September 15, 2013

Board of Directors
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Re: ICANN’s Proposal to Mitigate Name Collision Risks – .CBA Case Study

Dear Members of the ICANN Board:

On August 27, 2013, Verisign submitted several comments regarding ICANN’s New gTLD Collision Risk Mitigation proposal. In our comment, “New gTLD Security, Stability, Resiliency Update: Exploratory Consumer Impact Analysis,” we demonstrated that query volume alone is an inadequate measure of risk arising from name collisions; provided a candidate risk assessment matrix; and advocated that ICANN finally implement the prior recommendations from ICANN’s own Security and Stability Advisory Committee (“SSAC”), including the Scaling the Root studies. These recommendations were in line with Interisle Consulting Group’s observation in its August 2013 report prepared at the direction of the ICANN Board that stated “[a]n additional qualitative analysis of the harms that might ensue from [name] collisions would be necessary to definitively establish the risk of delegating any particular string as a new TLD label…”

Others choosing to prioritize speed over a secure and stable DNS operation have also submitted comments critical of ICANN’s risk categorization based solely upon query volume, but have drawn the incorrect conclusion. These applicants contend that ICANN’s proposal is too conservative and that delegations should be expedited, because, in their view, the risk of internal network name collisions is acceptable, even absent the qualitative analysis of each string as discussed in the Interisle Report. Other than Verisign’s Exploratory Consumer Impact Analysis,

1 See Name Collision in the DNS (Version 1.5, August 2, 2013), Interisle Consulting Group, I.I.C at 2-3 (“Interisle Report”).
no effort has been made to perform a qualitative analysis as recommended repeatedly, and absent this analysis, the potentially harmful consequences associated with the delegation of a new TLD label, and the associated risks, simply cannot be assessed.

Verisign’s analysis has focused on identifying some of the systematic risks that will be exposed by the new gTLD program and who the impacted parties are likely to be. In this context, we were intrigued when the Commonwealth Bank of Australia ("CBA") filed a public comment taking responsibility for the name collisions identified in the Interisle Report and associated with its .CBA application.

**Commonwealth Bank of Australia - .CBA**

CBA has applied to operate the TLD string .CBA. The .CBA string was placed by ICANN in the "uncalculated risk" group (specifically at position 153) based upon the analysis set forth in the Interisle Report. In an effort to follow the guidelines of ICANN’s New gTLD Collision Risk Mitigation proposal, and thus assess the risk of delegation of the .CBA string, CBA concluded in an August 23, 2013 comment to ICANN that after “some internal investigation,” the cause of the name collisions is “primarily from CBA internal systems” and “that it is within the CBA realm of control to detect and remediate said systems and internal certificate use.” Thus, CBA concluded that it could self-mitigate the name collision risks resulting from delegation of the .CBA TLD and that ICANN should therefore move the .CBA string to the “low risk” group of applications. CBA also represented that it would undertake a further investigation and verify the origins of the .CBA requests, and that it would conduct appropriate remediation upon the completion of its internal investigation. While we await that investigation and remediation plan, we conducted our own analysis of the .CBA queries. We believe our data and analysis shows without a doubt that CBA’s initial conclusions are incorrect.

More broadly, we believe that the .CBA assessment can serve as a useful case to test the components of ICANN’s risk mitigation proposal. Using .CBA as an example, we can assess whether ICANN’s interpretation of the Interisle Report and ICANN’s risk categorization is appropriate. Further, we can assess how effective ICANN’s plan to require applicants (and not ICANN) to conduct risk mitigation is likely to be.
Analysis of .CBA Queries

Verisign conducted a focused study on .CBA and then further narrowed its focus on two of the most active geographies (namely Japan and Brazil) in terms of errant queries to the root server system for .CBA for seven weeks based on data from 1.5 roots (100% of “A,” and ~50% of “J”). While the coverage from the vantage points of these servers suggests that our data has a correspondingly limited scope, we believe our analysis demonstrates that CBA’s analysis is measurably unreliable and inaccurate, as root server system query behaviors simply do not exist within CBA’s observation space, and are themselves source-anonymized or otherwise incomplete within the annual “day in the life (DITL)” repositories. Furthermore, we believe that a reasonable conclusion to draw is that ICANN’s risk mitigation proposal is not a practical or reliable option.

During the seven-week study period, Verisign observed approximately 10,000 root queries for the .CBA TLD per day. Many of the queries we observed (~80%) related to .CBA are from systems or devices utilizing DNS-based Service Discovery protocols such as BONJOUR, which, when signaled, typically respond with available services. These services often include printers, smart home and industrial automation systems, or other specialized devices/services. (BONJOUR predates ICANN’s new gTLD program by several years, and DNS-SD was recently published as a Standards Track RFC by the IETF.) Other queries appear to be the result of standards-based DNS resolution search list processing issues, and originate from McAfee’s popular anti-virus software, which transmits queries to confirm in real-time that certain resources are virus-free prior to execution and processing. Finally, the originator of many of the queries simply could not be identified absent direct interaction, which was deemed out of scope of this study but considered necessary to fully understand the scope of the problem in any qualitative manner.

It should be noted that the Internet Service Providers (“ISPs”) that operate the network connectivity services and recursive name server infrastructure (including NTT-ME, Stelmat, AT&T, Comcast, Telefonica, Telstra, Level(3) Communications, Embratel, Cox, Bell Canada, etc.) for the observed .CBA query sources may be impacted by the end system operators. This is
because these end system operators will most likely contact these ISPs for support services, and problem resolution assistance resulting from impacts of name collisions. The disruption to the ISP's business and residential networks and their subscribers could be substantial. Under ICANN's proposed risk mitigation plan, there is no mechanism to assist these infrastructure operators, or any acknowledgment of them as impacted parties. Commonwealth Bank of Australia, as registry operator, will bear sole financial liability to any third party, whether it be an injured ISP, network systems operator or otherwise, arising from the results of name collisions that occur as the proximate result of delegation and operation of the .CBA TLD. Indeed, should an injured third party seek to hold ICANN accountable for its losses in this regard, Commonwealth Bank of Australia as registry operator will be obligated to indemnify and defend ICANN and its agents for such claims. Furthermore, it should be noted that Commonwealth Bank of Australia's indemnification obligation to ICANN, and as a result its liability, is uncapped. These uncapped indemnification obligations, as well as uncapped liability, exist for all applicants that execute the New gTLD Registry Agreement.

While there were two major functional namespaces observed and identified, .CBA is used by more than 100 others in Japan alone. A sampling of the DNS-SD and McAfee queries can also be seen in the accompanying .CBA Focused Analysis presentation. These represent two new functional namespaces, beyond those identified in Verisign's Exploratory Consumer Impact Analysis. It should be noted that whatever the nature of many of the applications relying on non-delegation of .CBA, some at least appear sufficiently important to justify the use of real-time malicious software (malcode) protection techniques. The reliance on the non-delegation of .CBA for the correct operation of the malcode protection software itself is likely a result of standard search list processing issues that permeate nearly all of the applied-for strings. In

---

2 See New gTLD Registry Agreement §7.1(a) ("Registry Operator shall indemnify and defend ICANN and its directors, officers, employees, and agents from and against any and all third-party claims, damages, liabilities, costs, and expenses including reasonable legal fees and expenses, arising out of or relating to...the delegation of the TLD to Registry Operator, Registry Operator's operation of the registry for the TLD or Registry Operator's provision of Registry Services...").

3 See New gTLD Registry Agreement §5.3.
addition to inherent privacy issues with potentially sensitive information leakage, this finding may more specifically signal the expanded potential and ease of launching Man-In-The-Middle (MiTM) attacks as well as more easily enable the injection of malicious software when .CBA begins to resolve. Simple explanations of how spoofing could target these networks can be found in the public comment on the Proposal to Mitigate Name Collision Risks submitted by Dr. Eric Osterweil on September 11, 2013.4

Our measurement study reveals evidence of a substantial Internet-connected infrastructure in Japan that lies beneath the surface of the public-facing Internet, which appears to rely on the non-resolution of the string .CBA. This infrastructure appears hierarchical and seems to include municipal and private administrative and service networks associated with electronic resource management for office and residential building facilities, as well as consumer devices. However, further study is required to determine the nature and full extent of this infrastructure. A sampling of these queries can be seen in the accompanying .CBA Focused Analysis presentation.

While predominantly originating in Japan and Brazil, the data shows .CBA queries originating from more than 170 countries over less than two months of observation within a fraction of the root server system. Most registry operators much like Commonwealth Bank of Australia and their new gTLD partners, would face significant challenges in studying and identifying queries that originate from all over the globe. Preparing effective notifications in the official languages of the more than 170 countries from which .CBA queries originated in order to warn potentially impacted parties is a challenging task for anyone and even more so under the short, 30-day time frame proposed by ICANN. Further, assuming Commonwealth Bank of Australia successfully notifies the impacted parties, ICANN’s plan provides limited time for the impacted parties to actually remediate the name collisions and prevent disruptions or the introduction of vulnerabilities, and does not even provide for any means of educating potentially impacted parties of how to mitigate the issue once they are notified. And, finally, under ICANN’s proposal, ICANN is and will remain unaware of the naming collisions that Commonwealth Bank of Australia identifies and seeks to remediate.

4See http://forum.icann.org/lists/comments-name-collision-05aug13/msg00038.html.
Conclusions

While we believe even this analysis could be far more comprehensive, these results support the following conclusions:

- Root server system instrumentation is critically important, as ICANN's own SSAC has recommended repeatedly since 2010. Such a capability would allow issues such as those described here to be surveyed, studied, and identified, and responded to in a consistent, cohesive and deliberate manner for all applied-for strings by experienced analysts prior to delegation and immediately upon the enablement of this capability. 5

- Our study vindicates the Interisle Report's observation that additional qualitative analyses of the harms that might ensue from naming collisions is necessary to definitively establish the risk of delegating any particular string as a new TLD label.

- ICANN's risk mitigation plan improperly categorizes strings by arbitrary risk groups based on no apparent analysis beyond query volume, and with no survey whatsoever of the possible impacts.

- Applicants lack the experience and thus are a poor choice to perform such risk assessments and to operationalize the ICANN-prescribed "customer service" (which ICANN has not defined). Lacking root instrumentation, and thus unable to see much beyond their own internal usage of .CBA, the bank wrote to the ICANN public forum claiming that .CBA collisions could be self-mitigated. However, our analysis demonstrates that the bank is the source of at most 6% of the observed query volume.

5 Verisign continues to convey our eagerness to stand with ICANN in their leadership role here, as well as in their role as L-root operator, and align with all other willing root operators to as quickly as possible develop a sustainable root server system measurement apparatus to provide early warning and instrumentation across the system at the root. We would also note with dismay that this work is NOT currently underway within the existent work plan, nor has it been.
We are unaware of how many of the 952 or more Internal Names Certificates they possess, a topic that would need separate study and analysis.

- Our data vindicates the observation that applicants face increased risk of liability from end users and network operators upon delegation. Under ICANN's current constructs, applicants will bear this risk alone, and will indemnify ICANN should the delegation give rise to claims against ICANN.

Verisign’s risk analysis of just one string of more than 1,400 in just two of 170 geographies demonstrates that the as-yet unknown potential risks from new strings is real, not just theoretical. ICANN should consider this new data and analysis, and carefully review Verisign’s Exploratory Consumer Impact Analysis, integrating this with a comprehensive risk matrix and community input of what weights should be applied to each element of the risk matrix.

ICANN’s mission and primary priority is to coordinate and ensure the secure and stable operation of the DNS. ICANN, after five years and hundreds of millions of dollars invested by applicants and others in the new gTLD program, continues to ignore sound warnings from industry experts and their very own advisory committees, and as a result have failed to identify the readily discoverable and at-risk DNS usage described here. The community is owed an explanation as to why ICANN made the decision to limit the scope of the Interisle Report, and then subsequently decided not to expand the scope of the Report when its shortcomings, identified by Interisle itself as well as others, were plainly evident.

This analysis of .CBA demonstrates clearly how little can be known confidently until qualitative analysis of each individual string is conducted, and that what the community does not know can have unforeseen consequences, which could be severe. This is why SSAC, Interisle, and many others strongly advise that individual string risk analysis - the only way to categorize a string as anything other than unknown risk - should be performed and assessed prior to any delegation. The analysis also validates the concerns of parties such as General Electric, Verizon, the American Insurance Association, and the ISP and Connectivity Provider (ISPCP)
constituency, all of whom asked ICANN through submitted comments for additional time and study prior to proceeding with ICANN’s plan as proposed.

ICANN has reacted late to name collisions in a manner that does not properly prioritize security and stability. The facts make this clear: ICANN failed to act on SSAC advice; the Interisle study was late, limited, with no follow-up to its findings; no SSAC analysis has been published that would inform community comments; no effort has been made to develop qualitative risk analysis; new responsibilities and risks are transferred to applicants, without the tools to address them; and the broader community of affected parties is only now beginning to research the potential for impact for themselves and their clients.

With its risk mitigation plan, ICANN proposes to transfer certain security and stability responsibilities to applicants - a policy that subverts ICANN's core mission. This should be soundly rejected by the ICANN board, not ratified and continued.

This study of only one string shows that no one, ICANN or others, should assert or assume that collision risk is understood and acceptable without conducting proper risk analysis and incorporating informed community input.

Very truly yours,

Patrick S. Kane  
Senior Vice President, Naming and Directory Services  
VeriSign, Inc.
September 15, 2013
Page 9

Thomas C. Indelicato
Vice President and Associate General Counsel
VeriSign, Inc.

Danny McPherson
Vice President, Chief Security Officer
VeriSign, Inc.
Focused Analysis on New Applied-For gTLDs (Focus: .cba)

September 12, 2013
Evidence and measurements are critical in clarifying what the appropriate level of caution should be.

"gTLD strings pose risks? "Yes," "no," "yes, but..."

ICANN's community has structured do applied-for and risk-taking at the DNS root has global implications, and the security and stability of the DNS is serious. But, the community is contracted to act as a back-end registry for nearly 200 others.

This is why Verisign has applied for over a dozen strings and opportunities. The new gTLD program offers a lot of positive rewards.

The new gTLD program: risk vs. reward.
apartment complexes?

queries and virus scans that seem to be from residential
For example, why do we see DNS Service Discovery (SD)
and what might actually break for them
How many namespaces are actually going to be impacted,

impacted parties employing applied-for strings

semantics: information (namespaces) to identity
We use network-level information (such as ASNs) and
We add "who is impacted" to our "what's the problem" analysis
But, now we add a focused (per-9TLD) methodology

A candidate Risk Matrix

broad "spread" of risk across all applied-for strings with

In our recent Technical Report, we examined the

focused manner

Assessing risk can be done broadly and also in a
This presentation illustrates a deeper analysis of CBA Commonwealth Bank simply cannot know instrumentation and qualitative analyses, however, without broad root server system classified as "uncalculated risk" all strings w/ 952 internal names certificates, and Interisle Consulting Group ranked CBA as 153rd out of Intlehttps://rtium.com/qastrings/commss-räume-name-collision-34990004.htmloffice. "As the cause of the name collision is primarily from CBA;... it is within the CBA realm of primary source of CBA queries Commonwealth Bank of Australia claimed to be the exonerate individual applied-for strings Hoping to alleviate concerns, some have sought to... To illustrate the efficacy of this approach..."
Findings and Future Work

Namespace Definition and Characterization

Reprise our analysis of network spread for cba
Current study covered 100% of A root and an estimated 50% of J root.

- Queries from NTT-ME in Chiba, Japan primarily hit Tokyo site; when it was changed the scope of the findings.

- Operational constraint resulted in limited visibility across our sites, impacting accuracy and depth of our analysis.

Global interest but intense activity out of Japan.

NXD root traffic from 12 sites carrying both A+J between 7/16 and 9/5/2013.

We observed 504K queries for .ca, related to domains.

Spread: Sources of Queries for .ca
Heat map of query sources for CBA
<table>
<thead>
<tr>
<th>Top ASN's</th>
<th>Unique ASN's</th>
<th>What network sources are making these queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 20</td>
<td>Top 171</td>
<td>Japan generates ~79% of all queries for ~90% of all queries. A Top 20 ASN’s account for more than 1/785 (~88%) ASNS. Responsible for queries across 171 countries. 839 unique ASNs. 2&quot;.639 unique ASNs.</td>
</tr>
</tbody>
</table>
Breaking down the full queries

Example 14 label query:

- wpad.cba
- cabadomain.cba
- www.cba

protocols, and more
namespaces, services,
information about end user
some query names can leak

The queries vary in length
Here we focus on DNS-SD and McAfee GTI services.

- The semantic names of those who may suffer
- Boundaries of impacted parties

We leverage this to identify the logical configuration

Each define their namespace in the most significant labels

Information leakage

Each represent automated configuration attempts or

WPAD, IISATAP, Bonjour/DNS-SD, McAfee GTI

Vectors

Domain (SLD) that is queried for by any of our risk

Here we define namespace as a Second Level

In this work, we do this by analyzing "namespaces" collisions

Impacted parties

One primary goal is using semantics to identify

What do we mean by "namespace"
What is Bonjour?

Bonjour is a technology for networking devices and services on a local network. It enables automatic discovery of devices and services on a local network, also known as zero-configuration networking. Bonjour, also known as Apple Bonjour, enables automatic discovery of devices and services on the local network.

Anyone could potentially answer DNS-SD queries related to all CDA queries. Represents explicit DNS-SD queries. 06.881 (21.2%) of all DNS-SD queries leak from the local namespace when a machine thinks it exists in a "zone" that does not exist in global DNS.

Also enables smart home automation technologies like:

- Printers, Apple TV, etc.
- Thermostats, remote and physical access systems, energy management, etc.

A DNS service discovery protocol for network services like:


alarms, etc.; e.g.;
These namespaces can each be localized:

- isatap.
- wpad.
- slimalocal.cba

Search list processing or explicit configuration

related activities can help us identify „namespaces“

Distinctive query structure in the different service
Under TLD X there are Y number of namespaces relevant in Z region

• We automate these portion across any TLD

   diverse set of queries:

   • Only 1 sees activity from Australia and that namespace has the most
   • 2 are based in Canada
   • 5 are based in Brazil
   • 49 are based in Japan

   Of the 65 namespaces:

   • account for 80% of all queries seen in CBA

The namespaces conducting Bonjour and other DNS-SD queries

Generalized Impact Statement

Verisign Public
Makuhari Baytown High-rise in Chiba, Japan (4.9% of CBA guarantees)

Steimat is a networking company based in Culibra, Brazil.

Example Namespaces:
- DNS-SD
- Bonjour-based namespaces

63 different namespaces are making DNS-SD guarantees
Processing

Possible result of standards-based search list

Blocking responses impacts malware service

Active responses tell clients if malware is detected

Monitoring queries leaks into about files being scanned

Kamagaya, Japan

- 9-0 >label<.157c.1deb.3ea1.4t10.0 >label<.avrs.mcafee.com.parkside
- 9-y-0 >label<.157c.1deb.3ea1.2t10.0 >label<.avrs.mcafee.com.winsingseg.com

Essentially piggybacking on the DNS

DPIs, ARPS, etc. are being checked for malware,

GTI clients emit DNS queries whenever files (.exe's,

appropriately." http://mcafee.com/corporate/index.jsp=contentId=KB53735

from ... endpoint, it determines if this program is malicious and responds

"GTI provides the most up-to-date malware detection ... receives the request
East (link-ichikawa-03)

1-Link Ichikawa The Towers

Makuhari Baytown

Makuhari Baytown High-Rise in Chiba

JP (Parkside-Kamagaya)

Parkside Kamagaya – Rental Property in Chiba

30 different namespaces are making Mactee quarters

Example Namespaces
Liberal estimates for their traffic range from ~2-6% 

Some Australian quarters for "CBA"

Inspection the hostnames it appears they may be operating:

derivatives indicate "Commonwealth Bank of Australia" or obvious

There are no labels being queried in .cbs that explicitly

So, does CBA own .cbs?
appears to assume all liability for delegation of a CPA.

Under ICANN's risk mitigation plan, the bank would manage namespaces.

- Uses protocol/service-specific techniques to learn
- Namespaces in a repeatable/automated way

Our new systematic techniques allow us to discover
- Link Ichikawa, The Towers East, etc.
- Stellmat, Makuhari Bayside High-rise, Parkside Kamagaya, etc.
- Commercial entities in .cpa and residential and commercial entities

A possible relation between learned namespaces
- Namespaces communities

Has allowed us to discover additional service behaviors and
- Noun and quantitive analysis
- Focused analysis of gTLD strings enables more

Initial Findings
Conclusions

Summary in that:

Our analysis proves the wisdom of Internet's warning in their report's Executive

Corrections could easily be costly + resource intensive and should begin immediately.

Given lifespans of devices that employ DNS-SD, notification and upgrade.

Applied to strings; this may pose considerable risks.

DNS Service Discovery and apparent standards-based search lists interactions

Universal lifetimes exist until all certificates expire (Revocation alone is insufficient).

X.509 certificates serve as an indicator of usage for a given string and

Regarding early warning and instrument across root server system

Necessary Implementation of SA-CO4.5 & SA-CO4.6 recommendations

Indicators simply not within their current observation space.

Strings without visibility to root server system data and qualitative analysis.

Most applications do not seem to be quantified to assess the risks of delegating their
Thank You