UnitedTLD

Internet Security, Name Collisions and United TLD

September 17, 2013

Summary of United TLD's Position

In August 2013, the Interisle Consulting Group issued a report titled "Name Collision in the DNS." The report was commissioned by ICANN for the purpose of examining potential DNS stability risks associated with the delegation of new gTLDs. The report analyzes the issue of new gTLD strings that "collide" with non-delegated TLDs that may currently be in use in a private namespace. As a result of this report, ICANN has indefinitely delayed the delegation of all new gTLDs until ICANN has evaluated community comments and appropriate mitigation measures.

The concern about "collisions" is based upon the belief that name collisions will result and lead to adverse effects. These adverse effects, however, are neither defined nor quantified in the report, which leads some readers to believe that the negative effects could be catastrophic, which we do not believe to be the case. While we agree there are risks, these risks are minimal and the existing DNS infrastructure already faces these risks and does not negatively affect the security and stability of the Internet.

As an example, Interisle's own data shows that existing TLDs, such as .XXX had high levels of root traffic prior to their delegation and yet not a single example of a "risk to the Internet" can be shown to have occurred after the delegation of these TLDs.

United TLD's view is that there is no significant risk in the delegation in any of the applied for gTLDs that are considered "uncalculated" or "low" risk. These designations by Interisle are arbitrary and an analysis of the data used shows that the majority of the queries would remain NXDOMAIN even after delegation. The two TLDs flagged as "high" risk (.home and .corp) have a higher level of concern simply due to their traffic levels and their unique position as having been used as the default domain for consumer Internet equipment and in corporate networks. United TLD would support a well-defined study into mitigation approaches for these two gTLDs, provided there was a clear path to timely delegation.

Overstating the Problem

ICANN and Interisle's concerns are based on the analysis of queries to the root servers for non-existent TLDs. Since the proposed TLDs are un-delegated, the replies currently must be NXDOMAIN. This leads to the assumption that a response other than NXDOMAIN would introduce risk into the DNS for all TLDs once delegated.

There are a couple of problems with this viewpoint.

The first problem is that the Interisle report, and the resulting "high", "uncalculated", "low" classification by ICANN are based on numbers that include SLDs that could never be registered, either because they contain illegal characters, or are already reserved names, such as two letter SLDs.

Interisle's report shows that 50% of the traffic used in the study is likely from Google Chrome and from SRV type requests[1]. Domains that contain "_" as the starting character are ineligible for registration as second level domains. While this doesn't change the absolute rankings used in the classifications, it begins to show how grossly overstated the problem is.

Interisle admits that the traffic is ineligible in its report, but ICANN's classifications make no attempt to reconcile this and adjust the data that would result in a reclassification and move TLDs from uncalculated risk into the low risk classification

Secondly, there are NXDOMAIN responses to unregistered domains in existing TLDs and these are not perceived as a security concern by ICANN or the existing TLD operators. If this were a security concern we would expect those TLD operators and ICANN to propose a moratorium on the registration of new SLDs in any of those TLDs

Existing Permitted NXDOMAIN Risks

We believe there is risk in greater scope with currently active TLDs than the risk associated with delegation of the new proposed gTLDs.

For example, NXDOMAIN responses in .COM happen in far greater number than are seen for the proposed gTLDs. Although the DITL data only shows the query, not the response, an analysis of the DITL data compared with the .COM zone file for the same day provides an approximation of the NXDOMAINs. If the domain wasn't registered, the response was likely an NXDOMAIN.

The 2012 DITL data has 16 billion .COM queries in it. Comparing it to the .COM zone file for April 18, 2012, 136,905,037 second level domains were identified as being "unregistered". This results in 888,569,816 queries that likely resulted in NXDOMAIN responses. This is likely a greater number than any of the proposed gTLDs.

[1] *Table 12 – Proposed TLD usage as a percentages across all roots* – Interisle Name Collision Study Report Version 1.5 page 47/48: 10-character SLD 46% , _ldap, _kerberos, _dns-sd 4%

VeriSign has stated[2] that NXDOMAIN responses in existing TLDs do not pose the same risk as an NXDOMAIN in an undelegated TLD. While it is certainly possible to argue that the risks are different, the sheer volume of NXDOMAIN responses in the COM space make it far more likely that an adverse result will actually be seen in the .COM space than in an undelegated TLD.

An Existing Permitted Risk

One of the risks, which has been brought up as a major source of concern, is that of an internal SSL certificate suddenly being "external" and a malicious actor being able to take advantage of that by launching a man-in the-middle attack on unsuspecting web users. In public comments made by VeriSign, they have discussed the "go to a Starbucks…"[3] example to highlight the risks and negative outcomes that could occur. While we respect their concerns, we would like to highlight that the possibility of this incident occurring is minimal and would not be the result of an incidental name collision. For this risk to occur, the attacker would have to know what new gTLD the target was using internally, then register a domain in that new gTLD, obtain an SSL certificate and then find the right Starbucks that the target was using. With 20,891 locations world wide[4], Starbucks has more stores than most of the new gTLDs had hits in the Interisle report and you start to see how this risk is *de minimis*.

There is an existing risk that is far greater and, yet, is widely recognized as acceptable.

Domains are allowed to expire and be re-registered.

.COM and .NET have renewal rates of around 75%[5] on a base of 120 million domains[6]. That means approximately 40 million domains are expiring every year, or over 100,000 per day, plus the expirations happening in the other TLDs. These are 100,000+ domains per day that have existing traffic from existing Internet users that suddenly ends up "elsewhere" and can now be redirected.

This is not a theoretical risk and it is straightforward to document how an external certificate is issued to a new registrant after a domain expires. For example; "bobsflowers.com" uses an SSL cert to secure an ecommerce website. "bobsflowers.com" expires and is registered by a new, potentially malicious, owner and a new "bobsflower.com" certificate is legitimately issued. An end user will likely have no idea that something has changed.

Change "bobsflower.com" to "passport.co.uk" and "Bob the Flower Guy" to "Microsoft" and that's exactly what happened in November 2003. Thankfully, the new owner was a nice guy and gave the domain back to Microsoft rather than exploiting it**.**

[2] http://forum.icann.org/lists/comments-name-collision-05aug13/pdfgGgQZ2Oxuv.pdf

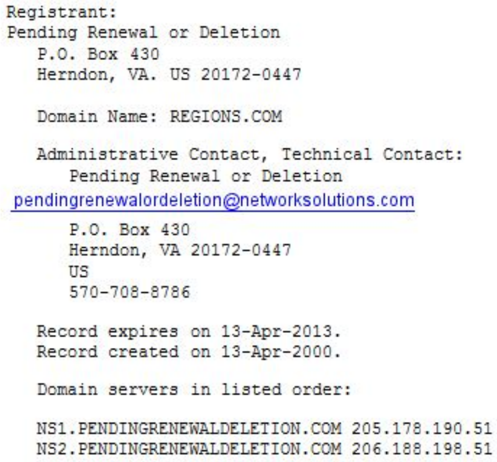
[3] http://forum.icann.org/lists/comments-name-collision-05aug13/pdfgGgQZ2Oxuv.pdf

[4] Loxcel Starbucks Map, March 22, 2013 http://www.loxcel.com/sbux-faq.html

[5] *The Domain Name Industry Brief, Volume 10 – Issue 1 – April 2013* published by VeriSign, lists the renewal rate at 72.5%

[6] *The Domain Name Industry Brief, Volume 10 – Issue 1 – April 2013 published by VeriSign,* states a combined total of 121.1 million domains.

The same problem has happened in the financial industry, Regions Bank, an FDIC insured bank in the U.S. failed to renew their domain on April 13, 2013. Network Solutions, their ICANN accredited registrar, switches the DNS on expired domains (NS1.PENDINGRENEWALDELETION.COM in this case), and puts up a generic Network Solutions branded web page. Network Solutions would also receive misdirected emails to Regions Bank with potentially sensitive information from Regions Bank clients.



```
Registrant:
Pending Renewal or Deletion
   P.O. Box 430
   Herndon, VA. US 20172-0447

   Domain Name: REGIONS.COM

   Administrative Contact, Technical Contact:
      Pending Renewal or Deletion
 pendingrenewalordeletion@networksolutions.com
      P.O. Box 430
      Herndon, VA 20172-0447
      US
      570-708-8786

   Record expires on 13-Apr-2013.
   Record created on 13-Apr-2000.

   Domain servers in listed order:

   NS1.PENDINGRENEWALDELETION.COM 205.178.190.51
   NS2.PENDINGRENEWALDELETION.COM 206.188.198.51
```

ICANN and the Internet community have worked together to help mitigate these types of risks, with policies such as Expired Registration Recovery Policy, but, at no time, was the entire renewal and registration process put on hold.

The entire “drop-catch” industry is based around tracking domains with high traffic and “catching” them after deletion for registration. This is a process that many existing registry operators support by supplying traffic data and scoring to the public to help facilitate the acquisition of domain names. This practice shows that existing TLD operators approve of the process and leads one to believe that there is minimal risk that existing traffic suddenly ends up “elsewhere”, which is the heart of the collisions issue being raised.

Existing TLDs Have Been Delegated Without Incident

The NTAG Letter to Board on Interisle Report references the VeriSign analysis of January 2006[7]. Of the seven gTLDs referenced, all had substantial number of queries and .xxx, .asia, .kp, .ax, .um, .cw and .sx were all delegated without incident.

In fact, the least queried TLD (.sx) had more queries than all but five of the proposed TLDs. Again; these TLDs were successfully delegated without incident.

[7] *New gTLD Security, Stability, Resiliency Update*: Exploratory Consumer Impact Analysis, Verisign Labs Technical Report #1130008 Version 1.0 August 5, 2013 http://techreports.verisignlabs.com/docs/tr-1130008-1.pdf

This is particularly important when considering the case of ".ASIA". VeriSign shows that in 2006,. ASIA was seeing more traffic than all but the proposed TLDs .HOME and .CORP were seeing in the 2013 DITL.[8]

.ASIA shares characteristics with the proposed TLDs. It is a dictionary word with broad recognition and is recognized as a geographical region, much as proposed gTLDs represent regions, products, and concepts. .ASIA was launched on April 10, 2007 and currently has over 500,000 domains registered[9.] The Internet's security and stability was never compromised and currently remains intact**.**

Conclusion

United TLD believes ICANN is bowing to industry pressure to delay the new gTLD program due to risks that are minimal, already appear and are accepted in the existing namespace. If name collisions in new gTLDs are a major risk for SSL certificate users, then one must also conclude that domain expiration and re-registration are also a risk, yet they have not been thought to threaten the security and stability of the Internet. If name collisions and the expectation of NXDOMAIN behavior is an issue, then how is it that seven new TLDs get launched without incident?

We understand and agree that there are some risks as described in the Interisle Report, but these are risks that we live with on a daily basis, due to the nature of an open, distributed Internet. ICANN does not require mitigation measures for existing current risks and consequently, ICANN should not further delay the delegation of the new gTLDs for the potential risks as outlined in the Interisle report.

In conclusion, we agree with the comments submitted by Neustar and other DNS experts, that there is no demonstrated reason to delay the delegation of any applied for TLD that is currently in the arbitrary classifications of "Low Risk" and "Uncalculated Risk" and to address the two "High Risk" strings in a reasonable and timely manner.

Wayne MacLaurin
Senior Vice President of Technology
United TLD

[8] *New gTLD Security, Stability, Resiliency Update*: Exploratory Consumer Impact Analysis, Verisign Labs Technical Report #1130008 Version 1.0 August 5, 2013 http://techreports.verisignlabs.com/docs/tr-1130008-1.pdf

[9] http://www.dot.asia/asia-gtld-surpasses-500k-domains-registered/