Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 26, 2014

W. Kumari
Google

November 22, 2013

A method for mitigating namespace collisions
draft-wkumari-dnsop-defense-collision-mitigate-03

Abstract

This document outlines a possible, but not recommended, method to mitigate the effect of collisions in the DNS namespace by providing a means for end users to disambiguate the conflict.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 26, 2014.

Copyright Notice

Table of Contents

1. Introduction / Background

Collisions in the DNS occur in multiple ways; one common case is that an organization has used an sub-domain (foo) of their primary domain (example.com) for corporate infrastructure, and then the string "foo" is delegated as a TLD. When an employee of the organization enters 'www.foo', is the goal to reach a machine in the internal namespace (www.foo.example.com) or the hostname 'www' in the 'foo' TLD?

This document describes a means of disambiguating these, and similar cases.

Implementation of these methods are not recommended; they are documented here to explain some of the pitfalls with approaches like these.

2. Mitigation

The mitigation described in this document involves presenting the multiple options to the user, and allowing them to indicate which of the names is the one they were trying to reach.

The mitigation would lookup the name in multiple namespaces. When if a conflict is detected, it would then provide a means for the user to indicate which one of the colliding names they wish to connect to, and return the disambiguated answer to the application. An additional feature could be for the mitigation to cache the user's choice, and / or provide a means to set priorities.

This could be accomplished in a number of ways, including:

Intercepting the resolution requests from the application in a "shim" type library

Replacing the resolver library entirelyT

Integrating this type of mitigation into applications (some web browsers already do something similar to this)

Proxying the request to a server that provides an interstitial page that allows the user to indicate the intended name (for applications such as HTTP requests)

There are a number of issues with this solution, including but not limited to:

- There may not be a human available to disambiguate the answer (unattended machines, mail servers, etc.)
- The human / user may have no idea which is the correct choice, especially in the case of a phishing attackor other malicious intent
- The additional latency introduced may cause the originating application to time out
- The user experience would be time consuming to select each site and subsite intended (www.intranet, images.intranet, etc.)
- Caching the responses could lead to problems when the user changes location (internal sites would fail when offsite, or otherwise lead to incorrect sites being loaded)

For these and other reasons, implementation of this technique is not recommended.

3. Implementation / Disclaimers

This document does not reference an implementation. Due to the numerous issues described above, we do not recommend this solution be implemented. We do not recommend that this be viewed as a solution to the namespace collision problem.

This is a very slight mitigation. It should not be viewed as a solution to the "namespace collision" issue.

4. IANA Considerations

This document contains no IANA considerations.

5. Security Considerations

While this method may make some users more aware of which version of a name they are going to (and so careful users may avoid some

phishing attacks), the security risks described above outweigh this potential benefit.

There are numerous security implications in this approach, including leaking internal names (secret-project.corp.example.com), users being tricked into selecting the incorrect choice when trying to disambiguate answers, etc.

For these reasons, it is not recommended that this solution be deployed.

6. Acknowledgements

The authors wish to thank some folk, including Fred Baker, Bob Braden, Carsten Bormann, Nevil Brownlee, Eric Burger, Brian Carpenter, Benoit Claise, Keith Drage, Martin J. Duerst, David Harrington, Paul Hoffamn, John Levine and Ted Lemon,

7. References

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication.]

From -00 to -01.

- Nothing changed in the template.

from -01 to -02

- Rewrite. Less flippant.

From -02 to -03:

- Changed to Informational. Suggestion from ISE:"I see only one remaining thing - you've changed its Intended Status to Experimental. I think Informational would be better, since 'Experimental' implies that you have an implementation and are publishing the document so that others can try it too. "

Author's Address

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net