DNS-OARC
Domain Name System Operations Analysis and Research Center

# DNS-OARC Briefing

## Motivation and Mission

The DNS is one of the most visible and mission-critical pieces of infrastructure underlying today's Internet. When the DNS stops working, so do all other applications, not just in the part of the Internet directly affected but potentially globally. A stable, reliable and secure DNS is key to maintaining public and government confidence in the management of a functioning Internet, and supporting innovation and its expansion.

The Internet industry today collectively faces some severe challenges from those with criminal and extremist malicious intent. These miscreants are driving a plague of spamming, phishing, botnets, DDoS, hacktivism, malware, spyware and other abuse, which is causing significant harm and expense to Internet end-users, providers, and society in general.

The DNS system is currently heavily implicated in both perpetration and as a target of this abuse. Recent examples include:

- the 300Gb/s Botnet DDoS reflection attack against SpamHaus in early 2013
- the use of "IN/ANY" query floods via major authoritative DNS server in recent years
- vulnerabilities in customer premises equipment allowing their open resolvers to be used as vectors for DDoS amplification attacks.
- various compromises of small country-code top-level DNS registries to hijack global brand domains in 2012.

Similar major incidents and issues date back over a decade - none of these types of problems are unlikely to diminish in the forseeable future.

The Domain Name System Operations Analysis and Research Center (DNS-OARC) is a non-profit, membership organization that seeks to improve the security, stability, and understanding of the Internet's DNS infrastructure.

DNS-OARC's mission is to build relationships among its community of members and facilitate an environment where information can be shared confidentially; to enable knowledge transfer by organizing workshops; to promote research with operational relevance through data collection and analysis; to increase awareness of the DNS's significance; and to offer useful, publicly available tools and services.

DNS-OARC exists to both co-ordinate and be part of the response to these challenges. OARC's community building ensures that during operational incidents, rapid sharing of critical information which is key to mitigating the impact is possible between trusted contacts in affected organizations. Post-incident, DNS-OARC's significant data capture and forensic analysis capabilities help track the cause and perpetrators. Additionally, DNS-OARC's outreach to the research, vendor and end-user communities develops the means to prevent such incidents in future.

# History and Governance

DNS-OARC was founded by Internet Systems Consortium Inc. (ISC) in 2004, as part of a joint research award with CAIDA from the National Science Foundation which included initial funding of DNS-OARC hardware for data collection and analysis.

It was intended since inception that DNS-OARC should operate as a fully-autonomous self-funding and governing organization, operated by and for its members, acting in a neutral fashion in their common interest. DNS-OARC was established as an independent legal entity in 2008 with a member-elected Board of Directors, and shortly afterwards gained nonprofit 501(c)(3) public benefit status.

Most of OARC's operating costs are funded by membership subscriptions, with some grant funding for specific research projects. OARC has a dedicated staff of 2, with ISC operating some DNS-OARC secretariat functions.

DNS-OARC was conceived as a membership organization where DNS operators, network researchers, software implementors and others could participate to share data, common problems and solutions in a secure environment. Currently DNS-OARC has some 60 members, including 9 root server operators, around 20 TLD operators, DNS product & service vendors, Regional Internet Registries, and researchers (see website for a full list of current members). This is growing at a rate of around 1 per month. All members are asked to sign the DNS-OARC Participation Agreement, which places obligations on DNS-OARC and all members to respect the confidentiality of data gathered and shared.

# Member Services

Successful membership organizations provide quality tangible services of direct benefit to their members, and this is very much part of DNS-OARC's mission. Current services include:

- **A secure, encrypted, jabber-based chat server** to give a rapid means of reaching trusted contacts and enabling confidential real-time multi-party discussions.
- **Public and member-only mailing lists** for discussion of current DNS operations issues.
- **Domain statistics collection** - using DSC software, DNS-OARC gathers summary data from root and TLD operators globally, and makes this available to members via a graphical interface.
- **DNS traffic collection**: DNS-OARC regularly takes part in *"Day in the Life of the Internet"* data-gathering exercises, where detailed logs of all queries to participating servers are captured over a 48-hour period. OARC has the capability to turn this full logging on during incidents and events, such as the IPv6 root delegation in 2008 and the DNSSEC root signing during 2010.
- **Large-scale server infrastructure** to upload, share, and analyze data with other DNS-OARC members and researchers.
- **Closed private mailing lists** for discussion of DNS operational security. Due to the often security- and business-sensitive nature of these discussion, participation in these is at the discretion of sponsoring DNS-OARC members only.
- **A Trust Platform** which securely allows relationships to be built and vetted between individuals working on DNS security issues.
- **Twice yearly workshops** at which DNS operations issues are presented and discussed. (For proceedings of the most recent meeting, see https://indico.dns-oarc.net/indico/).
- **Conference management and collaborative working tools** to allow OARC and members to easily set up physical and/or ad-hoc meetings.

OARC's framework for information sharing and operational communication underpins all this - getting early warning of problems can limit operational impact for a business, keep customers happy, and save money. OARC's mission can be described as leveraging shared interests and contacts among its members as a "trusted introducer". Having technical personnel learn "inside information" from their peers that they might not otherwise meet, can be the most effective way of gaining timely new knowledge at a fraction of the cost of sending them on training courses.

# Public Benefit

OARC inherits its founders' central mission of public benefit, and provides a vehicle for its members to act not just in their own interest, but towards the greater good of the Internet community as well. This is particularly important as more reliance is placed on the DNS every year to support current and future Internet-based activities and applications.

A critical component of OARC's capabilities and contribution is the availability of raw operational data. Many of the detailed underlying principles of Internet traffic engineering and failure modes are in fact poorly understood, and the only way to improve this state of affairs is application of the scientific method to the study of these on the large scale. However, the network operators who are in the best position to gather measurement data are not best resourced to perform analysis of this data. While the research community has both the skills and will to do this analysis, they cannot always easily obtain suitable data.

Forensic data analysis is also of immense value to law enforcement in tracking the perpetrators of crimes and infrastructure attacks. There are however concerns about privacy of end-user data gathered from the network. Making this data available to researchers and law enforcement, if done with appropriate safeguards, is clearly very much in the public interest, and OARC gives its members a way to demonstrate they are acting for the benefit of the community while minimizing risks to themselves.

It's also important to note that not all the threats to reliable, secure Internet operation are malicious. Studies performed by OARC partners such as CAIDA demonstrate that a significant amount of unwanted DNS traffic and operational problems are caused by misconfiguration of DNS or applications that depend on it. Part of OARC's mission is outreach to end-users, vendors and network operators to ensure that key knowledge reaches those who most need it.

The Internet industry has a long tradition of effective self-governance and self-regulation, and OARC seeks to continue this. Being seen, as an industry, to be responsibly and pro-actively tackling some of the most difficult issues facing us is not merely good business practice, but an effective strategy for heading off avoidable regulatory intervention.

# Future Evolution

OARC has been placed on a more stable footing, and undergone a review of its status and role since Keith Mitchell's re-appointment in September 2012. OARC performs a key role for which the membership growth indicates there is increasing demand.

The OARC Board has since 2012 set itself the objective of re-booting the organization, and to this end during Q1 2013 conducted a member survey and retreat. The output of this was a Development Plan, which can be found here. Significant progress with OARC's re-boot has already been made:

- Hiring of a full-time Systems Engineer.
- Re-structuring of Executive and Secretariat resources for more effective operation.
- A major hardware and software refresh as part of a longer-term Infrastructure Development Plan.
- Deployment of a conference management platform for enhanced workshop support
- Securing additional funds through member contributions and workshop sponsorship.

Further Development Plan objectives include:

- A detailed business plan to achieve 4-5 staff and $1M revenue targets on a 2-3 year timescale
- Creating a framework for development Project management and funding
- Seeking grant funding for development projects such as DSCng and DNS Benchmarking
- Implementing changes to meetings' lead-time, location, frequency and duration
- Improved member outreach, and cleaning up the status of non-paying members
- Improving relationships with the Research community

## Summary of Benefits of OARC Membership

- Co-ordination, assistance and information from TLD and other root server operators in the event of attacks against members' infrastructure.
- Participation in biannual member meetings and workshops at which DNS topics are presented and discussed.
- Interaction with key technical people at OARC's nearly 70 members.
- To demonstrate to customers, governments, law enforcement, and others you are supporting action to tackle abuse issues that threaten Internet stability.
- Access to an objective source of quantifiable data and peer-reviewed research
- The ability to share real data appropriately with the research community, contributing to the long-term public benefit of the Internet.
- The opportunity to track best operational practices at TLD, root, and other critical name servers.
- Support for the development of public benefit tools, services, and documents that educate and assist Internet users on important DNS issues.
- Voting rights and the possibility to be elected to the Board of Directors, which steers the direction of OARC.

# OARC Subscription Levels

| Category | Type | Annual Subscription | Contacts |
|---|---|---|---|
| 0 | Beneficial | In-kind | 2 |
| 1 | Bronze | $5500 | 3 |
| 2 | Silver | $8500 | 5 |
| 4 | Gold | $12500 | 8 |
| 5 | Platinum | >$12500 | >8 |