[This chapter will expand once the results of the CCT RT commissioned DNS Abuse Study are available]

The ubiquitous nature of domain names make them not only conduits of innovation but also of uses that abuse registration terms of use. This means that domain names can become intimately intertwined with cybercrime infrastructure.[1] Due to this reality, the community initially expressed concerns about whether the vast expansion of available gTLDs would result in increased DNS abuse. Consequently, the CCT-RT was tasked with examining the issues associated with the expansion of the DNS as well as the safeguards created to address such problems.

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.[2] The community identified the following areas of concern:

1) How do we ensure that "bad actors" do not run registries?
2) How do we ensure integrity and utility of registry information?
3) How do we ensure more focused efforts on combating identified abuse?
4) How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?[3]

Based on the community's feedback, ICANN identified several recommendations for safeguards aimed at mitigating these risks.[4] NIne safeguards were identified and recommended:

- Vet registry operators;
- Require Domain Name System Security Extension (DNSSEC) deployment;
- Prohibit "wildcarding";

---

[1] Framing Dependencies Introduced by Underground Commoditization, p.12 http://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/43798.pdf or https://cseweb.ucsd.edu/~savage/papers/WEIS15.pdf

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

[3] "Mitigating Malicious Conduct," ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

[4] "Mitigating Malicious Conduct," ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

- Encourage removal of "orphaned glue" records[5];
- 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[6].

The CCT-RT was tasked with analyzing the effectiveness of the 9 recommended safeguards. To the extent possible, the CCT-RT assessed the effectiveness of each of these safeguards using available implementation and compliance data. The CCT-RT examined the implementation of each. Additionally, the CCT-RT 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.[7]

With regarding with compliance to the first safeguard, vetting registry operators, all new gTLD applicants were required to provide full descriptions of the technical backend services that they would use, even where these services were subcontracted, as part of the application process. This was a first cut at ensuring technical competence. These descriptions were evaluated at the time of application but not thereafter.[8] Additionally, all applicants were required to pass Pre-Delegation Testing (PDT).[9] PDT included comprehensive technical checks of Extensible Provisioning Protocol (EPP), Name Server setup, Domain Name System Security Extensions (DNSSEC), and other protocols.[10] 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. In pursuance of the second safeguard, new gTLD registries are required to implement DNSSEC, and their compliance is actively monitored with compliance notices sent if and when checks fail.[11] DNSSEC is a set of protocols intended to increase the security of the Internet by adding authentication to DNS resolution to prevent

---

[5] A Records remaining once a domain name has been deleted from a registry. See http://www.securityskeptic.com/2009/10/orphaned-glue-records.html

[6] "Mitigating Malicious Conduct," ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

[7] The DNS Abuse Study will measure abuse in all gTLDs from 1 January 2014 until December 2016

[8] Technical requirements change over time which would make continual auditing difficult.

[9] P. 5-4, https://newgtlds.icann.org/en/applicants/agb/guidebook-full-04jun12-en.pdf

[10] https://newgtlds.icann.org/en/applicants/pdt

[11] See ICANN Registry Agreement, Specification 6, Clause 1.3, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

problems such as DNS spoofing[12] and DNS cache poisoning[13]. 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.[14] Complaints may be submitted to ICANN via an online tool, and wildcarding in a particular TLD is something that the technical community should notice fairly quickly (there should be a standardised approach to analyzing the effectiveness of the safeguard, i.e. after description of each safeguard or all descriptions to be dispensed of first and then a sub-section dealing with the effectiveness).[15]

Commented [1]: Waudo's comment: define in footnote

Commented [2]: Waudo's comment: define in footnote

To comply with the fourth safeguard, new gTLD registries are required to remove orphan glue records[16] when presented with evidence that such records have been used in malicious conduct.[17] Unmitigated orphan glue records can be used for malicious purposes such as fast-flux hosting botnet attacks.[18] 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.

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.[19] ICANN Compliance monitors adherence to the Thick WHOIS requirement on an active basis, for both reachability and format.[20] Syntax and operability accuracy are evaluated by the ICANN WHOIS Accuracy Reporting System (ARS) project.[21]

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.[22] ICANN monitors compliance with this requirement and publishes statistics, including remediation measures, in

---

12

13

14 See ICANN Registry Agreement, Specification 6, Clause 2.2

15 As of _____, no complaints have been reported via the online form available at https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form

16 These are DNS records tied to name server records that are no longer in the zone

17 See ICANN Registry Agreement, Specification 6, Clause 4.1

18 See ICANN Security and Stability Advisory Committee, "SSAC Advisory on Fast Flux Hosting and DNS," March 2008, https://www.icann.org/en/system/files/files/sac-025- en.pdf

19 https://whois.icann.org/en/what-are-thick-and-thin-entries

20 See ICANN Registry Agreement, Specification 10, Section 4.

21 See http://whois.icann.org/en/whoisars

22 Base Registry Agreement (updated 1/9/2014), Specification 6, Section 4,1, Abuse Mitigation.

its quarterly reports.[23] However, ICANN compliance does not monitor registry procedures for handling complaints.[24]

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.[25] Centralizing these data 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.

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.[26] As of October 5, 2016, ICANN reports that the ERSR has not been invoked for any new gTLD.[27]

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 voluntary create high security zones.[28] However, these proposals never reached the implementation stage.

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. Consequently, the CCT-RT's DNS abuse study[29] may provide insight as to whether the overall implementation of these safeguards are related to any change in the levels of DNS abuse compared to legacy gTLDs.

DNS abuse study

In preparation for the CCT-RT'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.[30] In doing so, the report assessed the various ways to

Commented [3]: This is accurate. More context should be inserted here. Compliance monitors whether or not a registry receives complaints about presence of abuse contact info. But it does not monitor the specific procedures. They may in the future depending on the outcome of the "Framework for Registry Operators to Respond to Security Threats", currently in drafting as a result of the inclusion of Provision 3b in Spec 11 of the RA. https://community.icann.org/display/S1SF/Security+Framework+Home

Commented [4]: Can we use a different source? "ICANN reports that the ERSR has not been invoked..."

Commented [5]: Needs additional context and description. please feel free to quote from or cite "New gTLD Program Safeguards Against DNS Abuse".

[23] https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en

[24] ICANN Compliance may in the future depending on the outcome of the "Framework for Registry Operators to Respond to Security Threats", currently in drafting as a result of the inclusion of Provision 3b in Spec 11 of the RA.https://community.icann.org/display/S1SF/Security+Framework+Home

[25] See ICANN Registry Agreement, Specification 4, Section 2.1. See also https://czds.icann.org/en

[26] https://www.icann.org/resources/pages/ersr-2012-02-25-en

[27] ~~Per email with ICANN staff member Brian Aitchison~~

[28] https://archive.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf

[29] Request for Proposal, https://www.icann.org/en/system/files/files/rfp-dns-abuse-study-02aug16-en.pdf

[30] "New gTLD Program Safeguards Against DNS Abuse Report", https://newgtlds.icann.org/en/reviews/dns-abuse/safeguards-against-dns-abuse-18jul16-en.pdf

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 available remedies depending upon the jurisdiction involved. Another challenge is the lack of data available regarding certain types of abuse. Nonetheless, there are core abusive 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 names seen in a zone.[31] Whereas, using a different methodology, previous research from the Architelos and the Anti Phishing Working Group has named .com the TLD with the largest number of domain names associated with abuse.[32] To date, there has not been a comprehensive study that has produced absolute ratios of abuse per legacy and new gTLD.

Domain names are often a key component of cybercrimes and enable cybercriminals to quickly adapt their infrastructure.[33] For example, Spam campaigns often correlate with phishing and other cybercrime.[34] Domain names are also used to assist with malware distribution and botnet command-and-control.

To the extent possible, the CCT-RT 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 CCT-RT has commissioned a comprehensive DNS abuse study to analyze levels of abuse in legacy and new gTLDs in order to draw correlations, where possible, to safeguard implementation.[35] The study will focus on rates of spam, phishing, malware distribution, and botnet command-and-control in the global gTLD DNS since January 1, 2014, including legacy and new gTLDs. The results will include:

[31] https://www.spamhaus.org/statistics/tlds/
[32] APWG's research focused on phishing: http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf; Architelos http://domainnamewire.com/wp-content/Architelos-StateOfAbuseReport2015.pdf
[33] https://its.ny.gov/sites/default/files/documents/symantec-internet-security-threat-report-volume-20-2015-social_v2.pdf
[34] Temporal Correlations between Spam and Phishing Websites, https://www.cl.cam.ac.uk/~rnc1/leet09.pdf; Spam campaign detection, analysis, and investigation
[35] Request for Proposal, https://www.icann.org/en/system/files/files/rfp-dns-abuse-study-02aug16-en.pdf

Commented [6]: +1 Stan. Comparing apples and oranges. The ratio of domains in new gTLDs is different than the absolute number of abusive domains in .com, the biggest TLD by far. Think this just needs some explanation and qualification, followed by a statement that we don't have the "apples to apples"—ie new to legacy ratios of abuse—yet. These are just some preliminary indicators.

Commented [7]: This isn't quite accurate. The DNS abuse study will not correlate between safeguards and abuse rates other than with the DNSSEC safeguard. However, the study will establish a baseline gauge of abuse rates in new and legacy that will enable further inquiry into the effectiveness of other safeguards. Recall that most technical safeguards are not amenable to quantitative inquiry. If we find there's proportionally less abuse in new gtlds, we can explore the hypothesis that it's because of safeguards. If there's proportionally more, we can explore why the safeguards aren't working.

Commented [8]: We (CCT-RT) will do our own correlation based on the data we receive from the study. We will have to caveat that it's merely a correlation.

1. Overall numbers of abusive domains per TLD, registrar, reseller, and privacy/proxy service, and geographic region from 1 January 2014 until December 2016, segmented according to the above DNS abuse activities.
2. Proportion of abusive domains per TLD, registrar, reseller, and privacy/proxy service, and geographic region from 1 January 2014 until December 2016, segmented according to the above DNS abuse activities.
3. A determination of the average time-to-live for abusive registrations, categorized according to TLD, registrar, reseller, and privacy/proxy service, and geographic region in order to demonstrate whether some abusive maliciously registered second-level domains under each TLD remain registered longer than others before being taken down.

The report will also include:

1. An analysis of the time-to-live of domain names involved in abuse, sub-divided according to "maliciously registered" versus "compromised" domains.
2. An analysis of the effects of DNSSEC deployment on the rates of abusive activities heretofore described.
3. An analysis whose timeframe incorporates the actual dates at which domain names for each new gTLD could resolve, distinguishing the sunrise period from general availability to capture the time frames in which abusive activity is most likely to occur (i.e., following the release of a domain name for general availability).

This comprehensive analysis will enable the CCT-RT to determine abuse rate correlations between registries and registrars, gTLD zones, and, to the extent applicable, corresponding safeguards. This research will also serve as a baseline for future CCT-RTs and other review teams. Draft results will be available to the CCT-RT by June 2017.

I note that this study will not be based on articulated analysis of the efficacy of each of the 9 identified safeguards - or am I wrong?