OF SOURCE PORT USAGE

Characteristic distribution among port number

Ranking by the client count

Before – July

1.	32768	0.73%
2.	53	0.58%
3.	32769	0.24%
4.	49155	0.11%
5.	1024	0.11%
6.	49156	0.09%
7.	32770	0.06%
8.	1025	0.05%
9.	1026	0.05%
10.	1027	0.04%

After – September

1.	32768	0.17%
2.	53	0.17%
3.	32769	0.05%
4.	1024	0.04%
5.	1025	0.02%
6.	32770	0.02%
7.	1026	0.01%
8.	32772	0.01%
9.	32771	0.01%
10.	1027	0.01%

Environmental Reason
- ✓OS default
- ✓NAT effect

32768,1024,49152…

Operational Reason
- ✓required by Firewall
- ✓distribution's default

53,14053,53000…

Ranking by the query count

Before – July

1.	32768	3.9%
2.	53	3.7%
3.	32769	3.5%
4.	14053	1.2%
5.	53000	1.1%
6.	32772	0.9%
7.	54088	0.9%
8.	49152	0.8%
9.	32777	0.7%
10.	34914	0.7%

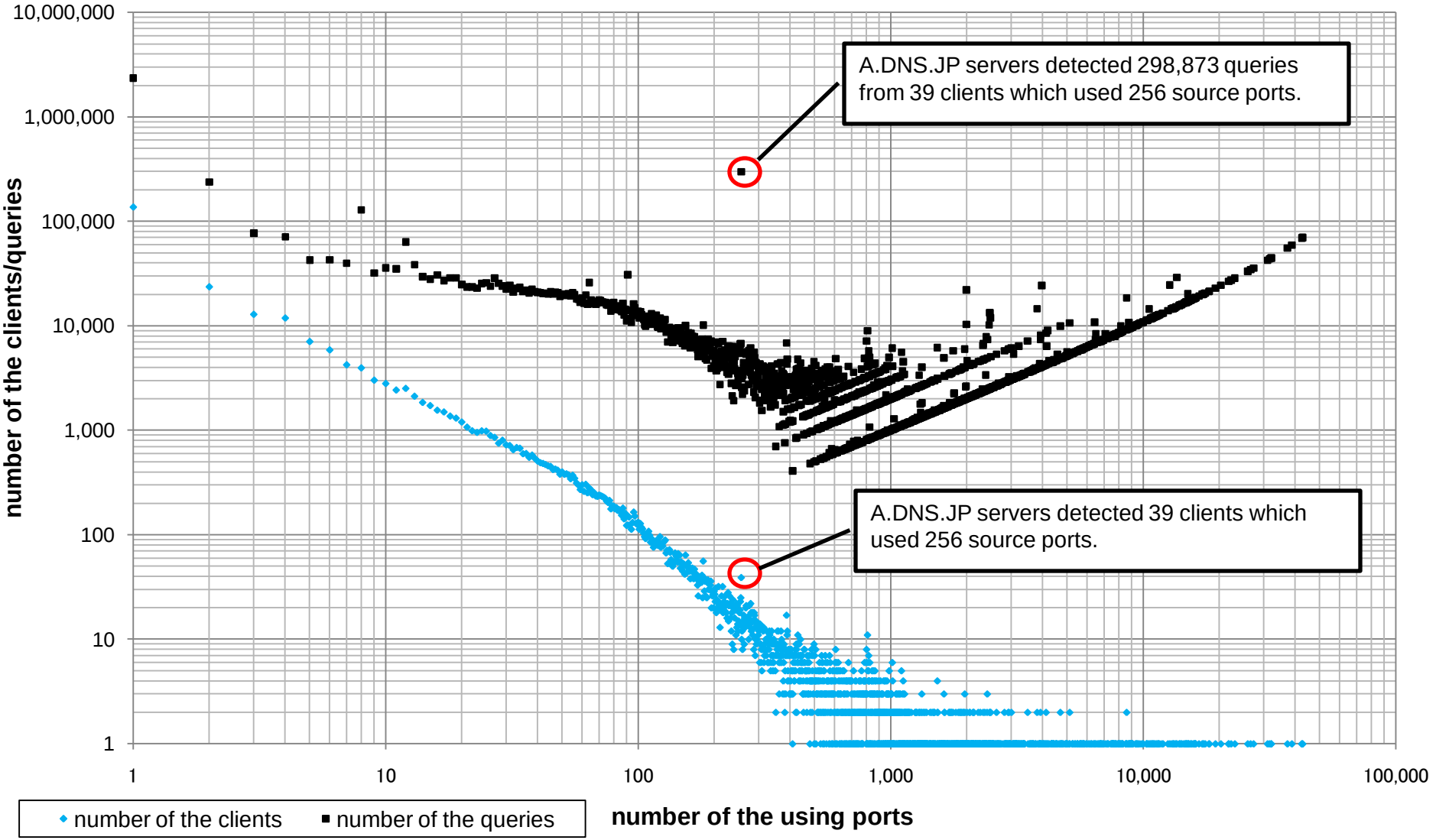
After – September

1.	53	2.1%
2.	32768	1.3%
3.	32769	0.5%
4.	32772	0.4%
5.	1024	0.2%
6.	1053	0.1%
7.	32770	0.1%
8.	32771	0.1%
9.	15282	0.1%
10.	39441	0.1%

How to show enough randomness

- Plotting two data in the same graph
  - detected number of the queries from the clients(Y axis) which use specific count of the source ports(X axis).
  - detected number of the clients(Y axis) which use specific count of the source ports(X axis).

number of the using ports and number of the clients/queries (2008/09/01 23:00-24:00 JST)

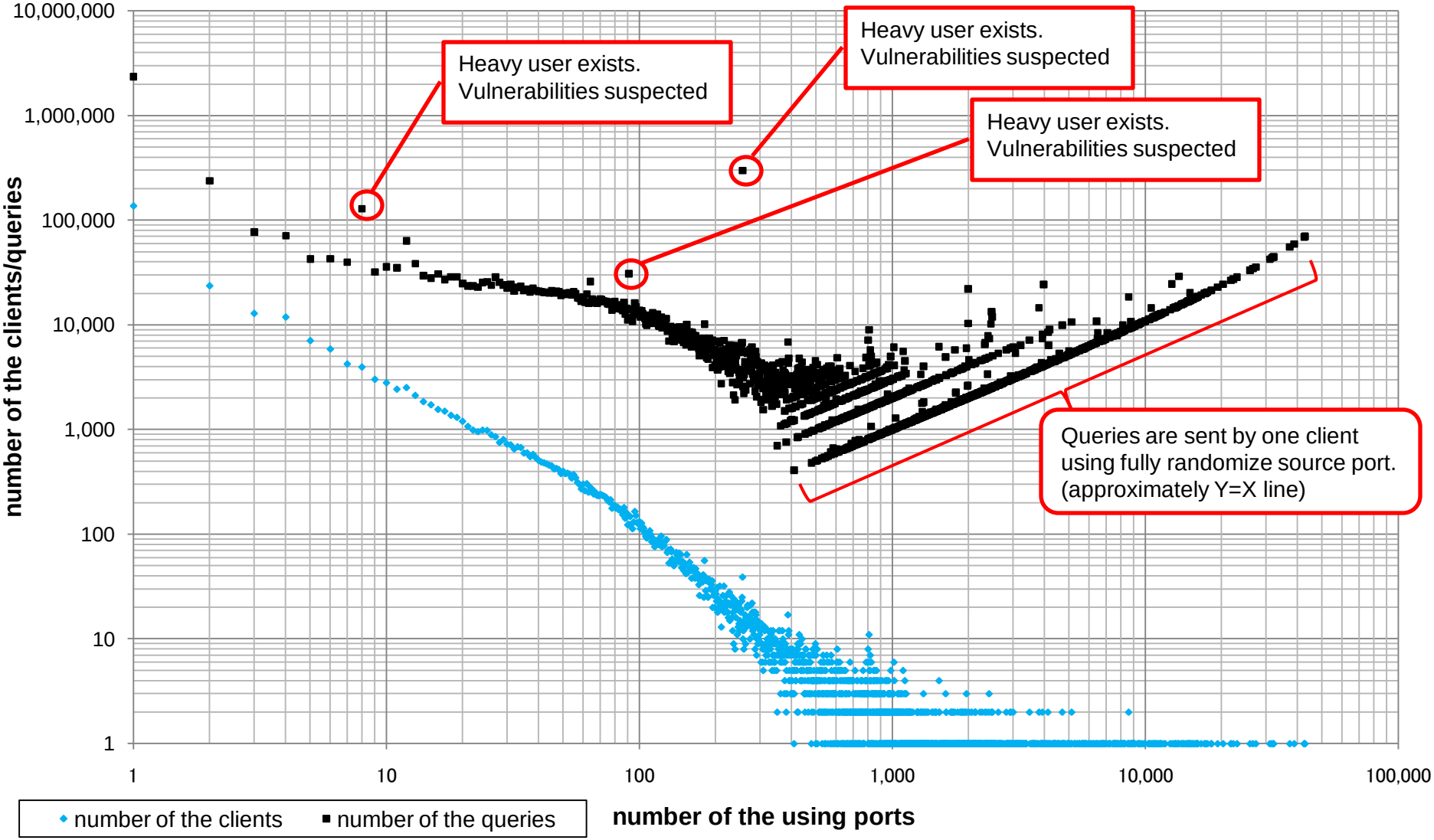


Overview of the graph

- Basically scatter charts for queries and clients make similar figure, because there is only small number of the heavy users.
- Exceptional dot is existence of the suspect vulnerable heavy users.

  → not enough randomness!
- Special shape
  - Y=X, Y=2X, Y=3X…
    - Fully randomize source port usage

number of the using ports and number of the clients/queries (2008/09/01 23:00-24:00 JST)



DISCUSSION

Discussion: specific hostname

- Current vulnerable heavy user
  - Specified hostname by the reverse DNS
    - Vulnerable *.jp heavy user
      - Generally decreasing
    - Some *.jp clients who have specific hostname
      - Relatively increasing

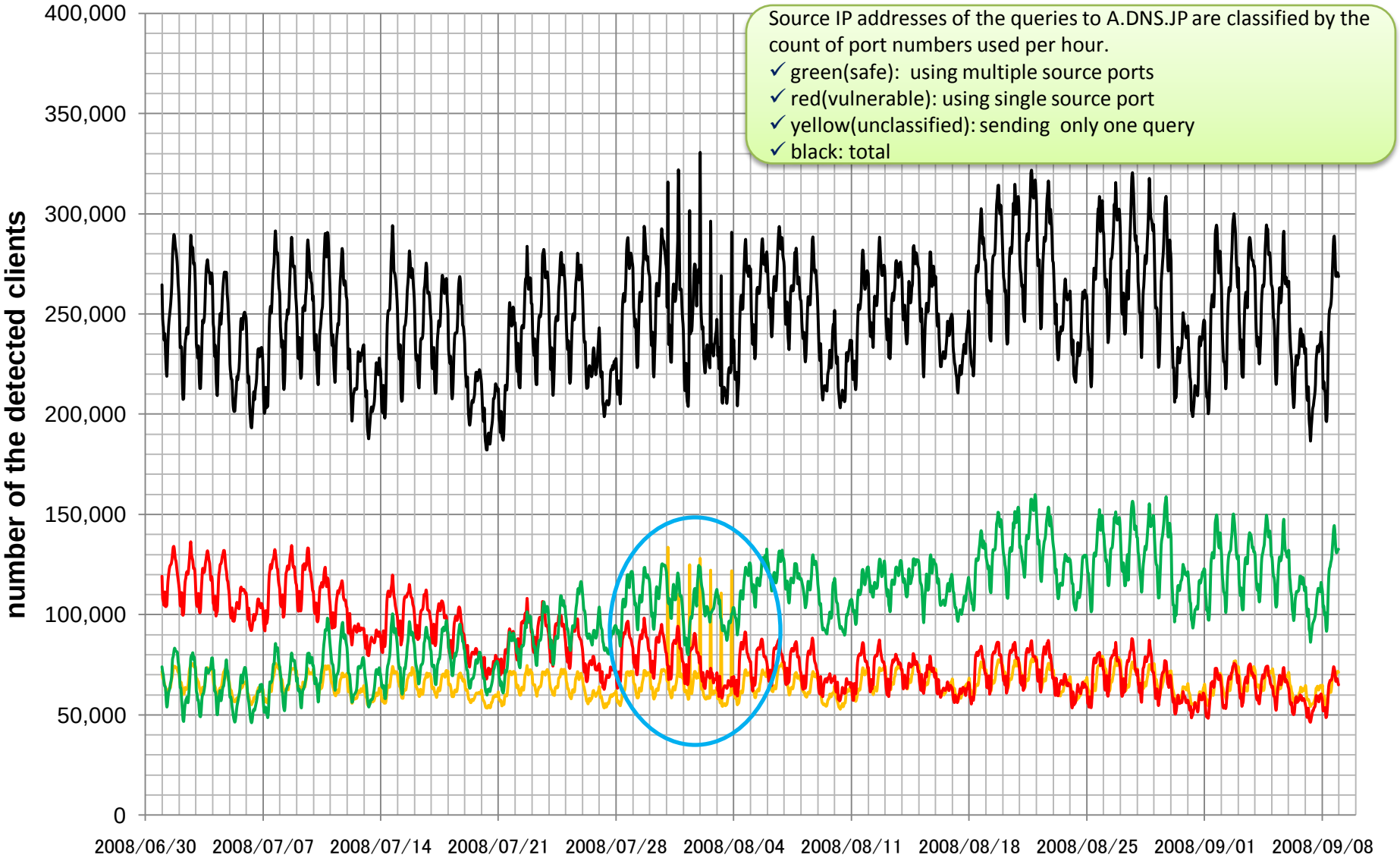
dns*.example1.jp …patched
ns*.example2.jp …patched
mta*.example3.jp …remaining
smtp*.example4.jp…remaining

- Supposed reason
  - SPAM detector
  - Mail-gateway Appliance

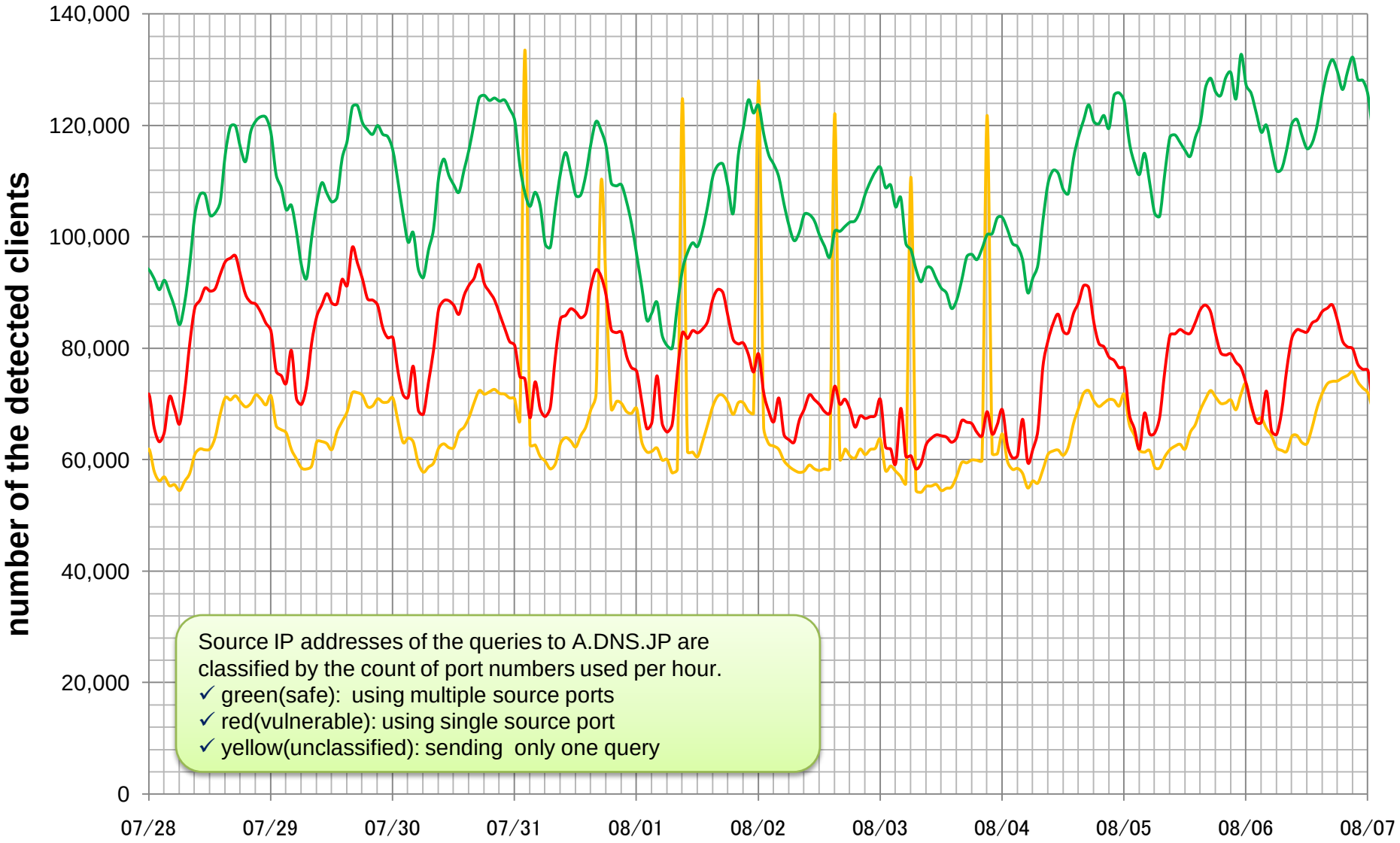
Discussion: Spike detected

- Progress report
  - Plotted time-series of the client count
  - Regularly spike observed between Aug 1st – Aug 4th

time-series data of the detected clients



time-series data of the detected clients



Discussion: Spike detected

- Observed spike
  - Every 15 hours
  - Each clients send only one query per hour
- Supposed reason
  - Scanned by botnet?
- Call for classification method
  - They send only one query.
  - How can I classify into base-line and spike?