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

The CCT-RT was tasked with analyzing the effectiveness of the safeguards that have been put in place to limit abuses ~~mitigate issues~~ that might result from ~~involved with~~ the expansion in the number of ~~of the~~ gTLDs, including …. ~~namespace~~. Technical safeguards aimed at preventing DNS abuse were developed as part of this process. To the extent possible, the CCT-RT assessed the effectiveness of each of these safeguards using available implementation and compliance data. Additionally, the CCT-RT commissioned a quantitative DNS abuse study to provide insight into the relationship, if any ~~on any correlations~~ that may exist between levels of abuse and implemented safeguards in the new gTLD name space.

DNS abuse is a prevalent problem in the DNS DOES MEAN THAT THERE IS A LOT OF IT?, intimately intertwined with cybercrime infrastructure.[1] Consequently, ICANN invited community feedback on DNS abuse and the risks posed from the ~~by~~ significantly expansion~~ding~~ in the DNS name space.[2] In doing so, ICANN 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]

MANY OF THESE TERMS NEED TO DEFINED, E.G., "BAD ACTORS", "INTEGRITY", "UTILITY".

Based on feedback from expert constituencies WHO WERE THEY? WHAT MAKES THEM "EXPERT"? , ICANN identified several recommendations for safeguards aimed at mitigating these possible abuses~~threat~~s.[4] These ~~technical~~ safeguards included initiatives to: vet registry operators, require Domain Name System Security Extension (DNSSEC) deployment, prohibit "wildcarding", encourage removal of "orphan glue" records, require "Thick" WHOIS records,

[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, https://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

centralize Zone File access, document registry- and registrar-level abuse contacts and policies, provide an expedited registry security request process, and create a draft framework for a high security zone verification program.[5] The CCT-RT examined the implementation of each. MANY OF THESE TERMS NEED TO DEFINED, E.G., “WILDCARDING”, “ORPHAN GLUE”.

All new gTLD applicants were required to provide ~~a~~ 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 ~~provided technical~~ descriptions were evaluated at the time of application but not thereafter.[6] Additionally, all applicants were required to pass Pre-Delegation Testing (PDT).[7] PDT included comprehensive technical checks of EPP, Name Server setup, DNSSEC, and other protocols.[8] Applicants were required to pass all of these tests before a domain name would be delegated. DEFINE TERMS. EPP?

Upon delegation, ~~the~~ registry operators were required ~~bound~~ to comply with the technical safeguards through their Registry Agreements with ICANN. New gTLD registries are required to implement DNSSEC, and their compliance is actively monitored with compliance notices sent if and when checks fail.[9] This set of protocols is intended to authenticate registry zones to prevent DNS spoofing and DNS cache poisoning. The Registry Agreement for new gTLDs also prohibits wildcarding to ensure that domain names only resolve for an exact match and that end users are not misdirected to another domain name.[10] DEFINE “CACHE POISONING”. It is not possible to monitor this safeguard on an ongoing basis, WHY NOT? but complaints may be submitted to ICANN via an online tool.[11]

Commented [DB1]: Calvin, why wouldn’t it be possible to monitor this on an ongoing basis by auditing queries and resolutions?

New gTLD registries are required to remove orphan glue records[12] when presented with evidence that such ~~a~~ records have~~s~~ been used in malicious conduct.[13] Unmitigated orphan glue records can be used for malicious purposes such as fast-flux hosting botnet attacks.[14] This

[5] “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

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

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

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

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

[10] See ICANN Registry Agreement, Specification 6, Clause 2.2

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

[12] These are DNS records tied to name server records that are no longer in the zone

[13] See ICANN Registry Agreement, Specification 6, Clause 4.1

[14] 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

requirement is reactive by design, but registry operators can~~ould~~ make it technically impossible for orphan glue records to exist in the first place.

~~The~~ Registry Agreements require~~s~~ 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.[15] ICANN Compliance monitors compliance with the Thick WHOIS requirement on an active basis, for both reachability and format.[16] However, syntax and operability accuracy are handled by the ICANN WHOIS Accuracy Reporting System (ARS) project.[17]

~~The~~ Registry Agreements also require~~s~~ all new gTLD registry operators to post abuse contact details on their websites and to notify ICANN of any changes to contact information.[18] ICANN monitors compliance with this requirement and publishes statistics, including remediation measures, in its quarterly reports.[19] However, it does not appear that ICANN compliance monitors registry procedures for handling complaints.

As per the Registry Agreements, new gTLD operators are required to make their zone files available to approved requestors via the Centralized Zone Data Service.[20] Centralizing these~~is~~ 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.[21] As of October 5, 2016, the ERSR has not been invoked for any new gTLD.[22]

In addition to the aforementioned safeguards, there were proposed BY WHOM? WHEN? technical safeguards for the voluntary creation of high security zones. However, these~~is~~ 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 ~~to~~ in the

[15] https://whois.icann.org/en/what-are-thick-and-thin-entries
[16] See ICANN Registry Agreement, Specification 10, Section 4.
[17] See http://whois.icann.org/en/whoisars
[18] Base Registry Agreement (updated 1/9/2014), Specification 6, Section 4,1, Abuse Mitigation.
[19] https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en
[20] See ICANN Registry Agreement, Specification 4, Section 2.1. See also https://czds.icann.org/en
[21] https://www.icann.org/resources/pages/ersr-2012-02-25-en
[22] Per email with ICANN staff member Brian Aitchison

expansion of the DNS. Consequently, the CCT-RT's DNS abuse study MOVE CITATION FROM BELOW HERE. may provide insight as to whether the overall implementation of these safeguards are related ~~correlated~~ 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.[23] 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 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.

WHO PREPARED THE REPORT. The report acknowledged the absence of a comprehensive comparative study of DNS abuse in new gTLDs versus legacy gTLDs. Nonetheless, some targeted data analytics 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.[24] ~~Whereas, p~~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.[25] NUMBER NOT THE SAME AS "number of domain names associated with abuse versus the number of domain names seen in a zone".

Domain names are often a key component of cybercrimes and enable cybercriminals to quickly adapt their infrastructure.[26] For example, Spam campaigns often correlate with phishing and

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

[24] https://www.spamhaus.org/statistics/tlds/

[25] 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

[26] https://its.ny.gov/sites/default/files/documents/symantec-internet-security-threat-report-volume-20-2015-social_v2.pdf

other cybercrime.[27] 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.[28] 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: IS THIS THE SAME AS THE STUDY DESCRIBED IN THE TRUST SECTION?

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 correlations between registries and registrars ???, their implementation of applicable safeguards, and DNS abuse rates. 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 March 2017.

[27] Temporal Correlations between Spam and Phishing Websites, https://www.cl.cam.ac.uk/~rnc1/leet09.pdf; Spam campaign detection, analysis, and investigation

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