SAC066
SSAC Comment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions

A Comment from the ICANN
Security and Stability Advisory Committee (SSAC)
6 June 2014

Preface

This is a Comment to the ICANN Board from the Security and Stability Advisory Committee (SSAC) concerning the JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions. The SSAC advises the ICANN community and Board on matters relating to the security, stability, and integrity of the Internet's naming and address allocation systems. This includes operational matters (*e.g.*, pertaining to the correct and reliable operation of the root name system), administrative matters (*e.g.*, pertaining to address allocation and Internet number assignment), and registration matters (*e.g.*, pertaining to registry and registrar services). 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 authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this Comment, references to SSAC members' biographies and statements of interest, and SSAC members' dissents to or withdrawals from the findings or recommendations in this Comment are at the end of this Comment.

Table of Contents

Executive Summary

The Security and Stability Advisory Committee (SSAC) has reviewed the Report prepared for ICANN by JAS Global Advisors (herein referred to as the "JAS") entitled "Mitigating the Risk of DNS Namespace Collisions: A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report." It has identified eight issues, and makes recommendations in relation to each of them. A summary of the recommendations is provided below; context, motivation, and discussion are provided in the sections that follow. The recommendations fall into two categories: those related to operational considerations and those related to strategic considerations.

Operational Recommendations:

- The Internet Corporation for Assigned Names and Numbers (ICANN) should expand the range of situations that would trigger an emergency response, for example national security, emergency preparedness, critical infrastructure, key economic processes, commerce, and the preservation of law and order.

- Instead of a single controlled interruption period, ICANN should introduce rolling interruption periods, broken by periods of normal operation, to allow affected end-user systems to continue to function during the 120-day test period with less risk of catastrophic business impact.

- ICANN should perform an evaluation of potential notification approaches against at least the requirements provided by the SSAC prior to implementing any notification approach.

- ICANN should implement a notification approach that accommodates Internet Protocol Version 6 (IPv6)-only hosts as well as IP Version 4 (IPv4)-only or dual-stack hosts.

- ICANN should provide clarity to registries on the rules and the method of allocation of blocked names after the conclusion of the test period.

Strategic Recommendations:

- ICANN should consider not taking any actions solely based on the JAS Phase One Report. If action is planned to be taken before the entire report is published, communications to the community should be provided to indicate this clearly.

- ICANN should in due course publish information about not yet disclosed issues.

- ICANN should seek to provide stronger justification for extrapolating findings based on one kind of measurement or data gathering to other situations.

1. Introduction

The term "name collision" refers to the situation where a name that is defined and used in one namespace may also appear in another. Users and applications intending to use a name in one namespace may actually use it in a different one, and unexpected behavior may result where the intended use of the name is not the same in both namespaces. The circumstances that lead to a name collision could be accidental or malicious. In the context of top level domains (TLDs), the conflicting namespaces are the global Internet Domain Name System (DNS) namespace reflected in the root zone as published by the Root Zone Management Partners (currently the Internet Corporation for Assigned Names and Numbers (ICANN), the U.S. Department of Commerce National Telecommunications and Information Administration (NTIA), and Verisign) and any other namespace, regardless of whether that other namespace is intended for use with the DNS or any other protocol.

With respect to collisions with names provisioned under ICANN's new generic TLD (gTLD) program, on 26 February 2014 ICANN published a report entitled "Mitigating the Risk of DNS Namespace Collisions: A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report," prepared for ICANN by JAS Global Advisors (hereinafter referred to as the "JAS Phase One Report")[1]. The JAS Phase One Report provides a set of recommendations that support an approach for identifying and managing the impact of current and future DNS namespace collisions, notifying operators of potential DNS namespace related issues and providing emergency response capabilities in the event that critical systems related to human health and safety are adversely impacted.

The SSAC thanks ICANN and the JAS for their efforts in addressing the name collision issue and the opportunity to comment on this work. In particular, the SSAC appreciates the constructive cooperation and collaboration of ICANN and JAS in providing, on a number of occasions, further information and clarification to inform the production of this report.

[1] See "Mitigating the Risk of DNS Namespace Collisions: A Study on Namespace Collisions in the Global Internet DNS Namespace and a Framework for Risk Mitigation, Phase One Report" at http://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-26feb14-en.pdf.

2. SSAC Comments

2.1 Clear and Present Danger to Human Life

a. Summary of JAS Recommendation

Recommendation 3 of the JAS Phase One Report states:

> "Emergency response options are limited to situations where there is a reasonable belief that the DNS namespace collision presents *a clear and present danger to human life*."

b. SSAC Comment

Recommendation 3 sets too high a barrier for the application of emergency response options. Limiting emergency response options to the situation of a "clear and present danger to human life" ignores a broad range of scenarios that may have substantial detrimental impact on, for example, national security, emergency preparedness, critical infrastructure, security protocols and mechanisms such as anti-virus software, key economic processes, commerce, or markets and the preservation of law and order.

c. SSAC Recommendation

Recommendation 1: ICANN should expand the range of situations that would trigger an emergency response, for example national security, emergency preparedness, critical infrastructure, key economic processes, commerce, and the preservation of law and order.

In making this recommendation, the SSAC recognizes that every situation will require the exercise of judgment and few decisions will be black and white.

2.2 Controlled Interruption Period

a. Summary of JAS Recommendation

Recommendation 6 of the JAS Phase One Report states:

> "ICANN require new TLD registries to publish the controlled interruption zone immediately upon delegation in the root zone. After the 120-day period, there shall be no further collision-related restrictions on the registry."

b. SSAC Comment

The JAS approach means that service for collision-affected users would be interrupted until those users are able to identify and fix the collision problem. This interruption could be as long as 120 days. A company that relied upon impacted systems to process payroll, track and order inventory, schedule customer visits, etc., might experience unreasonably lengthy business interruption.

It is also possible that only the most technically sophisticated system administrators will be aware of the potential for this type of service interruption and even fewer will be able to implement remediation easily, especially since no remediation techniques are currently offered to enable collision occurrence management.

While every approach to controlled interruption involves balancing trade-offs and exercising judgement, the SSAC considers that the single controlled interruption period as proposed in the JAS Phase One Report is not the optimal approach to test for, identify and remediate name collisions.

c. SSAC Recommendation

Recommendation 2: Instead of a single controlled interruption period, ICANN should introduce rolling interruption periods, broken by periods of normal operation, to allow affected end-user systems to continue to function during the 120-day test period with less risk of catastrophic business impact.

Controlled interruption periods starting at 24 hours and eventually lengthening to 30 days would be separated by periods of at least 3 days, to allow users or system administrators to identify or develop and put in place solutions or workarounds. Collisions detected during the earlier controlled interruption periods would potentially be resolved before the next interruption period. Even though the resolution periods will need to be long, recognizing that no resolution options are currently being considered as part of this occurrence management framework, this approach would at least eliminate prolonged downtimes and induced outages for end users and enterprises.

The rolling interruption periods should be lengthened as they progress to trigger collisions that occur at lower frequencies: e.g., only once every 7 days. For example, a process that may fail due to a collision might only be run weekly or monthly, and so a controlled interruption period of less than a week or month would not necessarily catch the collision. These longer interruption periods will also attract the attention of users or system administrators who may have ignored a shorter interruption period on the assumption that the (unknown) problem had been resolved.

Lastly, the controlled interruption does not have be a separate event in the overall launch sequence. It could run in parallel with some other periods,

2.3 Use of Localhost "Flag" IP Address

a. Summary of JAS Recommendation

The JAS Phase One Report recommends that during the test period the operator of the TLD use a unique "flag" IP address (127.0.53.53) to notify system administrators:

> "Because the primary objective is to communicate with system administrators through their logs, this unique and strange IP will hopefully be noticed and the administrator will search the Internet for assistance."

Use of this "Flag" address facilitates investigation by some end-user system administrators, but not for end-users in general.

b. SSAC Comment

The SSAC believes that the principal requirements for a notification system are:

1. *Effective Communication.* The chosen system should pass relevant information to affected parties effectively, via notification messaging and/or if possible, in a direct manner, recognizing that the target audience is a combination of technical system administrators and non-technical end-users. Examples of notification messaging could include Intrusion Defense System/Intrusion Prevention System/Data Leak Prevention (IDS/IPS/DLP) systems alerts, third party notifications from honeypot operators, or log file analysis. Direct notification could include application failures (non-resolution errors), walled-garden style web page notifications, and local log files. At minimum, "relevant information" should include the nature of the problem experienced by the user and a link to a page containing supplementary information including contact information for those responsible for administration of the test period (in case emergency response is requested) and the schedule for the test period.

2. *Measurability*. The chosen system should be measurable, such that it is possible to gauge the impact of name collisions and track how the impact changes with time. With a threshold of "Clear and Present Danger to Human Life" being designated, it is important to be able to determine when such a threshold could be reached. The SSAC's broader recommendations on threshold levels call for richer data collection. Measurements should at least include, but not be limited to, amount of traffic, types of traffic, and sources of traffic.

3. *Minimum Harm.* The chosen system should minimize the potential for collateral damage. For instance, address-based redirection has the potential to impact not only a huge array of standard protocols, but also non-standard protocols used within enterprises. The leakage of Personally Identifiable Information (PII) is an example of such collateral damage. External actors appointed to implement a

> mitigation system (e.g. appointed honeypot operators) must operate under a high standard of care.

Based on these three measures of effectiveness for a notification system, the SSAC would draw a different conclusion to the JAS Phase One Report on the most appropriate notification system. The JAS report seems to place privacy concerns ahead of other criteria such as effective notification and measurability and consequently recommends the "flag" address. However the SSAC considers that a wealth of operational experience exists in minimizing PII exposure by honeypots.

The SSAC advises ICANN to perform an evaluation against at least the criteria articulated above prior to implementing any notification approach. The SSAC has performed an initial analysis in Appendix A for community review. The SSAC understands that additional confidential information available to ICANN but not publicly released will most likely have an impact on the evaluation.

c. SSAC Recommendation

Recommendation 3: ICANN should perform an evaluation of potential notification approaches against at least the requirements provided by the SSAC prior to implementing any notification approach.

2.4 IPv4 Solution Only

a. Summary of JAS recommendation

Recommendation 7 of the JAS Phase One Report states:

> "ICANN require registries that have elected the "alternative path to delegation," rather than a wildcard, instead publish appropriate A and SRV resource records for the labels in the ICANN SLD Block List to the TLD's zone with the 127.0.53.53 address for a period of 120 days. After the 120-day period, there shall be no further collision-related restrictions on the registry."

b. SSAC Comment

The proposed approach of using the single "flag" address 127.0.53.53 for localhost is inadequate, as it is applicable to IPv4-only or dual-stack hosts only and does not support IPv6-only hosts. No direct equivalent exists in IPv6 space.

Support for IPv6-only clients is highly recommended. ICANN should deploy solutions with an eye to the future, and support for IPv6-only clients is necessary both to support the ongoing effort to deploy IPv6 on Internet-connected systems and to accommodate IPv6-only infrastructure that might be deployed internally, but for which dependencies on the global DNS namespace exist.

c. SSAC Recommendation

Recommendation 4: ICANN should implement a notification approach that accommodates IPv6-only hosts as well as IPv4-only or dual-stack hosts.

2.5 General Availability of Blocked Names

a. Summary of JAS recommendation

Recommendation 7 of the JAS Phase One Report states that:

> "ICANN require registries that have elected the "alternative path to delegation," rather than a wildcard, instead publish appropriate A and SRV resource records for the labels in the ICANN 2LD Block List to the TLD's zone with the 127.0.53.53 address for a period of 120 days. After the 120-day period, there shall be no further collision-related restrictions on the registry."

b. SSAC Comment

ICANN has not specified any restrictions on the allocation and activation of blocked names after the conclusion of the test period. ICANN should consider providing clarity to registries on the rules and the method of allocation of these names (e.g. sunrise, Trademark Clearing House (TMCH), land rush, etc.).

c. SSAC Recommendation

Recommendation 5: ICANN should provide clarity to registries on the rules and the method of allocation of blocked names after the conclusion of the test period.

2.6 Name Collision Framework Not Complete

a. Summary of JAS Recommendation

The statement of work (SOW) developed by ICANN staff calls for the following deliverables[2] as part of a Name Collision Occurrence Management Framework:

1.1 Develop a Risk Assessment Model
  1.1.1 Impact of malware/adware/clickfraud tools
  1.1.2 Analysis of Collisions in previous TLD delegations
  1.1.3 Analysis of Collisions in existing TLDs

[2] "Statement of Work for the Development of the Name Collision Occurrence Management Framework", ICANN, November 11, 2013, https://www.icann.org/en/about/staff/security/ssr/name-collision-sow-11nov13-en.pdf.

1.1.4 Monte Carlo Analysis
1.1.5 Survey Instruments
1.1.6 Develop a Taxonomy of Queries
1.2 Options to manage risks

While not providing details of its analyses in the publicly released version of its Phase One report, JAS does recommend the following mitigation measures:

1. If the new gTLD is .CORP, .HOME, or .MAIL, then the entire new gTLD must be blocked indefinitely (indeed, "permanently")
2. If the new gTLD hasn't already been delegated, then the entire new gTLD must undergo a new process called "controlled interruption"
3. If the new gTLD has already been delegated, i.e., via the "alternate path" with an SLD block list[3], then the SLDs on the block list are subject to controlled interruption.

b. SSAC Comment

The SSAC acknowledges that the publicly released version of the JAS Phase One report is only intended to go part way to delivering the requirements of the SOW, and that the full detail of the Name Collision Occurrence Management Framework is work in progress. Noting that the SOW calls for the final Framework to incorporate comment and input from the ICANN Community, the SSAC looks forward to providing such comment when the full Framework, along with its associated analyses, is able to be made public.

c. SSAC Recommendation

Recommendation 6: ICANN should consider not taking any actions solely based on the JAS Phase One Report. If action is planned to be taken before the entire report is published, communications to the community should be provided to indicate this clearly.

2.7 Incomplete Report

a. Summary of JAS Recommendation

In the JAS Phase One Report, certain technical details, experimental methods, and data have been omitted until vulnerabilities discovered during the study have been remediated.

On page 3 the JAS Phase One Report states:

[3] See "New gTLD Security and Stability Considerations. Verisign Labs Technical Report #1130007", Version 2.2, March 28, 2013. http://www.verisigninc.com/assets/gtld-ssr-v2.1-final.pdf and "Reports for Alternate Path to Delegation Published", ICANN, November 17, 2013. http://newgtlds.icann.org/en/announcements-an6d-media/announcement-2-17nov13-en.

> "After extensive discussions with impacted vendors, JAS is concerned that publication of the experimental methods and data contained in the complete JAS report may accelerate discovery of the vulnerability and/or serve to facilitate exploitation of the vulnerability after it is discovered. As such, pursuant to ICANN's process and out of an abundance of caution, JAS has recommended against publication of a complete draft report at this time."

b. SSAC Comment

Without having visibility of all details of the background of the findings, it is hard for SSAC to give clear recommendations or to assess the validity of the findings. Thus the SSAC recommends that ICANN publish information about the vulnerabilities in due course, at which point the SSAC may further comment.

c. SSAC Recommendation

Recommendation 7: ICANN should in due course publish information about not yet disclosed issues.

2.8 The Nature of Collisions

a. Summary of JAS Recommendation

The JAS Phase One Report offers the assumption that:

> "The modalities, risks, and etiologies of the inevitable DNS namespace collisions in the new TLD namespaces will resemble the collisions that already occur routinely in other parts of the DNS."

b. SSAC Comment

Such an assumption would be fully justified if the types of names being introduced as new gTLDs were similar to those that have been introduced in the past. However, many of the new gTLDs are introducing commonly used words and place names which have a high probability of existing in already established domain names at the second and third levels, as well as existing in internal namespaces. This may give rise to other types of name collisions that did not arise in the course of previous delegations.

Thus, caution should be exercised in adopting any conclusions based on this assumption without extensive further study. Extrapolating findings based on one kind of data gathering to different scenarios should not be made without very detailed investigation of whether the extrapolation is justifiable, and what adjustments should be made to the findings. Testing and mitigation proposals should allow for the possibility that new types of name collisions will occur.

c. SSAC Recommendation

Recommendation 8: ICANN should seek to provide stronger justification for extrapolating findings based on one kind of measurement or data gathering to other situations.

3. Acknowledgements, Statements of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four 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 all Committee members and any conflicts of interest—real, apparent, or potential—that may bear on the material in this document. The Dissents section provides a place for individual members to disagree with the content of this document or the process for preparing it. The Withdrawals section is a listing of individual members who have recused themselves from discussion of the topic. Except for members listed in the Objections and Withdrawals sections, this document has the consensus approval of all members of the Committee.

3.1 Acknowledgments

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

SSAC Members:
Joe Abley
Don Blumenthal
Patrik Fältström
James M. Galvin
Julie Hammer
Warren Kumari
Danny McPherson
Ram Mohan
Rod Rasmussen
Mark Seiden

ICANN staff:
Julie Hedlund
Barbara Roseman
Steve Sheng (editor)

3.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: https://www.icann.org/resources/pages/biographies-2014-06-06-en.

3.3 Dissents

There were no dissents to this Comment.

3.4 Withdrawals

David Conrad has withdrawn from this Comment due to a pre-existing relationship with JAS.

Appendix A: Alternative Notification Approaches

At a high level, there are at least four options for notifying potentially impacted parties, each occurring at varying stages in the transaction process. In this Appendix, the SSAC outlines these options, and provides an analysis.

1. **Do nothing.** Users of labels at any level of a domain name (e.g., www.corp.example.com, as a result of search lists [SAC064]), that collide with new gTLD strings in their operating environments will experience failures or misconnections and come to realize their configurations are problematic only after the new gTLD and domains within that gTLD are delegated and elicit operational impacts to their systems.

   SSAC Analysis: This approach provides no communication, is not measurable and does not attempt to mitigate any harm to any application or protocol. This is not acceptable, as previously conveyed by SSAC [SAC057 and SAC062]. Potentially impacted parties should be given some amount of forewarning and, ideally, context as well as an indication of potential remediation options. Vulnerabilities that result from name collisions may be subtle and might not necessarily result in immediately visible or distinctive failures.

2. Perform qualitative analysis of query sources as measured at root and TLD servers and provide proactive user notification.

   SSAC analysis: To perform qualitative analysis of query sources and notify users proactively, we need to have the ability to instrument measurements at the root server system or other levels of authoritative DNS, or to obtain the necessary visibility into other levels of the DNS hierarchy (e.g. recursive name server, end system, application, etc.) of recursion and caching in the system.[4] These temporal testing capabilities should be combined with a large-scale user education program.

   Given that we do not have these capabilities today, this approach is not a viable short-term option. Nevertheless, the SSAC notes that such measurement capabilities are needed, as previously recommended by SSAC in SAC045, SAC046, and SAC059. Such capabilities are also aligned with recommendations provided in SAC063 as it relates to DNSSEC Root Zone KSK Rollover.

3. Implement structured, short-term test periods ("controlled interruption"), in which end users utilizing a proposed gTLD will experience a failure, and then be given time (after each short-term test period) for planning and effectuating remediation efforts specific to their environment. This approach triggers the errors in a more controlled

[4] See Google Public Name Collision Comment, 2013, http://forum.icann.org/lists/comments-name-collision-05aug13/pdfkwCAlijJOp.pdf.

environment, and can be used as an early warning system to notify potentially impacted parties. There are two variations to notification in this approach:

3a: As recommended in the JAS Phase One Report, during the test period, the operator of the TLD will use a unique "flag" IP address (127.0.53.53) to notify system administrators.

SSAC Analysis: As a notification mechanism, the 127.0.53.53 approach requires system administrators noticing something unusual and then searching the Internet for assistance. It is unclear whether system administrators will notice or know what to do. Additionally, one of the main channels that system administrators will be notified of issues is through end-users. It is highly unlikely that end users will know what 127.0.53.53 might mean, let alone what to do with it.

The 127.0.53.53 approach does ensure no information leakage, and thus minimizes any privacy and legal issues from unintended connections. If minimizing information leakage is of the greatest concern, such an approach could be preferred.

3b: Instead of returning 127.0.53.53, addresses could be returned that direct the end user or system administrator to a web page that specifies the issue (a honeypot) and points to either potential solutions, or otherwise at least to Frequently Asked Questions (FAQs), documentation, consultants or expert groups who may be able to provide further information related the error condition and contextual remediation options. Care should be taken to cause minimal disruption to non-Hypertext Transfer Protocol (HTTP) requests directed at the honeypot.

SSAC analysis: As a notification mechanism, the honeypot offers the following advantages over 127/8:

- For HTTP traffic, the honeypot is more likely to get people's attention, and there is greater ability to disseminate information through a browser.
- For non-HTTP traffic, the honeypot is no worse a notification mechanism than the 127/8 approach.

As a data collection mechanism, honeypots could help operators and ICANN understand the scale of the impact of delegation by creating data streams that can be analyzed to understand the impact of a proposed TLD.

With the honeypot approach there is a risk of Personally Identifiable Information (PII) leakage. Traffic flow is created across the Internet and traffic is logged at the honeypot. Responses to non-HTTP transactions might introduce other collateral damage. If notification is a higher priority, then the honeypot approach could be preferred.

Extensive operational experience with such "honeypots" by various SSAC members (e.g., Internet Motion Sensor Project (IMS),[5] the Honeynet Project,[6] DNS changer[7]) suggests that this approach may be viable, and might lead to the best outcome, given the current impracticality of option 2 above, since it would provide the most direct mechanism for affected parties to be informed of such issues on their networks. The risk of exposure of PII or additional vulnerabilities to users could be managed with a clear data collection, retention and privacy policy. This approach would facilitate measurement of the impact of each controlled interruption and allow its effectiveness to be gauged. If we suppose such a honeypot only provided service over HTTP, and that inbound data from all other sources was refused in a manner designed to avoid client time-outs, the risk of collateral damage due to collection of data sent using non-HTTP protocols could be minimized.

[5] See Tracking Global Threats with the Internet Motion Sensor, NANOG 32, 2004. https://www.nanog.org/meetings/nanog32/presentations/bailey.pdf and The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets, USENIX SRUTI05, 2005,at https://www.usenix.org/legacy/event/sruti05/tech/full_papers/cooke/cooke_html/

[6] See at https://www.honeynet.org/.

[7] DNSchanger is the honeypot concept working at Internet scale. See: http://www.dcwg.org/.