From: Graeme Bunton
Date: Friday, April 22, 2022
To: Goran Marby

Subject: Moving Forward to Reduce DNS Abuse

Dear Goran,

Recently, the GNSO Small Team on DNS Abuse reached out to several communities, as well as the DNS Abuse Institute for input on what role the GNSO should play with regards to DNS Abuse. We took the opportunity to try to respond comprehensively, and I wanted to share that work with yourself and ICANN org staff.

Briefly the key points are:

- The community doesn't need to define DNS Abuse to move forward on issues with consensus, and so it shouldn't attempt to do so
- Website Content Abuse should be off the table due to both practical, and remit constraints
- The GNSO should conduct three sequential, incredibly focused efforts/PDPs on:
    - Malicious registrations used for distribution of malware,
    - Malicious registrations used for phishing,
    - Malicious registrations used for botnet command and control
- In addressing these specific harms and in this manner, the GNSO could:
    - Demonstrate that the MSM can be effective
    - Address a substantial majority of DNS Abuse
    - Minimize the potential impact to Registrants
    - Remain within the Bylaws

I would appreciate it if you would include this note and the attached letter on the ICANN correspondence page.

As always, if yourself or other ICANN staff have questions or comments, I'm always happy to serve as a resource.

Regards,

Graeme

Graeme Bunton
Executive Director, DNS Abuse Institute
647-702-3323
https://dnsabuseinstitute.org/ [dnsabuseinstitute.org]

Dear Philippe,

Thank you for the opportunity to provide the GNSO Small Team on DNS Abuse with input from the DNS Abuse Institute on appropriate GNSO approaches to DNS Abuse. In your letter you ask:

1. Does the Institute have any expectations with regards to possible next steps the GNSO Council could or should undertake in the context of policy development?
2. If yes, could you please provide further details on what specific problem policy development in particular would be expected to address as well as expected outcomes if policy development would be undertaken, taking into account the remit of ICANN and more specifically GNSO policy development in this context?

The short answer, in my view, is yes, the GNSO Council could play a very important role in policy development around DNS Abuse, and yes, there is an opportunity to move forward, but under the parameters detailed below. Ultimately, the DNS Abuse Institute recommends that the GNSO explore a series of hyper-focused sequential PDPs on issues of clear-cut DNS Abuse. In other words, a series of "micro-PDPs" on DNS Abuse has the potential to create incremental yet meaningful change in the way DNS Abuse is identified and addressed.

DNS Abuse: Symptoms, Causes, and Treatments

If DNS Abuse is a disease, we have, at best, an anecdotal understanding of the symptoms. From ICANN's DAAR, we have a general sense of DNS Abuse trends across the industry, but not by TLD or by registrar. Similar DNS Abuse reporting from others tends to be narrow, opaque, coloured by commercial interests, or some combination of all three. We do not know with any specificity how much of what types of abuse exist at registrars and TLDs, and how that changes over time. Clearly, prior to creating policy, the GNSO should have a robust understanding to what extent the issue is industry-wide, or if it is more acutely concentrated.

Further, if our understanding of the symptoms is anecdotal, we know even less about the necessary pre-conditions for abuse. How do local law, terms of service, payment methods, markets, and the prevalence of disposable domains influence rates of abuse? Understanding what drives rates of abuse is crucial to reducing it. The GNSO should have some understanding of these issues, and which are within its remit to address.

Lastly, we do not know much about the treatments for DNS Abuse. Beyond suspending domains, there are opportunities for sinkholing and intelligence collection, or even preventative approaches, such as malicious registration detection algorithms and registrar incentive programs. Preventing DNS Abuse and reacting to DNS Abuse are important but distinct topics, each with its own complicated considerations.

In the long term, the GNSO should understand the causes, symptoms and treatments for DNS Abuse if it's to help address abuse effectively.

Scoping: Less is More

I'm going to use the soapbox that you've kindly offered to make an argument for an approach that I think is crucial for successful work within ICANN on DNS Abuse, and I apologize in advance for being perhaps overly prescriptive. I'm going to elaborate on *how* to do this work, before getting into *what* this work should be.

This discussion will have two components, one on practical constraints, the other on limitations within ICANN's Bylaws.

Practically Scoping DNS Abuse

Online harms are a complicated global problem, of which abuse that uses domain names are a subset. I have personally led, participated in, or observed many community discussions on the definition of DNS Abuse. Collectively, this has revealed that there isn't always a shared understanding about what DNS Abuse encompasses and that a timely, effective, and satisfying resolution to this definitional question is practically out of reach. There are a multitude of edge-cases and specific interests at play, and we've seen, especially with privacy issues, how the ICANN community struggles to answer fundamental questions of this nature.

As such I would strongly encourage the GNSO to side-step the definitional issue entirely. Just simply do not have it. This is for two reasons:

- There is urgent work to be done on DNS Abuse issues that virtually no one disagrees with; and

- The ICANN community has already spent years attempting to define DNS Abuse. Continued definitional discussions will take years, contribute to volunteer burnout, and exacerbate existing community issues with producing and implementing timely policies.

Let me be as clear as possible. This GNSO does not need to fully and completely define DNS Abuse to move forward and create positive change on the DNS Abuse landscape. The GNSO can select from several issues central to DNS Abuse without worrying about the margins. Start at the center, and establish expertise and processes for addressing unambiguous harms at the core of DNS Abuse.

It's possible after spending time on the portions of DNS Abuse for which there is wide agreement, that the GNSO will need to consider if other types of DNS Abuse fall into its remit, but it will then be doing so from a place of strength and experience.

Scoping DNS Abuse work within ICANN's Bylaws

It is not just the practical issues of scoping that are relevant, there are also important considerations around ICANN's Bylaws and remit.

ICANN has recently been both clearer and firmer that regulation of Website Content Abuse[1] falls outside of its remit. ICANN Org recently published The Last Four years in Retrospect: A Brief Review of DNS Abuse Trends, in which it states that "depending on what you mean by DNS abuse, some types of abuse perpetrated via the Internet may not fall within ICANN's remit and capabilities as the technical coordinator of the DNS. ICANN is not and was not designed to be the Internet's content police."

This guidance harkens back to its 2015 Blog "ICANN is not the Internet Content Police," in which ICANN's then Chief Compliance Officer, Allen Grogan, detailed why it would not be appropriate for ICANN, given its technical remit, to be in the business of enforcing policies involving Website Content Abuses. Mr. Grogan states:

> "Allow me to say this clearly and succinctly – ICANN is not a global regulator of Internet content, nor should the 2013 Registr[ar] Accreditation Agreement (RAA) be interpreted in such a way as to put us in that role. Our mission is to coordinate, at the overall level, the global Internet's systems

[1] For more information on Website Content Abuse, see page 3 of the Framework to Address Abuse.

> of unique identifiers, and in particular, to ensure the stable and secure operation of the Internet's unique identifiers. …
>
> Though the appropriate interpretation of 2013 RAA is the subject of debate, there are clear-cut boundaries between ICANN enforcing its contracts and the enforcement of laws and regulations by the institutions mentioned earlier. A blanket rule requiring suspension of any domain name alleged to be involved in illegal activity goes beyond ICANN's remit and would inevitably put ICANN in the position of interpreting and enforcing laws regulating website content. At worst, it would put ICANN squarely in the position of censoring, or requiring others to censor, Internet content."

Mr. Grogan goes on to outline the complexities of why this must be so, notably including various legal schemas around the world that demonstrate how untenable this content regulation role would be. He notes the various (and sometimes conflicting) laws on blasphemy and religious defamation, hate speech, laws targeting political dissidents, and pornography. I thought this ICANN blog was very thoughtful and articulate and I'd encourage anyone curious about the question of ICANN's remit to read it.

Of course, the ICANN blog reflects the legal reality codified in ICANN's Bylaws. Section 1.1(c) of the ICANN Bylaws states:

> "ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers ***or the content that such services carry or provide***, outside the express scope of Section 1.1(a). For the avoidance of doubt, ICANN does not hold any governmentally authorized regulatory authority."

(emphasis added). Finally on this ground setting for any eventual PDP, I'd point out that the question of whether a policy on Website Content Abuse falls within ICANN's remit and would be enforceable in ICANN's contracts has already been asked by the GNSO to ICANN's Office of the General Counsel (ICANN OGC). As noted in the 2010 Registration Abuse Policies Working Group Final Report:

> "In the Issues Report that led to the RAPWG, the ICANN General Counsel 's office wrote: 'Is the issue in scope of GNSO Policy Making? Section 4.2.3 of

> the RAA between ICANN and accredited registrars provides for the establishment of new and revised consensus policies concerning the registration of domain names, including abuse in the registration of names, but **policies involving the use of a domain name (unrelated to its registration) are outside the scope of policies that ICANN could enforce on registries and/or registrars**.'"

(emphasis added). I know that there are parts of the ICANN Community that find this boundary unsatisfying and I appreciate where they are coming from. There are any number of voluntary initiatives out there regarding certain categories of Website Content Abuse, such as the Framework to Address Abuse, but ultimately Website Content Abuse questions fall outside of ICANN's remit and necessarily fall outside of what could be part of a PDP on DNS Abuse.

Recommended Approach: Exploration of Micro-PDPs on DNS Abuse

As mentioned above, there are issues of DNS Abuse with near universal agreement: specifically that malicious registrations used for the distribution of malware, phishing, or the operation of botnets are appropriately and reasonably addressed by registrars and registries. We all agree that this is clear-cut DNS Abuse, which means there is an opportunity to focus on this issue at the outset and make meaningful progress on abuse.

ICANN's current work on Transfer Policy provides a model for an approach. I would propose three seperate, sequential efforts, either narrowly scoped efforts or PDPs, for mitigating malicious[2] registrations:

- Malicious Registrations used for the distribution of Malware[3];
- Malicious Registrations used for Phishing;
- Malicious Registrations used for the operation of Botnet command and control systems.

By restricting the work to malicious registrations, the GNSO ensures that these efforts are within ICANN's remit, and avoids the complexities of issues involving actors outside of ICANN's contractual regime, like hosting companies and content distribution

[2] For more information on the difference between malicious registrations versus compromised domains, please see DNSAI Best Practice on Identifying Malicious Registrations

[3] For definitions of these terms, please see the Framework to Address Abuse, and the Internet and Jurisdiction Policy Network's Operational Approaches, Norms, Criteria and Mechanisms

networks. Focusing these PDPs on malicious registrations targets bad actors, and the impacts on legitimate registrants are correspondingly minimized.

The scoping constraints on the work should also influence the results. The outputs should be short, simple, easy to implement requirements. Not only would clear obligations for registrars to mitigate malicious registrations reduce DNS Abuse, these obligations would reflect existing industry best practices.

Concluding the above three PDPs would cover a substantial majority of DNS Abuse[4], and be a significant contribution to Internet trust and safety. Further, the expertise and experience the GNSO will have collectively gathered in the process will presumably be valuable for further work. This work could include processes for addressing DNS Abuse on compromised websites, where the remedies are more complex and the risks to domain registrants more substantial.

There are still real questions to be answered inside the above proposed PDPs, but by narrowly constraining them, the GNSO will be able make real, substantial progress on DNS Abuse in a timely fashion.

Thank you again for the opportunity to provide input on this topic, I hope the GNSO finds it useful. I and the DNS Abuse Institute are always happy to serve as a resource to the GNSO in the service of making the Internet safer for everyone.

Regards,

Graeme Bunton
Executive Director, DNS Abuse Institute

[4] See Prof. Maciej Korczynski's presentation from ICANN 73.