“What is all that crap?”

Analysis of DNS root server bogus queries

Authors: Daniël Sánchez & Joost Pijnaker

Education: System & Network Engineering

Supervisors: Cees de Laat (UvA)

Daniel Karrenberg (RIPE NCC)

Date: 07-02-2007 14:00

Agenda

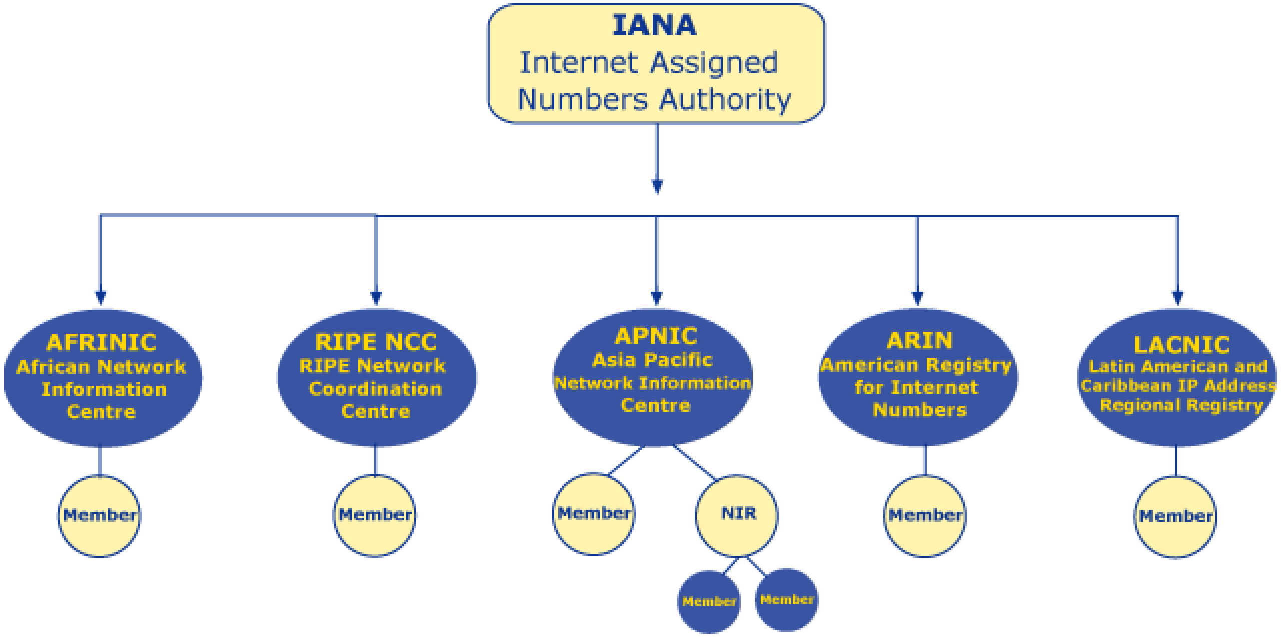
- Organisation
- Project introduction
- Research
- Conclusion
- Questions

Agenda

- Organisation
- Project introduction
- Research
- Conclusion
- Questions

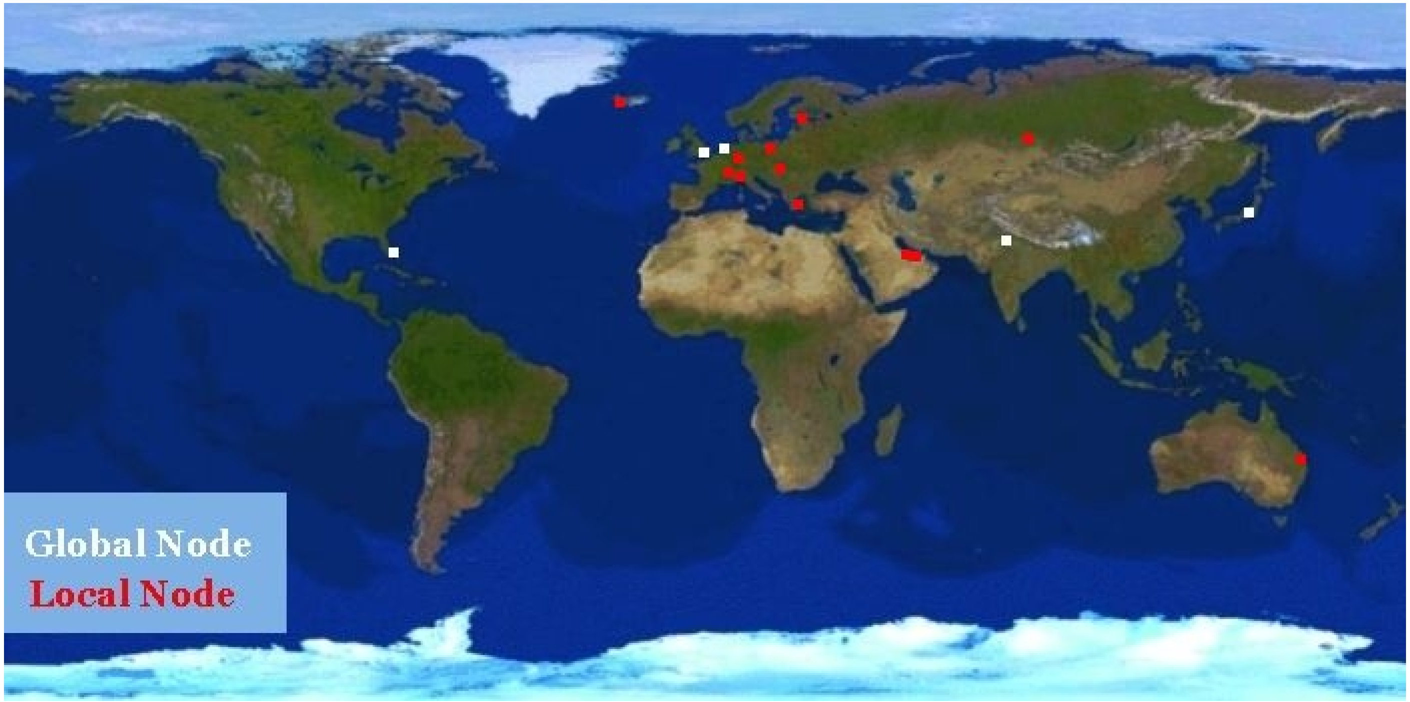
Organisation: RIPE NCC

Internet Resource Allocation


IANA
Internet Assigned Numbers Authority
AFRINIC
African Network Information Centre
RIPE NCC
RIPE Network Coordination Centre
APNIC
Asia Pacific Network Information Centre
ARIN
American Registry for Internet Numbers
LACNIC
Latin American and Caribbean IP Address Regional Registry
Member
Member
Member
NIR
Member
Member
Member
Member

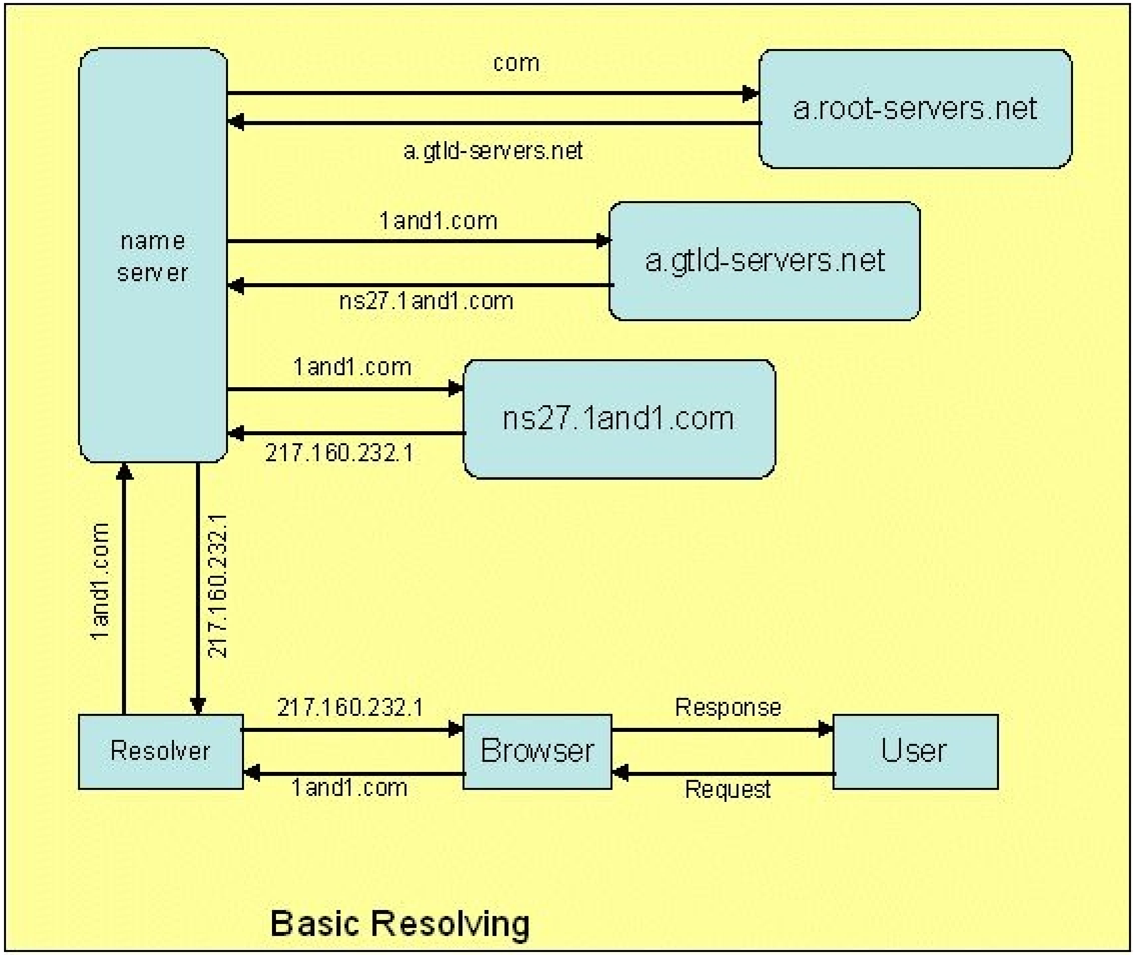
http://www.ripe.net

Organisation: K-Root server



http://k.root-servers.org

Organisation: DNS Root server



http://faq.oneandone.co.uk

Agenda

- Organisation
- Project introduction
- Research
- Conclusion
- Questions

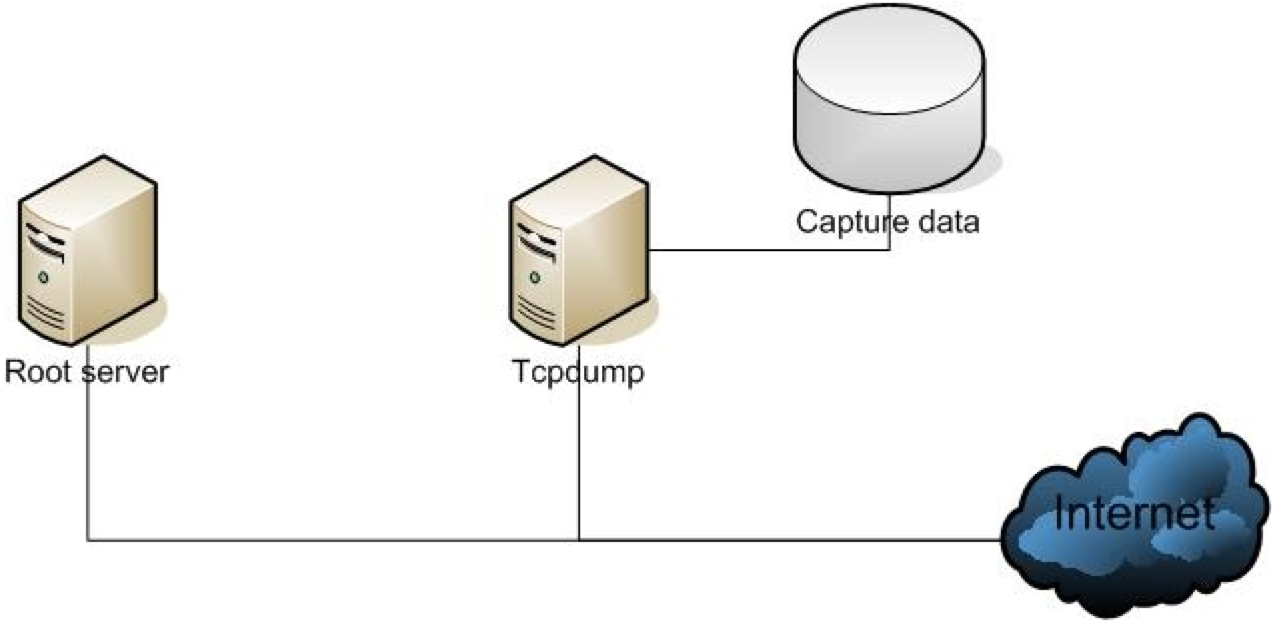
Agenda

- Organisation
- Project introduction
- Research
- Conclusion
- Questions

Project introduction

- Problem definition
- Research question
- Research scope
- Capture data
- Tools

Project introduction: Capture data



Project introduction: Tools

- Tcpdump
- Ethereal
- dnstop
- Scripts (awk, Ruby)

Agenda

- Organisation
- Project introduction
- Research
- Conclusion
- Questions

Agenda

- Organisation
- Project introduction
- Research
- Conclusion
- Questions

Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

Research: Bogus categories

- A for A queries
- Private IP reverse queries
- Reserved IP reverse queries
- Local domain queries
- Invalid TLD queries
- Identical query IDs queries
- Repeated queries
- TLD not cached queries

A for A queries

A? x.y.80.66.

Private IP reverse queries

PTR? 1.0.0.127.in-addr.arpa.

Reserved IP reverse queries

PTR? 192.168.253.241.in-addr.arpa.

Local domain queries

A? svr004.network.local.

Invalid TLD queries

A? Maschult1.Speedport_W_700V.

Same query IDs queries

id 5134, A? www.google.com.

id 5134, A? www.os3.nl.

Repeated queries

IP x.y.96.200 A? www.os3.nl.

IP x.y.96.200 A? www.os3.nl.

IP x.y.96.200 A? www.os3.nl.

IP x.y.96.200 A? www.os3.nl.

TLD not cached queries

IP x.y.96.200 A? www.os3.nl.

IP x.y.96.200 A? www.google.nl.

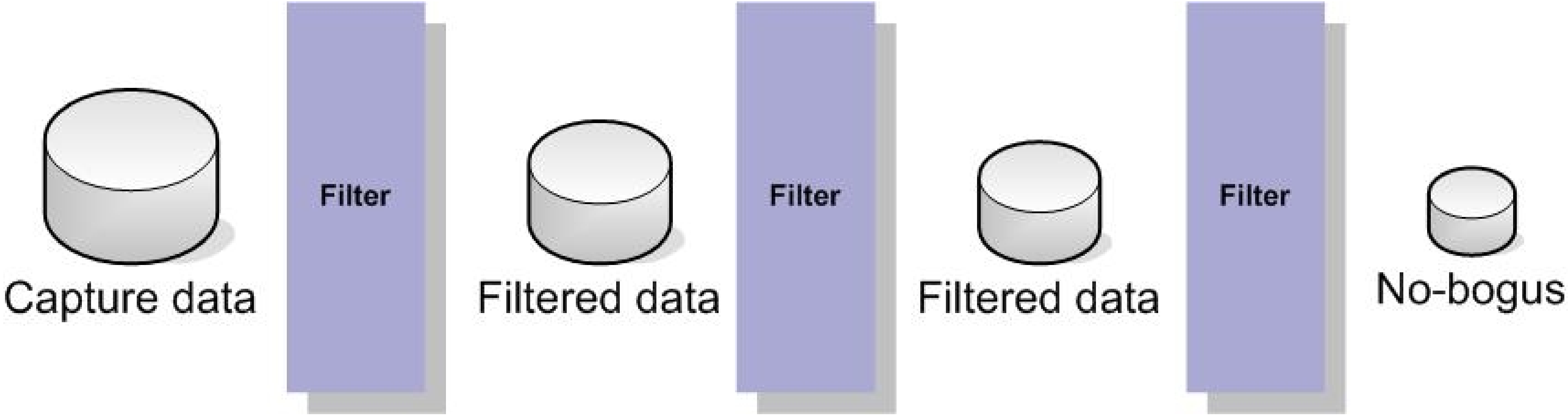
Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

Research: Filter capture data



Research: Filter capture data

```
17:10:34.283465 A? A-1FREEMAN.COM.INBOUND10.MXLOGIC.NET.
17:10:34.933914 A? A-1FREEMAN.COM.INBOUND10.MXLOGIC.NET.
17:10:35.203961 A? A-1FREEMAN.COM.INBOUND10.MXLOGIC.NET.
17:10:35.498391 A? A-1FREEMAN.COM.INBOUND10.MXLOGIC.NET.
```

▼

```
17:10:34.283465 A? A-1FREEMAN.COM.INBOUND10.MXLOGIC.NET.
```

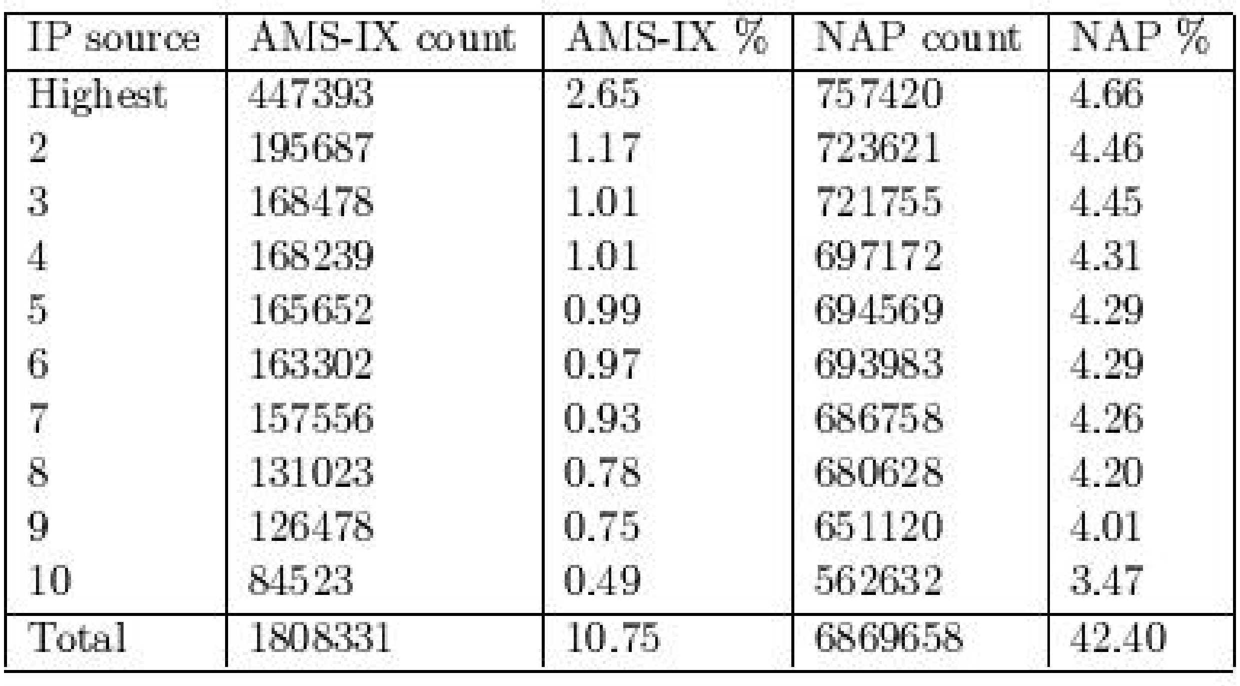
Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

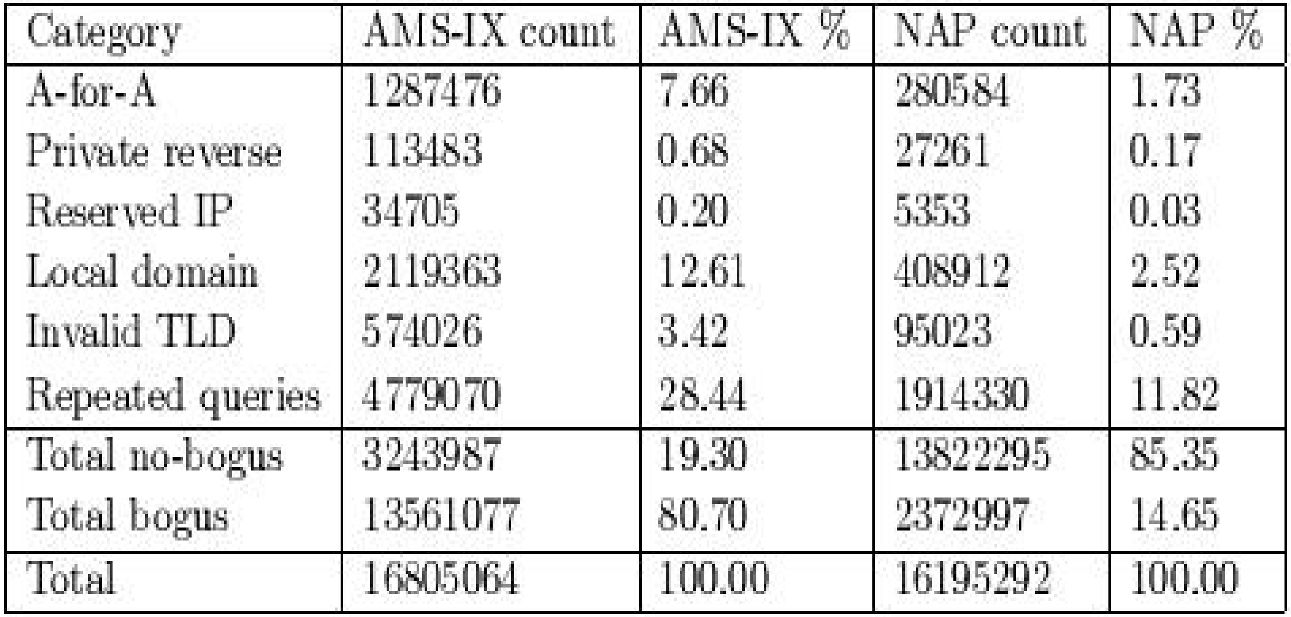
Research: Statistics



IP source	AMS-IX count	AMS-IX %	NAP count	NAP %
Highest	447393	2.65	757420	4.66
2	195687	1.17	723621	4.46
3	168478	1.01	721755	4.45
4	168239	1.01	697172	4.31
5	165652	0.99	694569	4.29
6	163302	0.97	693983	4.29
7	157556	0.93	686758	4.26
8	131023	0.78	680628	4.20
9	126478	0.75	651120	4.01
10	84523	0.49	562632	3.47
Total	1808331	10.75	6869658	42.40

Top 10 speakers

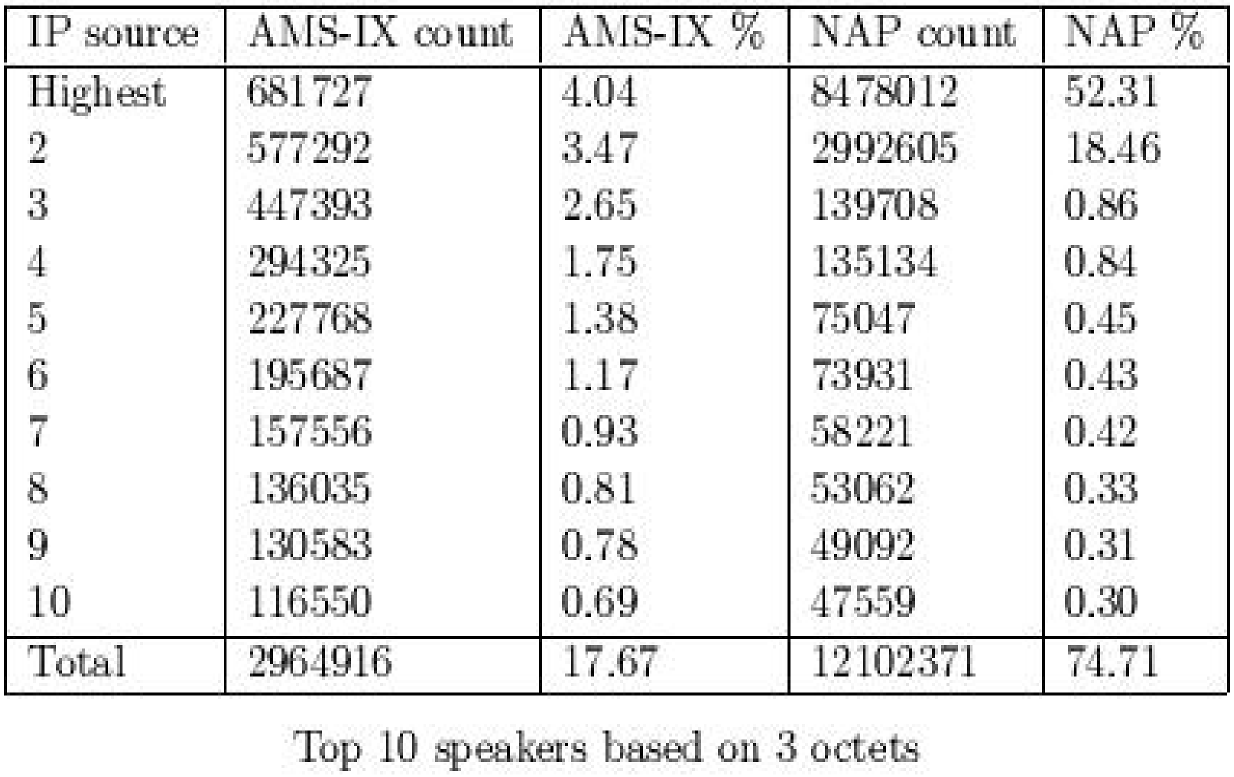
Research: Statistics



Category	AMS-IX count	AMS-IX %	NAP count	NAP %
A-for-A	1287476	7.66	280584	1.73
Private reverse	113483	0.68	27261	0.17
Reserved IP	34705	0.20	5353	0.03
Local domain	2119363	12.61	408912	2.52
Invalid TLD	574026	3.42	95023	0.59
Repeated queries	4779070	28.44	1914330	11.82
Total no-bogus	3243987	19.30	13822295	85.35
Total bogus	13561077	80.70	2372997	14.65
Total	16805064	100.00	16195292	100.00

Percentages of bogus queries

Research: Statistics



IP source	AMS-IX count	AMS-IX %	NAP count	NAP %
Highest	681727	4.04	8478012	52.31
2	577292	3.47	2992605	18.46
3	447393	2.65	139708	0.86
4	294325	1.75	135134	0.84
5	227768	1.38	75047	0.45
6	195687	1.17	73931	0.43
7	157556	0.93	58221	0.42
8	136035	0.81	53062	0.33
9	130583	0.78	49092	0.31
10	116550	0.69	47559	0.30
Total	2964916	17.67	12102371	74.71

Top 10 speakers based on 3 octets

Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

Research: Causes

- Software bugs
  - A for A, Private IP reverse
- Not updated software
  - A for A
- Misconfigured software
  - Private IP reverse, TLD not cached
- Firewalls
  - Repeated

Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

Research

- Determine bogus categories
- Filter capture data
- Statistics
- Determine possible causes
- Determine possible solutions

Research: Solutions

"Client" side:

- Install and use stable software
- Update software
- Configure software appropriatly

Research: Solutions

“Server” side:

- Access lists
- u(RPF)
- Contact software vendors
- Contact the owners of “big” sources
- Add additional servers

Agenda

- Organisation
- Project introduction
- Research
- Conclusion
- Questions

Agenda

- Organisation
- Project introduction
- Research
- Conclusion
- Questions

Conclusion

Statistics:

- Total % of bogus:
  AMS-IX: 80.70%
  NAP: 14.65%
- Top 10 IP addresses responsible:
  AMS-IX: 10.75%
  NAP: 42.40%
- Sources: 3 or 4 octets?

Conclusion

Solutions:

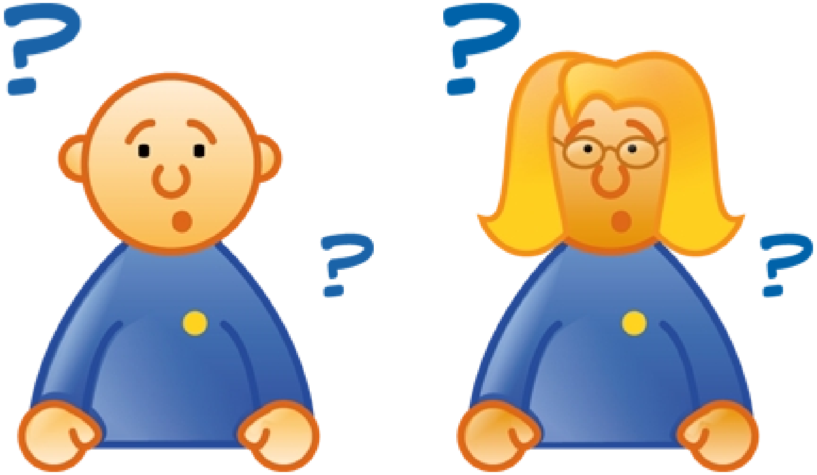
- Contact software vendors
- Contact owners big sources
- Add additional servers

Agenda

- Organisation
- Project introduction
- Research
- Conclusion
- Questions

Agenda

- Organisation
- Project introduction
- Research
- Conclusion
- Questions



Questions?