GAC Communiqués and Community Activity on DNS Abuse

February 2024

Contents

Background ... 3
GAC on DNS Abuse and Community Responses ... 5
1. Improved DNS Abuse Obligations ... 5
GAC Communiqués ... 5
Community Activity ... 6
Current Gaps ... 7
2. Enhanced DNS Abuse Reporting ... 8
GAC Communiqués ... 8
Community Activity ... 9
Current Gaps ... 10
3. Distinguishing between Malicious and Compromised Domains ... 11
GAC Communiqués ... 11
Community Activity ... 11
Current Gaps ... 12
4. DNS Abuse Measurement ... 13
GAC Communiqués ... 13
Community Activity ... 13
Current Gaps ... 15
Appendix 1: Summary Table ... 16

Background

This report has been written by the DNS Abuse Institute ("The Institute").[1] The Institute was created in 2021 by Public Interest Registry, the registry operator for the .ORG top-level domain, in furtherance of its non-profit mission.

The Institute focuses on initiatives to help reduce DNS Abuse by fostering collaboration, creating best practices, and developing open, industry-shared solutions provided at no cost. DNS Abuse is defined as being composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse). This definition was adopted from the work of the Internet and Jurisdiction Policy Network (I&JPN), a multistakeholder organization addressing the tension between the cross-border Internet and national jurisdictions, and is used in ICANN's contracts with accredited registries and registrars.

Work of the Institute is closely linked to activity within the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN's mission is to help ensure a stable, secure, and unified global Internet. ICANN operates a multistakeholder model and creates community-developed policies to facilitate the use of the Internet's systems unique identifiers, which includes domain names. Within this process, exists the Governmental Advisory Committee ("GAC").[2]

The GAC is an Advisory Committee to ICANN, composed of representatives from the governments Member States and Territories plus Observer Organizations, and created under the ICANN ByLaws. It provides input to ICANN on public policy aspects of ICANN's responsibilities with regard to the Internet Domain Name System (DNS). The typical format for this is in a GAC Communiqués, these are produced following each numbered ICANN meeting and include formal advice to the ICANN Board as well as the identification of important issues. The ICANN Board is obligated to respond to formal advice, it is not obligated to respond to issues of importance. The response of the ICANN Board to formal advice is tracked by ICANN, and GAC advice is itemized on the GAC website. Most of the references to DNS Abuse contained in GAC Communiqués are issues of importance rather than formal advice and therefore they did not require a formal response from the ICANN Board.

[1] https://dnsabuseinstitute.org/
[2] https://gac.icann.org/

GAC membership consists of national governments and distinct economies recognized in international fora; and, usually in an observer capacity, multinational governmental and treaty organizations and public authorities (including all the UN agencies with a direct interest in global Internet governance such as the ITU, UNESCO and WIPO).[3]

This report is intended to map references to DNS Abuse, particularly points of interest and action statements, made in GAC Communiqués from 2016 to June 2023 to relevant DNS community initiatives, including those undertaken by the Institute.

This reporting is designed for use by the ICANN community, and interested parties, to improve their understanding of the active steps the DNS community is taking to combat DNS Abuse, how the community has begun work on the recommendations laid out by the GAC, and where further work is needed. To illustrate this, we are presenting identified issues of importance to the GAC, then relating them to relevant community initiatives. We also identify current gaps, where the Institute believes additional attention is needed.

These issues have been categorized into four main themes: (1) contractual obligations, (2) enhanced reporting, (3) work on compromised and malicious registrations, and (4) measurement. Often these issues have also been raised in additional ICANN forums, including The Security and Stability Advisory Committee (SSAC) and The Generic Names Supporting Organization (GNSO). Finally, this report also includes an appendix which summarizes the references to DNS Abuse identified.

The Institute looks forward to continuing work to combat DNS Abuse alongside members of the DNS community, including GAC members. We welcome feedback on this document, in particular, we invite the community to share with us any additional DNS Abuse initiatives.

[3] https://gac.icann.org/work-products/public/fact-sheets-igf-ist.pdf

GAC on DNS Abuse and Community Responses

1. Improved DNS Abuse Obligations

GAC Communiqués

> "The creation of effective and enforceable requirements for registrars and registries to disrupt or mitigate DNS abuse will represent a positive and concrete first step in addressing [DNS Abuse] at ICANN" (ICANN76, 2023).[4]

This goal and its relevant actions intend to address the common complaint that ICANN lacks a comprehensive enforcement mechanism as there were no agreed-upon requirements to mitigate DNS Abuse in either the Registrar Accreditation Agreement (RAA) or Registry Agreement (RA). In particular, the GAC highlights the need to improve the specificity of these standard contracts: "Improved contract provisions could focus on the reporting and handling of DNS Abuse and enforcement of related contract requirements" (ICANN74, 2022).[5] The GAC also stated "[t]he following would assist in developing such contract provisions: abuse reporting at the registrar and registry level; more detailed breakdowns of the types of DNS Abuse measured; and availability of raw aggregated data" (ICANN74, 2022). This follows on from the GAC's 2016 Advice to the ICANN Board which requested information from ICANN on a variety of issues, including the diligence applied by ICANN in relation to '3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse' in the 2013 Registrar Accreditation Agreement (ICANN57, 2016).[6] ICANN responded to this request.[7]

In 2023, the GAC offered its support for contract negotiations between ICANN and Contracted Parties that improved existing DNS Abuse obligations and encouraged additional work (ICANN76, 2023).[8] These contract negotiations were anticipated to mandate Contracted Parties to address DNS Abuse. The increased clarity and depth of ICANN compliance obligations would allow ICANN a greater ability to facilitate negotiations and discussions with Contracted Parties if it's believed that they are not adequately mitigating and disrupting abuses. "The GAC. . . encourages

[4] https://gac.icann.org/contentMigrated/icann76-cancun-communique?language_id=1
[5] https://gac.icann.org/contentMigrated/icann74-the-hague-communique?language_id=1
[6] https://gac.icann.org/contentMigrated/icann57-hyderabad-communique?language_id=1
[7] https://gac.icann.org/advice/correspondence/incoming/Marby-to-Schneider-with-Enclosure-8Feb2017.pdf
[8] https://gac.icann.org/contentMigrated/icann76-cancun-communique

the Contracted Parties and ICANN to further consider, inter alia, proactive measures as well as positive incentives for registries and registrars in future work on DNS abuse mitigation or disruption" (ICANN76, 2023).

Community Activity

The community first made significant strides in this regard through voluntary mechanisms, most notably with the creation of the Framework to Address Abuse (the "Abuse Framework") in 2019. The Abuse Framework stands for the premise that a registrar or registry must take action when confronted with DNS Abuse (the Abuse Framework also has sections relating to certain limited categories website content abuses). The Abuse Framework launched with only eleven signatory registrars and registries, but has since grown to over fifty signatory registrars and registries (to include both gTLD and ccTLD registries). The definition of DNS Abuse set forth in the Abuse Framework has since been formally adopted as the definition of DNS Abuse by the Contracted Parties House.

From 2022 to 2023, ICANN and the Contracted Parties undertook a process of contract negotiations resulting in proposed amendments that would enhance obligations by requiring registrars and registry operators to promptly take reasonable and appropriate action to stop or otherwise disrupt DNS Abuse. The GAC provided a public comment on this proposal providing general support and identifying specific issues for consideration. The GAC comment welcomed the amendments, and noted they were a 'significant achievement' stating "[t]he proposed amendments are timely and relevant and, when adopted, will represent an important first step forward to combat DNS Abuse."[9] These amendments were adopted by the ICANN Board in January 2024 and marked a significant step towards improved DNS Abuse obligations.

The work of SSAC and the gNSO Council DNS Abuse Small Team provided significant momentum towards the contractual negotiations. The findings of SSAC115 made reference to the possibility of "universal expectations for all ICANN contracted registries and registrars to adhere to when it comes to the types of abuses they should address."[10] The work of the gNSO Council DNS Abuse Small Team also highlighted the limitations of the current contracts in terms of interpretation and

---

9 https://www.icann.org/en/public-comment/proceeding/amendments-base-gtld-ra-raa-modify-dns-abuse-contract-obligations-29-05-2023/submissions/governmental-advisory-committee-gac-18-07-2023

10 https://www.icann.org/en/system/files/files/sac-115-en.pdf A Report from the ICANN Security and Stability Advisory Committee (SSAC), 19 March 2021

enforcement. In particular, this work highlighted that ICANN Compliance believed the current (at the time) RAA "does not require registrars to take any specific action on the domain names that are subject to abuse reports."[11] The DNS Abuse Small Team noted its concern that this "may allow DNS abuse to remain unmitigated, depending upon the registrar's specific domain name use and abuse policies" and recommended that future work take place to confirm the gaps and possibly introduce minimum requirements.[12]

In terms of implementation, the Institute provides several initiatives that can help Contracted Parties as they consider the new contractual requirements. **NetBeacon**® [13] is a centralized abuse reporting tool that works to simplify and standardize the process of reporting online abuse to registrars and registries. This tool can aid Contracted Parties in the context of improved contract provisions that require a greater standard of reporting and handling DNS Abuse. NetBeacon is one option to help Contract Parties comply with more rigorous reporting requirements. Reporting from **DNSAI Compass** ("Compass"),[14] explained in further detail below in Measurement, provides contracted parties with an objective, external independent measure to benchmark their DNS Abuse levels against peers, and over time.

Current Gaps

It is necessary to provide greater awareness of tools that can aid in Contracted Parties in complying with the contract provisions. In order for Contracted Parties to comply with more rigorous requirements, there is a growing need for tools and mechanisms that aid in processes such as handling and managing DNS Abuse reports and taking prompt mitigation actions. While a number of tools and resources exist to improve the efficiency of these processes, connecting Contracted Parties with these is helpful as all parties work towards compliance. Measuring the impact of these amendments will also be crucial going forwards.

[11] DNS Abuse Small Team Report. 7 October 2022 https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf#page=16&zoom=100,557,181
[12] DNS Abuse Small Team Report. 7 October 2022 https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf#page=16&zoom=100,557,181
[13] https://netbeacon.org/
[14] https://dnsabuseinstitute.org/dnsai-compass/

2. Enhanced DNS Abuse Reporting

GAC Communiqués

The GAC expresses the importance of DNS Abuse mitigation, stressing that this work becomes increasingly important in relation to the upcoming new round of gTLDs. In light of this, it recognizes the importance and need for measurement and reporting initiatives. “Mitigating DNS Abuse continues to be an issue of concern and the GAC emphasizes the importance of building on the current work which includes effectively preventing, reporting and responding to DNS Abuse” (ICANN75, 2022).[15] In the ICANN76 Communiqué, the GAC welcomes information about the Abuse Contact IDentifier tool from the Registrar Stakeholder Group that works to identify to which parties it is appropriate to identify DNS Abuse.[16]

The GAC recognizes the need for efficient abuse reporting mechanisms and additional encouragement, facilitation, and education on this reporting process. It notes that “[e]nhanced Abuse Reporting would enable more focused dialogue within the ICANN community and provide the basis for targeted contractual improvements” (ICANN74, 2022).[17] In addition it noted that “[t]he GAC welcomes the launch of a free, centralized abuse reporting tool by the community in response to recommendations made in both SAC115 and the SSR2 Review Final Report.” (ICANN74, 2022).[18]

The SSAC called for centralized abuse reporting mechanisms in 2021 with SSAC115 which “proposes a general framework of best practices and processes to streamline reporting DNS abuse and abuse on the Internet in general” and called for the ICANN community to continue this work.[19] It outlined the following elements and recommended next steps, including: “1. encourage standard definitions of abuse (see Section 2); 2. encourage ‘notifier programs’ that will expedite and make more efficient abuse handling in certain parts of the ecosystem; 3. determine the appropriate primary point of responsibility for abuse resolution; 4. identify best practices for deployment of evidentiary standards; 5. establish standardized escalation paths for abuse resolution; 6. determine reasonable timeframes for action on abuse reports; and 7. create a single

[15] https://gac.icann.org/contentMigrated/icann75-kuala-lumpur-communique?language_id=1
[16] https://gac.icann.org/contentMigrated/icann76-cancun-communique
[17] https://gac.icann.org/advice/communiques/ICANN74%20The%20Hague%20Communique.pdf
[18] https://gac.icann.org/advice/communiques/ICANN74%20The%20Hague%20Communique.pdf
[19] https://www.icann.org/en/system/files/files/sac-115-en.pdf A Report from the ICANN Security and Stability Advisory Committee (SSAC), 19 March 2021

point of contact determination whereby a reporter can identify the type of abuse and get directed to appropriate parties."[20] The Second Security, Stability, and Resiliency (SSR2) Review Team Final Report also called for the establishment and maintenance of a "central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties."[21]

Community Activity

NetBeacon,[22] the Institute's centralized abuse reporting system, intends to address the problems of complexity and quality when it comes to reporting DNS Abuse, specifically phishing, malware, botnets, and spam, to registrars and registries. NetBeacon attempts to eliminate barriers to reporting online abuse, such as a lack of technical knowledge, confusion on how to report abuse, and the inability to navigate the DNS ecosystem. NetBeacon makes the reporting process more productive by standardizing and enriching reports, benefitting abuse reporters, registrars, and registries. Additionally, NetBeacon empowers individuals and organizations to report online abuse by simplifying the process through the automation of emailing registrars, thus enabling NetBeacon to serve as a succinct yet effective method of reporting.

The **Abuse Contact IDentifier tool (ACID Tool)**[23] provided by the Registrar Stakeholder Group (RrSG) aids in reporting DNS Abuse by enabling anyone to identify the appropriate parties, such as the hosting provider and email service provider, to report abuse to. The ACID Tool also makes registrar and registrant details relating to the entered domain name readily available. This tool makes it clear to which party the reporter should reach out to depending on what types of abuse or issues are suspected. By helping potential reporters feel confident in who they should report to and what their contact information is, abuse reporting becomes more accessible and approachable.

The multistakeholder network **Internet & Jurisdictions Network** has developed two relevant documents. Firstly, a **Due Diligence Guide For Notifiers:**[24] This document lists a series of questions notifiers should ask themselves in order to determine that making notices to operators

[20] https://www.icann.org/en/system/files/files/sac-115-en.pdf A Report from the ICANN Security and Stability Advisory Committee (SSAC), 19 March 2021
[21] https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf
[22] https://netbeacon.org/
[23] https://acidtool.com/
[24] https://www.internetjurisdiction.net/outcome/dns-level-action-to-address-technical-abuses-due-diligence-guide-for-notifiers-ref-20-113

is appropriate. Secondly, the **Minimum Notice Components for Technical Abuse**[25] includes a table that proposes a list of components that support actionable Notices for reporting technical abuse. To understand the concept of a "trusted notifier" as a reporter of DNS Abuse, the Internet & Jurisdiction Policy Network has also developed a **Trusted Notifiers: Typology and Framework Components**.[26]

Current Gaps

There is a lack of knowledge and awareness of reporting tools. While community initiatives are in practice to streamline and improve the reporting process, many potential reporters are unfamiliar with how, where, and with what evidence they should report suspected DNS Abuse.

Individuals who are trying to report abuse often have limited technical expertise, which can result in unclear or unactionable reports. People without technical knowledge should still be able to report abuse in a manner that provides report recipients with sufficient evidence to address suspected DNS Abuse, but this is not yet the case. In order for registrars and registries to make decisions on what if any course of action is appropriate, it's important for them to have sufficient evidence from reporters. One way to close this gap is to improve technical skills in the reporting community, for example, improving knowledge on extracting email headers and message bodies.[27]

---

25 https://www.internetjurisdiction.net/outcome/i-j-outcome-minimum-notice-components-for-technical-abuse-ref-20-109

26 https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-22-101-Trusted-Notifiers-Typology-and-Framework-2022.pdf

27 https://dnsabuseinstitute.org/making-phishing-reports-useful/

3. Distinguishing between Malicious and Compromised Domains

GAC Communiqués

The GAC acknowledges the importance of distinguishing between observed registration types, specifically maliciously registered and compromised domains, noting: "The GAC notes the ICANN73 community plenary session on 'Evolving the DNS Abuse Conversation,' which focused on malicious versus compromised domain names. It was universally agreed that the distinction is important, and the GAC supports the community exploring the opportunities highlighted in the session for further work to disrupt DNS Abuse" (ICANN73, 2022).[28]

"The GAC welcomed the many activities taking place across the ICANN community to address DNS Abuse, including . . . a forthcoming discussion paper from the Contracted Parties House on 'malicious vs. compromised' domains" (ICANN75, 2022).[29]

Community Activity

This differentiation between malicious and compromised domains is necessary because compromised domain names, created with benign intentions but exploited to cause harm, require different DNS Abuse mitigation strategies than malicious domain names, which are created with the intention of causing harm.

The research project **COMAR (Classification of Compromised versus Maliciously Registered domains)**[30] made advances in distinguishing malicious and compromised domains. The project from SIDN Labs, AFNIC Labs, and Grenbole Alps University was designed to automatically distinguish between compromised and malicious domains with 97% accuracy.[31] COMAR uses 38 extracted indicators or features they have studied that help indicate whether a domain is compromised or malicious. For example, one feature is that a benign but compromised domain includes a higher number of technologies used to build the website while a malicious website tends to use fewer technologies.

[28] https://gac.icann.org/contentMigrated/icann73-gac-communique?language_id=1
[29] https://gac.icann.org/contentMigrated/icann75-kuala-lumpur-communique?language_id=1
[30] https://comar-project.univ-grenoble-alpes.fr/
[31] https://www.sidnlabs.nl/en/news-and-blogs/distinguishing-exploited-from-malicious-domain-names-using-comar

The Institute freely provides articles such as **"Compromised Sites and Malicious Registrations: Best Practices for the Identification and Mitigation of DNS Abuse"**[32] that educate readers on the technical definitions of the compromised websites and malicious registrations, how to distinguish between the two, and what the best mitigation practices are for each. Education tools such as these draw attention to the cruciality of observed registration type distinctions while simultaneously offering tangible and actionable mitigation advice.

Compass produces charts in its publications that illustrate the observed registration type (malicious, compromised, and uncategorized) and how this changes over time for cases of phishing and malware. The data visualization also functions to separate phishing and malware individually, allowing readers to understand the observed registration type makeup of DNS Abuse. Individualized dashboards are also available, free of charge, to help domain registrars and registries to better understand and combat DNS Abuse.[33]

The **Internet & Jurisdictions Network's Operational Approaches: Norms Criteria and Mechanisms** document also identifies the importance of distinguishing between compromised and malicious registered domains. It notes that additional measures can be justified "to assist the registrant if the domain is obviously compromised by third parties without his/her knowledge." [34]

Current Gaps

Community discussions about DNS Abuse have begun to include discussions of malicious vs. compromised domain names, but more work is needed to ensure compromised domain names are appropriately mitigated. Understanding that a significant portion of phishing and malware cases relate to benign but compromised domains creates a need for more nuanced approaches to DNS Abuse mitigation and disruption practices in order to prevent undue restrictions and collateral damage. Compromised domain names require engagement with a wider part of the Internet ecosystem, such as hosting providers.[35] The issue of compromised domain name registrations also requires a wider public policy approach to improve cyber security hygiene across the general public, businesses, charities, and anyone who uses the Internet to register

[32] https://dnsabuseinstitute.org/best-practices-identification-mitigation-of-dns-abuse/
[33] https://dnsabuseinstitute.org/new-compass-dashboards/
[34] https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf
[35] https://dnsabuseinstitute.org/secure-your-website-save-the-internet/

domain names. As such, it is important that GAC members understand this distinction and how it could impact national and regional public policy making. One issue explored by the gNSO Small Team on DNS Abuse is the possibility of requesting the development of a Preliminary Issue Report to potentially inform a tightly defined Policy Development Process on DNS Abuse focusing on malicious registrations.[36]

4. DNS Abuse Measurement

GAC Communiqués

The GAC values advances made in DNS Abuse measurement. "Improvements to the measurement, attribution, and reporting of abuse are also much needed, and the GAC will continue to closely follow developments within the community related to any such improvements" (ICANN71, 2021)[37]. A greater industry understanding of DNS Abuse concentration, types, and other metrics offering insight into the DNS Abuse landscape can contribute to more successful DNS Abuse mitigation practices. Quantitative data on mitigation response times and analysis of abuse trends can illuminate weaknesses in DNS Abuse responses. "The GAC welcomed the many activities taking place across the ICANN community to address DNS Abuse, including … voluntary initiatives on measurement and reporting" (ICANN75).[38] Public availability of DNS Abuse trend information allows for more strategic conversations that improve DNS Abuse practices. The Second Security, Stability, and Resiliency (SSR2) Review Team Final Report also called for the identification of "registries and registrars whose domains most contribute to abuse."[39]

Community Activity

ICANN's **Domain Abuse Activity Reporting (DAAR) project**, a system created to study and report domain name registration and security threats across top-level domain registries, contributes to a better community understanding of DNS Abuse. DAAR's purpose is to help guide policy decisions

[36] DNS Abuse Small Team Report. 7 October 2022 https://gnso.icann.org/sites/default/files/policy/2022/correspondence/dns-abuse-small-team-to-gnso-council-07oct22-en.pdf#page=16&zoom=100,557,181
[37] https://gac.icann.org/contentMigrated/icann71-gac-communique?language_id=1
[38] https://gac.icann.org/contentMigrated/icann75-kuala-lumpur-communique?language_id=1
[39] https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf

in the ICANN community by generating a "robust, reliable, and reproducible methodology for analyzing security threat activity."[40] DAAR achieves this through collecting TLD zone data and Reputation Block List security threat data feeds. The compilation of statistics and data allows for the analysis of abuse activity on the registry level. DAAR's monthly reports identify general trends, break down individual security threats, and offer more metrics such as the percentage of security threat domains in a TLD per domain within a TLD zone.[41] The project's reports, methodology papers, and contextual documents collectively inform interested parties about the concentration of security threats within the TLD space and its changes over time.

Compass expands on the high-level abuse trends introduced by DAAR by creating monthly DNS Abuse reports on phishing and malware broken down by registrar and TLD.[42] Compass measures phishing and malware, and categorizes unique domain names as compromised vs. malicious domain registrations. It also measures whether the harm has been mitigated, and how quickly. Accompanying full-length reports are interactive charts that offer timely and detailed quantitative data. Compass also provides individual dashboards to registrars and registries, which include specific information on their zone. Additionally, the breakdowns of high and low volumes of observed maliciously registered domains by registrar in the June 2023 Report[43] offer more insight into DNS Abuse on the registrar and registry level.

The new ICANN funded project, **Inferential Analysis of Maliciously Registered Domains (INFERMAL),**[44] provides an important next step measurement. INFERMAL systematically analyzes the preferences of cyberattackers including domain name, security practices, and payment method. The findings from this project can expand knowledge on what mitigation measures and proactive actions may best prevent DNS Abuse.

The DNS Research Federation's Data Analytics Platform **DAP.LIVE**[45] is an open data platform offering metrics on malware, phishing, and abuse trends that can illuminate how and where DNS Abuse occupies the DNS ecosystem. Data on malware reports by URL, phishing reports by URL,

[40] https://www.icann.org/octo-ssr/daar
[41] https://www.icann.org/en/system/files/files/daar-monthly-report-31mar23-en.pdf
[42] https://dnsabuseinstitute.org/dns-abuse-if-we-cant-measure-it-does-it-exist/
[43] https://dnsabuseinstitute.org/wp-content/uploads/2023/06/V3-FINAL-DNSAI-Compass-Report-Combined.pdf
[44] https://www.icann.org/en/blogs/details/new-icann-project-explores-the-drivers-of-malicious-domain-name-registrations-25-04-2023-en ; https://infermal.korlabs.io
[45] https://dnsrf.org/

and top fifty phishing root domains are among a variety of data sources and packages that users can filter and sort through to generate tables, visualizations, and graphs. From quantifying phishing[46] to exploring registrant identification counts for specific domains,[47] DAP.LIVE creates spaces for users to investigate and work firsthand with DNS Abuse data, which may aid conversations on DNS Abuse mitigation.

Current Gaps

Measurement projects are currently limited by the quality of data that exists, which is usually drawn from reputation block lists created for the purposes of network protection rather than measurement of abuse. The next challenge for the DNS Community will be to create more detailed and accurate ways of measuring DNS Abuse, and to provide analysis on specific issues: for example, aging domains, and the impact of various policies and processes (e.g., incentive schemes).

[46] https://dnsrf.org/blog/dns-as-a-vector-for-phishing-attacks--different-victims--different-methodologies--different-results/index.html
[47] https://dnsrf.org/blog/brand-names-in-blockchain-domains---new-frontier-for-brand-owners/index.html

Appendix 1: Summary Table

Please note, this table is issue based summarizing this report. If a GAC Communiqué references multiple issues it is listed multiple times. Readers may find the GAC Advice itemized tracker and the ICANN Board response tracker helpful for further understanding GAC Advice and progress. Please note that most of the references to DNS Abuse contained in GAC Communiqués are issues of importance rather than formal advice and therefore they did not require a response from the ICANN Board.

Issue	GAC Communique	Details
Improved DNS Abuse Obligations	ICANN57, 2016	**GAC Advice to the Board:** requested information from ICANN on a variety of issues, including the diligence applied by ICANN in relation to '3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse' in the 2013 Registrar Accreditation Agreement (ICANN57, 2016). ICANN responded to this request.
	ICANN74, 2022	**Issues of Importance to the GAC:** "Improved contract provisions could focus on the reporting and handling of DNS Abuse and enforcement of related contract requirements" "The following would assist in developing such contract provisions: abuse reporting at the registrar and registry level; more detailed breakdowns of the types of DNS Abuse measured; and availability of raw aggregated data"
	ICANN76, 2023	**Issues of Importance to the GAC:** "The creation of effective and enforceable requirements for registrars and registries to disrupt or mitigate DNS abuse will represent a positive and concrete first step in addressing [DNS Abuse] at ICANN"

		In 2023, the GAC offered their support for contract negotiations between ICANN and Contracted Parties that improve existing DNS Abuse obligations and encouraged additional work. "The GAC … encourages the Contracted Parties and ICANN to further consider, inter alia, proactive measures as well as positive incentives for registries and registrars in future work on DNS abuse mitigation or disruption" (ICANN76, 2023).
Enhanced DNS Abuse Reporting	ICANN74, 2022	**Issues of Importance to the GAC:** "Enhanced Abuse Reporting would enable more focused dialogue within the ICANN community and provide the basis for targeted contractual improvements" In addition they noted that "The GAC welcomes the launch of a free, centralized abuse reporting tool by the community in response to recommendations made in both SAC115 and the SSR2 Review Final Report."
	ICANN75, 2022	**Issues of Importance to the GAC:** "Mitigating DNS Abuse continues to be an issue of concern and the GAC emphasizes the importance of building on the current work which includes effectively preventing, reporting and responding to DNS Abuse"
	ICANN76, 2023	**Issues of Importance to the GAC:** GAC welcomes information about the Abuse Contact IDentifier tool from the Registrar Stakeholder Group that works to identify to which parties it is appropriate to identify DNS Abuse.
Distinguishing between Malicious and Compromised Domains	ICANN73, 2022	**Issues of Importance to the GAC:** "The GAC notes the ICANN73 community plenary session on 'Evolving the DNS Abuse Conversation,' which focused on malicious

		versus compromised domain names. It was universally agreed that the distinction is important, and the GAC supports the community exploring the opportunities highlighted in the session for further work to disrupt DNS Abuse"
	ICANN75, 2022	**Issues of Importance to the GAC:** "The GAC welcomed the many activities taking place across the ICANN community to address DNS Abuse, including... a forthcoming discussion paper from the Contracted Parties House on "malicious vs. compromised" domains" (ICANN75, 2022).
DNS Abuse Measurement	ICANN71, 2021	**Issues of Importance to the GAC:** The GAC values advances made in DNS Abuse measurement. "Improvements to the measurement, attribution, and reporting of abuse are also much needed, and the GAC will continue to closely follow developments within the community related to any such improvements"
	ICANN75, 2022	**Issues of Importance to the GAC:** "The GAC welcomed the many activities taking place across the ICANN community to address DNS Abuse, including ... voluntary initiatives on measurement and reporting"