

NetBeacon Institute

2023 Annual Report

Letter from the Executive Director	3
The NetBeacon Institute	4
Institute Pillar: Innovation	5
NetBeacon Reporter (Formerly NetBeacon)	5
NetBeacon Measurement and Analysis Platform (MAP) (Formerly DNSAI: Compass)	7
NetBeacon Institute Partners	8
2023 in NetBeacon MAP Data	10
Institute Pillar: Collaboration	12
Participation	14
Institute Pillar: Education	15
Looking Ahead	16
Advisory Council	16
Appendix 1: Selected Media Coverage	18

Letter from the Executive Director

2023 was a year of exciting growth and momentum for the NetBeacon Institute. Building on the strong foundation laid in 2022 with the launch of our flagship initiatives—NetBeacon Reporter and the NetBeacon Measurement and Analytics Platform (MAP)—we dedicated 2023 to enhancing, refining, and expanding these key products, along with our relationships within the domain industry. Our hard work paid off, Resulting in a remarkable uptick in product adoption and our outreach calendars packed with meaningful engagements. We're thrilled to share more details on these accomplishments in this report.

In May 2024, we rebranded the DNS Abuse Institute as the NetBeacon Institute, with our flagship initiatives also receiving new names—NetBeacon and DNSAI: Compass became NetBeacon Reporter and the NetBeacon Measurement and Analytics Platform (MAP). Although the rebrand occurred mid-2024, for clarity and consistency, this annual report will use our new name and branding throughout.

The Institute is incredibly grateful for the trust and support shown by our *peers* within the domain and internet security industries.

Graeme Bunton,

Executive Director

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

The NetBeacon Institute

Founded in 2021, the NetBeacon Institute is dedicated to reducing DNS Abuse by fostering collaboration, establishing best practices, and creating open, industry-shared solutions—all offered at no cost. DNS Abuse is defined by the domain industry as malware, botnets, phishing, pharming, and spam when used as a delivery mechanism.

CALL OUT BOX: Institute Pillars:

Innovation — The Institute will drive innovation in combating DNS abuse. The Institute will create recommended practices with solutions for registries and registrars of varying sizes and resources, provide qualified parties with funding to conduct innovative research on cybersecurity and DNS Abuse related issues, and develop practical solutions to combat DNS Abuse.

Education — The Institute will serve as a resource for all interested stakeholders related to DNS Abuse. This includes maintaining a comprehensive resource library of existing information and practices regarding DNS Abuse identification and mitigation, promulgating abuse reporting standards (e.g., what is needed for a “good” notification on abuse), and publishing academic papers and case studies on DNS Abuse.

Collaboration — The Institute will serve as a networking forum and central resource for all interested stakeholders related to DNS Abuse issues.

Collaboration with technical and academic organizations working in the DNS Abuse space, registries, registrars, and security researchers will help enable the entire DNS to be better equipped to fight DNS abuse.

Institute Pillar: Innovation

DNS Abuse is a complex, global challenge, spanning across thousands of domain resellers, registrars, registries, and numerous hosting companies and content distribution networks. Making a meaningful impact requires coordinated, consistent strategies across the board. That's where the NetBeacon Institute comes in. We're at the forefront of developing innovative tools and technologies to help understand and reduce the complexity of mitigating abuse throughout the ecosystem. In 2022, we proudly launched our two flagship initiatives: NetBeacon Reporter and NetBeacon MAP, in hopes of fostering greater industry collaboration.

NetBeacon Reporter (Formerly NetBeacon)

NetBeacon Reporter, launched in June 2022 with the generous support of CleanDNS, is the Institute's centralized abuse reporting system. It was designed to help tackle two major challenges in reporting DNS Abuse:

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

Quality: The reports registrars and registries receive are often duplicated, lacking evidence, unactionable, and sometimes even involve domains outside their control, wasting time and resources with little benefit to the Internet.

NetBeacon Reporter is a free tool that simplifies DNS Abuse reporting for individuals and organizations and provides domain registrars with the information and tools they need to act confidently. DNS Abuse reports entered into NetBeacon Reporter are standardized and enriched with information from a number of online abuse databases. A screenshot is taken and the report is then sent to the appropriate domain registrar (gTLDs) or registry (for participating ccTLDs) for investigation and action.

Report Online Abuse

We'll walk you through everything you need to provide a meaningful, actionable online abuse report.

To start, please enter the address of the website or page you're reporting.

✓

Suspect site

Share a direct link to the site or page you're reporting.

Web address *

netbeacon.org

✓

✓

Registered with: Tucows Domains Inc. IANA 69

✓

Type of Abuse: Phishing

4

What we'll need...

Required Information:

Registrars need to see clear evidence of abuse before they're able to take action. We'll need:

- The date on which you encounter this harm.
- The name of the company or organization being impersonated.
- A brief description of the issue.

Helpful Information:

The following will greatly help investigators but are not required.

- The website of the company or organization being impersonated.
- Any files or screenshots that might help an investigation.
- Where it was accessible from.
- If the phish was sent via email, the sender's email address.
- The email message headers.
- The email message body.

BACK

CONTINUE

In 2023, the volume of abuse reports submitted through NetBeacon Reporter increased dramatically, from just a few hundred in 2022 to over twenty thousand by year's end. Reports came from three main sources:

- **Individual users** via the web interface, contributing about 5% of the total volume.
- **Institutional reporters**, primarily internet security and brand protection companies, provide about 45% of reports through the API.

- **Kor Labs**, our partner for NetBeacon MAP, accounting for the remaining 50%, also via API.

The integration between NetBeacon MAP data and NetBeacon Reporter ensures registrars receive timely, well-evidenced abuse reports based on the data they are measured against. Throughout the year, feedback from registrars was consistently positive, and report deliverability was high. The Institute actively investigated any bounced reports and reached out to registrars to resolve issues. The registrars for which deliverability remained a challenge were generally smaller with a limited number of reports.

In Q4 2023, we expanded NetBeacon Reporter to include ccTLDs as recipients of abuse reports.. As ccTLD registrars are not uniformly identifiable, we adopted a flexible approach allowing participating ccTLDs to choose whether to receive reports. They can then decide to take action or refer reports to their registrars as they see fit. By the end of the year, we had six participating ccTLDs, including some of the largest by Domains Under Management (DUM).

If you're a ccTLD operator interested in receiving abuse reports for your TLDs, please contact info@netbeacon.org.

NetBeacon Measurement and Analysis Platform (MAP) (Formerly DNSAI: Compass)

NetBeacon MAP provides reliable, independent, transparent, and granular way to measure DNS Abuse, ultimately helping to reduce it at the DNS level. Developed in collaboration with our academic research partner Kor Labs, NetBeacon MAP follows a formal methodology for data collection and analysis.

In 2023, the Institute achieved several milestones with NetBeacon MAP:

- Published 12 Monthly Analysis Reports, which provide insights into phishing and malware rates, mitigation rates and speeds, and registration types (maliciously registered or benign but compromised).
- Introduced Specific Reporting tables in June, highlighting registrars and TLDs with notably high or low abuse rates per 100,000 Domains Under Management (DUM) or per new registration.
- Created content aligned with our transparency principles, including a report on the inherent challenges of measuring online abuse and a blog detailing the difficulties encountered during measurement.
- Launched free Individual Dashboards for registrars and TLDs, offering zone-specific data and peer comparisons. All TLDs and ICANN-accredited registrars have access to a customized dashboard, and requests for access can be made to support@netbeacon.org.

NetBeacon Institute Partners

The Institute relies on the ongoing support of our valued partners.

Public Interest Registry (PIR) is a non-profit organization created by the Internet Society (ISOC), originally to manage the .ORG domain.

Public Internet Registry serves the public interest online. Its globally diverse team is committed to providing a stable online platform to enable people to do good things.

Clean DNS

The Institute partnered with the cybersecurity and investigative professionals at CleanDNS to develop the NetBeacon Reporter platform.

KOR Labs

The Institute partners with KOR Labs for the delivery of NetBeacon MAP. [KOR Labs](#) is led by Dr [Maciej Korczynski](#), a professor at Grenoble Alpes University in France.

The Institute collaborates with a number of organizations working to make the Internet safer for all by helping to reduce DNS Abuse.

- APNIC
- APTLD
- APWG
- Centr
- Global AntiScam
- Global Cyber Alliance
- ECO Top DNS
- ICANN
- Internet & Jurisdiction Policy Network
- Internet Infrastructure Association
- NameCheap
- Nominet

2023 in NetBeacon MAP Data

In 2023, our methodology identified 289,287 unique domain names linked to phishing and malware distribution. While domain registrations generally fluctuate, it's important to remember that the vast majority of the 350 million or so domains registered at any given time are not associated with malicious activities. NetBeacon MAP provides a deep analysis of the domains that are flagged for phishing or malware distribution.

NetBeacon MAP also differentiates between malicious and compromised registrations—an essential distinction for effective mitigation. Typically, registrars and registries are not best positioned to address compromised websites, as mitigation can risk collateral damage to other services using the domain. This often requires action from the web hosting provider or registrant.

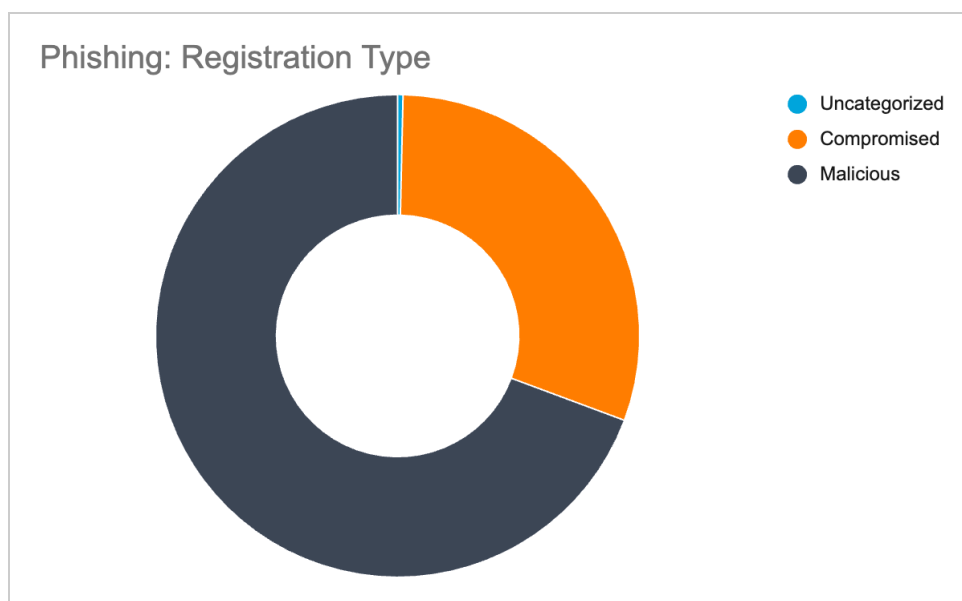
Phishing

In 2023, we observed:

- 267,144 unique domains associated with phishing attacks, with June seeing the lowest activity (18,794) and January the highest (25,934). The average was 22,262 per month.

Phishing: Registration Type

- Our methodology categorized 69% (185,160) of these domains as maliciously registered, meaning they were specifically created for phishing. Another 30% (81,029) were benign but compromised. A tiny fraction (less than 1%, 955) remained uncategorized.



Phishing: Mitigation

- We observed that 75% (199,367) of phishing domains were reasonably mitigated. About 20% (54,188) were not mitigated, while 5% (12,862) could not be categorized. A very small number (727, 0.27%) were unprocessed due to technical issues.

Malware

In 2023, we tracked:

- 22,143 unique domains associated with malware distribution, with August being the quietest month (163) and May the most active (5,227). Malware activity tends to fluctuate more than phishing, likely due to the activities of organized criminal groups and law enforcement actions.

Malware: Registration Type

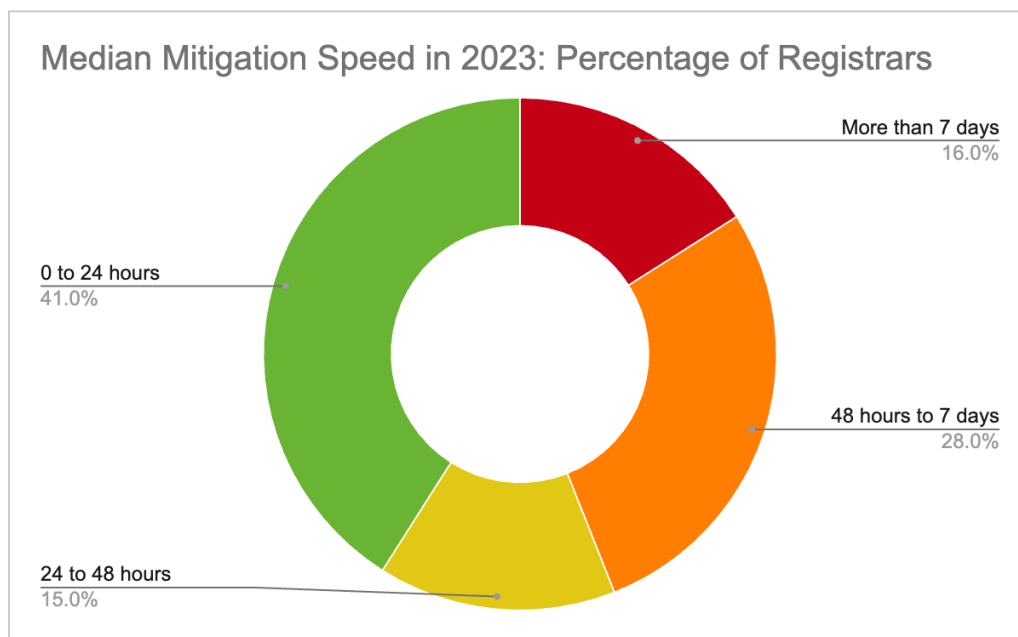
- Most malware domains (66%, 14,557) were categorized as benign but compromised, while 34% (7,418) were maliciously registered. Only 0.76% (168) were uncategorized.

Malware: Mitigation

- Mitigation rates for malware were high, with 81% (17,968) of domains being mitigated. About 15% (3,333) were not mitigated, and 4% (764) couldn't be categorized. A small number (78, 0.35%) were unprocessed due to technical issues.

Registrar Mitigation Speed

In 2023, 56% of registrars had a median observed mitigation time of 48 hours or less, covering both maliciously registered and benign but compromised domains. We believe this metric could be more accurate if it focused solely on maliciously registered domains, as compromised domains often require intervention from other parties like hosting providers. We aim to refine this metric in the future.



Institute Pillar: Collaboration

Making the Internet safer is inherently a collaborative endeavor involving many distributed actors making up the ecosystem. It requires voluntary

actions from numerous individual actors in the ecosystem and often relies on sharing of information to create a shared understanding. We engage collaboratively both within the DNS community and beyond. The primary purpose is to educate and share our free resources, as well as receive information from new stakeholders and new regions, enabling us to better serve our mission.

Engagement

The Institute is deeply engaged with the DNS community and beyond, participating actively in networks like the Internet and Jurisdiction Policy Network, the Global Cyber Alliance, TopDNS from ECO, and ICANN, especially within the Registry Stakeholder Group (RySG) DNS Abuse Group and the Contracted Party House (CPH) DNS Abuse Group. We also conduct regular outreach to broader stakeholders not typically involved in domain industry events, explaining DNS Abuse, industry activities, and the work of the Institute. These stakeholders include governments, law enforcement, civil society, trade organizations, special interest groups, and inter-governmental organizations. Looking ahead, we aim to expand our engagement to include more interactions with the Internet Security community.

Enablement

The Institute hosts a Slack community workspace for interested registrars and registries. This platform serves multiple purposes, from providing valuable feedback on Institute ideas and work to sharing information, tips, and actionable abuse intelligence. Participants frequently exchange advice and input on tackling abuse, making it a vibrant hub for collaboration.



Graeme Bunton presenting at the ICANN DNS Symposium, De Nang, September 2023

Participation

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

- ICANN76
- ICANN77
- ICANN78
- ICANN Presentations including:
 - GAC Capacity Building Webinar on DNS Abuse
 - At-large Policy Working Group
 - ccTLD DNS Abuse Standing Committee Session on measurement
 - geoTLD Session
 - SSAC Sessions
 - APAC DNS Forum Pre Event: Community Effort on DNS Abuse Reporting
- DNS Symposium & OARC Vietnam
- Global AntiScam Alliance Summit
- CENTR Jamboree – Serbia
- Nordic Domain Days DNS Abuse Workshop
- LAC DNS Week
- Eco TopDNS Webinar

- APTLD
- EuroSSIG
- LAC DNS Week Panel
- CENTR Jamboree
- CENTR L&R
- Convergent 2023 – Internet Association of Australia Ltd
- Ecuador ccTLD Webinar (nic.ec)



Rowena Schoo presenting to the GeoTLD Group at ICANN78 in Hamburg, October 2023

Institute Pillar: Education

In 2023, the Institute published several reports and articles to support and expand on key topics presented at numerous events throughout the year. These publications aim to educate and inform the community, driving forward the conversation on DNS Abuse and its mitigation.

- [Account Takeover Advisory](#)
- [A Holistic Approach to Tackling DNS Abuse for Registrars and Registries](#)
- [Challenges in Measuring DNS Abuse](#)

- [Generic Anti-Abuse Policy \(Translated in to Chinese\)](#)
- [A New Phase in Measuring DNS Abuse](#)
- [Technical Resources for Combating DNS Abuse](#)
- [DNSAI Compass: Six Months of Measuring Phishing and Malware](#)

Looking Ahead

As we look towards 2025 we will be focused on ensuring we have the resources to expand and improve our two flagship initiatives with additional features: NetBeacon MAP and NetBeacon Reporter. We will also look for ways to deepen our engagement with stakeholders and ensure we progress with feedback and input from users of our products and the wider Internet community.

Advisory Council

The Institute would like to thank its advisory council for its time and contributions. Members at the end of 2023 were:

Member	Affiliation
Alissa Starzak	Cloudflare
Ashley Heineman	GoDaddy
Bertrand de la Chapelle	Internet & Jurisdiction
Bruce Tonkin	.au Domain Administration Ltd. (auDA)

Bruna Martins Dos Santos	Data Privacy Brasil Research Association
Chris Disspain	Identity Digital
Crystal Ondo	Google Registrar and Registry
Drew Bagley	CrowdStrike
Jeff Bedser	CleanDNS
John Crain	ICANN
Keith Drazek	Verisign
Maciej Korczynski	Associate Professor, Univ. of Grenoble and Principal at KOR Labs

Appendix 1: Selected Media Coverage

- “Blog – ICANN 78: DNS Abuse Discussions Take Front Stage – CENTR.”
<https://www.centr.org/news/blog/icann78-dns-abuse-discussions-take-front-stage.html>.
- “DNSAI Compass: Six Months of Measuring Phishing and Malware.”
<https://circleid.com/posts/20230216-dnsai-compass-six-months-of-measuring-phishing-and-malware>.
- “DNSFilter: The Spectre in the Room: Let’s Talk About DNS Abuse.”
<https://www.dnsfilter.com/blog/the-spectre-in-the-room-lets-talk-about-dns-abuse>.
- *From Awareness to Action: How the Community Responds to DNS Abuse*, 2023. <https://www.youtube.com/watch?v=xACUS3jL7rU>.
- “ICANN’s ‘Day of DNS Abuse Discussions’ Draws More Than 125 Participants.”
<https://www.icann.org/en/blogs/details/icanns-day-of-dns-abuse-discussions-draws-more-than-125-participants-27-09-2023-en>.
- “Malicious Domains: Where They Are, and What We Can Do about Them”
<https://internet.asn.au/events/malicious-domains-where-they-are-and-what-we-can-do-about-them/>.
- “Registrars Take Action Against DNS Abuse at ICANN.”
<https://www.eurodns.com/blog/how-working-groups-tackle-dns-abuse>.

- “The Director of DNS Abuse Institute Has Visited PUNTUEUS | Puntu.Eus.”
<https://puntu.eus/en/the-director-of-dns-abuse-institute-has-visited-puntueus/>.
- “topDNS Best Practice Series: DNSAI Compass Dashboards – Benchmarking the Prevalence and Persistence of Malware and Phishing for Registries and Registrars – Eco.”
<https://international.eco.de/event/topdns-best-practice-series-dnsai-compass-dashboards-benchmarking-the-prevalence-and-persistence-of-malware-and-phishing-for-registries-and-registrars/>.