DNS ABUSE INSTITUTE

ANNUAL REPORT

2021

Table of Contents

The DNS Abuse Institute: Annual Report

The DNS Abuse Institute (DNSAI) has existed for just over a year, and given the global interest in its mission to reduce DNS Abuse, it is appropriate to produce this annual report. The report captures the period from February 2021 to March 2022, much of which was spent planning and establishing projects. As all of the work of the DNSAI is new, we'll provide context for why particular projects or approaches were selected, as well their current status.

Questions, comments, and requests for more information can be sent to info@dnsabuseinstitute.org.

Creation and Planning

Public Interest Registry (PIR), as part of its non-profit mission, launched the DNSAI on February 16th, 2021, and Director Graeme Bunton started the same day. The creation of the DNSAI, with its three pillars of Innovation, Education, and Collaboration was very positively received by the press and the interested community.

Work immediately began on assessing the DNS Abuse landscape to identify opportunities and challenges, with the goal of producing a plan to guide and focus Institute efforts. At its simplest, the DNSAI exists to remove as much of the complexity and difficulty of mitigating DNS Abuse as possible, from the domain registration ecosystem. The Institute's success will be determined by how effective it is in identifying the right initiatives, and executing on that vision.

Supporting Quotes

"*I'd like to congratulate Public Interest Registry for establishing the DNS Abuse Institute. We hope it will continue to foster the necessary dialogue across the range of stakeholders who share the goal of combating DNS Abuse, and will eagerly follow the Institute's work as it develops.*"

Göran Marby, President and CEO, ICANN

"As the DNS industry participates in these rapidly changing times, we are excited to work with the new DNS Abuse Institute to help make the Internet a better place. We think that Graeme is the right person for the job and look forward to working together with the rest of the industry on these thorny problems. Together we all can lead on behalf of the Open Internet."

Elliot Noss, CEO, Tucows

"Technical abuse in the DNS is a critical issue that should be addressed by the entire DNS community. We applaud Public Interest Registry for its creation of the DNS Abuse Institute. CENTR and its members look forward to participating in broad discussions and contributing our expertise on these important topics."

Peter Van Roste, General Manager, CENTR

"Congratulations to PIR for launching the DNS Abuse Institute. This is a big step in the right direction. The Institute will serve as a catalyst and help bring together actors from across the DNS community to address DNS Abuse in its many forms. We look forward to participating in this important effort."

David Redl and Fiona Alexander, Salt Point Strategies

"*DNS Abuse remains a substantial challenge, and it will take a broad range of stakeholders to come together to address it collaboratively. I want to thank PIR for leading in this space and launching this new Institute. I believe that the DNS Abuse Institute can serve as a central forum for bringing together concerned parties to discuss DNS Abuse and related issues.*"

Steve Crocker, Edgemoor Research Institute, Former Chair ICANN

"The creation of the DNS Abuse Institute is a natural progression from the foundations laid by the work of the Internet and Jurisdiction Policy Network's Domains and Jurisdiction Program and the concrete outcomes its Contact Group produces. We look forward to working with the Institute to develop further guidance that can be widely adopted to help address abuses through action at the DNS level. Congratulations to PIR on this substantial achievement, and we wish the Institute the best of luck in this worthy endeavor."

Bertrand de La Chapelle, Executive Director, Internet & Jurisdiction Policy Network

"The Global Cyber Alliance is focused on providing businesses and governments the tools they need to slow and stop DNS Abuse. We see the new Institute as highly complementary to our efforts. It will help bring the DNS community together and build alignment about what needs to be done to fight abuse of the DNS."

Leslie Daigle, Global Technology Officer, Global Cyber Alliance

Institute Roadmap

The DNSAI published its Roadmap in June 2021. The Institute Roadmap put forward a simple mission for the Institute: to reduce DNS Abuse. Without qualifications, caveats, or complications, the DNSAI intends to reduce DNS Abuse quickly and pragmatically, looking for opportunities that deliver the greatest impact, in the least amount of time, with the most efficient use of resources.

The Roadmap captured a number of key contextual pieces to combatting DNS Abuse. First is the crucial understanding of the two primary approaches of reducing abuse: preventative and reactive methods. The second key piece is an understanding of domain industry marketplace dynamics. The DNSAI chose to focus initially on work related to improving reactive approaches to reducing DNS Abuse. Preventative approaches require technology development and implementation at the registry or registrar, which could generate substantial costs, and would be in competition with other business priorities.

Using the Institute's three pillars of Innovation, Collaboration and Education as guidelines, the DNSAI Roadmap laid out plans for technology development projects, data collection, and educational outputs all focused on reducing DNS Abuse.

Advisory Council

The DNSAI established an advisory council to provide insights and guidance to the Institute as it plans and executes its mission. The Institute has been very fortunate to attract an extraordinary and diverse group of people to help guide it, including former ICANN board members, ccTLD executives, and security practitioners.

The initial membership of the Advisory Council is:

MEMBER	AFFILIATION
Drew Bagley	Crowdstrike
Bertrand de la Chapelle	Internet & Jurisdiction Policy Network
Chris Disspain	Donuts
Ashley Henieman	GoDaddy
Maureen Hilyard	PIR Advisory Council / ALAC
Maciej Korczynski	University of Grenoble
Vineet Kumar	Cyber Peace Foundation
Dean Marks	Coalition for Online Accountability
Crystal Ondo	Google
Bruna Santos	Data Privacy Brasil Research Association
Rowena Schoo	Nominet
Bruce Tonkin	auDA
Jeff Bedser	PIR Board Liaison / CleanDNS Inc.

The Advisory Council meets quarterly to review work and provide strategic input. Terms are staggered between one and three years in duration.

Institute Pillar: Innovation

DNS Abuse is a complicated global problem. It's spread across thousands of domain resellers, registrars, and registries, as well as an untold number of hosting companies and content distribution networks. Meaningful reductions in DNS Abuse require coordinated and consistent approaches. To this end, the DNS Abuse Institute is engaged in the development of tools and technologies aimed at both understanding and reducing the complexity of mitigating abuse across the ecosystem.

NetBeacon™

In April 2022 the DNSAI announced NetBeacon, formerly known as the Centralized Abuse Reporting Tool (CART).

Goals

The need for a centralized abuse reporting tool has been discussed within the ICANN community for quite some time, and a number of community outputs contemplate something similar. For example, ICANN's Second Security, Stability, and Resiliency (SSR2) Review Team's Final Report recommended that "ICANN org should establish and maintain a central DNS Abuse complaint portal that automatically directs all abuse reports to relevant parties." Similarly, ICANN's Security and Stability Advisory Committee (SSAC) recommended in SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS that ICANN develop a "Common Abuse Response Facilitator" as a single place to report abuse could make a substantial and immediate impact towards reducing DNS Abuse.

NetBeacon is intended to solve two related problems:

- **Complexity:** Reporting DNS Abuse to registrars and registries currently requires technical knowledge and ability to navigate the entire ecosystem, and is onerous, confusing, non-standardized, and extremely difficult to do at Internet-scale.

- **Quality:** The DNS Abuse reports that registrars and registries receive are duplicative, unevidenced, unactionable, often containing domains that don't belong to them, and consume time and resources with little of that effort improving the Internet.

The DNSAI is well-positioned to develop and deliver a tool to address these problems because (a) it can move quickly as it is unencumbered by many proces requirements, (b) it can work beyond the limited remit of ICANN and can coordinate with hosting and content delivery networks, as well as ccTLD registry operators, (c) it provides a neutral third party to steward potentially commercially sensitive data.

Progress

After publishing its Roadmap, the DNSAI immediately began creating NetBeacon project requirements and conducting high level discussions with potential development partners. The primary features for a successful tool were identified as a single place where anyone can report DNS Abuse that:

- Easy and straightforward to use.
- Standardizes abuse report requirements.
- Standardizes the format of abuse reports (into XARF).
- Enriches abuse reports with information from external API based sources (like RBLs, Hybrid Analysis, VirusTotal).
- Enables registrars and registries to embed the forms on their own websites.
- Distributes the abuse reports to the appropriate party via email.
- Accepts and distributes reports via an API.

The DNSAI spoke with a number of potential vendors to get a sense of the cost and timing involved in developing such a tool. Over the course of those conversations CleanDNS revealed that it had a number of the required features already developed as part of its own technology, and that it was willing to license them and provide continued NetBeacon development to the Institute at no cost. Jeff Bedser is the CEO of CleanDNS and also serves on PIR's Board of Directors. The PIR Board reviewed the CleanDNS proposal under its conflict of interest policy (with Jeff Bedser recusing) and determined that the proposal was in the best interest of the Institute (and PIR) as it resulted in significant cost savings and also an accelerated timeline for the delivery of NetBeacon.

Development of NetBeacon is on track, with the DNSAI intending to launch publicly in June 2022. Launching NetBeacon is just the beginning, further development could extend to enabling the reporting of harms to hosting companies, establishing escalation paths, and enabling abuse report receivers to opt into other types of harms. An example of the phishing reporting form is included in Fig. 1.

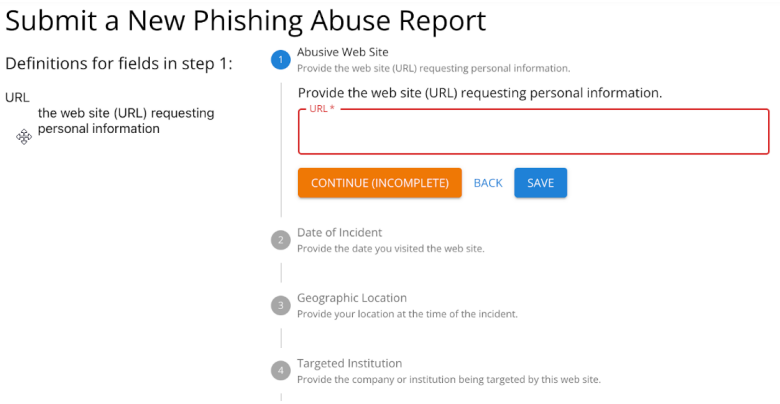

Fig. 1: NetBeacon Phishing Form

DNSAI Intelligence

Goals

Alarmingly little is actually known about the prevalence of DNS Abuse within the domain registration industry. ICANN's DAAR project, while technically sound, only provides high-level trends and no actionable data. Similar measurement projects from security companies have been criticized for having opaque methodology and/or apparent biases. If DNS Abuse were a disease, the community has only an anecdotal view of the symptoms, without knowing the causes or the opportunities for treatment. Further, in order for the DNSAI to be a credible and relevant resource on DNS Abuse, it needs to have a second-to-none understanding of exactly what types of abuse are occurring where. The DNSAI Intelligence platform is intended to fill this space.

Progress

In order to resolve the above issues, the DNSAI developed a set of requirements upon which a robust understanding of DNS Abuse could be built.

The key criteria for a DNSAI Intelligence platform are:

- Rigorous processes and transparent methodology High quality abuse data sources evidenced to the greatest extent possible.
- Capability to:
  - Report at both the TLD and registrar level.
  - Report on multiple types of DNS Abuse.
  - Distinguish between malicious registrations and compromised websites.

The reports created through the DNSAI Intelligence platform are also intended to collect data on how long DNS Abuse remains online, and will attempt to compare abuse against new domain creation numbers. Collectively, this is an extremely ambitious set of requirements.

Currently, the DNSAI Intelligence platform is in the final stages of contracting with a vendor to provide the above data. In anticipation of an agreement the vendor has been collecting data since the beginning of 2022 enabling more longitudinal reporting. We expect to publish our first set of DNSAI Intelligence reports in July of 2022.

Institute Pillar: Collaboration

The DNSAI views collaboration as an operating approach and a service, and the DNSAI aims to fulfill both of these perspectives. First, given the complexity of DNS Abuse, the Institute is well aware it can't possibly solve all of the problems alone. As such, the DNSAI fosters collaborative relationships with organizations like the Internet and Jurisdiction Policy Network, the Internet Infrastructure Coalition, TopDNS from ECO, the Global Cyber Alliance Domain Trust project, and the ICANN community where appropriate. The Institute has also engaged with RIPE, governments, law enforcement agencies, ccTLD and gTLD registry operators, and schools of Internet governance. The DNSAI's mission is to reduce DNS Abuse, and will collaborate with anyone genuinely working towards that goal.

DNSAI Forums

The DNSAI produced two online forums to build awareness of both the Institute and DNS Abuse. The first forum, "Recent Trends and the Current State of DNS Abuse", was held in March of 2021 and designed to build community understanding of the prevalence of DNS Abuse across the ecosystem. It featured panelists Ashley Heineman (GoDaddy), Jeff Bedser (iThreat), John Crain (ICANN), and Chris Lewis-Evans (UK National Crime Agency).

The second forum in May 2021, "Exploring the Edges to Reach Consensus", dove into the contentious issue of the definition of DNS Abuse. Panelists Maciej Korczynksi (University of Grenoble), Mason Cole (Perkins Coie), and Farzaneh Badiei (Yale Law School), discussed the role of content and its relationship to DNS Abuse.

Both of the forums were well attended and received positive feedback for their open and direct discussions.

Participation

The DNSAI has participated in numerous events over the course of the past year, highlights include:

- Panel Discussion on DNS Abuse with the ICANN Board
- Introduction to the DNSAI at RIPE82
- APAC DNS Forum Webinar on Best Practices
- APTLD Pacific IGF
- LACTLD Illegal Content Workshop
- 2021 Middle East DNS Forum
- Virtual School of Internet Governance
- AFRALO Capacity Building: DNS Abuse
- 2021 TLDCON
- OECD Meeting on DNS Security
- GoDaddy Corporate Domains User Group
- ICANN73 Tech Day Presentation on Preventative Methods
- ICANN73 Roundtable on DNS Abuse
- ICANN73 Plenary on Malicious Registrations and Compromised Websites

Discussion Platforms

There is a clear need within the domain registration industry for a trusted and safe discussion platform for exchanging information. Beyond the sharing of approaches and best practices, registries and registrars have insights into the operations of cybercrime, and the trends and patterns of exploitation and abuse. The DNSAI has begun working towards such a collaboration platform. The first step has been to informally invite registrars to collaborate and participate in requirements gathering for initiatives like NetBeacon. As the DNSAI expands its work, it will continue to invite new participants to join its collaboration spaces.

Institute Pillar: Education

To fulfill its educational pillar, the DNSAI strives to provide practical and meaningful content to a diverse set of audiences. Ultimately, these resources will live in an online library, offering materials from the DNSAI as well as other external sources. The goal is to provide a single repository for all of the best information and research on DNS Abuse. The DNSAI website, with the accompanying resource library, will be relaunched in 2022.

In the meantime, the DNSAI is prioritizing a substantial list of potential educational outputs and developing collaborations with other organizations in the ecosystem, including the Internet and Jurisdiction Policy Network, ECO's TopDNS, and the DNS Abuse Subgroup of the ICANN Contracted Party House.

Best Practice 01: Compromised Sites and Malicious Registrations

The DNSAI's first best practice was written for front line DNS Abuse personnel at domain registrars and registries. It provides reasoning as to why the distinction between these types of harms is required, and then draws on the latest academic research to provide a set of simple rules to apply in order to make the distinction and take appropriate action. This best practice is available as a longer blog post as well as a condensed shareable PDF.

Best Practice 02: Secure your Website, Save the Internet

The DNSAIs second best practice is thematically related to its first, but was written for a very different audience. Given that a substantial amount of DNS Abuse occurs via compromised websites, it seemed sensible to collect and publish a set of best practices for end users and website operators on how to ensure their content management system remains secure. This best practice was written with a non-technical audience in mind and provides an extensive list of concrete actions to reduce compromise and subsequent abuse.

Looking Forward

The first half of 2022 is going to be incredibly busy for the DNSAI as we launch two major initiatives and continue to build our educational and collaborative capabilities. In the second half of the year, we'll focus on cleaning up loose ends from two product launches and prioritizing future enhancements.

Mitigation-Specific Abuse Feeds

Looking further down the road, there are two obvious places for the DNSAI to work. The first, is to examine the existing DNS Abuse feeds and to determine if there is a gap in the marketplace that the DNSAI should fill. Current reputation block lists (RBLs) are primarily developed for network protection and not for DNS Abuse mitigation at the registrar or registry level. This creates issues with false positives, as well as with evidence standards, which prevent widespread RBL adoption among registrars and registries. This is not meant to be a criticism of those RBLs as the network protection functionality is important. Rather, it demonstrates there is a possible gap to fill with an RBL that focuses specifically on mitigation at the registrar or registry level taking into account the respective role of those operators in DNS.

Preventative Approaches

The second opportunity for future work is for the DNSAI to explore preventative approaches to DNS Abuse. Preventing abuse before it occurs requires being able to identify potentially harmful registrations before they resolve. Projects like COMAR demonstrate that it is possible to identify malicious registrations, though that project used many attributes not available at the time of registration. Further, most preventative solutions by nature require introducing some form of friction in the domain registration process; something the entire industry has been trying to reduce for more than twenty years. There are, however, some opportunities where registrar interest in reducing fraud overlaps with a more general interest in reducing abuse. There is also an opportunity to look at incentives at either the registrar or registry level for downstream actors that are successful at keeping DNS Abuse levels low. Understanding and exploiting those areas could lead to a substantial reduction in harms for very little cost. DNSAI Executive Director Graeme Bunton previewed some initial thinking about these opportunities at ICANN73, as part of TechDay[1].

Capacity

There is a very long and perpetually evolving list of issues the DNSAI could or should be working on. While most ancillary functions like finance, marketing, and legal are provided by PIR, the work of outreach, planning, strategy, organizing, and writing have to this point been the responsibility of a single person. In order to execute on the DNSAI's ambitious plans, we are in the process of bringing additional people on board.

While there is no doubt in PIR's long term commitment to help fund the Institute, with increased resources comes increased cost. As the DNSAI demonstrates its value and a track record of success, it is hoped that additional opportunities for support will arise.

Appendix 1: Selected Media Coverage

- AuDA Leaders in Tech Q&A : Leaders of tech Q&A: Graeme Bunton on driving down DNS abuse | auDA
- Ask Mr. DNS Podcast: Episode 62
- Packet Pushers Podcast: Heavy Networking 606: Dealing With DNS And Domain Name Abuse | Packet Pushers
- .Org launches DNS Abuse Institute, to be led by Graeme Bunton - Domain Name Wire | Domain Name News
- PIR to offer industry FREE domain abuse clearinghouse

[1] See video at 8:00: https://icann.zoom.us/rec/play/Ie0sW9ow3NZaBFoDTSwSyR5fLMN9gDFFSE-DdI_bpWm5dNCX1omVLQNmjW5wQR9Fo-t4rMPQa2VrUEm1v.sUoPujBQqJMURkbX

DNS Abuse Institute | 11911 Freedom Drive | 10th Floor, Suite 1000 | Reston, VA 20190 | info@dnsabuseinstitute.org