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 directly affected part of the Internet but potentially globally. A stable, reliable and secure DNS is key in maintaining public and government confidence in the management of a functioning Internet. And a functioning Internet is key in the innovation and expansion of Internet technologies.

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. Here are some recent examples::

- The use of "IN/ANY" query floods via major authoritative DNS servers in recent years.
- The DDoS attack on the B, C, G & H Root servers at 5 million qps in December, 2015 (https://www.theregister.co.uk/2015/12/08/internet_root_servers_ddos/).
- Insecure Internet of Things (IoT) devices continue to be a large source of traffic for DDoS attacks. The rapid proliferation of these devices continues to widen the field of attack targets.

- 2016 saw the largest DDoS attack in history, which took out most of the Eastern Seaboard of the United States. The attack initially targeted Dyn and primarily used the Mirai Botnet to control IoT devices (https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/).
- According to Akamai's 2Q2017 report, "Businesses across the globe were hit by the *WannaCry* and *Petya* malware strains, potentially costing the economy in excess of $4 billion. The *Mirai* botnet continues to be used to attack organizations, while at the same time older strains of malware are being retooled for new uses, such as the *PBot* botnet."

Similar major incidents and issues have occurred for well over a decade and these types of problems are unlikely to diminish in the foreseeable future.

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

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

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

History and Governance

DNS-OARC was founded by Internet Systems Consortium, Inc. (ISC) and CAIDA in 2004 and was established as an independent legal entity with nonprofit 501(c)(3) public benefit status in 2008. Most of OARC's operating costs are funded by membership subscriptions, with some grant funding for specific research projects.

DNS-OARC was conceived as a membership organization where DNS operators, network researchers, software implementers and others could participate to share data, common problems and solutions in a secure environment. DNS-OARC has grown to over 100 members, including 11 root server operators, around 40 TLD operators, DNS product and service vendors, Regional Internet Registries, and researchers (see website for a full list of current members). Membership is growing at a rate of around one 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:

- **Three yearly workshops** at which DNS operations issues are presented and discussed. (For proceedings of past meetings, see: https://www.youtube.com/results?search_query=dns+oarc).
- **OpenSource Tools** development, including drool, dsc, dnscap, packetq and others.
- **DNS Dataset** library available for research currently >230TB
- **Public and member-only mailing lists** for discussion of current DNS operations issues.

- **Domain statistics collection**: Using DSC software, DNS-OARC gathers summary data globally from root and TLD operators, 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 logging on during incidents and events, such as the Collisions Study of 2013, and the Root Key (KSK) Rollover of 2017/2018.
- **Large-scale server infrastructure** to upload, share and analyze data with other DNS-OARC members and researchers.
- **Closed private groups** for discussion of DNS operational security. Due to the often security- and business-sensitive nature of these discussions, participation in these groups is at the discretion of sponsoring DNS-OARC members only.
- **A trust platform,** which allows secure relationships to be built and vetted between individuals working on DNS security issues.
- **Discounted software development** rates for higher level members.
- **Member-Only Portal** for accessing data and making connections.

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 peers they might not otherwise meet can be an effective way of gaining new knowledge at a fraction of the cost of sending them to training courses.

OARC Member Subscription Levels

Level of Membership	Annual Subscription	Contacts
Supporter	In-Kind	1
Blue	$1,100	2
Bronze	$6,500	3
Silver	$10,000	5
Gold	$15,000	8
Platinum	$25,000	12
Diamond	$50,000+	18

Here are some recent quotes from our current members:

"OARC is the only organization of its kind, dedicated to DNS operations and research. Given my company's deep involvement with DNS and my personal interest, I simply have to be a member and attend the workshops, which have consistently high-quality content."

"OARC is a unique venue that brings together DNS vendors, operators of DNS services and researchers - the workshops provide a unique and valuable insight into the current state of the art of the DNS.

"DNS-OARC provides the invaluable mingling of DNS operators, developers, researchers, to communicate, collaborate, and share data via workshops, mail lists, and

shared computing resources. Without this association I would not be aware of the current problems facing the DNS and Internet community nor be a part of their solutions."

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 toward 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 contributions 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 a 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 the 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, researchers, public agencies 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 proactively tackling some of the most difficult issues facing us is not merely good business practice, but an effective strategy for heading off avoidable regulatory attention.

Future Evolution

OARC performs a key role for which the membership growth indicates there is increasing demand. Our financials are stable while maintaining budget and

OARC upholds its relevance through biennial Board retreats and member surveys. Ongoing planning for growth and sustainability has resulted in several milestones:

- Staffing increases in contractor hours over the last two years, resulting in System Admin changes and Development improvements.
- Verisign funding of DNSCAP RSSM extensions, and Comcast Grant for additional work on drool DNS Replay Tool.
- A Record >10TB DITL 2017 and similar in 2018 data gathering completed.
- New Member Portal giving better access and new services.
- Formed a Board sub-committee to implement Data Privacy survey findings.
- Regular member consultations via workshops and surveys.

In 2020 we plan to:

- Further software tool development. Development of Soteria funded by Swedish Internet Stiftelsen
- Pilot new DNS stats data-sharing platforms.
- Implement Data Privacy survey findings.
- Upgrade analysis capacity/cluster.

If you want to promote our plans, help your organization, and be a part of the solution with us, why not become a member?

Here are some reasons:

Access to and participation in the world's premier community of DNS technical experts.

Influence development of open tools and services to support your infrastructure operations.

Ability to share and analyze a unique dataset perspective into global DNS operations.

Use of community coordination resources to respond to incidents and threats.

Support a trusted neutral party free of vested interests in the DNS space.