OARC Update

Keith Mitchell
OARC Programme Manager
RIPE55 DNS WG
25th October 2007

Presentation

- OARC Overview
- More Feb 07 Root DDoS Attack Analysis
- Open Recursive Resolvers
- Whois Query Data Sharing, Anyone ?
- DNSCAP
- DITL 2008

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 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 Services

- http://public.oarci.net website
- Twice-yearly open meetings
- <dns-operations@lists.oarci.net> mailing list
- DSC Data Gathering
- Data Analysis
- Private DNS mailing lists
- Encrypted jabber.oarc.isc.org chat server
- Member https://oarc.isc.org portal

OARC 2007 Activities

- 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
- Next OARC meeting and DNS researcher workshop in Los Angeles 2nd/3rd November (after ICANN)

Root DDoS Attack Feb 07

- With grateful acknowledgements to John Kristoff - see:
  - `http://public.oarci.net/dns-operations/workshop-2007/Kristoff-Feb07-attacks.pdf`
- Attack was *only* against F, G, L, M and some .info servers (plus a botnet)
- Root attacks have high profile, but much mis-reporting of what happened in the media

Further Attack Analysis

- About 4-5000 bots on Microsoft Windows boxes
- About 65% from South Korea
- About 19% from United States
- About 3.5% from Canada
- About 2.5% from China
- The rest from various places
- *Note:* these are bot numbers, bps distribution differs

Further Attack Analysis

- Botnet controller was based in USA, located via DNS
- Still active until late May
- Motivation unclear:
  - test ?
  - demonstration of strength ?

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:
  - John Kristoff (UltraDNS)
  - Rick Wesson (Support Intelligence)
  - April Lorenzen
  - Duane Wessels
- 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

"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
- Will be repeating in January 2008 – further root/TLD participants sought

OARC Future Activity

- Meeting in Los Angeles Nov 2nd/3rd
  - http://public.oarci.net/oarc/workshop-2007/
- "DITL" in January 2008 – please contact me if you'd like to collect and submit data
- Recruit dedicated engineer
- Further develop trusted communications platform
- Develop Domain Statistics Collector s/w

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

Questions ?