RSSAC056:
RSSAC Advisory on Rogue DNS Root Server Operators

An Advisory from the ICANN Root Server System Advisory Committee (RSSAC)
7 July 2021

Preface

In this report, the ICANN Root Server System Advisory Committee (RSSAC) examines both measurable and subjective activities of a root server operator (RSO) that could be considered rogue to inform future Root Server System (RSS) governance bodies. Future RSS governance bodies may use this document to develop a more complete definition of rogue RSO actions and will ultimately be the authority in determining subjective factors such as intent, when judging the actions of a RSO. The audience of this report is the Board of Directors of the Internet Corporation for Assigned Names and Numbers (ICANN), future root server system governance bodies, and, more broadly, the Internet community.

The RSSAC advises the ICANN community and Board on matters relating to the operation, administration, security, and integrity of the Internet's Root Server System. The RSSAC has the following responsibilities:

1. Communicate on matters relating to the operation of the Root Servers and their multiple instances with the Internet technical community and the ICANN community
2. Communicate on matters relating to the administration of the Root Zone with those who have direct responsibility for its administration
3. Engage in ongoing threat assessment and risk analysis of the Root Server System and recommend any necessary audit activities to assess the current status of the root servers and the root zone
4. Respond to requests for information or opinions from the ICANN Board.
5. Report periodically to the Board on its activities
6. Make policy recommendations to the ICANN community and Board

The RSSAC has no authority to regulate, enforce, or adjudicate. The advice offered in this report should be evaluated on its merits.

A list of the contributors to this report, references to RSSAC Caucus members' statements of interest, and RSSAC members' objections to the findings or recommendations are at the end of this report.

Table of Contents

Table of Contents **3**

1 Introduction **4**

2 Relationship to RSSAC037 **4**

2.1 Guiding Principles of the Root Server System 4

2.2 RSSAC037 and the Term “Rogue” 5

3 Descriptions of a Rogue Operator **5**

4 Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals **7**

4.1 Acknowledgments 7

4.2 Statements of Interest 8

4.3 Dissents 8

4.4 Withdrawals 8

1 Introduction

The purpose of the root server system (RSS) is to provide responses to queries for data in the root zone. Its intended users are caching recursive DNS (Domain Name System) resolvers who need to know the contents of the root zone. These resolvers trust that every query to any RSO will be answered correctly; this trust is based on decades of positive experience.

A rogue operator has the potential to adversely affect this trust in a variety of ways. Some adverse effects include denying or delaying root zone resolution, violating the privacy of users, causing users to interact with the wrong endpoints, and eroding users' confidence in the global DNS. While protections within the DNS protocol and at other layers of the protocol stack can help mitigate these effects on end users, a rogue operator would be a serious issue.

In RSSAC037, the RSSAC provided some examples of how a RSO might go rogue and described how those behaviors should be dealt with. This document examines objective and subjective criteria for considering a RSO as rogue. A non-exhaustive list of rogue behaviors is provided, with examples and reasons.

Given the evolution of RSS governance, this document aims to inform future RSS governance bodies on the types of RSO activities that might be considered rogue. Future RSS governance bodies may use this document to develop a more complete definition of rogue RSO actions.

In this document, a RSO is an operator of one of the nameservers listed in the authoritative root zone from IANA, as described in RSSAC030, “RSSAC Statement on Entries in DNS Root Sources.”[1] This document acknowledges that some queries sent to a root server may be answered by responders that are not operated by a RSO. This could be due to an alternate configuration of a resolver, packet interception, or other reasons. Such “non-RSO responders” are outside the scope of this document and are not considered in the description of rogue behaviors. Responses received from non-RSO responders cannot be considered as evidence of rogue behaviors of a RSO. Discerning which responses are from non-RSO responders may be a difficult task.

Finally, throughout this document, unless otherwise indicated, “the root zone” always refers to the authoritative root zone from IANA.[2]

2 Relationship to RSSAC037

2.1 Guiding Principles of the Root Server System

In RSSAC037, “A Proposed Governance Model for the DNS Root Server System,”[3] the RSSAC articulated eleven principles that guided the development and operation of the RSS and RSOs,

[1] See RSSAC030: RSSAC Statement on Entries in DNS Root Sources
[2] See RSSAC026v2: RSSAC Lexicon
[3] See RSSAC037: A Proposed Governance Model for the DNS Root Server System

and which should remain core principles going forward. The RSSAC has since published these principles with an additional new explanatory text as a standalone document in RSSAC055.[4] These principles provided a high-level framework for the RSSAC Caucus in our discussion of rogue behaviors.

2.2 RSSAC037 and the Term "Rogue"

Section 6 of RSSAC037 describes how a potential RSS governance model might work in different scenarios. Specifically, Section 6.5 describes a scenario in which a RSO "goes rogue." Examples of rogue behavior in RSSAC037 include a RSO intentionally not serving the correct contents of the root zone file and a RSO not answering queries from selected entities. Section 6.5 of RSSAC037 describes how such behaviors might be reported and handled.

This document is informed by RSSAC037, and expands on the examples of Section 6.5 of RSSAC037 by examining objective and subjective criteria for considering a RSO's activities as rogue, along with a few examples of those behaviors. Determining whether these behaviors are rogue also involves determining the intent of the RSOs. This subjectivity makes the determination difficult and prone to faulty analysis.

3 Descriptions of a Rogue Operator

This section describes representative actions of a RSO that may be considered rogue in terms of the guiding principles outlined in RSSAC055. Actions of a root server operator that are deemed deliberate or that are in repeated violation of these core principles may qualify as rogue operations. Accidental, mistaken, or temporary conditions that are reasonably remediated (such as testing new software) should not be considered rogue behavior. Future governing bodies have the difficult task of determining the intent behind potentially rogue actions. This includes differentiating between temporary or accidental actions, and actions carried out with the intent to deceive or negatively impact the querier.

The following is a list of objective measurements or observations of how an operator can be considered "rogue," based on the guiding principles from RSSAC055. The examples listed here are illustrative and not meant to be exhaustive.

1. **Incorrect Response Data**: A RSO intentionally gives an answer to a query in which any of the record sets in the Answer section of the response differ from those contained in the root zone. Examples include responses with record sets that have more or fewer records than the corresponding record sets in the root zone, and responses where any record in a record set has values different from the record set in the root zone.

2. **Extra Response Data**: A RSO intentionally gives an answer to a query in which the Authority or Additional sections contains correct data from the root zone**,** but also include

[4] See RSSAC055: Principles Guiding the Operation of the Public Root Server System

additional data not found in the root zone; for example, the insertion of an AAAA or glue record for a name that only has an A record.

3. **Bad or Incorrect Error Codes**: A RSO intentionally gives a negative answer to a query for which there is data in the root zone. Examples include responses with an RCODE of SERVFAIL at a time when the same server is giving NOERROR responses, responses with an RCODE of NOTIMP for queries that other RSOs can answer, and responses with an RCODE of FORMERR for queries that other RSOs can answer.

4. **Omitting DNSSEC**: A RSO intentionally returns responses that omit DNSSEC-related records from the root zone for queries that have the DO bit set. Examples include not returning RRSIG records and not returning NSEC records.

5. **Incorrect DNS Protocol Usage**: A RSO intentionally responds to queries in a manner that is not supported by standards-track Request for Comments (RFCs). Examples include using undefined RCODEs, undefined OPCODEs, a malformed response, and improper values in EDNS0 fields.

The following is an non-exhaustive example of subjective observations that could be considered "rogue," based on the guiding principles from RSSAC055.

1. **Intentionally Degraded Service:** A RSO purposely degrades service to queries based on the source of the queries, except in the case in which the RSO is under attack. Examples include sources based on country, ethnic or religious status, or service provider. For example, this could be done by dropping packets, delaying responses, or routing methods beyond what would be considered normal traffic engineering.

Note that this document is primarily discussing rogue operators in the form of rogue RSO organizations. Because RSOs hire many individuals to fulfill their root service obligations, it is possible that an individual in an organization may perform actions that are considered rogue by this document. An organization should generally not be considered rogue based on the behavior of individuals unless those actions are left unresolved.

4 Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the RSSAC process. The Acknowledgments Section lists the RSSAC Caucus members, outside experts, and ICANN staff who contributed directly to this particular document. The Statement of Interest Section points to the biographies of all RSSAC Caucus members. The Dissents Section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals Section identifies individual members who have recused themselves from discussing the topic with which this Advisory is concerned. Except for members listed in the Dissents and Withdrawals Sections, this document has the consensus approval of the RSSAC.

4.1 Acknowledgments

The RSSAC thanks the following members of the caucus and external experts for their time, contributions, and reviews in producing this report.

RSSAC Caucus members
Ken Renard (Work Party Leader)
Abdulkarim Oloyede
Barbara Schleckser
Brad Verd
Di Ma
Duane Wessels
Fred Baker
Hiro Hotta
Jaap Akkerhuis
Jeff Osborn
Kazunori Fujiwara
Kevin Wright
Mallory Knodel
Marc Blanchet
Nicolas Antoniello
Paul Hoffman
Paul Muchene
Peter DeVries
Russ Mundy
Shinta Sato
Warren Kumari
Wes Hardaker
Yazid Akanho

ICANN Staff
Andrew McConachie

Danielle Rutherford
Justin Caton
Ozan Sahin
Steve Sheng (editor)

4.2 Statements of Interest

RSSAC caucus member biographical information and Statements of Interests are available at: https://community.icann.org/display/RSI/RSSAC+Caucus+Statements+of+Interest

4.3 Dissents

There were no dissents.

4.4 Withdrawals

There were no withdrawals.