Safeguards

Version with Additions by David Taylor [TD1] generally and specifically on Recommendation D
18 June 2018

DNS Abuse

The widespread availability and relative accessibility of domain names as unique global identifiers has created opportunities for both innovative technologies and a multitude of malicious activities. Bad actors have misused these universal identifiers for cybercrime infrastructure[1] and directed users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud. Each of these activities may constitute a form of DNS abuse. Determinations as to how to characterize these forms of abuse depend largely upon local laws, the roles played by other infrastructure providers, and subjective interpretations. Nonetheless, consensus exists on what constitutes technical DNS abuse, or technical abuse of DNS infrastructure, as demonstrated by community findings associated with the development of the New gTLD Program. These forms of abuse include malware, phishing, and botnets, as well as Spam when used as a delivery method for these forms of abuse.

Due to the misuse of domain names, the community initially expressed concerns about whether the vast expansion of available gTLDs would result in increased DNS abuse. The CCTRT was tasked with examining issues associated with the expansion of the DNS, including the implementation of safeguards designed to preempt identified risks.[2]
Prior to the approval of the New gTLD Program, ICANN invited feedback from the cybersecurity community on DNS abuse and the risks posed from the expansion in the DNS name space.[3] The community identified the following areas of concern:

How do we ensure that "bad actors" do not run registries?

[1] Bursztein et. al., "Framing Dependencies Introduced by Underground Commoditization," (paper presented at the proceedings of the 2015 Workshop on the Economics of Information Security, Delft, Netherlands, 22–23 June 2015), https://research.google.com/pubs/pub43798.html, p. 12.

[2] The US Department of Commerce and ICANN Affirmation of commitments specifies "malicious abuse issues" as one of the issues to be analyzed prior to expanding the top-level domain space. Furthermore, the AoC requires the CCT Review Team to analyze the "safeguards put in place to mitigate issues involved in the introduction or expansion" of new gTLDs. Consequently, the CCT Review Team Terms of Reference define the work of the team to include a review of the "effectiveness of safeguards" and "other efforts to mitigate DNS abuse." Furthermore, the GAC's 2015 Buenos Aires Communiqué requested "that the ICANN community creates a harmonised methodology to assess the number of abusive domain names within the current exercise of assessment of the New gTLD Program." See https://gacweb.icann.org/download/attachments/27132037/BA%20MinutesFINAL.pdf?version=1&modificationDate=1437483824000&api=v2; Likewise, the 2015 Dublin Communiqué requested that the ICANN Board "develop and adopt a harmonized methodology for reporting to the ICANN community the levels and persistence of abusive conduct…that have occurred in the rollout of the New gTLD Program." See https://gacweb.icann.org/display/GACADV/2015-10-21+gTLD+Safeguards+%3A+Current+Round

[3] "ICANN (3 October 2009), *Mitigating Malicious Conduct*, accessed 9 November 2016, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf. Feedback came from groups such as the Anti-Phishing Working Group (APWG), Registry Internet Safety Group (RISG), the Security and Stability Advisory Community (SSAC), Computer Emergency Response Teams (CERTs), the banking/financial and wider Internet security communities.

Formatted: Font:11 pt, Not Bold, Font color: R,G,B (219,96,51)

Formatted: Font:11 pt, Not Bold, Font color: R,G,B (219,96,51)

Formatted: Font:11 pt, Not Bold, Font color: R,G,B (219,96,51)

Deleted: made them conduits of

Deleted: ,

Deleted: including those used for

Deleted: purposes

Deleted: Consequently, b

Deleted: directing

Deleted: enabling

Deleted: However, d

Deleted: greater

Deleted: many technical forms of

Comment [TD1]: Better lower case unless defined?

How do we ensure integrity and utility of registry information?
How do we ensure more focused efforts on combating identified abuse?
How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?[4]

Based on the community's feedback, ICANN identified several recommendations for safeguards aimed at mitigating these risks.[5] Nine safeguards were identified and recommended:

- Vet registry operators
- Require Domain Name System Security Extension (DNSSEC) deployment
- Prohibit "wildcarding"
- Encourage removal of "orphaned glue" records[6]
- Require "Thick" WHOIS records
- Centralize Zone File access
- Document registry- and registrar-level abuse contacts and policies
- Provide an expedited registry security request process
- Create a draft framework for a high security zone verification program[7]

Formatted: Indent: Left: 0.5", No bullets or numbering

The CCTRT was tasked with analyzing the effectiveness of the nine recommended safeguards. To the extent possible, the CCTRT assessed the effectiveness of each of these safeguards using available implementation and compliance data.[8] The CCTRT examined the implementation of each. Additionally, the CCTRT commissioned a quantitative DNS abuse study to provide insight into the relationship, if any, that may exist between levels of abuse and implemented safeguards in the new gTLD name space.[9]

With regard to the first safeguard, vetting registry operators, all new gTLD applicants were required to provide full descriptions of the technical back-end services that they would use, even where these services were subcontracted, as part of the application process. This was an initial evaluation to ensure technical competence. These descriptions were evaluated only at the time of application.[10] Additionally, all applicants were required to pass Pre-Delegation Testing (PDT).[11] PDT included comprehensive technical checks of Extensible Provisioning Protocol (EPP), Name Server setup, Domain Name System Security Extensions (DNSSEC), and other

[4] Ibid.
[5] Ibid.
[6] The Security Skeptic, "Orphaned Glue Records," 26 October 2009, accessed 2 February 2017, http://www.securityskeptic.com/2009/10/orphaned-glue-records.html. These are records remaining once a domain name has been deleted from a registry.
[7] ICANN, "Malicious Conduct."
[8] See ICANN, New gTLD Program Safeguards (2016).
[9] ICANN (2 August 2016), Request for Proposal For Study on Rates of DNS Abuse in New and Legacy Top-Level Domains, accessed 2 February 2017, https://www.icann.org/en/system/files/files/rfp-dns-abuse-study-02aug16-en.pdf. The DNS Abuse Study measures common forms of abuse – such as spam, phishing, and malware distribution – in all gTLDs from 1 January 2014 until December 2016. See SIDN Labs and the Delft University of Technology (August 2017), Statistical Analysis of DNS Abuse in gTLDs Final Report, accessed 23 October 2017, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf
[10] Technical requirements change over time, which would make continual auditing difficult.
[11] ICANN, *Applicant Guidebook* (June 2012), Section 5-4.

protocols.[12] Applicants were required to pass all of these tests before a domain name would be delegated.

Upon delegation, registry operators were required to comply with the technical safeguards through their Registry Agreements with ICANN. The second safeguard mandated that new gTLD registries implement DNSSEC, with active monitoring of compliance and notices sent to non-compliant registries.[13] DNSSEC is a set of protocols intended to increase the security of the Internet by adding authentication to DNS resolution to prevent problems such as DNS spoofing[14] and DNS cache poisoning.[15] All new gTLDs are DNSSEC signed at the root level, which is not indicative of second level domain names in the zone being signed.[16]

For the third safeguard, the Registry Agreement for new gTLDs prohibits wildcarding to ensure that domain names only resolve for an exact match and that end users are not misdirected to another domain name by a synthesized response.[17] Complaints against registry operators for permitting wildcarding may be submitted to ICANN via an online interface.[18] A registry's use of wildcarding is easily detectable because every query will receive a response, instead of a "name error," even if the domain name is not valid.[19] This means that a user will be redirected to a similar domain name. It appears that all new gTLD operators are in compliance with this safeguard.[20]

To comply with the fourth safeguard, new gTLD registries are required to remove orphan glue records when presented with evidence that such records have been used in malicious conduct.[21] Unmitigated orphan glue records can be used for malicious purposes such as fast-flux hosting botnet attacks.[22] This requirement is reactive by design, but registry operators can make it technically impossible for orphan glue records to exist in the first place and some do. Since 2013 there have been no ICANN org complaints related to orphan glue records.[23]

Deleted: Compliance

[12] ICANN, "Pre-Delegation Testing (PDT)," accessed 2 February 2017, https://newgtlds.icann.org/en/applicants/pdt
[13] ICANN, "Registry Agreement," accessed 2 February 2017, https://www.icann.org/resources/pages/registries/registries-agreements-en, Specification 6, Clause 1.3.
[14] SANS Institute, *Global Information Assurance Certification Paper*, accessed 2 February 2017, https://www.giac.org/paper/gcih/364/dns-spoofing-attack/103863. DNS spoofing occurs "when a DNS server accepts and uses incorrect information from a host that has no authority giving that information" (p. 16).
[15] Sooel Son and Vitaly Shmatikov, "The Hitchhiker's Guide to DNS Cache Poisoning" (paper presented at the 6th International ICST Conference on Security and Privacy in Information Networks, Singapore, 7-9 September 2010), https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf. DNS cache poisoning occurs when the temporary cached data stored by a DNS resolver is intentionally altered to map DNS resolutions to IP addresses routed to invalid or malicious destinations (p. 1).
[16] ICANN, "TLD DNSSEC Report," accessed 26 April 2017, http://stats.research.icann.org/dns/tld_report/. This does not include .aero.
[17] ICANN, "Registry Agreement," Specification 6, Clause 2.2
[18] ICANN, "Wildcard Prohibition (Domain Redirect) Complaint Form," accessed 2 February 2017, https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form.
[19] https://www.icann.org/groups/ssac/documents/sac-015-en
[20] As of 1 January 2017, no complaints have been reported via this form. See also "DNSSEC Deployment Report," accessed 1 January 2017, https://rick.eng.br/dnssecstat/
[21] ICANN, "Registry Agreement," Specification 6, Clause 4.1
[22] ICANN Security and Stability Advisory Committee (March 2008), *SSAC Advisory on Fast Flux Hosting and DNS*, accessed 2 February 2017, https://www.icann.org/en/system/files/files/sac-025-en.pdf
[23] ICANN, Contractual Compliance Reports, https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en

For the fifth safeguard, Registry Agreements require new gTLD operators to create and maintain Thick WHOIS records for domain name registrations. This means that registrant contact information, along with administrative and technical contact information, is collected and displayed in addition to traditional Thin WHOIS data at the registry level.[24] ICANN org monitors adherence to the Thick WHOIS requirement on an active basis, for both reachability and format.[25] Syntax and operability accuracy are evaluated by the ICANN WHOIS Accuracy Reporting System (ARS) project.[26] The Impact of Safeguards chapter of this report further explains the ARS and related compliance issues. The CCTRT notes with concern that the availability of public WHOIS and indeed the very existence of Thick WHOIS as per this fifth safeguard is in jeopardy given the situation post May 25th 2018 with the implementation of the GDPR. The current change to WHOIS access policy applying globally, irrespective of where the Registrants or Registrars are located or whether they have any connection or nexus with the European Union is likely to have a significant impact on the level of DNS abuse if bad actors are able to carry out their nefarious activity unidentified.

Registry Agreements also require all new gTLD registry operators to post abuse contact details on their websites and to notify ICANN of any changes to contact information.[27] ICANN monitors compliance with this requirement and publishes statistics, including remediation measures, in its quarterly reports.[28] The Registry Agreements require registry operators to respond to well-founded complaints but do not mandate specific procedures for doing so. Consequently, there is no standard by which ICANN org can assess the particular means by which registry operators resolve complaints. There were 55 complaints related to abuse contact data in 2016,[29] 61 in 2015,[30] 100 in 2014,[31] and 386 in 2013.[32]

On the sixth safeguard, new gTLD operators are required via the Registry Agreement to make their zone files available to approved requestors via the Centralized Zone Data Service.[33] Centralizing these data sources enhances the ability of security researchers, IP attorneys, law enforcement agents, and other approved requestors to access the data without the need to enter into a contractual relationship each time. There were 19 complaints related to bulk zone file access in 2016,[34] 27 in 2015,[35] and 55 in 2014.[36] No data was available in the ICANN 2013 Contractual Compliance Report.

Deleted: Compliance

Comment [TD2]: Thought we needed something on WHOIS/GDPR here given the fifth safeguard

Formatted: Superscript

Deleted: compliance

[24] ICANN, "What are thick and thin entries?", accessed 2 February 2017, https://whois.icann.org/en/what-are-thick-and-thin-entries
[25] ICANN, "Registry Agreement," Specification 10, Section 4.
[26] ICANN, "WHOIS Accuracy Reporting System (ARS) Project Information," accessed 2 February 2017, https://whois.icann.org/en/whoisars
[27] ICANN, "Registry Agreement," Specification 6, Section 4.1.
[28] ICANN, "Contractual Compliance Reports 2016," accessed 2 February 2017, https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en
[29] https://www.icann.org/en/system/files/files/annual-2016-31jan17-en.pdf
[30] ICANN, "Contractual Compliance Reports 2015," accessed 2 February 2017, https://www.icann.org/resources/pages/compliance-reports-2015-04-15-en
[31] ICANN, "Contractual Compliance Reports 2014," accessed 2 February 2017, https://www.icann.org/resources/pages/compliance-reports-2014-2015-01-30-en
[32] ICANN, "Contractual Compliance Reports 2013," accessed 2 February 2017, https://www.icann.org/resources/pages/reports-2013-02-06-en
[33] ICANN, "Registry Agreement," Specification 4, Section 2.1; ICANN, "Centralized Zone Data Service," accessed 2 February 2017, https://czds.icann.org/en
[34] ICANN, "Contractual Compliance Reports 2016."

To enhance the stability of the DNS, ICANN created the Expedited Registry Security Request (ERSR) process, which permits registries "to request a contractual waiver for actions it might take or has taken to mitigate or eliminate" a present or imminent security incident.[37] As of 5 October 2016, ICANN reports that the ERSR has not been invoked for any new gTLD.[38]

In addition to the aforementioned safeguards, ICANN, in response to community input, proposed the creation of the High Security Zone Verification Program whereby gTLD registry operators could voluntarily create high security zones.[39] An advisory group conducted extensive research to determine standards by which registries would abide to be deemed a High Security Zone. However, the proposals never reached the implementation stage due to a lack of consensus.

The technical safeguards, enforced through contractual compliance, imposed requirements upon new gTLD registries and registrars that purportedly mitigated risks inherent in the expansion of the DNS. The CCTRT's DNS abuse study[40] provides insight into whether the overall implementation of these safeguards reduced the levels of DNS abuse compared to legacy gTLDs.

DNS Abuse Study

In preparation for the CCTRT's review of "safeguards put in place to mitigate issues involved in…the expansion" of gTLDs, ICANN issued a report analyzing the history of DNS abuse safeguards tied to the New gTLD Program.[41] In doing so, the report assessed the various ways to define DNS abuse. Some of the challenges to defining DNS abuse arise because of the various ways that different jurisdictions define and treat DNS abuse. Certain activities are considered to be abusive in some jurisdictions but not others. Some of these activities, such as those solely focused on intellectual property violations, are interpreted differently not only in terms of substance but also in terms of remedies available in the applicable jurisdiction. Another challenge is the lack of data available regarding certain types of abuse. Nonetheless, there are core technical abuse behaviors for which there is both consensus and significant data available. These include spam, phishing, malware distribution, and botnet command and control.

The ICANN report acknowledged the absence of a comprehensive comparative study of DNS abuse in new gTLDs versus legacy gTLDs. Nonetheless, some metrics suggest that a high percentage of new gTLDs might suffer from DNS abuse. For example, Spamhaus consistently ranks new gTLDs amongst its list of "The 10 Most Abused Top-Level Domains" based on the ratio of the number of domain names associated with abuse versus the number of domain

---

[35] ICANN, "Contractual Compliance Reports 2015."
[36] ICANN, "Contractual Compliance Reports 2014."
[37] ICANN, "Expedited Registry Security Request Process," accessed 2 February 2017, https://www.icann.org/resources/pages/ersr-2012-02-25-en.
[38] ICANN Registry Services, email discussion with Review Team, July 2017.
[39] ICANN (18 November 2009), *A Model for a High-Security Zone Verification Program*, accessed 2 February 2017, https://archive.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf; icann.org, "Public Comment: High Security Zone TLD Final Report," 11 March 2011, https://www.icann.org/news/announcement-2011-03-11-en
[40] ICANN, *Request for Proposal*. SIDN Labs and the Delft University of Technology, "DNS Abuse in gTLDs".
[41] ICANN, *New gTLD Program Safeguards* (2016)

names seen in a zone.[42] Whereas, using a different methodology, previous research from Architelos and the Anti-Phishing Working Group named .com the TLD with the largest number of domain names associated with abuse.[43] A 2017 report from PhishLabs also concluded that half of all phishing sites are in the .com zone, with new gTLDs comprising 2% of all phishing sites.[44] However, the same report found that phishing sites in new gTLD zones have increased 1000% since the previous year. This appears to have coincided with an overall significant increase in phishing attacks during 2016.[45]

Domain names are often a key component of cybercrime and enable cybercriminals to quickly adapt their infrastructure.[46] For example, spam campaigns often correlate with phishing and other cybercrime.[47] Domain names are also used to assist with malware distribution and botnet command and control. Troubling statistics and incidents observed by network operators have led to perceptions that many new gTLDs offer little more than abuse.[48] In fact, some Internet security companies have advised customers to block all network traffic to and from specific TLDs.[49] Such practices run counter to ICANN's Universal Acceptance efforts. Although 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

Deleted: nothing

Deleted: Whereas, beyond the safeguards,

Deleted: registries and registrars

Deleted: to

Deleted: e

Deleted: , which

[42] Spamhaus, "The World's Most Abused TLDs," accessed 2 February 2017, https://www.spamhaus.org/statistics/tlds/

[43] Anti-Phishing Working Group (29 April 2015), *Phishing Activity Trends Report: 4th Quarter 2014*, accessed 2 February 2017, http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf; Architelos (June 2015), *The NameSentry℠ Abuse Report: New gTLD State of Abuse 2015*, accessed 2 February 2017, http://domainnamewire.com/wp-content/Architelos-StateOfAbuseReport2015.pdf

[44] PhishLabs, 2017 Phishing Trends & Intelligence Report, p. 23-24, https://pages.phishlabs.com/rs/130-BFB-942/images/2017%20PhishLabs%20Phishing%20and%20Threat%20Intelligence%20Report.pdf. New gTLDs comprised 8% of the overall TLD market during this time period when .tk is excluded from the data universe. See Kevin Murphy, Phishing in new gTLDs up 1,000% but .com still the worst, Domain Incite, Feb. 20, 2017, http://domainincite.com/21552-phishing-in-new-gtlds-up-1000-but-com-still-the-worst

[45] Lindsey Havens, APWG & Kaspersky Research Confirms Phishing Trends & Intelligence Report Findings, March 2, 2017, available at https://info.phishlabs.com/blog/apwg-kaspersky-research-confirms-phishing-trends-investigations-report-findings; Darya Gudkova, et. al., Spam and phishing in 2016, Kaspersky Security Bulletin, February 20, 2017, available at https://securelist.com/kaspersky-security-bulletin-spam-and-phishing-in-2016/77483/; APWG, Phishing Trends Activity Report, Feb. 23, 2017, available at http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

[46] Symantec (April 2015), *Internet Security Threat Report*, accessed 2 February 2017, https://its.ny.gov/sites/default/files/documents/symantec-internet-security-threat-report-volume-20-2015-social_v2.pdf

[47] Richard Clayton, Tyler Moore, and Henry Stern, "Temporal Correlations between Spam and Phishing Websites" (paper presented at the LEET'09 Proceedings of the 2nd USENIX Conference on Large-Scale Exploits and Emergent Threats, Boston, MA, 21 April 2009) https://www.cl.cam.ac.uk/~rnc1/leet09.pdf.

[48] Tom Henderson, The new internet domains are a wasteland, Network World, July 5, 2016, http://www.networkworld.com/article/3091754/security/the-new-internet-domains-are-a-wasteland.html

[49] In a 2015 report, Blue Coat advised network operators to block all traffic to or from ".work, .gq, .science, .kim and .country". See Blue Coat, DO NOT ENTER Blue Coat Research Maps the Web's Shadiest Neighborhoods, September 2015, p. 7, available at https://www.bluecoat.com/documents/download/895c5d97-b024-409f-b678-d8faa38646ab

ICANN-contracted parties and hence not directly subject to ICANN's enforcement authority over standard contract requirements, including the safeguards under discussion in this report.[50]

In light of the dynamic DNS environment, snapshots of new gTLD abuse do not account for the full variety of registration rules and safeguards in the 1000+ new gTLDs that have been delegated since 2013. Accordingly, it is difficult to find definitive distinctions between abuse rates in legacy gTLDs compared to new gTLDs without performing a comprehensive assessment. To the extent possible, the CCTRT has sought to measure the effectiveness of the technical safeguards developed for the New gTLD Program in mitigating various forms of DNS abuse. As part of this process, the CCTRT commissioned a comprehensive DNS abuse study to analyze levels of technical abuse[51] in legacy and new gTLDs, to inform this review and potentially serve as a baseline for future analysis.[52] The ICANN-selected vendor, a joint team comprised of researchers from Delft University of Technology in the Netherlands (TU Delft) and the Foundation for Internet Domain Registration in the Netherlands (SIDN), delivered a final report on 9 August 2017.[53]

<u>DNS Abuse Study Methodology</u>

The DNS Abuse Study relied upon zone files, Whois records, and 11 distinct domain name blacklist feeds to calculate rates of technical DNS abuse from 1 January 2014[54] through the end of 31 December 2016.

The analysis includes:

a. Absolute counts of abusive domains per gTLD and registrar from 1 January 2014 until 31 December 2016, taking into account sunrise periods and dates of general availability for registration
b. Abuse rates, based on an "abused domains per 10,000" ratio (as a normalization factor to account for different TLD sizes), per gTLD and registrar from 1 January 2014 until 31 December 2016
c. Abuse associated with privacy and proxy services
d. Geographic locations associated with abusive activities
e. Abuse levels distinguished by "maliciously registered" versus "compromised" domains
f. An inferential statistical analysis on the effects of security indicators and the structural properties of new gTLDs, (i.e. number of DNSSEC-signed domains, parked domains,

---

[50] Secure Domain Foundation, The Cost of Doing Nothing, June 2015, p. 8, https://securedomain.org/Documents/SDF_Report1_June_2015.pdf; Registrars must impose flow down contractual requirements onto resellers with which they contract. However, the resellers are not ICANN-accredited. See Registration Accreditation Agreement, 3.12 Obligations Related to Provision of Registrar Services by Third Parties

[51] Phishing, malware hosting, and spam. Initially, the RT sought to include botnet domains in the analysis. However, discrete historical data on botnets was unavailable for the timeframe of the study. Nonetheless, botnet associated domain names (hosting and command and control) were included in the malware blacklists.

[52] ICANN, Request for Proposal.

[53] SIDN Labs and the Delft University of Technology, "DNS Abuse in gTLDs".

[54] The first new gTLD delegations began in October 2013.

Deleted: I

Deleted: hundreds of

Deleted: ascertain

Deleted: and

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted: List Paragraph, Indent: Left: 0", First line: 0"

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted: List Paragraph, Indent: Left: 0", First line: 0"

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted: List Paragraph, Indent: Left: 0", First line: 0"

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted: Indent: Left: 0", First line: 0"

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted: Indent: Left: 0", First line: 0"

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

number of domains in each new gTLD, as well as the number of domains resolving to content)

DNS Abuse Study Findings

The report makes many significant findings regarding DNS abuse associated with new gTLDs as compared to legacy gTLDs. Generally, the DNS Abuse Study indicates that the introduction of new gTLDs did not increase the total amount of abuse for all gTLDs. Nonetheless, the results demonstrate that the nine aforementioned safeguards alone, do not guarantee a lower rate of abuse in each new gTLD compared to legacy gTLDs. Instead, factors such as registration restrictions, price, and registrar-specific practices seem more likely to affect abuse rates.[55]

Abuse is migrating to new gTLDs

Legacy gTLDs still account for most domain name registrations and, perhaps consequently, the highest volume of phishing and malware associated domain names.[56] Nonetheless, the overall rates of abuse[57] in legacy and new gTLDs were similar by the end of 2016. Moreover, there are distinct trends with regard to specific types of abuse. For example, by the end of 2016, spam registrations in legacy gTLDs had declined while those in new gTLDs saw a significant increase. In the last quarter of 2016, 56.9 of every 10,000 legacy gTLD domain names were on spam blacklists whereas the rate for new gTLD domain names was 100 times more: 526.6 domain names per 10,000 registrations.[58]

Some abuse trends showed overlap. The top five legacy gTLDs with the highest rates of phishing also had the highest rates of domain names tied to malware distribution.[59] Phishing and malware abuse rates in legacy gTLDs more often resulted from compromised domain names rather than malicious registrations. There are much higher rates of compromised legacy gTLD domain names than new gTLDs.

Specific to malware distribution,[60] the top 5 new gTLDs with the highest rates of abusive domain names were .top, .wang, .win, .loan, and .xyz. Since the end of 2015, the .top TLD has had the highest rate of abusive registrations for **all legacy and new gTLDs**.[61] Each of these TLDs offered low-priced registrations, usually at levels lower than those for a .com registration.

The DNS Abuse Study distinguishes between domain names registered specifically for malicious purposes and domain names registered for legitimate purposes that were subsequently compromised.[62] The results of the study indicate that the introduction of new gTLDs has corresponded with a decrease in the number of spam-associated registrations in legacy gTLDs, and an increase in the number of spam-associated registrations in new gTLDs.[63] This, along with the fact that the total number of spam registrations remains stable,[64] suggests

[55] P.24-25
[56] P.24
[57] Defined by the number of abusive registrations per total registrations associated with a contracted party
[58] p.24
[59] p.12
[60] Based on the StopBadware data feed
[61] p.13
[62] Compromised domain names include domain names for which the domain name registration or the website may have been hacked.
[63] p. 2
[64] See DNS Abuse Study, figures 24, 36, and 38, corresponding to the absolute number of spam domains for different spam feeds

Deleted: with

Deleted: ,
Deleted: and

Formatted: Font:Bold
Deleted:

Deleted:
Deleted: while
Deleted: malicious
Deleted: have increased

that perhaps miscreants are shifting from registering domain names in legacy gTLDs to new gTLDs. Within this trend, there are specific new gTLDs that serve as primary targets of opportunity for abusive registrations, whether due to lax registration policies and abuse enforcement or low price. In fact, some registrars are almost entirely associated with abusive, rather than legitimate, registrations.

Abuse is not universal in new gTLDs

Even though abuse is growing in new gTLDs, it is by no means rampant across all new gTLDs. Instead, by the end of 2016, this phenomenon was highly concentrated. Five new gTLDs, exhibiting the highest concentration of domain names used in phishing attacks (APWG last quarter 2016), accounted for 58.7% of all blacklisted new gTLD domain names.[65] Whereas, Spamhaus blacklisted at least 10% of all domain names registered within only 15 new gTLDs. And, approximately a third of all new gTLDs did not have a single instance of abuse, as reported on blacklists, in the final quarter of 2016.

Two registrars highlighted by the Study had overwhelming rates of abuse. Alarmingly, more than 93% of the new gTLD registrations sold by Nanjing Imperiosus Technology, based in China, appeared on SURBL's blacklists. For much of 2016, abuse rates associated with this registrar grew at significant rates. ICANN eventually suspended Nanjing in January 2017, citing its failure to pay fees in compliance with the RAA.[66] However, ICANN did not rely upon the sustained, unabated, high abuse rates as the reason for its suspension of Nanjing, which in and of itself may not have violated the RAA.

Another registrar, Alpnames Ltd., based in Gibraltar, was associated with a high volume of abuse from the .science and .top domain names. The Study notes that this registrar used price promotions that offered domain name registrations for $1 USD or sometimes even free.[67] Moreover, Alpnames permitted registrants to randomly generate and register 2,000 domain names in 27 new gTLDs in a single registration process. Bulk domain names using domain generation algorithms are commonly associated with cybercrime.[68] At the time of this report, Alpnames remained ICANN-accredited. There is no contractual prohibition or safeguard against the bulk registration of domains.

Many attributes can play a role in the volume or rate of abuse in a particular TLD. In terms of absolute size, new gTLDs are no different than legacy gTLDs in that the larger the size of the TLD, the higher the total number of domain names associated with abuse.[69] However, analyzing attributes of cross-TLD registry operators, suggests that many of the operators associated with the highest rates of abuse had low-priced domain registration offerings.

The Study concluded that domain names registered for malicious purposes often contained strings related to trademarked terms.[70] Specifically, of the 88 .top domain names associated with abuse in the fourth quarter of 2015, 75 of them included exact or misspelled versions of Apple, iCloud, or iPhone, implying that the domain names were used in a phishing campaign

[65] P.11
[66] https://www.icann.org/uploads/compliance_notice/attachment/895/serad-to-hansmann-4jan17.pdf
[67] p.20
[68] Aditya K. Sood, Sherali Zeadally, "A Taxonomy of Domain-Generation Algorithms", IEEE Security & Privacy, vol. 14, no. , pp. 46-53, July-Aug. 2016, doi:10.1109/MSP.2016.76
[69] p.15
[70] p. 12

Deleted: suffering from
Deleted: Nevertheless
Deleted: y
Deleted: were not the actionable reason.
Deleted: Whereas
Deleted: the Study
Deleted:
Formatted: English (US)
Formatted: Font:10 pt, English (US)
Formatted: English (US)
Formatted: Font:10 pt, English (US)
Formatted: English (US)

against users of Apple, Inc. products and services. These registrations should have raised reasonable suspicions at the time of registration but were nonetheless delegated and later associated with abuse.

The Study found a statistically weak but positive correlation between the number of parked domains in a new gTLD zone and the rate of abuse.[71] Oddly, there was also a weak positive correlation between the number of DNSSEC signed domain names and abuse in a new gTLD zone.[72] The use of privacy/proxy services to mask registrant Whois data is more common in legacy than new gTLDs. Regardless, the Study did not find any statistically significant relationship between the use of such services and domain name abuse. Above all, the Study identified a relatively stronger correlation between restrictive registration policies and lower rates of abuse. Nonetheless, even new gTLDs with open registration policies varied greatly in abuse rates, suggesting that other key variables, such as price and differences in registry and registrar anti-abuse practices may also influence abuse rates.

DNS abuse is not random

Price and registration restrictions appear to affect which registrars and registries cybercriminals will choose for DNS abuse, making low-priced domain names with low barriers to registration attractive attack vectors.[73] Nonetheless, these same qualities, of low prices and no registration restrictions, may be appealing for registrants with legitimate interests and further the overarching goal of a free and open Internet. High prices and/or onerous registration restrictions would not be compatible with many business models focused on open registration and low prices. However, monetary incentives based on fees paid to ICANN may nevertheless provide an impetus for such contracted parties to better prevent systemic DNS abuse by proactively screening registrations and detecting malfeasance.[74] For example, there is precedent for ICANN adjusting its fee structure to address behavior harmful to the DNS, such as abolishing the automatic fee refund for domain tasters.[75] Similarly, the CCT Review Team proposes the development of mandates as well as incentives to reward best practices preventing technical DNS abuse and strengthening the consequences for culpable or complacent conduits of technical DNS abuse. These recommendations may be applicable to curb other misuse of domain names to the extent the community reaches consensus on other forms of DNS abuse.

We are concerned at the high levels of DNS abuse concentrated in a relatively small number of registries and registrars and geographic regions. Of particular concern, this DNS abuse appears to have continued unremedied for an extended amount of time in some cases.

Recommendations 1 to 5 are designed to address the reality that the new gTLD safeguards did not, on their own, prevent technical DNS abuse. In addition to means available today to prevent and mitigate DNS abuse, we propose new incentives and tools to combat abuse that will:

---

[71] p.16

[72] p.16

[73] p. 25

[74] This is a best practice in other parts of the Internet infrastructure ecosystem. For example, the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) has encouraged hosting providers to adopt a "vetting process to proactively identify malicious clients before they undertake abusive activities" and to take measures to "prevent abusers from becoming customers," M3AAWG, Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers, March 2015, p. 4, available at https://www.m3aawg.org/sites/default/files/document/M3AAWG_Hosting_Abuse_BCPs-2015-03.pdf

[75] http://www.washingtonpost.com/wp-dyn/content/article/2008/01/30/AR2008013002178.html

Deleted: were presumably

Deleted: u

Deleted: among

Deleted: ,

Deleted:

Deleted: easy

Deleted: s

Deleted: Consequently

Deleted: exist

Deleted: registry and registrar operators

Deleted: price

Deleted: ;

Deleted: gone on

Formatted: English (US)

Formatted: Font:10 pt, English (US)

Formatted: English (US)

Formatted: English (US)

Formatted: Font:10 pt, English (US)

Formatted: English (US)

a. Encourage and incentivize pro-active abuse measures as per Recommendation 1

b. Introduce measures to prevent technical DNS abuse as per Recommendation 2

c. Ensure that the data collection is ongoing and acted upon as per Recommendation 3

d. Consider an additional mechanism where, despite Recommendations 1, 2 and 3, registry operators or registrars that have not effectively mitigated the technical DNS abuse. A dispute resolution process should be considered to enable injured parties to take action as in Recommendation 4 (note this lacks Review Team consensus. See Minority Statement in Appendix 6). Indeed, there should be more emphasis on ICANN org where further steps are needed to address high levels of DNS abuse. If the level of abuse has not been reduced to acceptable levels, as per the commitment of the Registry or Registrar, then the failure of the contracted party to implement the plan should constitute a breach of the RAA/RA. If the contracted parties commit to not exceeding a minimum DNS abuse, then the DADRP become less necessary, and less likely to be used. This translates to positive outcomes for all parties due to decreased levels of DNS Abuse.

e. Make available reseller information associated with registrations per Recommendation 5.

Recommendation A: Consider directing ICANN org to negotiate amendments to existing Registry Agreements, or in consideration of new Registry Agreements associated with subsequent rounds of new gTLDs, to include provisions in the agreements to provide incentives, including financial incentives, for registries, especially open registries, to adopt proactive anti-abuse measures.[76]

Rationale/related findings: ICANN is committed to maintaining "the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet."[77] The new gTLD safeguards alone do not prevent technical abuse in the DNS and have consequently failed to meet their intended goal in preventing the abuse phenomenon from spreading to new gTLDs. The CCT Review Team's analysis and the DNS Abuse Study indicate that abuse rates are correlated to registration restrictions imposed on registrants and registration prices (i.e., abuse rates tend to go down with increased registration restrictions and

[76] The CCTRT looked for examples of practices that could assist in proactively minimizing abuse. One such example has been proposed by EURid, the operator of the .EU registry, which will soon test a delayed delegation system. See https://eurid.eu/en/news/eurid-set-to-launch-first-of-its-kind-domain-name-abuse-prevention-tool/ and https://eurid.eu/media/filer_public/9e/d1/9ed12346-562d-423d-a3a4-bcf89a59f9b4/eutldecosystem.pdf. This process will not prevent registrations but instead delay activation of a registration if a domain name is identified as being potentially abusive by machine learning algorithms. Future review teams could study this effort to consider its effectiveness and whether it could serve as a potential innovative model to help foster trust and a secure online environment. In addition, the .XYZ registry may provide another example of proactive measures to combat abuse. The .xyz registry purports to have a zero-tolerance policy toward abuse-related activities on .xyz or any of their other domain extensions using a sophisticated abuse monitoring tool enabling proactive monitoring and detection in near real-time, suspending domains engaging in any of the abusive activities set out. Future review teams could explore the effectiveness of this approach by examining abuse rates over time and comparing the levels of abuse both before and after this policy.

[77] ICANN, Bylaws for Internet Corporation for Assigned Names and Numbers, Section 1.2(a)(i), available at https://www.icann.org/resources/pages/governance/bylaws-en/#article1

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted: List Paragraph, Outline numbered + Level: 3 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted: List Paragraph

Formatted: List Paragraph, Outline numbered + Level: 3 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted

Formatted: List Paragraph, Outline numbered + Level: 3 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Formatted

Formatted … [1]

Deleted: Compliance

Formatted … [2]

Deleted: and

Deleted:

Deleted: a clean-up is identified as being necessary

Formatted … [3]

Deleted: come down

Formatted … [4]

Formatted … [5]

Deleted: a level of obligation is there

Formatted … [6]

Formatted … [7]

Deleted: not only does

Deleted: but also

Formatted … [8]

Formatted … [9]

Formatted: Indent: Left: 0.5", No bullets or numbering

Formatted … [10]

Formatted … [11]

Deleted: ,

Deleted: in its discussions with registries,

Deleted: negotiations

Deleted: to

Deleted: .

Deleted: A

Deleted: may influence rates too

high domain name prices). Some registries are inherently designed to have strict registration policies and/or high prices. However, a free, open, and accessible Internet will invariably include registries with open registration policies and low prices that must adopt other measures to prevent technical DNS abuse. Registries that do not impose registration eligibility restrictions can nonetheless reduce technical DNS abuse through proactive means such as identifying repeat offenders, monitoring suspicious registrations, and actively detecting abuse instead of merely waiting for complaints to be filed. Therefore, ICANN should incentivize and reward operators that adopt and implement proactive anti-abuse measures identified by the community as as effective for reducing technical DNS abuse. Operators that have already adopted such measures, prior to the creation of an incentive program, should be rewarded as well.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG

Prerequisite or Priority Level: High

Consensus within team: Yes

Details: The ICANN Board should consider urging ICANN org to negotiate with new and legacy gTLD registries to include in the registry agreements fee discounts available to registry operators with open registration policies that implement proactive measures to prevent technical DNS abuse in their zone. ICANN should verify compliance with incentive programs to ensure bad actors are not receiving incentives despite acting in bad faith. It is not intended that the adoption of proactive anti-abuse measures in exchange for incentives, should form the basis of an argument to shift liability for underlying abuse incidents to the registry operator.

Success Measure: More registries, even though with open registration policies, will adopt proactive anti-abuse measures such that there is a decrease in the overall rates of technical DNS abuse in their zones.

Recommendation B: Consider directing ICANN org, in its discussions with registrars and registries, to negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements to include provisions aimed at preventing systemic use of specific registrars for technical DNS abuse.

Rationale/Related Findings: Current policies focus on individual abuse complaints. However, registrars and registry operators associated with extremely high rates of technical DNS abuse have continued to operate and faced little incentive to prevent technical DNS abuse. Moreover, there currently exist few enforcement mechanisms to prevent systemic domain name abuse associated with resellers. Published research, cybersecurity analysis, and DNS abuse monitoring tools highlight concentrated, systemic DNS abuse for which there are no adequate, actionable remedies. Systemic use of particular registrars and registries for technical DNS abuse threatens the security and stability of the DNS, the universal acceptance of TLDs, and consumer trust.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG

Prerequisite or Priority Level: High

Deleted: the implementation of
Deleted: such registry operators to
Deleted: in
Deleted: to
Deleted: e
Deleted: in open gTLDs
Deleted: Compliance
Deleted: initiatives
Deleted: for
Deleted: to
Formatted: Font:Bold
Deleted: ing

Consensus within team: Yes

Details: The ICANN Board should consider directing ICANN org to negotiate amendments to the Registrar Accreditation Agreement and Registry Agreement provisions aimed at preventing systemic use of specific registrars for technical DNS abuse. Such language should impose upon registrars, and, through down-stream contract requirements their affiliated entities such as resellers, a duty to mitigate technical DNS abuse, whereby ICANN may suspend registrars and registry operators found to be associated with unabated, abnormal and extremely high rates of technical abuse. It is important for ICANN Org to gather relevant data, conduct analysis, and act on actionable information. Accordingly, ICANN should initiate an investigation into a contracted party's direct or indirect (such as through a reseller) involvement with systemic technical abuse and take whatever remedial actions are warranted if they receive and verify information, whether or not through a formal complaint, indicating unabated, abnormal, and extremely high rates of technical abuse. Upon making a finding and contacting the contracted party, such findings may be rebutted upon sufficient proof that the findings were materially inaccurate. The following factors may be taken into account when making a determination: whether the registrar or registry operator 1) engages in proactive anti-abuse measures to prevent technical DNS abuse, 2) was itself a victim in the relevant instance, 3) has since taken necessary and appropriate actions to stop the abuse and prevent future systemic use of its services for technical DNS abuse.

Success Measure: Contractual language is adopted which empowers ICANN to investigate and engage in enforcement actions against registries and registrars associated with systemic technical abuse such that there are no contracted parties serving as enablers of systemic technical abuse for which ICANN cannot bring an enforcement action.

Recommendation C: Further study the relationship between specific registry operators, registrars and DNS abuse by commissioning ongoing data collection, including but not limited to, ICANN Domain Abuse Activity Reporting (DAAR) initiatives. For transparency purposes, this information should be regularly published, ideally quarterly and no less than annually, in order to be able to identify registries and registrars that need to come under greater scrutiny, investigation, and potential enforcement action by ICANN org. Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remediate problems identified, and define future ongoing data collection.

Rationale/Related Findings: The DNS Abuse Study commissioned by the CCT-RT identified extremely high rates of abuse associated with specific registries and registrars as well as registration features, such as mass registrations, which appear to enable abuse. Moreover, the Study concluded that registration restrictions correlate with abuse, which indicates that there are many factors to consider and analyze in order to extrapolate cross-TLD abuse trends for specific registry operators and registrars. The DNS Abuse Study has highlighted certain behaviors that are diametrically opposed to encouraging consumer trust in the DNS. Certain registries and registrars appear to either positively encourage or at the very least willfully ignore DNS abuse. Such behavior needs to be identified rapidly and acted upon quickly by ICANN org, as determined by the facts and evidence presented. The DNS Abuse Study, which provided a benchmark of technical abuse since the onset of the new gTLD program, should be followed up with regular studies so that the community is provided current, actionable data on a regular basis to inform policy decisions.

Deleted: a,

Deleted: Compliance

Deleted: ICANN must base such findings on multiple verifiable reliable evidence and sources

Deleted: and s

Deleted: by the registrar

Formatted: Font:Bold, Font color: Text 1

Deleted: higher priority

Deleted: Compliance

Deleted: means

Deleted: for which to account

Deleted:

Deleted: action must be taken

Deleted: compliance

Deleted: deemed necessary

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG, SSR2 Review Team.

Prerequisite or Priority Level: High

Consensus within team: Yes

Details: The additional studies need to be of an ongoing nature, collecting relevant data concerning DNS abuse at both the registrar and registry level. The data should be regularly published, thereby enabling the community and ICANN org in particular to identify registries and registrars that need to come under greater compliance scrutiny and thereby have such behavior eradicated.

Success Measure: Comprehensive, up-to-date technical DNS abuse data is readily available to the Community so that problems can be identified and data-driven policy initiatives can be measured for efficacy.

Recommendation D: A DNS Abuse Dispute Resolution Policy ("DADRP") should be considered by the community to deal with registry operators and registrars that are identified as having excessive levels of technical abuse. ICANN needs the power to take down abusive domain names . The RAA needs to be amended to enable ICANN Compliance to deal with registry operators or registrars that allow excessive levels of domain name abuse. The DADRP would be envisaged as a community empowerment tool, for combating abuse, to be set up and implemented within 12 months of the date of the CCTRT Final Report. What is considered an excessive level needs to be defined, but it could, for example be over 10% of their domain names are blacklisted domain names. Such registry operators or registrars should in the first instance be required to a) submit an explanation to ICANN org for the high rate of DNS abuse, b) commit to remedy that abuse within a certain time period, and c) incorporate proactive anti-abuse measures within a certain time period. Failure to comply will result in a DADRP being available to any party injured by the abuse in question, should ICANN not take any action themselves.

Rationale/Related Findings: The DNS Abuse Study commissioned by CCT-RT identified extremely high rates of abuse associated with specific registrars and registries. Changes to Whois accessibility may inhibit third party anti-abuse efforts, and it is important for the community to have a recourse mechanism against entities in the event that ICANN Compliance is unable to for whatever reason. It is critical to have a mechanism to deal with this abuse. Abusive registrations threaten the security and stability of the DNS, affecting end users around the globe, and this would provide an additional arm to help combat that abuse. Indeed, this goes back to the situation prior to the approval of the New gTLD Program, when ICANN invited feedback from the cybersecurity community on DNS abuse and the risks posed from the expansion in the DNS name space.[78] One of the specific areas of concern identified by the community was how do we ensure that "bad actors" do not run registries? This Recommendation is a fail safe if bad actor registries and registrars are identified and where

[78] "ICANN (3 October 2009), *Mitigating Malicious Conduct*, accessed 9 November 2016, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf. Feedback came from groups such as the Anti-Phishing Working Group (APWG), Registry Internet Safety Group (RISG), the Security and Stability Advisory Community (SSAC), Computer Emergency Response Teams (CERTs), the banking/financial and wider Internet security communities.

Deleted: compliance

Deleted: .

Formatted: Font:Bold, Font color: Text 1

Formatted: Font color: Text 1

Comment [TD3]: Highlighting the RAA issues and need for community empowerment tool.

Comment [TD4]: What is excessive needs to be discussed in the sub team

Deleted: (

Deleted: to define, e.g.

Deleted:)

Deleted: i

Deleted: Compliance

Deleted: why this is

Deleted: clean up

Deleted: / or

Comment [TD5]: Seeking to define (loosely as not our role to set out the specifics) who would bring a complaint

Deleted: adopt stricter registration policies

Formatted

Deleted:

Deleted: important

Deleted: , particularly if it's prevalent in certain registries.

Deleted: behavior

Comment [TD6]: Suggested raison d'etre based on first part of our DNS abuse section.

Deleted: needs to be eradicated from the DNS

ICANN Compliance may not be, for whatever reason, in a position to deal with the abuse concentrated in those registries or registrars. When the community looks at this recommendation we would flag that re-sellers and their roles in any concentrated abuse at a registry or registrar should also be considered and once the DADRP is implemented suitable clauses should be in place in the respective contracts where resellers can be terminated by the registrar concerned if they are the source of the abusive domain name registrations. Moreoever the recent changes to the WHOIS system has caused an unprecedented reaction by brand owners and law enforcement and the previous ability to effectively self help by identifying the culprit behind the malicious behaviour may no longer be available, or is at the very least significantly hindered by the lack of public WHOIS and this further underlines the need for such a mechanism.

The need for such a community empowerment tool, is demonstrated in the case study set out at Annex X.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, the Subsequent Procedures PDP WG and the SSR2 Review Team

Prerequisite or Priority Level: High

Consensus within team: Majority consensus but not unanimity (see Minority Statement in Appendix 6.1 Minority Statements)

Details: Contract enforcement is one route to dealing with this high level of DNS abuse, by enforcing existing and future provisions of the Registrar Accreditation Agreement to prevent systemic use of specific registrars for technical DNS abuse as per Recommendation 2. However, in addition, a specific DADRP should be considered as it could also help in deal with such DNS abuse, could serve as a significant deterrent, and help prevent or minimize such high levels of DNS abuse. Such a procedure could apply to registry operators or registrars that are identified as having excessive levels of abuse. Excessive levels of abuse (could be defined, for example where a registry operator has over 10% of their domain names blacklisted by one or more heterogeneous blacklists (e.g. StopBadware SDP, APWG, Spamhaus, Secure Domain Foundation, SURBL and CleanMX). A DADRP should set out specific penalties. Examples from the DNS Abuse Study of new gTLDs with over 10% of their domain names blacklisted, according to Spamhaus for example are .science (51%), .stream (47%), .study (33%), .download (20%), .click (18%), .top (17%), .gdn (16%), .trade (15%), .review (13%), and .accountant (12%). Thus, each of these registries would be obliged to review their second level domain names being used for DNS abuse and explain the reasons for the excessive DNS abuse, commit to remedying the abuse within a certain timeframe, and adopt stricter registration policies if necessary to ensure that relevant contract terms exist to effectively deal with such registrations. If the domain names at issue are not responded to in a satisfactory and timely manner, and in the event ICANN does not take immediate action, then a DADRP may be brought by an affected party. The process should involve a written complaint to the registry, time allotted for a response from the registry, and an oral hearing. Final decisions should be issued by an expert panel which could recommend one or more enforcement mechanisms to be agreed upon by the community.

For purposes of this recommendation, a registrar acting under the control of a registry operator would also be covered by the DADRP. Hence, it would be important to ensure that "registry

Comment [TD7]: Covering resellers for discussion

Comment [TD8]: WHOIS changes post May 25th make this all the more necessary

Formatted: Font:

Deleted: ICANN Compliance

Deleted: any amendments to

Deleted: be very

Deleted: ful

Deleted: ing

Deleted: and it

Deleted: also

Deleted: Registry

Deleted: to

Deleted: SCIENCE

Deleted: STREAM

Deleted: STUDY

Deleted: DOWNLOAD

Deleted: CLICK

Deleted: TOP

Deleted: GDN

Deleted: TRADE

Deleted: REVIEW

Deleted: ACCOUNTANT

Deleted: should

Deleted: why

Deleted: this is

Deleted: cleaning these up

Deleted: there exist

Deleted: ual

Deleted: handle

Comment [TD9]: Needs the negative

Comment [TD10]: Underlines needs to be timely

Deleted: not cleaned up

Deleted: ily

Deleted: Compliance

Deleted: so

Deleted: is

operator" shall include entities directly or indirectly controlling, controlled by, or under common control with, a registry operator, whether by ownership or control of voting securities, by contract or otherwise where 'control' means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether by ownership or control of voting securities, by contract or otherwise. The evolution of ICANN Compliance and the RAA should be considered and if the community is of the view that future revisions to the terms of the RAA give ICANN Compliance the necessary tools to deal with DNS abuse effectively then the DADRP can and should be revisited. In any event, the DADRP should be revisited within 24 months of coming into existence.

Recommendation E: ICANN should collect data about and publicize the chain of parties responsible for gTLD domain name registrations.

Rationale/Related Findings: At present, there is no consistent mechanism for determining all of the ICANN contracted and non-contracted operators associated with a gTLD domain name registration. Whois records often do not distinguish between registrars and resellers. The DNS Abuse Study commissioned by the CCT-RT, for example, was unable to discern resellers from registrars to determine the degree to which technical DNS abuse rates may be driven by specific-resellers may affect levels of technical DNS abuse. This data should be available to enhance data-driven determinations necessary for recommendations proposed the CCT-RT, supplement new gTLD program safeguards, and improve ICANN contractual compliance determinations.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, the Subsequent Procedures PDP WG, the SSR2 Review Team, Registration Directory Service Review Team

Prerequisite or Priority Level: High

Consensus within team: ???

Details: Whois information is an important source of data for technical DNS abuse analysis. Safeguards, such as the Thick Whois requirements, do not mandate that resellers are listed in Whois records. Consequently, the full chain of parties to a registration transaction is not readily discernable. Without such information, it is difficult to determine the extent to which technical abuse is correlated to individual resellers, rather than registrars. For example, with such data hidden, it would be possible for a reseller associated with extremely high levels of abuse to remain in operation under a registrar with relatively normal levels of technical abuse. This would, in effect, permit systemic technical abuse by a non-contracted party. Although the reseller is theoretically bound by flow down contract requirements, in practice this systemic DNS abuse often remain difficult to attribute and tends to goes unabated. Whereas, collecting and publicizing such information would enable end users to readily determine the registry, registrar, and reseller associated with a domain name registration to remove the mask of parties responsible for mitigating technical DNS abuse. This would allow for more granular DNS

Comment [TD11]: Seeking to cover evolution of the RAA which may mean the DADRP no longer needed.

Deleted: T

Deleted: C

Deleted: C

Deleted: obfuscated

Deleted: , though

Deleted: to

Deleted: opaqueness

abuse analysis and transparency for Internet users, thereby enhancing community accountability efforts, and contractual compliance enforcement.

Formatted: Font:(Default) Calibri, Font color: Text 1

Page 11: [1] Formatted	Drew Bagley	2/27/18 4:45:00 PM

List Paragraph, Outline numbered + Level: 3 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Page 11: [2] Formatted	Drew Bagley	2/27/18 4:44:00 PM

Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Page 11: [3] Formatted	Drew Bagley	2/27/18 4:44:00 PM

Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Page 11: [4] Formatted	Drew Bagley	2/27/18 4:44:00 PM

Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Page 11: [5] Formatted	Drew Bagley	2/27/18 4:44:00 PM

Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Page 11: [6] Formatted	Drew Bagley	2/27/18 4:44:00 PM

Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Page 11: [7] Formatted	Drew Bagley	2/27/18 4:44:00 PM

Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Page 11: [8] Formatted	Drew Bagley	2/27/18 4:44:00 PM

Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Page 11: [9] Formatted	Drew Bagley	3/3/18 1:03:00 AM

Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)

Page 11: [10] Formatted	Drew Bagley	2/27/18 4:45:00 PM

List Paragraph, Outline numbered + Level: 3 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Page 11: [11] Formatted	Drew Bagley	2/27/18 4:44:00 PM

Font:(Default) Arial, 11 pt, Font color: R,G,B (219,96,51)