

August 27, 2013

Submitted electronically

Re: Proposal to Mitigate Name Collision Risks

The Association for Competitive Technology (“ACT”) was founded in 1998 by independent software developers concerned about how the interactions between major companies and policy makers affected small and medium-sized developers. ACT is listed on the European Union Transparency Register and its Washington, D.C. office is a registered 501(c)(6) non-profit organization in the United States. Specifically, the institutional purpose of ACT, as detailed in its U.S. charter documents, is directly related to the benefit of the application developer community because its purpose is to “enhance public understanding of the high quality of its members’ products and services and its members’ commitment to innovation and technological advancement.”

ACT is an established institution with an ongoing relationship with the clearly delineated mobile application community. ACT’s membership includes more than 5,000 small and mid-size mobile application “app” developers and information technology firms. ACT is an international group of leading members of the app industry (“Industry”). In addition to its small business membership, ACT includes sponsors such as Apple, AT&T, BlackBerry, eBay, Facebook, Intel, Microsoft, Oracle, PayPal, VeriSign, and Verizon.

ACT has been a prominent advocate and educational organization at a crucial time in the rapid expansion of the Industry. As a voice of the Industry, ACT has several concerns regarding ICANN’s proposal on new gTLD collision risk management published on August 5, 2013.

I. Importance of DNS

DNS plays a central role in the functionality of the internet. It is easy to forget that entering www.actonline.org into a browser window requires information to travel around the world to many different servers before it can be displayed. Use of a DNS to resolve a critical resource, such as a mail server’s service address, can require multiple uses of global resources.

It has become vital that the growth of DNS is slow and methodical, since significant changes in the system can have a tremendous impact on the global economy. Almost every industry, from software to health care to banking to hotels, relies on DNS for access to information and communication tools.

Companies, large and small, have set up their intranets to make use of internal TLDs (iTLDs) with the expectation that certain strings would not be valid DNS TLDs. Because a TLD like .dev has not been assigned, it can be used to assign for internal-use-only network names for servers that provide essential infrastructure such as database, email, and document sharing servers. Critical company resources are built with iTLDs as the only way to access them. These iTLDs are often hard-coded into customized software often created by small businesses which are used by businesses to access to their internal networks.

Changes which affect the stability of access to that system can have devastating impacts on those varied industries. The current pace of releasing DNS root zone TLDs has the potential to affect that stability.

II. Problems with the Current TLD Release Structure

A. Cause Confusion

An iTLD may be used by employees to access a company intranet to check their company email while sitting in a coffee shop or access their files while in an airport. Employees often connect to corporate resources through the creation of a Virtual Private Network (VPN) which creates a private tunnel for the IP traffic between the remote location and the company's network. When the employee is not connected to the VPN, the iTLD will not resolve to anything, which is expected.

However, when the response resolves to a new TLD, non-company servers will direct a user to the new owner of the TLD. Furthermore, DNS caching may cause the result of DNS queries pointing to entirely different services depending on the specific sequence in which domains were queried and how long ago they were queried. Suddenly, an employee's email stops working outside the office when he or she is not on the company server. Indeed, once an employee returns to the office, their email problem may suddenly be resolved with no clear explanation as to the cause. For many, even the most technically savvy, this problem could go on for a significant period of time before it is diagnosed. In the meantime, there is no reliable access to services like email which are vital for many businesses.

Many systems administration manuals suggest that Local Area Networks (LANs) should configure iTLDs as local DNS TLDs for strings that do not exist in the DNS. It's a widely used and endorsed technique for managing networks. Millions of businesses, from the giants of the industry to small mobile app companies with fewer than ten employees, depend on reliable access to their intranet and the internet to run their business. If these services suddenly become unreliable, it will create confusion and uncertainty in the business community and has the potential to cause serious financial damage.

B. Create Security Risks

In addition to confusion, release of TLDs currently used as iTLDs could cause significant security risks. A common tool used to breach security today is to set up a phishing website similar to a legitimate website, like an online banking website, to trick users into entering personal data. Security measures can be put in place, including use of a security badge such as https:// to guard against this type of domain name forgery. The SSL certificates that are used for https encryption are typically granted by verifying the ownership of a particular domain.

If TLDs are released which match those used as iTLDs, the domain name confusion in servers could result in personal information being sent to the owner of the TLD even if security measures are put into place. For example, a mail server, not understanding the change in the status of the TLD, could automatically transmit information like username and password when an individual connects to their email. Because SSL certificates match the entire domain and are signed by a universally accepted signing authority, they would only reinforce a false sense of security, which is the opposite of what they were designed, and depended upon, to do.

C. Require Significant Resources to Fix

Like the Y2K problem, the use of iTLDs is pervasive and encoded in software. It will be a difficult task to amend all the software which would be affected by the release of a TLD. First, there is the issue of actually identifying the problem to fix. As previously stated, the disruption caused by the introduction of a previously unused TLD is not an easy problem to diagnose. In many cases it will require the technical staff of a company to be informed of the problem with sufficient time to fix it before it disrupts a company's operations. The disruption is especially significant for small businesses, which do not have the staff to monitor this issue or dedicate to finding a solution within the small time allotted under the current ICANN plan.

Second, fixing the systems and the software associated with an iTLD requires significant time and expertise. Much of the software which could malfunction with the introduction of a TLD was created a number of years ago. Many of the code's creators have moved on to larger roles in the technical community and some no longer code. The resources required to recode software to avoid any conflict with new TLDs will be extensive and will have to be done by experienced programmers rather than less-experienced staff. The new resource requirement to amend these problems will be especially taxing on small businesses like app developers who are already having a hard time finding qualified and experienced coders to work on existing products.

III. Conclusion

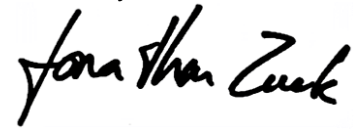
We are excited for the important steps ICANN is taking to create a more diverse internet environment. However, such steps have the potential to cause enormous harm.

To that end, ACT suggests the following recommendations:

- ICANN resources should be dedicated to a public awareness campaign of potential problems resulting from a string resolving to a different TLD. A significant danger in assigning a new TLD is the confusion caused, as described in section II.A. A public awareness campaign could work to reduce any harmful effects caused when a query for a TLD string – one that has historically resulted in a negative response – begins to resolve to a new TLD.
- ICANN should slow or temporarily suspend the process of delegating TLDs at risk of causing problems due to their frequency of appearance in queries to the root. While we appreciate the designation of .home and .corp as high risk, there are many other TLDs which will also have a significant destructive effect. The snapshot approach used to classify the TLDs does not adequately assess the risk and 120 days delay proposed is not sufficient to inform consumers of the potential problem and allow resolution of the issue. We request that additional time is given in order to resolve these problems.
- ICANN should consider reserving specific TLDs permanently for internal use. In order to allow for the consistency the market needs, there needs to be TLDs which can be reliably used for internal use only. As previously mentioned, making the changes required by the release of a TLD will take significant resources. By marking TLDs for internal use only, it ensures that these changes need only be made once and they can be relied upon going forward.

Thank you for the opportunity to address these important issues.

Sincerely,

A handwritten signature in black ink that reads "Jonathan Zuck". The signature is written in a cursive, flowing style.

Jonathan Zuck
President