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 misuse these universal identifiers for cybercrime infrastructure[1] and directing users to websites enabling other forms of crime, such as child exploitation, intellectual property infringement, and fraud. Each of these activities may constitute a form of DNS abuse. However, determinations depend largely upon local laws, the roles played by other infrastructure providers, and subjective interpretations. Nonetheless, greater consensus exists on many technical forms of DNS abuse as demonstrated by community findings associated with the development of the New gTLD Program.

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?
> How do we ensure integrity and utility of registry information?
> How do we ensure more focused efforts on combating identified abuse?

---

[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.

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]

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

---

[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.

[12] ICANN, "Pre-Delegation Testing (PDT)," accessed 2 February 2017, https://newgtlds.icann.org/en/applicants/pdt

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 Compliance complaints related to orphan glue records.[23]

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

---

[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

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 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]

---

[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."

[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.

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 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

---

[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)

[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

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. Whereas, beyond the safeguards, efforts to combat domain name abuse vary greatly amongst registries and registrars. Some entities do not act until a complaint is received. In contrast, other registrars take proactive steps to check registrant credentials, block domain name strings similar to known phishing targets, and scrutinize domain name resellers, which are not ICANN-contracted parties.[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 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. To the extent possible, the CCTRT has sought to measure the effectiveness of the technical

---

[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

[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

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]

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[54] through the end of 31 December 2016.

The analysis includes:

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

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

Abuse associated with privacy and proxy services

Geographic locations associated with abusive activities

Abuse levels distinguished by "maliciously registered" versus "compromised" domains

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, 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 compared with 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 in legacy 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 saw a significant increase. In the last quarter of 2016, 56.9 of every 10,000 legacy gTLD domain names were on spam

---

[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.

[55] P.24-25

[56] P.24

blacklists whereas the rate for new gTLD domain names was 526.6 domain names per 10,000 registrations.[57]

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.[58] 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,[59] 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.[60] 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.[61] 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, while malicious registrations have increased in new gTLDs.[62] This, along with the fact that the total number of spam registrations remains stable,[63] 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.

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, 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.[64] 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

---

[57] p.24

[58] p.12

[59] Based on the StopBadware data feed

[60] p.13

[61] Compromised domain names include domain names for which the domain name registration or the website may have been hacked.

[62] p. 2

[63] See DNS Abuse Study, figures 24, 36, and 38, corresponding to the absolute number of spam domains for different spam feeds

[64] P.11

its failure to comply with the RAA.[65] 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 domain name registrations for $1 USD or sometimes even free.[66] 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.[67] 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.[68] Whereas, analyzing attributes of cross-TLD registry operators, the Study 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.[69] 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 against users of Apple, Inc. products and services. These registrations were presumably suspicious at the time of registration but 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.[70] Oddly, there was also a weak positive correlation between the number of DNSSEC signed domain names and abuse in a new gTLD zone.[71] 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 among other key variables, such as price, 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 easy registrations attractive attack vectors.[72] Nonetheless, the same qualities may be appealing for registrants with

---

[65] https://www.icann.org/uploads/compliance_notice/attachment/895/serad-to-hansmann-4jan17.pdf

[66] p.20

[67] 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

[68] p.15

[69] p. 12

[70] p.16

[71] p.16

[72] p. 25

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.[73] For example, there is precedent for ICANN adjusting its fee price structure to address behavior harmful to the DNS, such as abolishing the automatic fee refund for domain tasters.[74] 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. 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; this DNS abuse appears to have gone on 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:

- Encourage and incentivize pro-active abuse measures as per Recommendation 1
- Introduce measures to prevent technical DNS abuse as per Recommendation 2
- Ensure that the data collection is ongoing and acted upon as per Recommendation 3
- 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 Compliance and where a clean-up is identified as being necessary. If the level of abuse has not come down, as per the commitment of the Registry, then the failure of the contracted party to implement the plan should constitute a breach of the RAA/RA. If a level of obligation is there, then not only does the DADRP become less necessary, but also less likely to be used. This translates to positive outcomes for all parties due to decreased levels of DNS Abuse.

Recommendation A: Consider directing ICANN org, in its discussions with registries, to negotiate amendments to existing Registry Agreements, or in negotiations of new Registry Agreements associated with subsequent rounds of new gTLDs, to include provisions in the agreements that mandate or provide incentives, including financial incentives, for registries, especially open registries, the adoption of proactive anti-abuse measures.[75]

---

[73] 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

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

[75] 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

Rationale/related findings: ICANN is committed to maintaining "the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet."[76] The new gTLD safeguards alone do not prevent technical abuse in the DNS and have therefore failed to stop the proliferation of technical abuse issues flagged by the community prior to the expansion of the DNS.. Abuse rates are correlated to registration restrictions imposed on registrants and registration prices may influence rates too. 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 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 impose mandates upon or incentivize and reward those that have already adopted or implement proactive anti-abuse measures identified by the community as best practices to reduce technical DNS abuse.

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 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. If mandated, then this requirement should be focused on the technical abuse related to the security and stability of the Internet, enforced like other contractual requirements, and not shift liability for the underlying abuse to the operator.

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.

---

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.

[76] 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

Rationale/Related Findings: Current policies focus on individual abuse complaints. However, registrars and registry operators associated with extremely high rates of technical DNS abuse continue operating and face 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

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 flow down 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. ICANN Compliance should initiate an investigation into a contracted party's direct or indirect (such as through a reseller) involvement with systemic technical abuse if they 1) receive a formal complaint alleging unabated, abnormal, and extremely high rates of technical abuse, or 2) if they are otherwise made aware of such a situation, such as via published research, as by the ICANN Security Team or SSAC. Upon initiating an investigation, ICANN Compliance should confirm any findings based upon reliable sources and a technical verification of the 1) the abusive nature of domain names, such as through testing by the ICANN Security Team, and/or 2) other verifiable evidence that the operator is facilitating systemic 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.

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 and higher priority by ICANN Compliance. 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 means that there are

many factors for which to account 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 action must be taken by ICANN compliance as deemed necessary. 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.

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 compliance in particular to identify registries and registrars that need to come under greater compliance scrutiny and thereby have such behavior eradicated.

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 abuse (to define, e.g. over 10% of their domain names are blacklisted domain names). Such registry operators or registrars should in the first instance be required to a) explain to ICANN Compliance why this is, b) commit to clean up that abuse within a certain time period, and / or adopt stricter registration policies within a certain time period. Failure to comply will result in a DADRP, 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 registries. It is important to have a mechanism to deal with this abuse, particularly if it's prevalent in certain registries. Abusive behavior needs to be eradicated from the DNS and this would provide an additional arm to combat that abuse.

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: ICANN Compliance is one route to dealing with this high level of DNS abuse, enforcing existing and any amendments to 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 be very helpful in dealing with such

DNS abuse, and it could also serve as a significant deterrent and help prevent or minimize such high levels of DNS abuse. Registry operators or registrars that are identified as having excessive levels of abuse (to be defined, for example where a registry operator has over 10% of their domain names blacklisted by one or more heterogeneous blacklists (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 should be obliged to review their second level domain names being used for DNS abuse and explain why this is, commit to cleaning these up within a certain timeframe, and adopt stricter registration policies if necessary to ensure that there exist relevant contractual terms to effectively handle such registrations. If the domain names at issue are not cleaned up satisfactorily, 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 be covered by the DADRP so it is important to ensure that “registry 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.