ICANN Tech Day – host presentation

Adam Leach, Roy Arends
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.
Contents

• Welcome to the .UK
• Introduction to Nominet R&D
• Adventures in big-data and DNS analytics
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
Build innovative new products and services that create new opportunities

Our focus: Cyber-security, Internet of Things, big-data & analytics and of course DNS
ADVENTURES IN BIG-DATA AND DNS ANALYTICS
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.

roy.arends@nominet.org.uk
Current DNS analysis and visualization tools are dated

DCS currently represents the best tools we have for DNS analysis
**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.
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.
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
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.
Cryptolocker infections

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