ICANN Tech Day – host presentation

Adam Leach, Roy Arends

Adam Leach, Director R&D

Adam joined Nominet in July 2013 and is responsible for leading Nominet's R&D initiatives, managing innovation and new product development.

Previously Adam was at Ovum, a global analyst firm, leading Ovum’s research in smart devices providing market insight and intelligence on consumer technology. Whilst at Ovum he was a regular commentator on the technology news in the press, appearing on the BBC News, Wall Street Journal, The Guardian and The Financial Times. Prior to this Adam worked for Vodafone defining its software strategy for smartphones.

Adam's background is in software engineering and he was the technical lead for the world’s first smartphone the Nokia Communicator.

adam.leach@nominet.org.uk

@adamhleach

nominet innovation
ideas. transformed

Contents

- Welcome to the .UK
- Introduction to Nominet R&D
- Adventures in big-data and DNS analytics

nominet® innovation
ideas. transformed

Adam Leach, Director R&D

WELCOME TO THE .UK

Nominet manages over 10.5 million domains in the UK zone

Most well known for .co.uk, however, from June 2014 now accepting .uk registrations

nominet innovation
ideas. transformed

Build innovative new products and services that create new opportunities

Our focus: Cyber-security, Internet of Things, big-data & analytics and of course DNS

nominet innovation
ideas. transformed

nominet® innovation
ideas. transformed

Roy Arends, Research Fellow

ADVENTURES IN BIG-DATA AND DNS ANALYTICS

roy.arends@nominet.org.uk

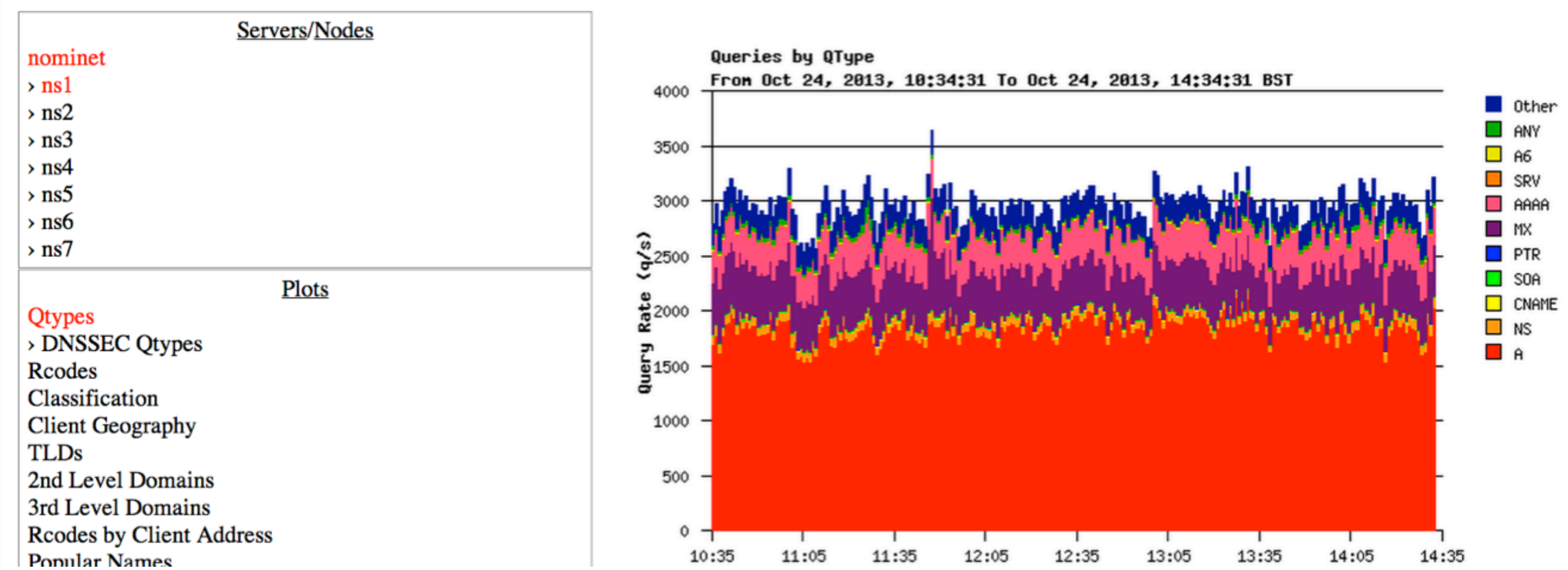
Roy Arends, Research Fellow

Roy joined Nominet in February 2006 and is responsible for all things research (outreach, Academia), DNS, helping innovation and new product development. Additionally, he is a technical advisor to Nominet's technical team.

Roy has co-authored the IETF DNSSEC standards and has initiated many open-source products that are in use today, such as Unbound, OpenDNSSEC and FPDNS. Roy has been a director at DNS-OARC and was responsible for running CERT-NL.

Currently, he is mainly active in the area of Big Data and Cyber Security.

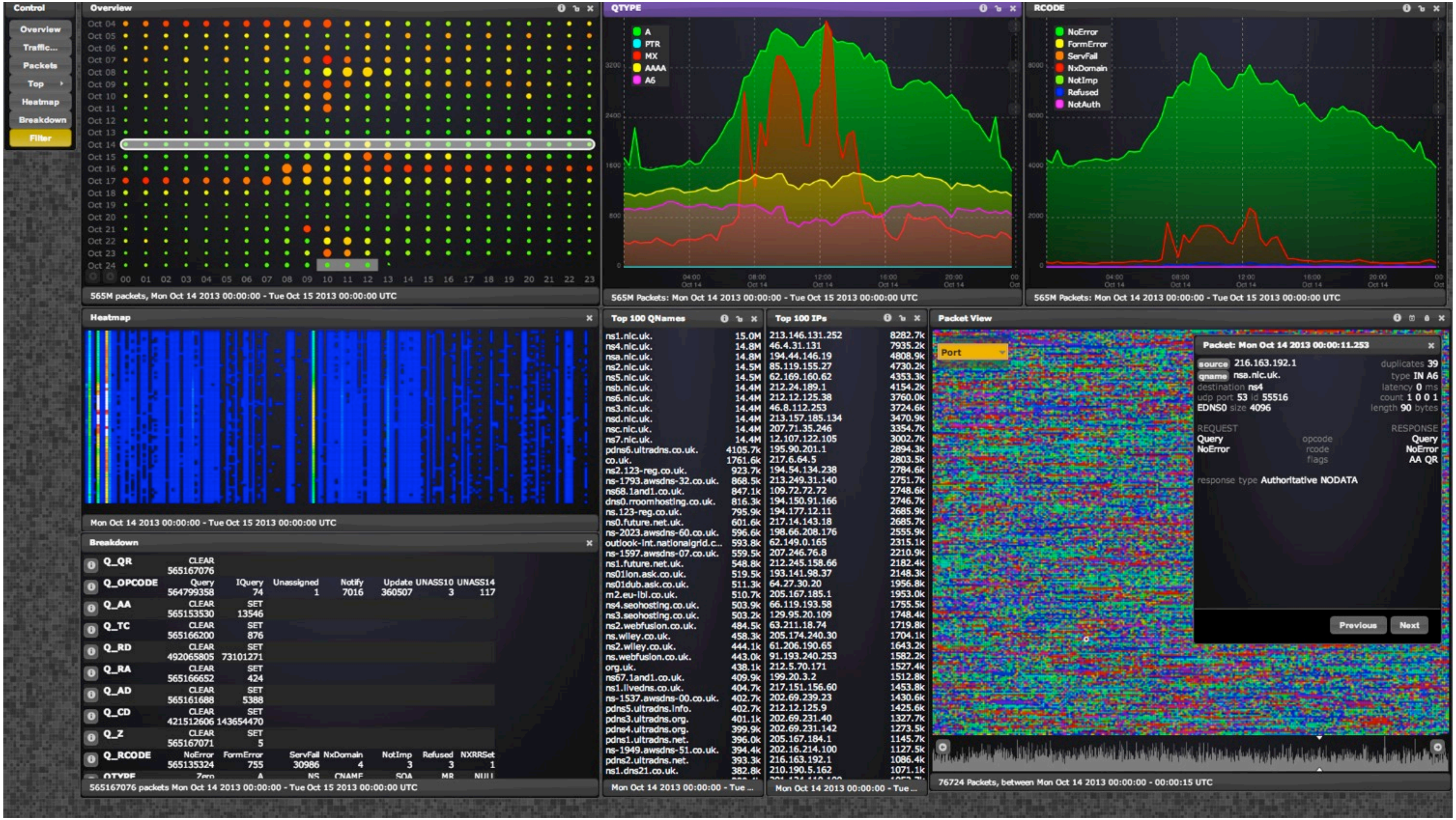
nominet innovation
ideas. transformed



Current DNS analysis and visualization tools are dated

DCS currently represents the best tools we have for DNS analysis

nominet innovation
ideas. transformed



565M packets, Mon Oct 14 2013 00:00:00 - Tue Oct 15 2013 00:00:00 UTC

565M Packets: Mon Oct 14 2013 00:00:00 - Tue Oct 15 2013 00:00:00 UTC

565M Packets: Mon Oct 14 2013 00:00:00 - Tue Oct 15 2013 00:00:00 UTC

Mon Oct 14 2013 00:00:00 - Tue Oct 15 2013 00:00:00 UTC

Breakdown

```
Q_QR          CLEAR
          565167076
Q_OPCODE      Query    IQuery  Unassigned   Notify     Update UNASS10 UNASS14
          564799358        74           1     7016     360507       3     117
Q_AA          CLEAR       SET
          565153530     13546
Q_TC          CLEAR       SET
          565166200       876
Q_RD          CLEAR       SET
          492065805  73101271
Q_RA          CLEAR       SET
          565166652       424
Q_AD          CLEAR       SET
          565161688      5388
Q_CD          CLEAR       SET
          421512606 143654470
Q_Z           CLEAR       SET
          565167071         5
Q_RCODE     NoError FormError    ServFail NxDomain   NotImp  Refused NXRRSet
          565135324       755       30986        4        3        3       1
QTYPE          Zero         A          NS    CNAME      SOA       MR    NULL
```

565167076 packets Mon Oct 14 2013 00:00:00 - Tue Oct 15 2013 00:00:00 UTC

Top 100 QNames

ns1.nic.uk.	15.0M
ns4.nic.uk.	14.8M
nsa.nic.uk.	14.8M
ns2.nic.uk.	14.5M
ns5.nic.uk.	14.5M
nsb.nic.uk.	14.4M
ns6.nic.uk.	14.4M
ns3.nic.uk.	14.4M
nsd.nic.uk.	14.4M
nsc.nic.uk.	14.4M
ns7.nic.uk.	14.4M
pdns6.ultradns.co.uk.	4105.7k
co.uk.	1761.6k
ns2.123-reg.co.uk.	923.7k
ns-1793.awsdns-32.co.uk.	868.5k
ns68.1and1.co.uk.	847.1k
dns0.rroomhosting.co.uk.	816.3k
ns.123-reg.co.uk.	795.9k
ns0.future.net.uk.	601.6k
ns-2023.awsdns-60.co.uk.	596.6k
outlook-int.nationalgrid.c...	593.8k
ns-1597.awsdns-07.co.uk.	559.5k
ns1.future.net.uk.	548.8k
ns01lon.ask.co.uk.	519.5k
ns01dub.ask.co.uk.	511.3k
m2.eu-ibl.co.uk.	510.7k
ns4.seohosting.co.uk.	503.9k
ns3.seohosting.co.uk.	503.2k
ns2.webfusion.co.uk.	484.5k
ns.wiley.co.uk.	458.3k
ns2.wiley.co.uk.	444.1k
ns.webfusion.co.uk.	443.0k
org.uk.	438.1k
ns67.1and1.co.uk.	409.9k
ns1.livedns.co.uk.	404.7k
ns-1537.awsdns-00.co.uk.	402.7k
pdns5.ultradns.info.	402.7k
pdns3.ultradns.org.	401.1k
pdns4.ultradns.org.	399.9k
pdns1.ultradns.net.	396.0k
ns-1949.awsdns-51.co.uk.	394.4k
pdns2.ultradns.net.	393.3k
ns1.dns21.co.uk.	382.8k

Mon Oct 14 2013 00:00:00 - Tue ...

Top 100 IPs

213.146.131.252	8282.7k
46.4.31.131	7935.2k
194.44.146.19	4808.9k
85.119.155.27	4730.2k
62.169.160.62	4353.3k
212.24.189.1	4154.2k
212.12.125.38	3760.0k
46.8.112.253	3724.6k
213.157.185.134	3470.9k
207.71.35.246	3354.7k
12.107.122.105	3002.7k
195.90.201.1	2894.3k
217.6.64.5	2803.5k
194.54.134.238	2784.6k
213.249.31.140	2751.7k
109.72.72.72	2748.6k
194.150.91.166	2746.7k
194.177.12.11	2685.9k
217.14.143.18	2685.7k
198.66.208.176	2555.9k
62.149.0.165	2315.1k
207.246.76.8	2210.9k
212.245.158.66	2182.4k
193.141.98.37	2148.3k
64.27.30.20	1956.8k
205.167.185.1	1953.0k
66.119.193.58	1755.5k
129.95.20.109	1748.4k
63.211.18.74	1719.8k
205.174.240.30	1704.1k
61.206.190.65	1643.2k
91.193.240.253	1582.2k
212.5.70.171	1527.4k
199.20.3.2	1512.8k
217.151.156.60	1453.8k
202.69.239.23	1430.6k
212.12.125.9	1425.6k
202.69.231.40	1327.7k
202.69.231.142	1273.5k
205.167.184.1	1145.7k
202.16.214.100	1127.5k
216.163.192.1	1086.4k
210.190.5.162	1071.1k

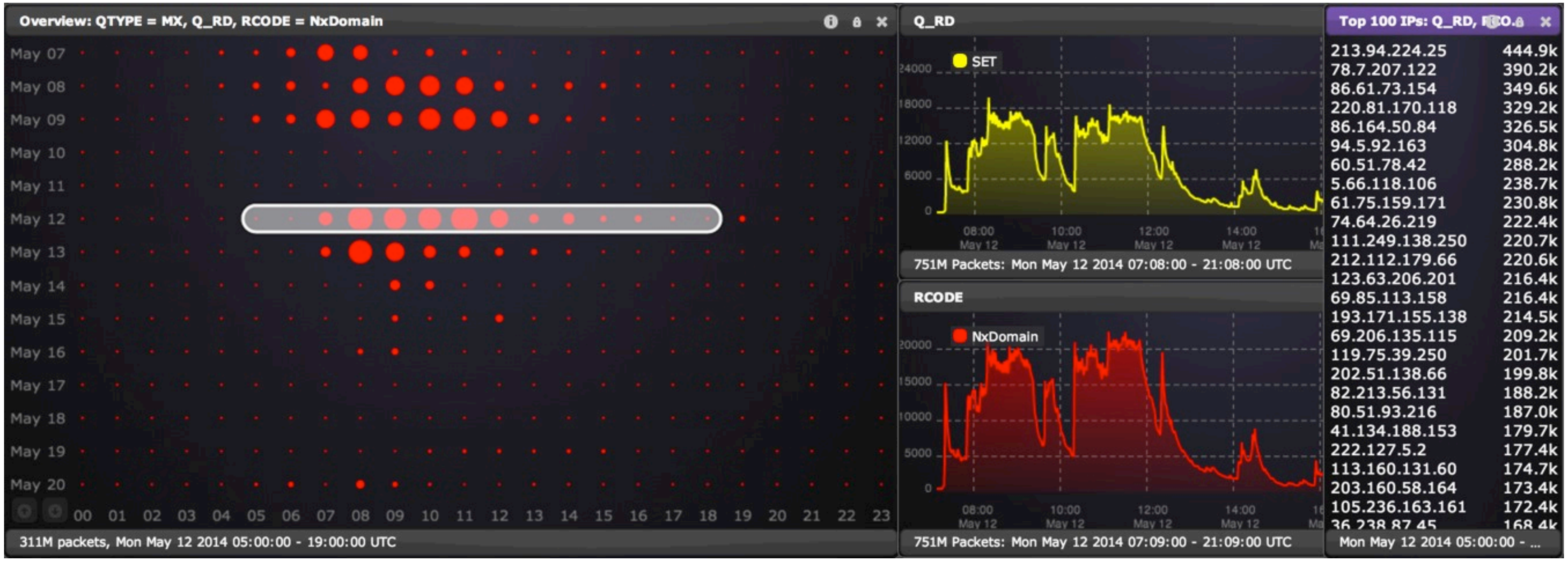
Mon Oct 14 2013 00:00:00 - Tue ...

Packet: Mon Oct 14 2013 00:00:11.253

source 216.163.192.1		duplicates 39
qname nsa.nic.uk.		type IN A6
destination ns4		latency 0 ms
udp port 53 id 55516		count 1 0 0 1
EDNS0 size 4096		length 90 bytes
REQUEST		RESPONSE
Query	opcode	Query
NoError	rcode	NoError
	flags	AA QR

response type Authoritative NODATA

76724 Packets, between Mon Oct 14 2013 00:00:00 - 00:00:15 UTC



Overview: QTYPE = MX, Q_RD, RCODE = NxDomain

311M packets, Mon May 12 2014 05:00:00 - 19:00:00 UTC

Q_RD

751M Packets: Mon May 12 2014 07:08:00 - 21:08:00 UTC

RCODE

751M Packets: Mon May 12 2014 07:09:00 - 21:09:00 UTC

Top 100 IPs: Q_RD, RCO.

213.94.224.25	444.9k
78.7.207.122	390.2k
86.61.73.154	349.6k
220.81.170.118	329.2k
86.164.50.84	326.5k
94.5.92.163	304.8k
60.51.78.42	288.2k
5.66.118.106	238.7k
61.75.159.171	230.8k
74.64.26.219	222.4k
111.249.138.250	220.7k
212.112.179.66	220.6k
123.63.206.201	216.4k
69.85.113.158	216.4k
193.171.155.138	214.5k
69.206.135.115	209.2k
119.75.39.250	201.7k
202.51.138.66	199.8k
82.213.56.131	188.2k
80.51.93.216	187.0k
41.134.188.153	179.7k
222.127.5.2	177.4k
113.160.131.60	174.7k
203.160.58.164	173.4k
105.236.163.161	172.4k
36.238.87.45	168.4k

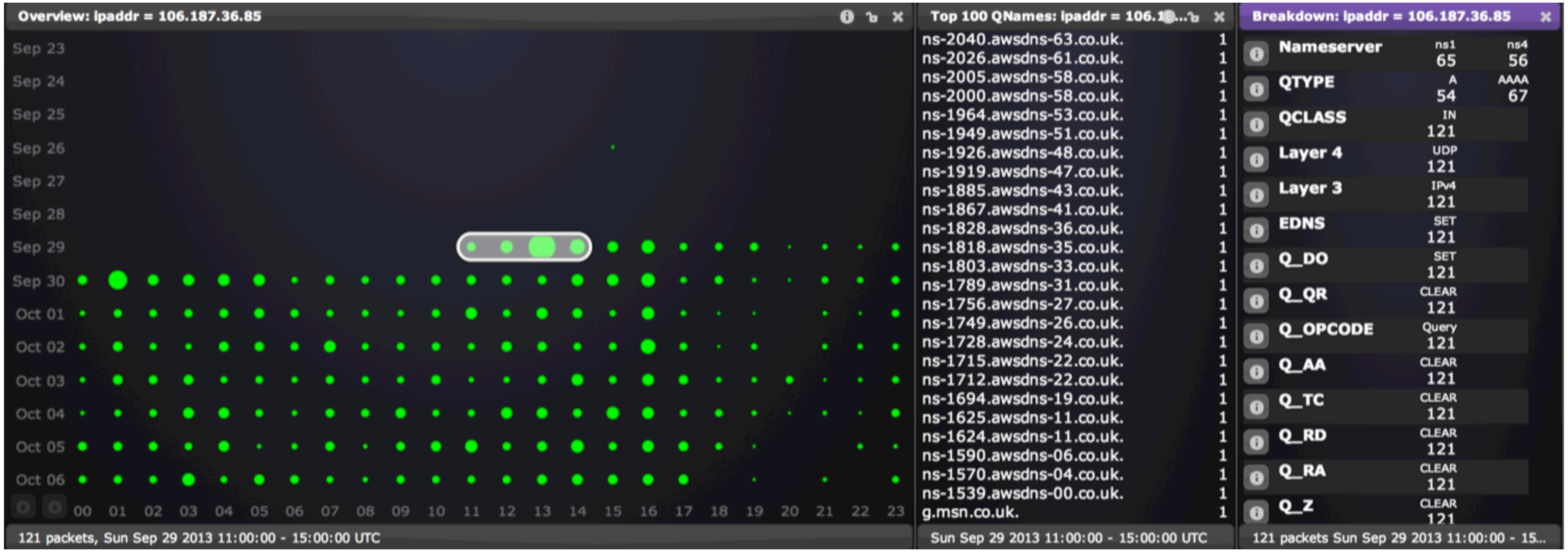
Mon May 12 2014 05:00:00 - ...

Botnet Tracking

Large Spam run trails in DNS.

The dots show the volume of DNS requests for type MX, with RD bit set, that result in NXDOMAIN, per hour.

nominet innovation
ideas. transformed


Overview: ipaddr = 106.187.36.85

121 packets, Sun Sep 29 2013 11:00:00 - 15:00:00 UTC

Top 100 QNames: ipaddr = 106.1...

ns-2040.awsdns-63.co.uk.	1
ns-2026.awsdns-61.co.uk.	1
ns-2005.awsdns-58.co.uk.	1
ns-2000.awsdns-58.co.uk.	1
ns-1964.awsdns-53.co.uk.	1
ns-1949.awsdns-51.co.uk.	1
ns-1926.awsdns-48.co.uk.	1
ns-1919.awsdns-47.co.uk.	1
ns-1885.awsdns-43.co.uk.	1
ns-1867.awsdns-41.co.uk.	1
ns-1828.awsdns-36.co.uk.	1
ns-1818.awsdns-35.co.uk.	1
ns-1803.awsdns-33.co.uk.	1
ns-1789.awsdns-31.co.uk.	1
ns-1756.awsdns-27.co.uk.	1
ns-1749.awsdns-26.co.uk.	1
ns-1728.awsdns-24.co.uk.	1
ns-1715.awsdns-22.co.uk.	1
ns-1712.awsdns-22.co.uk.	1
ns-1694.awsdns-19.co.uk.	1
ns-1625.awsdns-11.co.uk.	1
ns-1624.awsdns-11.co.uk.	1
ns-1590.awsdns-06.co.uk.	1
ns-1570.awsdns-04.co.uk.	1
ns-1539.awsdns-00.co.uk.	1
g.msn.co.uk.	1

Sun Sep 29 2013 11:00:00 - 15:00:00 UTC

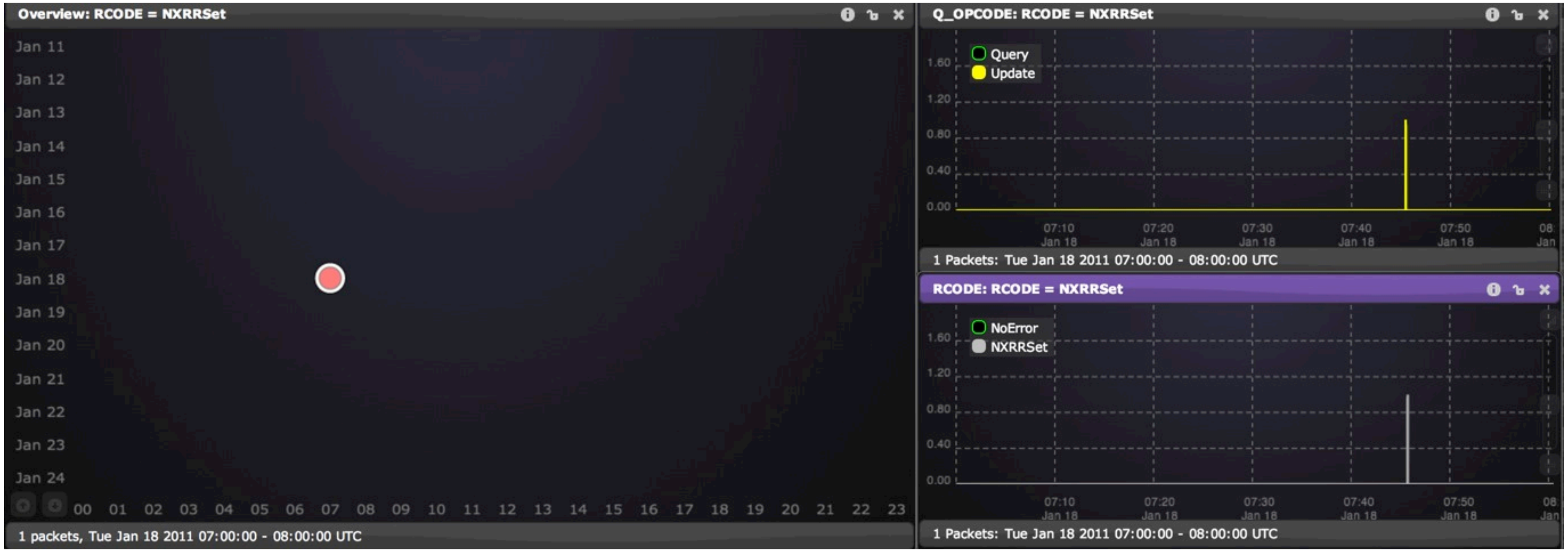
Breakdown: ipaddr = 106.187.36.85

Nameserver	ns1 65	ns4 56
QTYPE	A 54	AAAA 67
QCLASS	IN 121	
Layer 4	UDP 121	
Layer 3	IPv4 121	
EDNS	SET 121	
Q_DO	SET 121	
Q_QR	CLEAR 121	
Q_OPCODE	Query 121	
Q_AA	CLEAR 121	
Q_TC	CLEAR 121	
Q_RD	CLEAR 121	
Q_RA	CLEAR 121	
Q_Z	CLEAR 121	

121 packets Sun Sep 29 2013 11:00:00 - 15...

DNS Changer tracking

Sudden DNS activity for a single resolver.
A sudden flurry of DNS requests by DNS-Changer. The vast amount of awsdns requests might indicate where their infrastructure is located.



1 packets, Tue Jan 18 2011 07:00:00 - 08:00:00 UTC

1 Packets: Tue Jan 18 2011 07:00:00 - 08:00:00 UTC

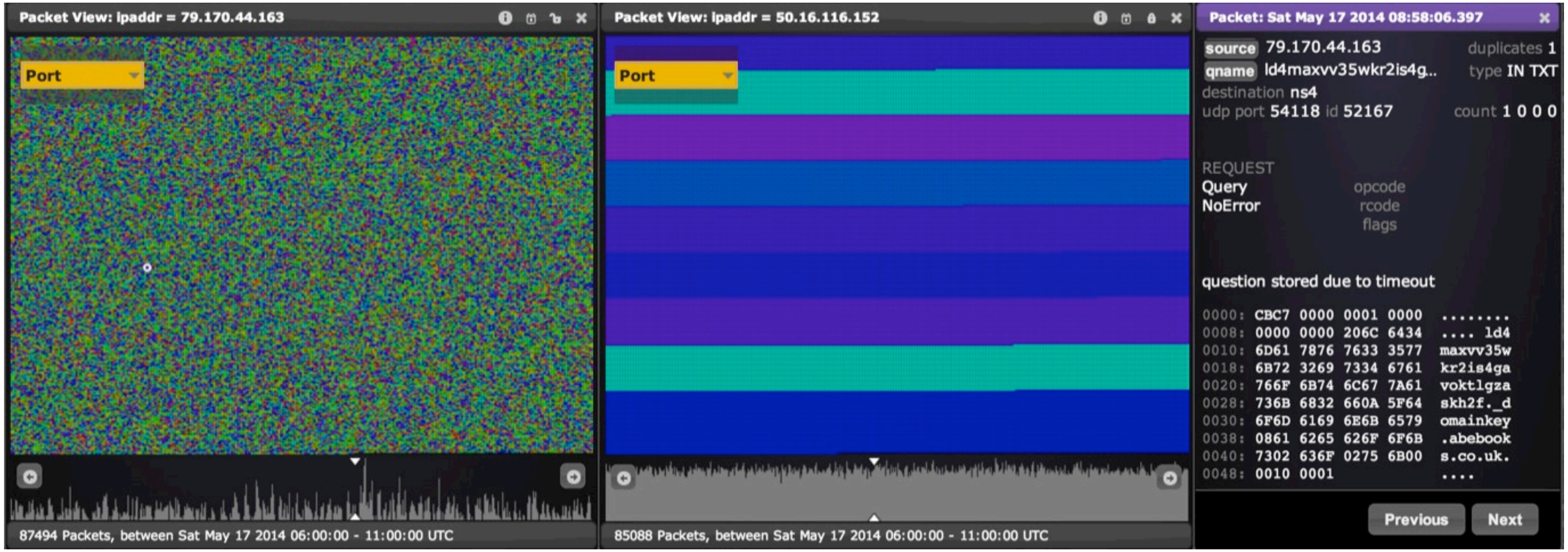
1 Packets: Tue Jan 18 2011 07:00:00 - 08:00:00 UTC

BIND Packet of Death (CVE-2011-2464)

Configured to show NXRRSet responses (only used in Dynamic Updates) from secondary nameservers.

One single packet found in daily churns of 3 to 5 Billion DNS requests

nominet innovation
ideas. transformed



Packet View: ipaddr = 79.170.44.163
Port
87494 Packets, between Sat May 17 2014 06:00:00 - 11:00:00 UTC
Packet View: ipaddr = 50.16.116.152
Port
85088 Packets, between Sat May 17 2014 06:00:00 - 11:00:00 UTC
Packet: Sat May 17 2014 08:58:06.397

source 79.170.44.163 duplicates 1
qname ld4maxvv35wkr2is4g.. type IN TXT
destination ns4
udp port 54118 id 52167 count 1 0 0 0

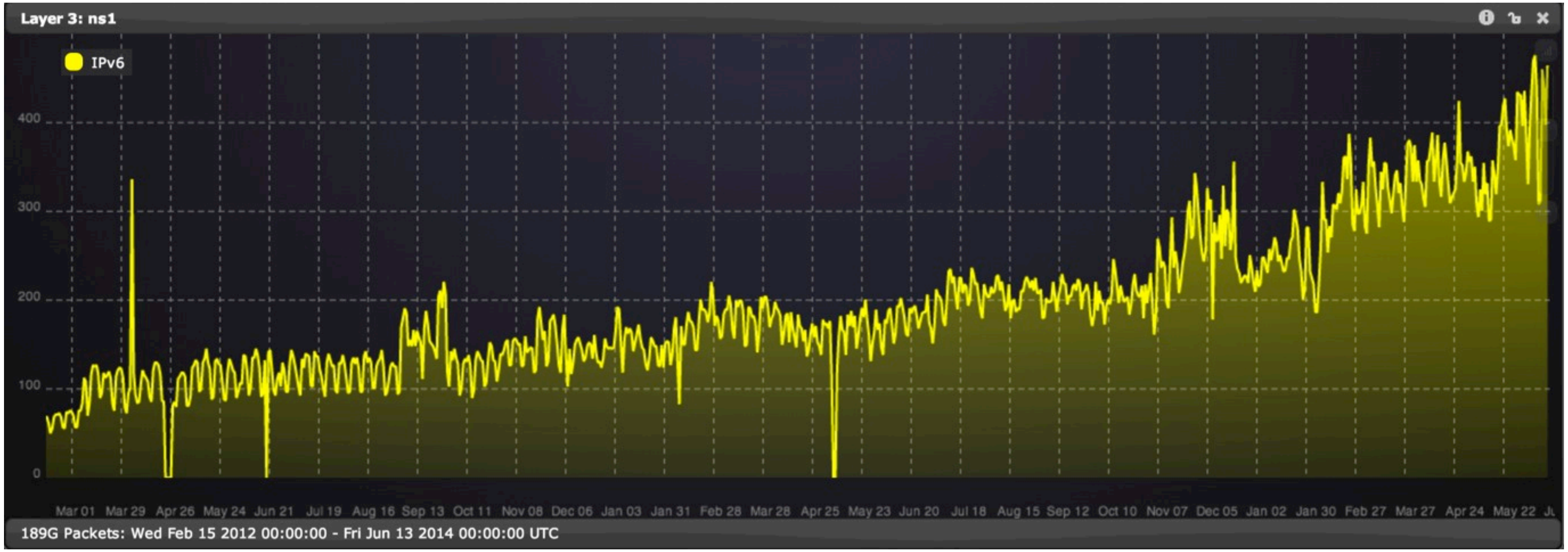
REQUEST
Query opcode
NoError rcode
flags

question stored due to timeout

```
0000: CBC7 0000 0001 0000  ........
0008: 0000 0000 206C 6434  .... ld4
0010: 6D61 7876 7633 3577  maxvv35w
0018: 6B72 3269 7334 6761  kr2is4ga
0020: 766F 6B74 6C67 7A61  voktlgza
0028: 736B 6832 660A 5F64  skh2f._d
0030: 6F6D 6169 6E6B 6579  omainkey
0038: 0861 6265 626F 6F6B  .abebook
0040: 7302 636F 0275 6B00  s.co.uk.
0048: 0010 0001            ....
```

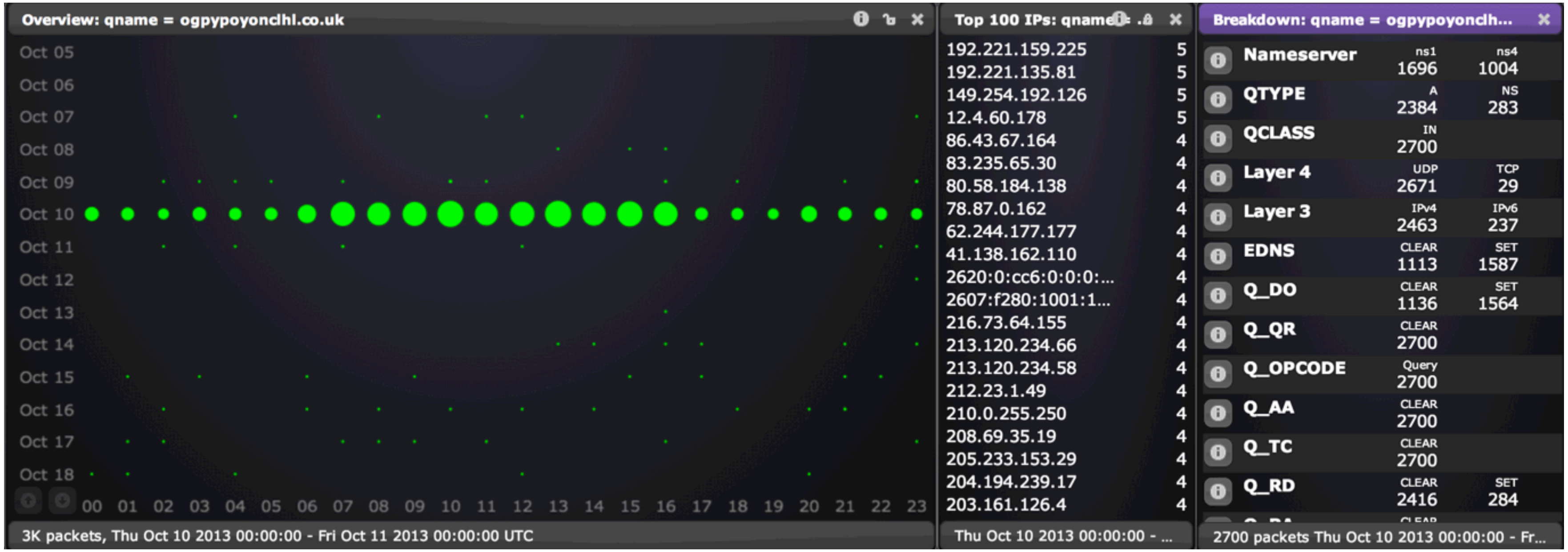
Randomised vs Predictable Port Numbers

Configured to show packet traces from two different resolvers. The resolver on the left randomises its source port. The resolver on the right increases its port every so often.



The uptake of IPv6

Configured to show a daily trend of traffic over IPv6 to a single nameserver over a 2.5 year period.



Overview: qname = ogpypoyonclhl.co.uk

3K packets, Thu Oct 10 2013 00:00:00 - Fri Oct 11 2013 00:00:00 UTC

Top 100 IPs: qname

192.221.159.225	5
192.221.135.81	5
149.254.192.126	5
12.4.60.178	5
86.43.67.164	4
83.235.65.30	4
80.58.184.138	4
78.87.0.162	4
62.244.177.177	4
41.138.162.110	4
2620:0:cc6:0:0:0:...	4
2607:f280:1001:1...	4
216.73.64.155	4
213.120.234.66	4
213.120.234.58	4
212.23.1.49	4
210.0.255.250	4
208.69.35.19	4
205.233.153.29	4
204.194.239.17	4
203.161.126.4	4

Thu Oct 10 2013 00:00:00 - ...

Breakdown: qname = ogpypoyonclh...

Nameserver	ns1 1696	ns4 1004
QTYPE	A 2384	NS 283
QCLASS	IN 2700	
Layer 4	UDP 2671	TCP 29
Layer 3	IPv4 2463	IPv6 237
EDNS	CLEAR 1113	SET 1587
Q_DO	CLEAR 1136	SET 1564
Q_QR	CLEAR 2700	
Q_OPCODE	Query 2700	
Q_AA	CLEAR 2700	
Q_TC	CLEAR 2700	
Q_RD	CLEAR 2416	SET 284

2700 packets Thu Oct 10 2013 00:00:00 - Fr...

Cryptolocker infections

Configured to show queries related to the Cryptolocker Malware.
This shows that the DGA is seeded by date.

nominet innovation
ideas. transformed

nominet®

innovation