Donuts' Comments Regarding Proposal to Mitigate Name Collision Risks

Thank you for the opportunity to comment on the subject of potential name collision, and the Interisle report specifically. Donuts respectfully submits the following comments.

Executive Summary

The potential for serious collision involving certificates and non-existent domains (NxDs) has been overstated and can be remediated without delaying any new gTLDs. Certificate collision is very unlikely unless a precise series of unlikely actions intending harm is put into place, any one of which, if interrupted, removes the risk of harm. Successful delegation of previous gTLDs with pre-existing NxD traffic and the everyday registration of SLDs, with pre-existing NxD traffic by existing registries (such as .COM) has proven that NxD traffic does not cause public end-user harm.

Donuts believes the process leading to the study is as flawed as the staff's recommendations based on it. The collision issue has been examined for many years, and a last-minute report—produced with no community input—raises significant competition concerns. Applicants will document, in the next 21 days, data that will be far more indicative of the minimal scope of any problem. Upon review of that data, the ICANN Board should elect to proceed with delegation of all approved gTLDs.

Certificates

Donuts agrees with accelerating the resolution of the certificate collision issue, and that a constructive collaboration with certificate authorities is far more warranted than is delay. As the NTAG noted in its comment[1], the Board can, and should, contact certificate authorities regarding probable delegation of new TLDs and that the 120 day process should open immediately.

As a practical matter, the risk of actual harm involving certificate collision is extremely low. For such harm to occur, a bad actor would need to make a long series of efforts and rely on various dependencies. In the case of the oft-discussed .CORP, for example, the problem exists **only if all** of the following were to come to pass:

1. .CORP is inserted in the ICANN root
2. a .CORP subdomain that has one or more previously issued certificates is inserted into the .CORP zone (call this SLD "SLD.CORP")
3. those preexisting certs for SLD.CORP are not revoked
4. the registrant for SLD.CORP gets a new certificate for SLD.CORP
5. the registrant for SLD.CORP deploys the new certificate on a server
6. the registrant for SLD.CORP accepts secure connections from previous users of SLD.CORP, potentially collecting information which is not from the registrant's users, but from the old users of the previously non-existent SLD.CORP
7. the registrant causes harm with the information collected

[1] http://forum.icann.org/lists/comments-name-collision-05aug13/pdfZTEoM8cx1g.pdf

If any of the above issues **do not** occur, then neither does the collision problem. The staff's remedy, as proposed, is to eliminate step #1 entirely, blocking .CORP from entering the root. However, *any of the other steps may be blocked with the same total problem elimination effect*.

For example, another solution that provides the absolute mitigation guarantee some in the community seem to seek would be preventing issuance of certificates in .CORP (blocking step 4) until the problem is mitigated, or by blocking one of the other steps, such as the revocation of the other certs (step 3, for example).

Preventing issuance of certificates for all .CORP subdomains is not something any registry operator prefers, let alone the certificate authorities because any certificates they sell for new gTLDs after delegation would not be usable, dramatically lowering demand for such certificates. However, it's a useful perspective for the relative gravity of the situation.

How would blocking of certificate issuance be accomplished? The registry simply creates a policy where no sub-domain in the proposed TLD may be allowed to deploy a certificate on a server listed in the gTLD zone. How would that policy be enforced by the registry? Simply by the registry looking up the name in the DNS, finding the corresponding IP address, and going to the server to attempt to obtain a certificate. If the test obtains a certificate then the subdomain (SLD.CORP in this example) is removed from the .CORP zone (utilizing step 2 above to remediate)..

To accomplish the same end result (absolutely no harm) sought by some in the community, any of steps 1 through 7, or a combination thereof, could be employed, not solely step 1.

Non-existent domains

As context for our comment on NxDs, we restate here some important notes from the NTAG comment:

- The problem is overstated. Overall there are very few NxD requests in applied-for TLDs. Only 3% of the total requests conflict with strings that are actually being considered under the new TLD program. Even this 3% figure may be overstated due to the difference in TTL and the behavior of caching resolvers. Additionally, the 3% figure is further overstated because over 40% of the 3% is caused by the Google Chrome browser performing DNS lookups for random 10-character names. The report also did not compare the 3% NxD traffic to all applied-for TLDs with the NxD traffic that currently exists in existing TLDs, such as .COM. Is the number of NxD queries to all of the applied for TLDs more or less than the same number for one existing TLD? This would be a very useful comparison to gauge whether or not the problem is overstated.
- There is little focus on the real risks. In Section 5 of the report, "Name Collision Etiology", Interisle attempts to explain the origin of the spurious requests for non-existing domains. We believe that merely counting the number of requests for each string is completely insufficient when judging risk, and that any reasonable conclusions made from the data must take into account the true origin of the "collision".[2]
- Previous expansion caused no known issues. Analysis using data from January 2006, prior to the launch of several active TLDs, found that .XXX (as but one example) received more pre-delegation queries than any other new TLD. However, .XXX was launched without incident with no identified technical issues since. Other TLDs with pre-existing NxD traffic (.ASIA, .KP, .AX, .UM, .SX—even .CO, similar as it is to .COM) have launched with a) none of the problems predicted by Interisle and b) with no absolutely no approval delays due to "name collisions."
- Risks already exist. Interisle's and Verisign's identified risks exist today, **including NXD**

[2] In the appendix to its letter, NTAG provided clearer analysis of the risks and mitigation possibilities for each category proposed by Interisle.

traffic in .COM. Verisign allows SLDs with pre-existing NxD traffic to be registered every day in .COM yet ICANN is not asking for a suspension of registrations in .COM while such "risks" are mitigated. Neither should a delay be requested in new TLD delegation.

- Risk measurement is easily tampered with. Any model of risk measurement based on total query counts is flawed. Donuts believes the counts are not accurate in the first place; we further assert data collected after TLD strings were made public causes query rates higher than they previously were, exacerbating the "negative" result. Donuts also agrees the Interisle report makes no mention of investigating the possibility that some of these requests were issued intentionally. ICANN should be wary of the precedent that such an easily manipulated metric will be used to make multi-million dollar business decisions.

Donuts points out that the report is missing some critical data. For example, it did not look at NxD traffic in existing TLDs, including .COM. Nor did it examine specific subdomains that receive NxD traffic in the so-called problem TLDs (the 20%). If a small number of SLDs in any TLD receive NxD traffic *and* if it is deemed that pre-existing NxD traffic is an unknown risk (even though its currently ignored in .COM) then those few SLDs could very easily be blocked from registration by the registry, allowing other SLDs in these TLDs to exist and deliver the good to the public for which this whole program is designed. It's a remarkable leap to make decisions without such important data.

The 80-20 rule

There is no factual basis in the study recommending halting delegation process of 20% of applied-for strings. As the paper itself says, "The Study did not find enough information to properly classify these strings given the short timeline." Without evidence of actual harm, the TLDs should proceed to delegation. Such was the case with other TLDs such as .XXX and .ASIA, which were delegated without delay and with no problems post-delegation. SLDs with pre-existing NxD traffic should be allowed to be registered in those TLDs, also just as they are allowed everyday in .COM and other TLDs.

Process

The process leading to this report is terribly flawed.

With due respect to ICANN's security and stability community, it's very difficult to understand why such a report was rushed at the last minute, when the collision issue and other stability issues have been so thoroughly examined for so long during the over *eight-year* process leading to new TLDs. That process resulted in some strings being disallowed for stability and security reasons such as .LOCAL, LOCALHOST, .EXAMPLE, .GTLD-SERVERS, .ROOT-SERVERS, .TEST, .INVALID and many others.

Staff has inexplicably migrated to a new process. Usually, the community has the opportunity to contribute to the discussion before any report is produced and implemented (demonstrated by a unilateral decision to delay contracting for the TLDs in the 20%). The community was denied that opportunity here and presented with a *fait accompli* statement about what should happen and what is happening, without sufficient regard for accurate data due to the rushed nature.

Applicant Guidebook Reliance

The well-thought-out AGB is the contract between applicants and ICANN. Applicants relied on the terms of that agreement for preparation of their applications and in anticipation of providing predictable services to the domain name system. The AGB certainly permitted applications for the hundreds of names now subject to discussion regarding collision, and presumably the AGB took into account the extensive community discussions and previous SSAC reports about security and stability.

Even the GAC Principles on new gTLDs state: "All applicants for a new gTLD registry should therefore be evaluated against transparent and predictable criteria, **fully available to the applicants prior to the initiation of the process**." (Emphasis added)

We encourage immediate resolution to this issue so as to avoid continual accrual of material harm to applicants.

Applicants were permitted to apply for new TLDs and were assured of competent technical evaluation for security and stability. Many—including *all* of Donuts' applications—have been duly approved. They have *all* already passed the stringent stability and security evaluation, which was developed by ICANN over many years and is a very significant part of the TLD application approval process for which ICANN received tens of millions of dollars from Donuts to evaluate. A last-minute challenge to these approvals suggests considerations other than true technical concerns, and constitutes basis for Donuts to consider a full range of options for its own resolution of this situation.

Contracting

The contracting process apparently now has been delayed for certain strings in the identified 20% of strings in discussion. This is completely unnecessary. Donuts' applied for .CAB (#201 in the ranking of potential issues), which is one that has been held up for contracting, yet no one has shown there are any certificates existing for any SLD in .CAB. At 201 in ranking, .CAB NxD traffic would be far lower than that of .ASIA when it launched. It is preposterous to hold contracts hostage to this process.

Independent study

It is no surprise that names in potentially valuable TLDs are already being attempted to be used before such TLDs are actually delegated by ICANN. This fact speaks to the pent-up demand for good names in such TLDs—TLDs that will be competitive to existing TLDs, and increasing competition is a pillar of ICANN's existence. Donuts notes that the Interisle study makes recommendations based on 2013 traffic data. However, examination of 2012 data by Interisle shows that total queries to "problem" NXDs is a far lower number. It is unlikely this is coincidental—more likely, the increased attention to new gTLDs caused an increase in queries. Looking only at data produced after publication of the new gTLD application list is not a reliable way to draw conclusions about risks to the root.

Donuts and others have donated hardware to the Domain Name System Operations Analysis and Research Center (OARC) for the purpose of producing non-biased data to correctly inform the community of the scope of any potential issue and further suggestions for outright elimination of any risks, let alone mitigation. (Risks that either did not exist or did not come to pass in the delegation of prior TLDs, despite absolutely no mitigation by those registries.) This data will be available before the end of September and Donuts strongly encourages the full consideration of this information.

Recommendations

Donuts recommends to the Board the following:

- Allow all applications to proceed uninterrupted, as no harmful collision issue has been conclusively demonstrated compared to other, existing, TLDs.
- Accelerate the handling of the collision issue by consulting proactively with certificate authorities, with the participation of applicants, and if a 120-day revocation process must proceed, begin that period immediately.
- Carefully consider a) the harm elimination and mitigation methods described here, and b) the results of the applicant study on collision against the rushed and inaccurate report currently before the community.

Thank you for the opportunity to comment on this issue.