CA/Browser Forum

Thursday, 7 March 2013

Fadi Chehadé, Chief Executive Officer and
Dr. Stephen D. Crocker, Chairman of the Board
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536 USA

Sent via facsimile +1 310 823 8649

RE: Proposed delegation of .corp as a gTLD

Dear Messrs. Crocker and Chehadé:

This letter is submitted with great urgency to alert you to an important security concern identified by some of our members regarding the delegation of **.corp** as a generic Top Level Domain. The CA Browser Forum is an unincorporated association of Certification Authorities[1] and Browsers. Recent analysis by our members and others of certificates visible on the public internet indicate that a significant number of organizations use .corp as their internal domain suffix. By comparing information obtained from the public internet with non-public information obtained from our members, we think we might be seeing just the tip of the iceberg because it signals that there may be an even greater problem beyond just those enterprises with .corp certificates and include those who have provisioned their DNS infrastructures with .corp for internal routing.

While RFC 2606 reserves names which are guaranteed not to be delegated (.localhost, .example, etc.), these are not suitable for company internal use because some of them are treated specially by networking equipment in a way incompatible with this use and also by their very meaning as English strings--no-one wants to operate an “invalid” or “example” network. We have discovered a variety of commonly used internal/private TLDs such as .internal, .local, .locale, .private, .pvt, .lan, .dom, .site, and .home, among others, but .corp is far more common. Users of networks want more than just bare names for their internal machines and not all networks can be easily or quickly migrated to FQDN-only environments, although the CA Browser Forum does recommend that they do so.

We believe that .corp has attained *de facto* reserved status and cannot be delegated without breaking thousands of networks around the globe with the potential of security and stability problems and confidential information leakage. Others have recognized this fact. RFC 6762 extends RFC 2606 for .local (used by Apple's Bonjour protocol), and ".corp" is mentioned in Appendix G as a “Private DNS Namespace”. Furthermore, while not a current best practice, network configuration advice given by

[1] Certification Authorities issue digital certificates for use in server authentication and encrypted communication via the SSL/TLS protocol. These certificates are used both on the public internet and internally within companies.

some network professionals over the last 10+ years have suggested similar approaches, such as choosing "domain.corp" [2] or "domain.local"[3] for internal domains.

Considering certificates particularly: the use of a new gTLD before the expiration or revocation of existing "internal use" certificates that happen to contain names ending in that gTLD string will compromise the security of domain registrants within that new gTLD. For this and other reasons, the CA/Browser Forum members will cease issuing publicly trusted certificates to internal domains in 2015. Furthermore, the CA/Browser Forum recently adopted a rule requiring that CAs revoke certificates within 120 days after ICANN publishes notice that a new gTLD delegation agreement has been signed. However, some members of the CA/Browser Forum expressed that a 120-day period is not long enough for customers to respond and reconfigure their internal environments to not conflict with newly active gTLDs. The Forum believes this will not work well for .corp because of the sheer number of networks that will have to be reconfigured.

If .corp were to be excluded from delegation and reserved for the public commons, scores of large enterprise networks could avoid costly and rushed reconfigurations, and CAs could avoid the revocation of thousands of certificates which would need to be replaced by their owners. ICANN should consider the reservation of at least one suitable TLD for internal use, and .corp is an obvious, front-running candidate. If ICANN does not act to reserve one, the problems for internal enterprise networks will continue as more and more TLDs are removed from possible internal use without any "safe harbors" created. In other words, as the .corp situation demonstrates, there are no "future-proof" internal TLDs that companies can safely choose because who's to say that internal networks won't have to be renamed again in, say, three years' time when ICANN approves the creation of even more gTLDs?

We look forward to coordination with ICANN going forward in this matter. If we can be of any assistance in answering additional questions you may have, please feel free to contact us collectively at questions@cabforum.org, or me specifically at 801-701-9678 or ben@digicert.com.

Sincerely yours,

Benjamin T. Wilson, JD CISSP
Chair, CA/Browser Forum
SVP Industry Relations and General Counsel, DigiCert

---

[2] http://www.archivum.info/microsoft.public.windows.server.dns/2006-03/00178/Re-AD-DNS-naming.html

[3] MS Knowledge Base Articles 555521, 556086, 940726, and 2736842 at http://support.microsoft.com/kb/.