I. Safeguards

DNS Abuse

The accessibility of domain names as unique global identifiers has made them conduits of innovative technologies, including those used for malicious purposes. Consequently, bad actors leverage such universal identifiers for cybercrime infrastructure, victimizing people across the globe through DNS abuse.[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 CCTRT was tasked with examining issues associated with the expansion of the DNS, including the implementation of safeguards designed to preempt identified risks.[2]

Deleted: The ubiquitous nature of domain names makes them not only conduits of innovation but also attractive for malicious purposes intimately intertwined with

Deleted: advent

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?
- 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]

[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.

[4] Ibid.

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]

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 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

Deleted: 9

[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.
[10] Technical requirements change over time, which would make continual auditing difficult.
[11] ICANN, *Applicant Guidebook* (June 2012), Section 5-4.
[12] ICANN, "Pre-Delegation Testing (PDT)," accessed 2 February 2017, https://newgtlds.icann.org/en/applicants/pdt

Deleted: will
Deleted:
Deleted: and botnet command-and-control

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 Compliance complaints related to orphan glue records.[23]

---

[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 Compliance 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.

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 compliance 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.

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

[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."
[35] ICANN, "Contractual Compliance Reports 2015."
[36] ICANN, "Contractual Compliance Reports 2014."

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

Comment [DB1]: Add Sub headings and intro paragraph w/ the 3 most important findings

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 available remedies depending upon the jurisdiction involved. 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 names seen in a zone.[42] Whereas, using a different methodology, previous research from Architelos and the Anti-Phishing Working Group named .com the

[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*.
[41] ICANN, *New gTLD Program Safeguards* (2016)
[42] Spamhaus, "The World's Most Abused TLDs," accessed 2 February 2017, https://www.spamhaus.org/statistics/tlds/

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 nothing more than abuse.[48] In fact, some Internet security companies have advised customers to block all network traffic to specific TLDs.[49] Such practices run counter to ICANN's Universal Acceptance efforts. Nonetheless, snapshots of new gTLD abuse do not account for the full variety of registration rules and safeguards in the hundreds of new gTLDs that have been delegated since 2013. Accordingly, it is difficult to ascertain definitive distinctions between abuse rates in legacy and new gTLDs without performing a comprehensive assessment.

---

[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

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[50] in legacy and new gTLDs, to inform this review and potentially serve as a baseline for future analysis.[51] 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.[52]

DNS Abuse Study Methodology

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[53] through the end of 31 December 2016.

The analysis includes:

1. Absolute counts of abusive domains per gTLD and registrar from 1 January 2014 until 31 December 2016
2. 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
3. Abuse associated with privacy and proxy services
4. Geographic locations associated with abusive activities
5. Abuse levels distinguished by "maliciously registered" versus "compromised" domains
6. An inferential statistical analysis on the effects of DNSSEC, domain parking, and registration restrictions on abuse levels
7. An analysis of timeframes to determine the 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).

DNS Abuse Study Findings

The report makes many significant findings regarding DNS abuse associated with new gTLDs compared with legacy gTLDs. Notably, the DNS Abuse Study indicates that the introduction of new gTLDs did not increase the total rate 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.

Legacy gTLDs still account for most domain name registrations and, perhaps consequently, the highest volume of registered domain names linked to abuse.[54] Nonetheless, the overall *rates* of abuse in legacy

[50] Phishing, malware hosting, and spam. Initially, the RT sought to include botnet domains in the analysis. However, historical data on botnets was unavailable for the timeframe of the study.
[51] ICANN, *Request for Proposal*.
[52] SIDN Labs and TU-Delft, *Statistical Analysis of DNS Abuse in gTLDs* (August 2017), accessed 24 August 2017, https://www.icann.org/news/announcement-2017-08-09-en
[53] The first new gTLD delegations began in October 2013.
[54] P.24

Formatted: Underline

Formatted: Underline

Deleted: The analysis included: . ... [1]

Deleted: resulting report made

Deleted: botnet command and control,

and new gTLDs were similar by the end of 2016, and 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 rose by nearly one order of magnitude. 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 526.6 domain names per 10,000 registrations.[55]

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.[56] 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, 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 malware-related registrations for all legacy and new gTLDs.[57] Each of these TLDs offered low priced registrations, sometimes 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,[58] The results of the study indicate that the introduction of new gTLDs has corresponded with a decrease in the number of malicious registrations in legacy gTLDs, while malicious registrations have increased in new gTLDs. This suggests 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 price. In fact, some registrars are almost entirely associated with abusive, rather than legitimate, registrations.

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, suffering from highest concentration of domain names used in phishing attacks (APWG last quarter 2016) accounted for 58.7% of all blacklisted new gTLD domain names.[59] Whereas, Spamhaus blacklisted at least 10% of all domain names registered within 15 new gTLDs. Nevertheless, 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 comply with the RAA.[60] However, the sustained, unabated, high abuse rates were not the actionable reason.

Another registrar, Alpnames Ltd., based in Gibraltar, was associated with a high volume of abuse from .science and .top domain names. The Study notes that this registrar used price promotions that offered

Deleted: At this point

Deleted: 5

Deleted: d maliciously

Deleted: domain names from

Deleted: legitimate domain names

Deleted: the

Deleted: However

Deleted: the

Deleted: However,

[55] p.24
[56] p.12
[57] p.13
[58] Compromised domain names include domain names for which the domain name registration or the website may have been hacked.
[59] P.11
[60] https://www.icann.org/uploads/compliance_notice/attachment/895/serad-to-hansmann-4jan17.pdf

domain name registrations for $1 USD or sometimes even free.[61] 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.[62] At the time of this report, Alpnames remained ICANN-accredited.

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.[63] Whereas, analyzing attributes of cross-TLD registry operators, the Study concluded that low price registrations corresponded to operators associated with the highest rates of abuse.[64]

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.[65] Oddly, there was also a weak positive correlation between the number of DNSSEC signed domain names and abuse in a new gTLD zone.[66] 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 strong 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 among other key variables, such as price, differences in registry and registrar anti-abuse practices may also influence abuse rates.

Price and registration restrictions appear to incentivize behavior amongst cybercriminals engaged in DNS abuse, making low priced domain names with easy registrations attractive attack vectors. Nonetheless, the same qualities may be appealing for registrants with legitimate interests and the overarching goal of a free and open Internet. Consequently, monetary incentives may exist for registry and registrar operators to prevent systemic DNS abuse by proactively screening registrations and detecting malfeasance. For example, there is precedent for ICANN adjusting its fee price structure to address behavior harmful to consumers, such as abolishing the automatic fee refund for domain tasters.[67] Similarly, the CCT Review Team proposes the development of incentives to reward best practices preventing technical DNS abuse and strengthening the consequences for culpable or complacent conduits of technical DNS abuse.

Recommendation: The ICANN Board should pass a measure to provide ICANN fee discounts to registry operators with open registration policies that implement proactive measures to prevent technical DNS abuse in their zone.

Deleted: through which
Deleted: s
Deleted: could be
Deleted: e
Deleted: ed
Deleted: s
Deleted: one instance
Deleted: Analyzing
Deleted: those associated with the highest rates of abuse.
Deleted: whois
Deleted: there may be a
Deleted: .
Formatted: Font:Bold

[61] p.20
[62] 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
[63] p.15
[64] These includes prices as low as $.50 USD, which is even lower than those of .com registration prices. p.25
[65] p.16
[66] p.16
[67] http://www.washingtonpost.com/wp-dyn/content/article/2008/01/30/AR2008013002178.html

Rationale: The new gTLD safeguards alone to not prevent technical abuse in the DNS. Abuse rates are strongly correlated to domain name registration prices and as well as registration restrictions imposed on registrants. 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 abuse. Therefore, ICANN should incentivize and reward the implementation of proactive anti-abuse measures by such registry operators.

Formatted: Font:Bold

Recommendation: The ICANN Board, with advisement from the GNSO PDP, must adopt amendments to the Registrar Accreditation Agreement to prevent systemic use of specific registrars for technical DNS abuse. Such language should impose upon registrars a duty to mitigate technical DNS abuse, whereby ICANN may suspend registrars found to be associated with unabated, abnormal and extremely high rates of technical abuse. ICANN must base such findings off multiple verifiable reliable sources and such findings may be rebutted by the registrar upon sufficient proof that the finding was wrong, the registrar engages in proactive anti-abuse measures to prevent technical DNS abuse, the registrar was itself a victim in the relevant instance, or that the registrar has since taken necessary and appropriate actions to stop the abuse and prevent future systemic use of its services for technical DNS abuse.

Deleted: **Future review teams, including the SSR2, should identify proven effective practices from new gTLD registry operators with statistically low rates of abuse to create best practices for registry operators. Such practices should mitigate increases in domain name abuse associated with low priced and free registrations. To the extent such practices can be identified and incorporated into policies, ICANN should provide a fee discount to registry operators implementing such practices to incentivize proactive anti-abuse behavior, and the implementation of such practices should be validated through auditable means.**

Formatted: Font:Bold

Rationale: Current policies focus on individual abuse complaints. However, registrars associated with extremely high rates of technical DNS abuse continue operating and are provided with little incentive to prevent technical DNS abuse that threatens the security and stability of the DNS and harms consumers.

Formatted: Font:Bold

Page 7: [1] Deleted	Drew Bagley	8/27/17 11:33:00 PM

The analysis included:

An analysis of the time-to-live of domain names involved in abuse, subdivided according to "maliciously registered" versus "compromised" domains.

An analysis of the effects of DNSSEC deployment on the rates of abusive activities heretofore described.

An analysis of timeframes to determine the 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).