OARC Update

Keith Mitchell
OARC Programme Manager

OARC Workshop
Los Angeles
2nd November 2007

Presentation

- OARC Overview
- OARC Governance Update
- Open Recursive Resolvers
- Whois Query Data Sharing, Anyone ?
- DNSCAP
- 2008 Activity Plan

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
- ChangeIP.com
- CIRA
- Cisco
- CMU CERT
- 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
- NIC.MX
- NIDA
- NLnet Labs
- Nominet UK
- NTT
- OpenDNS
- PIR
- Registro.B
- RIPE NCC
- Shinkuro
- SIDN
- Team Cymru
- 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
    - shared ticketing system

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 Refugees”

OARC 2007 Activities

- DITL 2007
- Member meeting and open DNS Operators' workshop at Chicago in July
  - `http://public.oarci.net/dns-operations/workshop-2007`
- 6-person Policy Council elected for first time
- Revised Participation Agreement approved
- OARC meeting and DNS researcher workshop in Los Angeles 2nd/3rd November

OARC Membership Agreement Changes

1. "Participation Agreement" throughout
2. Housekeeping, typos
3. Allows for dormant non-contributing members to be downgraded
4. Mechanism for changes to agreement and making them binding on all members
5. Increase size of Policy Council from 3 to 6 members
6. Revise membership categories

OARC Participation Benefits

	Root Member	Member	Beneficial	Affiliate**	Contributor**	Associate**	Public
Open mailing list participation							
Attend DNS operations workshops							
Public website access							
Private web portal access							
Analysis login							
Attend member meetings							
Access data							
Submit data							
Jabber chat login							
Voting Rights							
Member mailing list participation							
Shared ticketing access							
Jabber private groupchat							
Sponsor private groups							
Root Server Advisory Group							

New Participation Levels

• Category 0, *Beneficial*		2 PoCs
• Category 1, *Normal*		3 PoCs
• Category 2, *Expanded*		5 PoCs
• Category 3, *Supporting*		8 PoCs
• Category 4, *Sustaining*		>8 PoCs
• *Affiliate*	Submit & Access data	1 PoC
• *Associate*	Access data only	1 PoC
• *Contributor*	Submit data only	1 PoC

OARC Policy Council

- Elected by members for first time in Jul 07
- Provides member governance and budgetary oversight to ensure neutrality and relevance of OARC
- Monthly meetings
- Contact by e-mail to: <council@oarc.isc.org>

Policy Council Members

- John Kristoff, UltraDNS
- Matt Larson, VeriSign *(RSAC representative)*
- George Michaelson, APNIC
- Keith Mitchell, OARC Secretariat (ISC)
- Gerry Sneeringer, UMD (*D* root)
- Andrew Sullivan, Afilias

Policy Council Workplan

- Define bye-laws for Council
  - e.g. rotation beyond initial 1-year terms
  - voting tie-break mechanism
- Review budget for 2008 and set fee levels
  - fee increase of ~25% in new calendar year likely, details being worked upon
- Prioritize OARC activities and projects

Open Recursive Resolvers

- ORRs are DNS caching resolvers which will answer queries from anywhere on the Internet
- Have already been used as amplifier in a number of DDoS attacks (e.g. EDNS0)
- Various efforts to measure the extent of the problem
- All suggest it is serious, potentially millions of ORRs out there ☹

Open Recursive Resolvers

- Surveys have been conducted by:
  - David Dagon (Georgia Tech)
  - April Lorenzen
  - John Kristoff (UltraDNS)
  - Duane Wessels
  - Rick Wesson (Support Intelligence)
- ORRs represent a clear and present danger to the infrastructure of all DNS operators, and OARC wants to help tackle this

ORR Data Sharing

- OARC is providing a repository for members and researchers to share open resolver data
- A number of contributors to date
- Some visualisations of surveys ("Hilbert Curve" maps) available
- More data and analysis welcome !

Whois Query Data Sharing

- Many registries (TLD, also RIRs) suffer ongoing data-mining attacks against their whois services
- Most are however required to provide this service
- It is difficult to differentiate between legitimate and valid query sources
- Would sharing query source data be helpful ?

Whois Query Data Sharing

- Registries could contribute whois source IP address data to OARC
- Do analysis to help better characterise how to optimise/protect service
- Could be correlated with other botnet data to detect abusive query sources

DNSCAP – Can Do Things TCPDUMP Won't !

- Close/reopen output files on a set schedule
- Search by DNS message type
- Select by DNS initiator or responder
- Listen to multiple interfaces
- Dump messages in DiG (text) format
- Select messages using regular expressions

DNSCAP Status

- DNSCAP is available via anoncvs, see http://public.oarci.net/tools/dnscap/
- Delayed the “final release” while the command line syntax evolved and settled
- It's time to declare that it's finished, and focus on other work (NCAP)
- These features and ideas being revisited as part of a larger NCAP toolworks

OARC 2008 Activities

- "DITL" in January
  - please contact me if you'd like to collect and submit data
- Finalize co-operation agreements with CENTR and APTLD
- Recruit dedicated engineer
- Further develop trusted communications platform
- Develop Domain Statistics Collector s/w
- Facilitate tackling Open Recursive Resolvers
- Two more meetings – seeking hosts/sponsors !

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`
- Slides:
  `http://public.oarci.net/files/workshop-2007/Mitchell-OARC-update.pdf`

Questions ?