ICANN | GAC

Governmental Advisory Committee

Distribution	Public
Date	18 September 2019

GAC Statement on DNS Abuse

ICANN's Governmental Advisory Committee (GAC) looks forward to the upcoming cross-community discussion on DNS Abuse during ICANN66 and appreciates the Registries Stakeholder Group's August 19, 2019 Open Letter to the Community on this topic.

Protecting the public from security threats and DNS Abuse is an important public policy issue. The GAC has issued advice, provided guidance and comments, organized cross-community discussions, and advocated for stronger contractual provisions to safeguard the public.[1] Our current remarks will provide further context on this topic by discussing: 1) why DNS Abuse is a vital topic; 2) the existing definitions and contractual obligations regarding DNS Abuse; and 3) the Competition, Consumer Trust, and Consumer Choice Review Team's findings and recommendations on DNS Abuse. Through this discussion, we hope to lay the foundation for a productive and informed cross-community discussion in Montreal.

Why DNS Abuse Is a Vital Topic

With each passing year, the global cost of cybercrime rises, reaching an estimated $600B in 2018.[2] Cybercriminals exploit and abuse the DNS to accomplish their schemes,[3] and email remains by far the most common vector of initial compromise,[4] with a sharp increase in phishing attacks against consumers.[5]

If the public is to trust and rely upon the Internet for communications and transactions, those tasked with administering the DNS infrastructure must take steps to ensure that this public resource is safe and secure. Recent privacy laws, including the EU's General Data Protection Regulation, have limited the public availability of information about the owners of domain names, creating challenges for law enforcement and cyber-security professionals tasked with combatting threats to the safety and security of the Internet.[6]

---

[1] The GAC has provided this input both independently and through the Public Safety Working Group. *See e.g.,* the following: GAC Communiqués: ICANN46 Beijing; ICANN 53Buenos Aires, ICANN54 Dublin; and ICANN57 Hyderabad; ICANN community presentations on DNS Abuse during ICANN57, 58, and 60; and 2009 Law Enforcement Recommendations (endorsed by GAC during ICANN 38).

[2] McAfee Economic Impact of Cybercrime – No Slowing Down available at: https://www.csis.org/analysis/economic-impact-cybercrime; Accenture 2019 Cost of Cybercrime, available at https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

[3] *See e.g.,* Symantec Internet Threat Security Report (Feb. 2019) available at: https://www.symantec.com/security-center/threat-report.

[4] Verizon's 2019 Data Breach Investigations Report available at https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[5] Akamai's 2019 State of the Internet available at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-attack-economy-report-2019.pdf

[6] *See e.g.,* ICANN GDPR and WHOIS Users Survey conducted by Anti Phishing Working Group and Messaging, Malware and Mobile Anti-Abuse Working Group available at https://www.securityskeptic.com/2019/03/facts-figures-whois-policy-changes-impair-blacklisting-defenses.html

ICANN's recent and ongoing reviews, required under the Bylaws highlight the importance of:

- the **effectiveness of security efforts to deal with actual and potential challenges and threats to the security and stability of the DNS**, and the extent to which the **security efforts are sufficiently robust to meet future challenges** and threats;[7]
- **consumer protection**, security, stability and resiliency, **malicious abuse** issues, sovereignty concerns, and rights protection prior to, or concurrent with, authorizing an increase in the number of new top-level domains;[8]
- **improv[ing] accuracy and access to generic top-level domain registration data**, as well as consider safeguards for protecting such data;[9]
- the **effectiveness** of the then **current gTLD registry directory service** and **whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust** and safeguarding registrant data[10] [emphasis added]

In addition, ICANN is considering the contours for a second round of gTLDs which provides new opportunities for including within contracts incentives for the adoption of best practices shown to reduce such abuse and increase the cost of business to abusive or criminal actors.

Consequently, now is the right time to consider these issues and contemplate the best path forward in support of ICANN's commitment to both preserve **and enhance** the administration of the DNS, including the "operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet."[11] In this regard, governments and public authorities are especially well-placed to provide input.[12]

Existing Definitions of DNS Abuse and ICANN Contract Obligations

The Competition, Consumer Trust and Consumer Choice (CCT) Review team which comprised stakeholders from across the ICANN community, looked to existing definitions of DNS Abuse within the ICANN community when they sought to examine DNS Abuse in new gTLDs compared to legacy gTLDs and assess whether the existing safeguards were sufficient.[13] Noting that ICANN community findings demonstrated that "consensus exists on what constitutes DNS Security Abuse, or DNS Security Abuse of DNS infrastructure," **the CCT Review Team referred to DNS Abuse as "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names.**"[14] The CCT Report used the term "DNS Security Abuse" to refer to more technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse.[15]

These definitions are consistent with ICANN standard contracts for registries and registrars. ICANN's standard Registry Agreement required new gTLD registry operators to include provisions in their Registry-Registrar Agreements (RRA) that prohibited registrants from:

[7] ICANN Bylaws, §4.6 (c), Security, Stability, and Resiliency Review.
[8] ICANN Bylaws, §4.6 (d), Competition, Consumer Trust and Consumer Choice Review.
[9] ICANN Bylaws, §4.6 (e), Registration Directory Service Review.
[10] *Id.*
[11] ICANN Bylaws, §1.2(a) Commitments.
[12] Indeed recognizing the vital role of governments and public authorities play in contributing when matters raise public policy issues is one of ICANN's Core Values. ICANN Bylaws, §1.2(b) Core Values.
[13] *See* CCT Final Report (Sept. 18, 2018) at pp. 88-109. For more on how abuse has been characterized by the ICANN Community, see the Registration Abuse Policies Working Group's Final Report (29 May 2010): https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf
[14] CCT Final Report at p. 88 and accompanying fns. *See also* p. 3 of the "New gTLD Program Safeguards Against DNS Abuse: Revised Report" (2016).
[15] CCT Final Report at p. 8.

> distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.[16]

Further, Registry Operators must "periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, **such as** pharming, phishing, malware, and botnets."[17] [emphasis added]. We note that this list is illustrative rather than exhaustive. Complementing the Registry provisions, ICANN's standard contract for Registrars requires registrars to promptly "investigate and respond appropriately to any reports of abuse."[18] Taken together, these sources, developed within the ICANN multistakeholder community comprise a common foundational understanding of what comprises DNS Abuse.

CCT Review Team Finds DNS Abuse Concentrated Among Certain Registries and Registrars and Develops Recommendations

The CCT Team observed that Domain names are often a key component of cybercrimes, are used to assist with malware distribution and botnet command-and-control and that spam campaigns often correlate with phishing and other cybercrime.[19] Notably, the Review Team pointed out that

> [a]lthough ICANN's standard contracts for registries and registrars have mandated consistent use of specified safeguards, efforts to combat domain name abuse vary greatly amongst the contracted parties. Some entities do not act until a complaint is received. In contrast, other registrars take proactive steps, such as checking registrant credentials, blocking domain name strings similar to known phishing targets, and scrutinizing domain name resellers. Domain name resellers are not ICANN-contracted parties and hence not directly subject to ICANN's enforcement authority over standard contract requirements. . . [20]

In order to better understand the effectiveness of the new gTLD safeguards, the CCT Review team commissioned a study that analyzed rates of spam, phishing, and malware distribution in the global gTLD from 2014 to 2016, distinguishing between legacy and new gTLDs and released the ensuing report.[21] Significantly, the DNS Abuse Study makes clear that there are significant abuse issues in the DNS. Regarding the new gTLD program, the Study notes that over 50% of registrations in certain new gTLDs were abusive.[22] Other highlights of the Study included the following:

- New gTLDs have become a growing target for bad actors;
- Legacy gTLDs have higher concentrations of compromised domains while bad actors frequently choose to maliciously register domain names using one of the new gTLDs;
- The registry operators of the most abused new gTLDs compete on price;
- Phishing and malware abuse rates of new gTLDs are converging with the rates of legacy gTLDs over time;
- Five new gTLDs with the highest concentration of domains used in phishing attacks according to the Anti-Phishing Working Group blacklist contained 58.7% of all of the blacklisted domains in the new gTLDs;

[16] ICANN Registry Agreement, Specification 11, 3(a).
[17] ICANN Registry Agreement, Specification 11, 3(b). This provision has been the repeated topic of GAC questions, concerns and advice which arose because ICANN's implementation of this safeguard while requiring Registries to monitor for security threats, did not obligate Registry Operators to act in response to security threats. *See* Singapore (2014), Los Angeles, London. The GAC's Beijing Communiqué included not only a duty to monitor for security threats but a duty to respond in the event certain dire security threats are detected. The GAC advised in the case of security threats that pose an "actual risk of harm", Registry Operators will notify the relevant Registrar, and if the Registrar fails to take "immediate action" then "suspend the domain name until the matter is resolved." Beijing Communiqué at p. 7.
[18] ICANN Registrar Agreement, § 3.18.
[19] CCT Review Team Final Report at p. 93.
[20] CCT Review Team Final Report at p. 93.
[21] *See* https://www.icann.org/news/announcement-2017-08-09-en
[22] Statistical Analysis of DNS Abuse in gTLDs Final Report (9 August 2017): https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

- New gTLDs experienced a significantly higher percentage of spam in the last quarter of 2016 than legacy gTLDs (ten times higher than Legacy gTLDs);
- Domain names registered for malicious purposes often contained strings related to trademarked terms
- Abuse counts primarily correlate with strict registration requirements: *i.e.*, bad actors prefer to register domains in standard new gTLDs, which are generally open for public registration, rather than in community new gTLDs, where registries may impose restrictions on who or what entities can register domain names.

The CCT Review Team concluded that factors such as registration restrictions, price, and registrar-specific practices were likely to affect abuse rates.[23] Consequently, the CCT Review Team recommended that:

- the ICANN organization negotiate amendments to existing Registry Agreements, or in consideration of new Registry Agreements associated with subsequent rounds of new gTLDs, **include provisions in the agreements to provide incentives, including financial incentives for registries, especially open registries, to adopt proactive anti-abuse measures** [emphasis added];
- ICANN Org negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements to include provisions aimed at preventing systemic use of specific registrars or registries for DNS Security Abuse. In particular, ICANN should establish thresholds of abuse at which compliance inquiries are automatically triggered, with a higher threshold at which registrars and registries are presumed to be in default of their agreements;
- Further study the relationship between specific registry operators, registrars, and DNS Security Abuse by commissioning ongoing data collection, including but not limited to, the ICANN Domain Abuse Activity Reporting (DAAR) initiative. For transparency purposes, this information should be regularly published, ideally quarterly and no less than annually, in order to enable identification of registries and registrars that require greater scrutiny, investigation, and potential enforcement action by the ICANN organization. Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remedy problems identified, and define future ongoing data collection; and
- ICANN should collect data about and publicize the chain of parties responsible for gTLD domain name registrations.

ccTLD Registries' Best Practices

In recent years, an increasing number of ccTLD registries have adopted pro-active anti-abuse measures to address DNS-facilitated crime and both keep their zone free of abuse and repel bad actors by making their domain names as unattractive to bad actors as possible. These measures range from stronger authentication methods, including identity checks[24], to the use of data-based fraud prediction models which combine data registration and infrastructure metrics to identify and predict domain registrations made for harmful purposes[25]. These proven best practices should be implemented by gTLD registries and registrars.

Conclusion

This Community is uniquely positioned to assess and choose what policies should be taken to safeguard the public from DNS abuse. We agree with the Registries Stakeholder group that the success of their product (and indeed the DNS) depends on their ability to offer a reputable product that users can trust. In order to grapple more effectively with DNS Abuse and promote a more trustworthy DNS, we encourage the Community to seriously consider adopting the recommendations described above as they provide actionable steps that can *and should* be taken to address DNS abuse. The GAC looks forward to engaging with other community groups about this topic at ICANN 66 in Montreal.

[23] CCT Final Report at p. 94, citing DNS Abuse Study at pp. 24-25.
[24] See e.g., ICANN64 Session on Lessons Learned: How .DK successfully reduced abusive domains and https://www.dk-hostmaster.dk/en/news/mandatory-identification-nemid and https://www.dk-hostmaster.dk/en/news/dk-hostmaster-makes-online-fraud-more-difficult
[25] See https://eurid.eu/en/news/identification-of-malicious-dns/