State of the DNS 2022

WLAN: EMG High Speed

topDNS Workshop, Brussels, November 8 & 9, 2022

WE ARE SHAPING THE INTERNET.
YESTERDAY. TODAY. BEYOND TOMORROW.

topDNS

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Your Host - Facts & Figures

- Leading voice of Internet infrastructure providers
- Established 1995
- 1.000+ members
- Offices in Cologne, Berlin & Brussels
- Founding member of EuroISPA
- Sole shareholder of DE-CIX operator
  - 30+ IXPs, FFM: 11+ Tbit/s peak traffic

topDNS

CentralNic

CleanDNS

iQ

leaseweb

nic.at

.org

REALTIME REGISTER

VERISIGN

Your Logo Here

Jeffrey Bedser

CEO

CleanDNS Inc.

Marcus Busch

Managing Director

Leaseweb

Brian Cimbolic

Vice President, General Counsel

Public Interest Registry

Keith Drazek

VP of Policy & Government Relation

VeriSign, Inc.

LG Forsberg

CTO

IQ Global AS

Theo Geurts

CIPP/E Privacy & GRC Officer

Realtime Register B.V.

Kelly Hardy

Head of Registry Policy

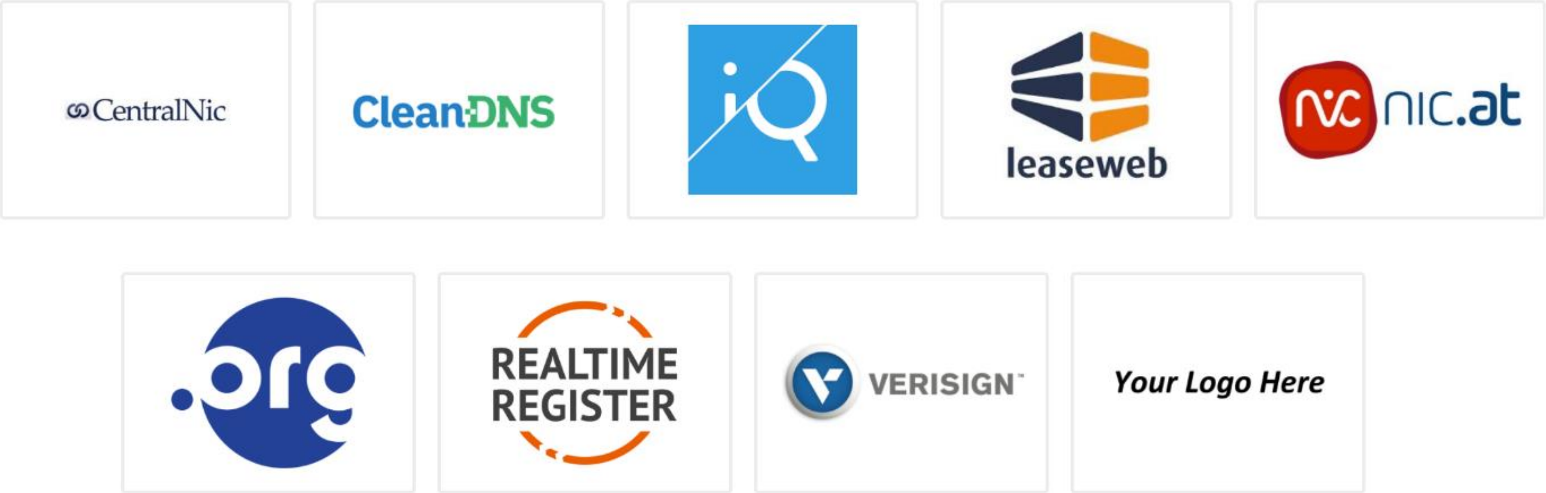
CentralNic

Robert Schischka

CEO

nic.at GmbH

Join the Steering Committee!



Welcome and Housekeeping

- Chatham House Rules
- Recording just for purposes of preparing our report
- Please use the MS Teams room to raise your hands to make it is easier for remote participants to follow.

Tour de Table

- Name
- Position
- Entity you represent
- Industry / Sector, e.g.
  - Registry, Registrar, Hosting Company
  - Industry Association
- Why do you think this is important?

Framing the Issue

Thomas Rickert

Methodology & Outcome

- Recommendations in the study provide a good overview of the proposals discussed in varioius fora
- Discussion in 6 Segments covering the recommendations.
- We are not limited to the recommenations – if you have other ideas, please share them
- Around 20‘ per recommendation only
- Structured dialogue required

Methodology & Outcome

- No rehashing of commentary on the study
- Discussion of what should best be done with an open mind
- Lightning Talks followed by discussion
- Rapporteur will summarize the main findings
- Report to be published after the workshop
- Follow-up to analyze progress

Methodology & Outcome

- Outline of Recommendation(s)
- What has been addressed since the publication of the study?
- By whom? How?
- What is missing to be successful?
- How to prioritize and what is efficient?
- What recommendations might need refinement based on new findings?
- Who can do what by when?

The Predicaments in Responding to DNS Abuse

Bertrand de la Chapelle

The Size of the Issue

Rowena Schoo

How Definitions Stand in the Way of Being Productive

Thomas Rickert

The Definition War (?)

- … is not helpful, but why do we have it?
- ICANN vs ccTLDs vs the real world
  - Let's talk about abuse scenarios and not get hung up on definitions
  - eco abuse table shows a variety of scenarios and outlines who should take action

Segments

- Registration Data Issues
  - Recommendations 1, 2, 3, 4, 5, 8
- Exchange of Intelligence
  - Recommendations 6, 7, 21, 25
- Preventative Measures
  - Recommendations 9, 10, 11, 16

Segments

- Carrots & Sticks
  - Recommendations 12, 13, 14, 15
- Enhancing Security
  - Recommendations 17, 18, 19, 20, 22, 23
- Awareness Raising & Capacity Building
  - Recommendations 24, 26, 27
- Conclusions & Next Steps

Segment 1: Registration Data Issues

Segment 1, Recommendations on

- Access to WHOIS / RDAP – registrar information (Rec. 1)
- Zone File Data access (Rec. 2)
- E-Mail contactability (Rec. 3)
- E-Mail contacts for role contacts (Rec. 4)
- Standardized and centralized system for access to registration data (Rec. 5)
- Accuracy (Rec. 8)

Lightning Talks

- Theo Geurts, Realtime Register
- Peter van Roste, CENTR
- Gavin Brown, CentralNic
- Thomas Rickert, eco

Theo Geurts - Realtime Register

- Combatting DNS Abuse is a business model
- Investigations create intelligence
- Abuse reports equals valuable intelligence
- Resellers lack knowledge

Thomas Rickert on Rec. 5

- ICANN‘s SSAD / Whois Disclosure System
- Centralized system possible for gTLDs, but not ccTLDs
- Pointing reporters to the right registrar is key.
- Whois data potentially overrated
- Registrar has account holder data as well and can take action swiftly for a violation of T&Cs in case of inaccurate registration data.

Thomas Rickert on Rec. 5

- Registration Data Access does not help when it comes to compromised domain names
- It is more important for registrars / hosting companies to act swiftly on abuse reports
- Quality of reporting is important
- ICANN pilot should be supported

Segment 1 Discussion

Segment 2:
Exchange of Intelligence

Segment 2, Recommendations on:

- A standardized abuse reporting system (Rec. 6),
- Exchange of information between parties involved (Rec. 7),
- CERTs should subscribe to feeds on open DNS resolvers and notify them to limit the number of open DNS resolvers (Rec. 21) and

Segment 2, Recommendations on:

- DNS Service providers should formally collaborate with Member State’s institutions, Law Enforcement authorities & Trusted Notifiers (Rec. 25).

Lightning Talks

- Rowena Schoo, DNSAI
- Jeff Bedser, CleanDNS
- Thomas Rickert, eco
- Bertrand de la Chapelle, Internet & Jurisdiction
- Robert Schischka, nic.at

Thomas Rickert on Rec. 7

- Verification of reports is an issue
- topDNS Hub helps build on your colleague‘s expertise and helps avoid the duplication of efforts
- List of domain names not to transfer in as registrars

Robert Schischka on Rec. 21

- Intensify notification efforts to reduce the number of open DNS resolvers (and other open services), which are among the root causes of distributed reflective denial-of-service (DRDoS) attacks.

Remark: Open DNS resolvers might be a TOOL used to amplify attacks, but the are not a ROOT CAUSE. No one attacks because there are open resolver but maybe by (ab)using them.

Developments in recent years

- While it is true that open resolvers can by used for DNS based attacks, theses attack pattern are not the most dominant way in todays threat landscape.
- One of the reasons is that volumetric attacks can be „easiert“ mitigated than more sophisticated attack patterns.

Developments in recent years

- Other protocols like NTP or SSDP can make use of millions CPEs and are much hard to block.
- Open resolver do have a purpose – eg. avoid censorship, provide customer choice, avoid unnecessary dependencies and foster resillience.

Developments in recent years

- Projects like DNS4EU actually try to support this goals by providing (free) alternatives to services like 8.8.8.8 (which is an open resolver run by a very large and „dominant“ organization“
- The „elephant in the room“ might be IoT devices, not so much intentionally setup open resolvers as a community service.

Important take aways

- Intentionally setup and carefully operated open resolver, run by trained staff are NOT the problem – because it is usually in their own best interest not to be abused, blocked or create troubles.

Important take aways

- What should be addressed are services run by „accident“ eg. lazy configuration or setups which just enable every possible service to avoid customers complaints or configuration „overhead“.

Suggestion

- Those who operate an open recurser (or any other service) shall have defined ways to be contacted and shall monitor their service for abuse patterns.
- Companies bringing devices in the field (CPEs, IoT, ...) shall be required to address security issues in a timely manner and shall define which services they support and ban anything else.

Segment 2 Discussion

Segment 3:
Preventative Measures

Segment 3, Recommendations on

- Similarity search tools or surveillance tools (Rec. 9),
- Offering IPR holders services to preventatively block infringing domain name registrations (Rec. 10),
- Predictive algorithms to prevent abusive registrations to be used by registries and registrars (Rec. 11) and
- The issue of free hosting and subdomains (Rec. 16).

Lightning Talks

- Jordi Iparraguirre, EURid
- Lori Schulman, INTA
- Jeff Bedser, CleanDNS
- Brian Cimbolic, Public Interest Registry (PIR)
- Robert Schischka, nic.at

Segment 3 Discussion

Segment 4:
Carrots & Sticks

Segment 4, Recommendations on

- Monitoring and reporting abuse rates, deaccreditations (Rec. 12),
- Rewarding players with low abuse rates (Rec. 13),
- Registries to maintain access to URL/domain blocklists, identify registrars with high / low abuse rates and provide incentive structures (Rec. 14) and
- Hosting providers should be monitored, abuse rate limits, incentive structures (Rec. 15).

Lightning Talks

- Keith Drazek, Verisign
- Brian Cimbolic, PIR
- Jeff Bedser, cleanDNS
- Rowena Schoo, DNSAI

Segment 4 Discussion

Segment 5:
Enhancing Security

Segment 5, Recommendations on

- DNSSEC for ccTLDs (Rec. 17),
- Registrants should have easy access to DNSSEC (Rec. 18),
- Discounts for DNSSEC use (Rec. 19),
- ISPs running DNS resolvers should configure DNSSEC validation (Rec. 20),

Segment 5, Recommendations on

- Security Community to measure and educate about DMARC, SPF (Rec. 22)
- IP source address validation for incoming and outgoing traffic (Rec. 23)

Lightning Talks

- Patrick Kötter, Sys4 AG
- Gavin Brown, CentralNic
- Peter van Roste, CENTR
- Jeff Bedser, cleanDNS

Segment 5 Discussion

Segment 6: Awareness Raising and Capacity Building

Segment 6, Recommendations on

- The harmonisation/approximation of the practices of ccTLDs by the adoption of the good practices available (Rec. 24),
- Awareness-raising and knowledge-building activities to make the consumers, IPR holders, or other affected parties aware of existing measures tackling DNS abuse (Rec. 26) and

Segment 6, Recommendations on

- Knowledge-sharing and capacity-building activities between all intermediaries and stakeholders involved in the fight against DNS abuse (Rec. 27).

Lightning Talks

- Peter van Roste, CENTR
- Jeff Bedser, cleanDNS
- Thomas Rickert, eco
- Robert Schischka, nic.at

Thomas Rickert on Rec. 27

- topDNS is all about sharing information and expertise
- eco membership covers different types of intermediaries
- Papers, Workshops, Trainings (in the making)
- Example: Workshop at Nordic Domain Days resulting in the **Stockholm Recommendations**.

Stockholm Recommendations

1. Publish an anti abuse policy covering DNS abuse and contact details for abuse reports.
2. Have staff that is trained to process DNS abuse reports.
3. Try to find out if there are DNS abuse issues with your customers.
4. Be responsive to abuse reports and take action as soon as possible.

Stockholm Recommendations

5. Share information from reports you cannot handle with a party that is better placed to take action.
6. Explore opportunities for the exchange of intelligence.
7. Use tools. They provide data, insights and guidance.
8. Act swiftly if the issue requires urgency.
9. Let proportionality guide your actions.
10. Be part of the solution, not the problem.

Segment 6 Discussion

Summary of Findings & Conclusions

Let's identify…

- measures that are most effective
- measures that are low hanging fruits
- measures to focus our attention on
- ways forward to operationalize them
- who can do what by when and what we need to be successful

What to focus on?

- Measure 1 – Your idea goes here!
- Measure 2
- Measure 3
- Measure 4
- Measure 5
- ...

Segment 1

- Promote a cohesive approach to validation based on NIS2.
- Promote a risk-based approach to accuracy.
- Continue to work at ICANN and promote the WHOIS Disclosure System and add functionalities beyond the pilot if possible.
- ...

Segment 2

- Promote Netbeacon and Acidtool.
- Create or promote trusted spaces for collaboration between different stakeholders (topDNS Hub).
- ...

Segment 3

- Educate and raise awareness about existing services and projects (Webinar series).
- ...

Segment 4

- Promote Services such as QPI
- ...

Segment 5

- Your suggestion goes here
- ...

Segment 6

- Your suggestion goes here
- …

Thank you for your participation!

WE ARE SHAPING THE INTERNET.

YESTERDAY. TODAY. BEYOND TOMORROW.

topDNS

eco

ASSOCIATION OF THE INTERNET INDUSTRY