PayPal

Friday, 15 March 2013

Fadi Chehadé, Chief Executive Officer
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

RE: Proposed delegation of invalid names from SAC 045 and RFC 6762

Dear Messrs. Crocker and Chehadé:

This letter Is submitted to ensure that you are aware of the significant security issues related to delegating gTLDs that are currently in wide use as *de facto,* private TLDs as identified by the ICANN Security and Stability Advisory Committee (SSAC) report *SAC 045 Invalid Top Level Domain Queries at the Root Level of the Domain Name System* (http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf) and additionally identified in RFC 6762. (http://tools.ietf.org/html/rfc6762)

As ICANN's own analysis has revealed, there are a number of invalid TLDs in wide use, primarily in internal networks, but which are often queried on the public Internet. This situation is so common that just the top 10 such invalid TLDs represent 10% of the **total** query load at the root servers – and this most likely reflects systems that are only temporarily operating outside of the a network context where these names do resolve. (e.g. a corporate laptop temporarily taken to a public WiFi hotspot.)

Unfortunately, the SSAC's analysis and recommendations fall short of what is needed by primarily considering the potential impact of the widespread use of such names to the **applicants** for these names. The considerable security and operational risks to **users** of these names is not given adequate consideration. Delegating these names will put millions of users and high value systems at considerable risk.

These are the top ten invalid queries from SAC 045, plus those gTLD suffixes identified in RFC 6762:

- invalid
- wpad
- home
- belkin
- corp
- lan

- domain
- localdomain
- localhost
- local
- intranet
- internal
- private

It is clear that these strings that are intended for use as internal network identifiers. Indeed, it was common practice for nearly twenty years to configure internal organizational networks in this manner; not as a deliberate abuse of the DNS, but as a best practice recommended by major software and hardware vendors and as a security best practice. These choices may have been ill-advised, especially in light of ICANN's decisions to broaden the gTLD space. Regardless, they are widespread, were made in good faith, and are often very difficult to change. For example, re-naming a Microsoft Active Directory Forest is often operationally impossible.

The costs of suddenly delegating these names publicly will be severe to those who depend on them today and many internal networks will be disrupted. Administrators will be forced to block these names from resolving to the public network to maintain continuity in their operations, but hidden costs will remain.

Consider a typical enterprise laptop configured to look for network services ending in ".corp". What happens when that system roams to a public network, such as the user's home or a public WiFi hotspot? Potentially dozens of services may attempt to resolve their endpoints and reconnect, including:

- Browser bookmarks, home pages and saved tabs
- Email clients
- Chat clients
- File synchronization services
- Administrative policy services and agents
- Directory services

Most of these services use stored authenticators or credentials, and authenticate their server endpoint using HTTPS, accepting any certificate that chains to a trusted root. If the recipient of an ICANN delegation ".corp" set up, for example, wildcard records and buys a legitimate wildcard certificate, that organization will find itself bombarded with sensitive data from such clients, including:

- Usernames and passwords in plaintext
- NTLM authentication blobs subject to forwarding attacks
- Kerberos tokens with bearer semantics
- HTTP cookies

If the appropriate service endpoints are available, these clients will next begin to dump confidential data and potentially pull incorrect information and apply damaging state changes. The potential for malicious abuse is extraordinary, the incidental damage will be large even in the absence of malicious intent, and such services will become immediate targets of attack as they inadvertently collect high-value credentials and private data from potentially millions of systems.

ICANN should consider not just the potential costs and unwanted network traffic sent to applicants for these names, but the substantial and severe costs imposed on the general Internet community arising from delegation of names that have been common *de facto* private network suffixes for nearly two decades. At minimum, the top ten observed invalid TLDs plus those recommended for use by RFC 6762 should be permanently reserved for private use to prevent large scale disruption and damage to the millions of users and systems that rely upon them today. A more prudent approach would be to consider the negative externalities for each of the applied for new gTLDs.

While such an approach might delay the launch of new gTLDs, launching these gTLDs and experiencing security issues on a large scale would prove harmful to ICANN, users, and the Internet.

Sincerely,

Brad Hill
Bill Smith
PayPal Information Risk Management