OARC Status

Keith Mitchell

OARC Programme Manager

DNS Operations Meeting

27th July 2007

OARC Mission

- Provide trusted channels for Internet incident reporting and handling
- Facilitate confidential sharing of DNS operations data
- Interface with research community for analysis and publication
- Outreach to vendors, end-users and law enforcement

OARC Motivation

- DNS infrastructure makes everything work as expected
- DNS outage of any network service provider or large content provider affects everyone using the Internet
- The DNS is increasingly involved:
  - as abuse victim
  - as abuse vector
  - for abuse detection and mitigation

OARC Motivation

- Increasing incidence of attacks against the DNS
- DNS increasingly implicated in and compromised by Botnet activity
- A lot of unwanted traffic on the Internet is a result of DNS misconfiguration
    - e.g. in-addr queries to RFC1918 addresses
- New DNS technology challenges
    - DNSSEC, IDN, ENUM, IPv6

OARC Members

- Afillias
- AFNIC
- APNIC
- Autonomica
- BFK
- Cambridge Univ
- ChangeIP.com
- CIRA
- Cisco
- Cogent
- CZ.NIC
- Damballa
- DENIC
- eNom
- EP.net
- F-root
- Georgia Tech
- Google
- **ICANN**
- II-F
- Internet Perils
- ISC
- ISoc-IL
- **JPRS**
- Microsoft
- NASA Ames
- **NASK**
- **NIC.CL**
- NIDA
- NLnet Labs
- Nominet UK
- NTT
- *OpenDNS*
- PIR
- Registro.BR
- RIPE NCC
- Shinkuro
- **SIDN**
- Team Cymru
- UMR.edu
- NeuStar/uDNS
- UMD.edu
- **VeriSign**
- **Yahoo!**
- WIDE

OARC Member Services

- DSC Data Gathering
- Data Analysis
- Member-only mailing list
- Other closed DNS mailing lists
- Encrypted jabber.oarc.isc.org chat server
- https://oarc.isc.org portal

OARC Public Services

- Twice-yearly open meetings for DNS researchers and operators
- <dns-operations@lists.oarci.net> mailing list
- http://public.oarci.net website
- Home for:
  - "Orphan Projects"
  - "Flood Victims"

OARC 2007 Progress

- Data gathering for DITL project, Jan
  - CAIDA DatCat workshop
- Co-ordination and data gathering during root attack, Feb
- Outreach during NANOG, RIPE, CENTR, UKNOF, AusCERT etc meetings
- 7 new members, mostly paying ☺
- Chicago meetings, Jul

“Day in the Life of the Internet”

- Wide-ranging collaborative research project to improve “network science” by building up baseline of regular Internet measurement data over 48-hour periods
- See http://www.caida.org/projects/ditl/
- DNS data gathered via OARC is one part of this

DITL 8-10th Jan 2007

- OARC has supported this annually since 2004
- DNS query data gathered close to participating root and TLD servers using tcpdump into “PCAP” files
- Uploaded via ssh script to central OARC RAID system
- Available to OARC members for analysis

DITL Jan 2007 Participants

c.root-servers.net	Cogent
e.root-servers.net	NASA
f.root-servers.net	ISC
k.root-servers.net	RIPE NCC
m.root-servers.net	WIDE
as112.namex.it	NaMEX
b.orsn-servers.net	FunkFeur
m.orsn-servers.net	Brave GmbH

DITL Challenges

- Too much data
  - problem of success !
  - ran out of disk space 2 hours before end
  - “in-flight” upgrade to fix this...
- Limited space on collecting servers
- Bandwidth loss due to Taiwan quake
- Too close to seasonal holiday
- Bleeding-edge platforms

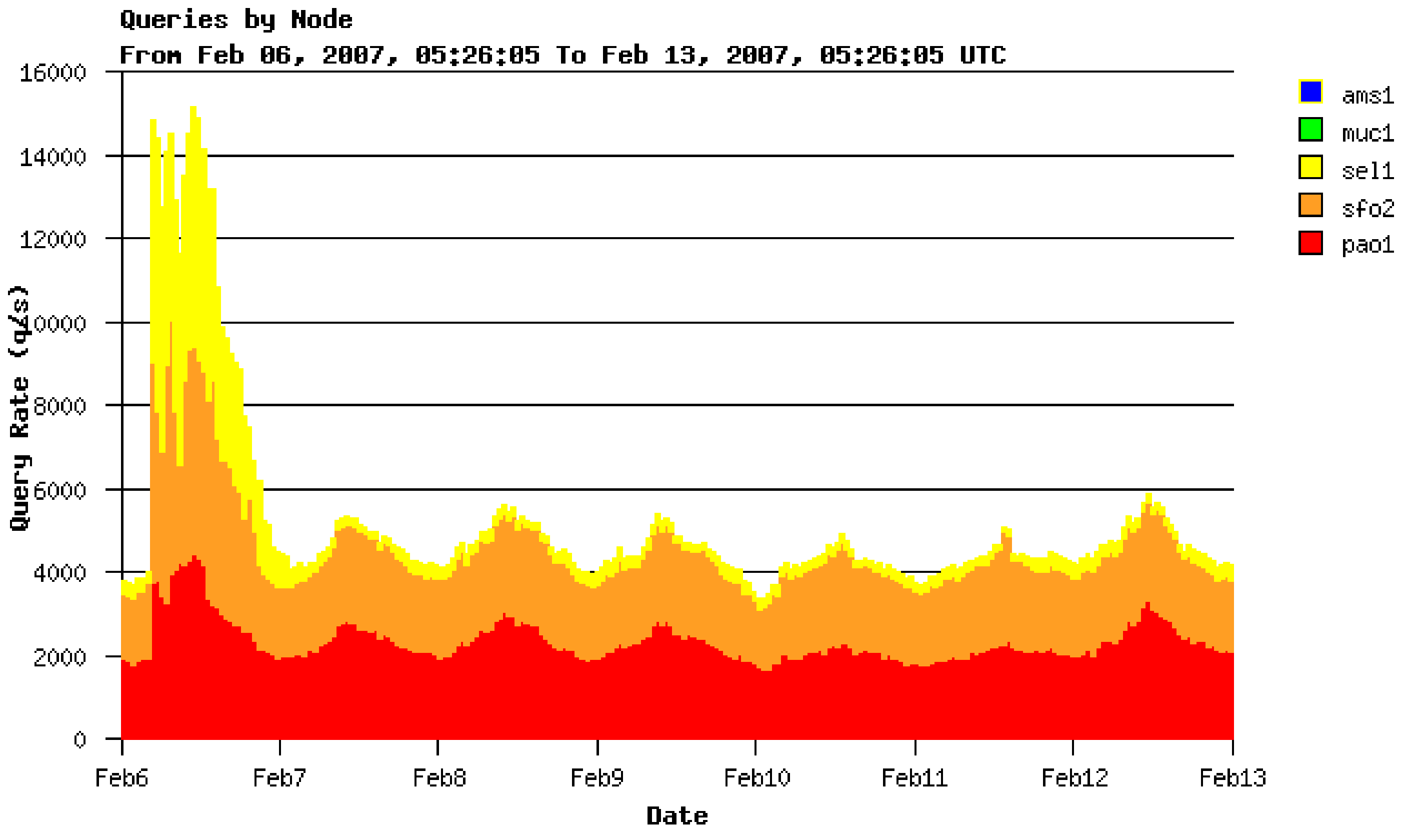
DITL Lessons Learned

- Do pending upgrades and estimate of data volumes **before** you start !
- Simple legalities = enlarged participation ☺
- Data uploading was harder than gathering
  - dry-runs helpful
- Disable auto-rotation
- Generate, preserve, share and validate data MD5 checksums
- Upgraded hardware performed well overall

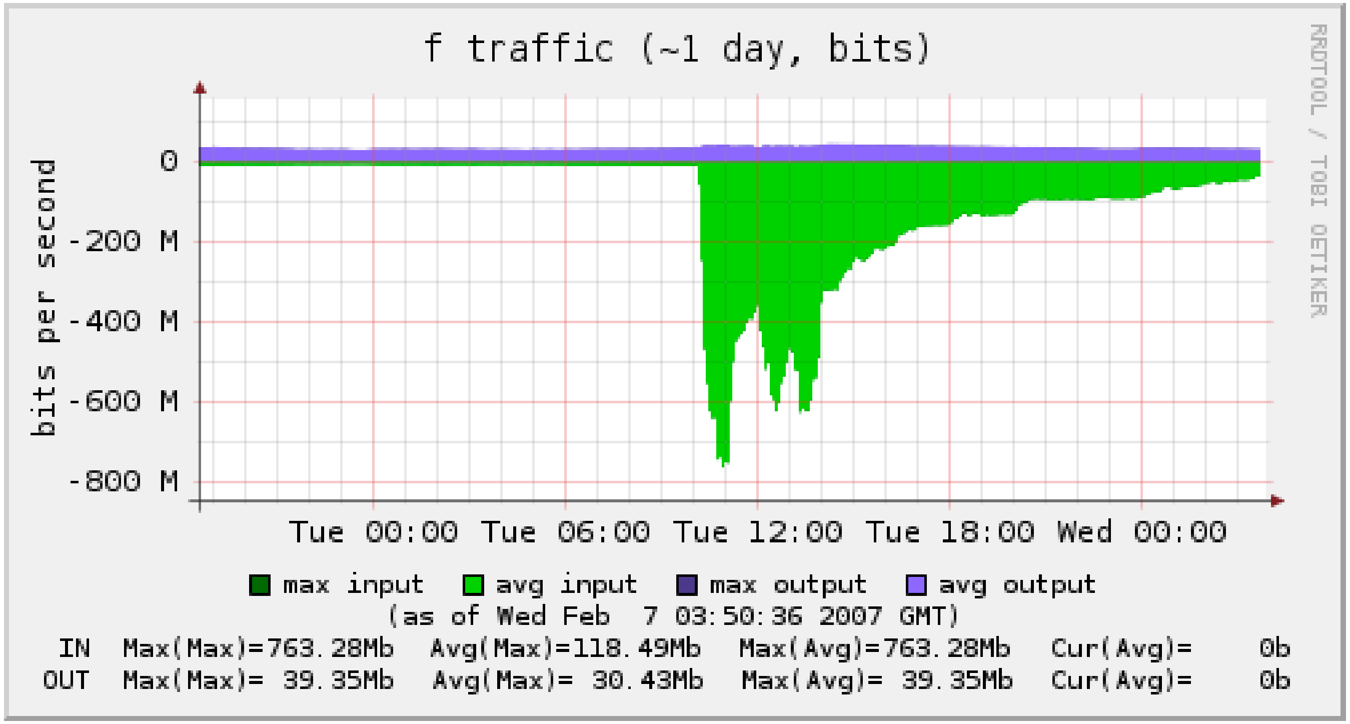
DITL Results

- OARC RAID now holds over 2TB of data
  - available for research analysis
  - space for at least as much again
- Report summarising outcomes available to participants and OARC members
- More roots interested for next time
- Left us in great shape to do it again without notice 4 weeks later...

Root DDoS Attack



Aggregated traffic on F root



```
                    (as of Wed Feb  7 03:50:36 2007 GMT)
 IN  Max(Max)=763.28Mb  Avg(Max)=118.49Mb  Max(Avg)=763.28Mb  Cur(Avg)=    0b
OUT  Max(Max)= 39.35Mb  Avg(Max)= 30.43Mb  Max(Avg)= 39.35Mb  Cur(Avg)=    0b
```

Attack Observations

- Anycast works !
  - end-users not really impacted
  - some F-root nodes impacted, but service overall maintained
  - non-anycast nodes (G, L) hit hardest
- Further presentations and analysis by John Kristoff (UltraDNS) and Steve Conte (ICANN) during this meeting

OARC Futures

- Additional resources required
- Further develop trusted communications model
- “Passive DNS” - major project to aggregate live DNS resolver data
  - seeking infrastructure funding and partners

OARC Further Info

- Web: https://oarc.isc.org
- E-mail: keith_mitchell@isc.org
- Jabber: keith@jabber.oarc.isc.org
- Phone: +1 650 423 1348 (EST)
  +44 778 534 6152
- Paper:
  http://public.oarci.net/files/oarc-briefing.pdf

http://public.oarci.net/dns-operations/workshop-2007/Mitchell-OARC-status.pdf

Questions ?