SAC 050
DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee on Blocking of Top Level Domains at the Domain Name System

An Advisory from the ICANN
Security and Stability
Advisory Committee
(SSAC)
14 June 2011

Preface

This is an Advisory of the Security and Stability Advisory Committee (SSAC). The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). The SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

The contributors to this Advisory, reference to the committee members' biographies and statements of interest, and committee members' objections to the findings or recommendations in this Advisory, are at end of this Advisory.

Table of Contents

1. DNS Blocking: Benefits Versus Harms

Blocking or altering responses to Domain Name System (DNS) queries is increasingly prominent. Domain name or Internet Protocol (IP) address filtering (or otherwise preventing access to web content as a matter of security policy) may be viewed by some organizations as a natural extension of historical telephony controls that aimed to block people within an organizations from incurring toll charges.

Technical approaches to DNS blocking are intended to affect users within a given administrative domain, such as a privately or publicly operated network. Preventing resolution of the domain name into an IP address will prevent immediate connection to the named host, although circumvention techniques may enable connectivity to the intended system anyway (this includes simply accessing the site via IP address rather than via a Fully Qualified Domain Name (FQDN)). A DNS resolver or network operator could also rewrite a DNS response to contain an IP address mapping the operator chooses, whether rewriting a Non-Existent Domain (NXDOMAIN) response or re-writing the DNS response for an existing FQDN, with potentially harmful effects on DNS Security Extension (DNSSEC)-supporting name servers and their users. A particularly coarse-grained approach is for an operator to silently discard DNS responses, although this results in non-deterministic behavior and may itself be problematic.

Regardless of the mechanism used, organizations that implement blocking should apply these principles:

1. The organization imposes a policy on a network and its users over which it exercises administrative control (i.e., it is the administrator of a policy domain).

2. The organization determines that the policy is beneficial to its objectives and/or the interests of its users.

3. The organization implements the policy using a technique that is least disruptive to its network operations and users, unless laws or regulations specify certain techniques.

4. The organization makes a concerted effort to do no harm to networks or users outside its policy domain as a consequence of implementing the policy.

When these principles are not applied, blocking using the DNS can cause significantly more collateral damage or unintended consequences with no remedy available to affected parties.

The evolution of Internet technology is based on an adaptation of the first principle of practicing medicine – *primum no nocere* (first, do no harm) – that requires healthcare providers to consider the possible harm that an intervention might cause. In the case of

blocking DNS, and irrespective of whether the blocking applies to Top Level Domains (TLDs) (e.g .example) or second (e.g. example.example) and third level (e.g. example.example.example) domains, "doing no harm" means creating no circumstances where Internet users outside of the organization's policy domain are adversely affected by the organization's policy or implementation.

All technical approaches to DNS blocking, and even more so attempts to circumvent the blocking, will have some impact on the security and/or stability of users and applications, and on the coherency or universal resolvability of the global namespace. The SSAC cannot draw a line between "good DNS blocking" and "bad DNS blocking," at any TLD layer, although the Committee can offer to investigate the observable impacts of various approaches to blocking, and it can suggest guidelines to use in evaluating which approaches to blocking are likely to incur the fewest unintended consequences and least harm outside the blocked domain. For example, negative impacts of DNS blocking of specific domains or host names on DNS security have been described in a recent white paper.[1]

The SSAC understands that the subject of blocking of DNS comes in the wake of the addition of the XXX Generic TLD (gTLD) to the root. The SSAC does not have sufficient information to take a position regarding this action, however, the Committee wishes to make clear that, regardless of whether blocking applies to TLDs or sub-levels, minimizing harm requires a concerted effort to not create circumstances where Internet users outside an organization's policy domain are adversely affected by that organization's policy or implementation. Extending this organization-based ethical framework to sovereign nations would require greater understanding of the political landscape than the SSAC currently has. But we can also say with certainty that country-level blocking of entire TLDs fundamentally interferes with the goal of providing a single, unified naming system for Internet resources. If implemented without some formal ethical framework to minimize harm to external parties, blocking may induce more adverse effects than intended on broader communities, exacerbating the problem(s) that such blocking is intended to solve. In addition, blocking at the second and third level domains as well as the TLD level may give rise to alternative name systems and/or roots, which would be destabilizing and disruptive for the Internet.

2. Acknowledgments, Statements of Interests, and Objections, and Withdrawals

These sections provide the reader information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent or potential, that may bear on the material in

[1] See <http://www.redbarn.org/files_redbarn/PROTECT-IP-Technical-Whitepaper-Final.pdf>.

this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

2.1 Acknowledgments

The committee wishes to thank the following SSAC members and other contributors for their time, contributions, and review in producing this Report.

KC Claffy
Steve Crocker
Patrik Fältström
Jim Galvin
Warren Kumari
Jason Livingood
Danny McPherson
Ram Mohan
Dave Piscitello
Bruce Tonkin
Paul Vixie

2.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/committees/security/biographies-25mar11-en.htm.

2.3 Objections and Withdrawals

There were no objections or withdrawals.