RSSAC0XX:
RSSAC Advisory on Rogue DNS Root Server Operators

A Report from the ICANN Root Server System Advisory Committee (RSSAC)

{DAY} {MONTH} 2021

Preface

In this report, the ICANN Root Server System Advisory Committee (RSSAC) examines measurable and subjective root server operator (RSO) activities that could be considered rogue. The purpose of this document is to inform future Root Server System (RSS) governance bodies on types of RSO activity that might be considered rogue and the risks that these activities may pose to the Internet community. Future RSS governance bodies may use this document for developing 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 an 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. It 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 that administration.
3. Engage in ongoing threat assessment and risk analysis of the Root Server System and recommend any necessary audit activity to assess the current status of root servers and the root zone.
4. Respond to requests for information or opinions from the ICANN Board of Directors.
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 merit.

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 in this report are at the end of this report.

Table of Contents

Table of Contents **3**

1 Introduction **4**

2 Related Work **5**

2.1 Guiding Principles of the Root Server System 5

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 give authoritative answers to queries about the DNS root. Its intended users are caching recursive DNS resolvers who need to know the contents of the root zone. These resolvers trust that every query to any root server operator (RSO) will be answered correctly; that trust is based on many decades of positive experience.

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

In this document, we examine objective and subjective criteria for considering an RSO as rogue. We provide an non-exhaustive list of rogue behaviors, with examples and supporting reasons.

Given the evolution of root server system governance, this document aims to inform future RSS governance bodies on the types of RSO activity that might be considered rogue and the risks that these activities may pose to the Internet community. Future RSS governance bodies may use this document for developing 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 an RSO.

In this document, an RSO is an operator of one of the nameservers listed in the authoritative root zone from IANA, as described in RSSAC030[1], “RSSAC Statement on Entries in DNS Root Sources”, This document acknowledges that some queries sent to a root name server may be answered by responders that are not operated by an RSO. This could be due to an alternate configuration of a resolver, by packet interception, as well as 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 an 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.

[1] See https://www.icann.org/en/system/files/files/rssac-030-04nov17-en.pdf

2 Related Work

2.1 Guiding Principles of the Root Server System

In RSSAC037,[2] "A Proposed Governance Model for the DNS Root Server System," the RSSAC articulated eleven principles that guided the development and operation of the RSS and RSOs, and which should remain core principles going forward. The RSSAC has since published these principles with additional new explanatory text as a standalone document in RSSACXXX.[3] These principles provide a high level framework for the working group in our discussion of rogue behaviors.

2.2 RSSAC037 and the Term "Rogue"

Section 6 of RSSAC037 describes how a potential root server system governance model might work in different scenarios. Specifically, Section 6.5 describes a scenario in which an RSO "goes rogue". Examples of rogue misbehavior in RSSAC037 are the RSO intentionally not serving the correct contents of the root zone file, the RSO not answering queries from selected entities, and the RSO misusing funds from the Financial Function (FF). Section 6.5 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 an RSO's activities as rogue, as well as providing an expanded list of rogue behaviors, with examples and supporting reasons. This document, however, does not go into intent, detection, and mitigation of such behaviors because those are appropriate for future governance bodies to determine.

3 Descriptions of a Rogue Operator

This section describes representative actions of an RSO that may be considered rogue in terms of the guiding principles outlined in RSSAC037. Actions of a root server operator that are deemed deliberate or 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 that would separate such temporary, or accidental, actions with true intent to deceive or negatively impact the query source.

[2] See https://www.icann.org/en/system/files/files/rssac-037-15jun18-en.pdf
[3] <editor note: add the URL in the new RSSAC publication on principles>

The following is a list of objective measurements or observations of how an operator can be considered "rogue", based on the guiding principles from RSSAC037. The examples listed here are illustrative, and are not meant to be exhaustive.

1. *Changed answers:* An RSO intentionally gives an answer to a query where any of the record sets in the Answer or Authority or Additional sections of the response differ from those contained in the root zone. Examples include responses with record sets that have 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. *Incorrect additional answers:* An RSO intentionally gives an answer to a query where the Answer, Authority, or Additional sections contain correct data from the root zone, but also include additional data not found in the root zone. Examples include responses with extra NS records that are not the root zone.

3. *Bad error codes:* An RSO intentionally gives a negative answer to a query for which there is any 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:* An 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. *Bad DNS usage:* An RSO intentionally responds to queries in a manner that is not supported by standards-track RFCs. Examples include using undefined RCODEs, undefined OPCODEs, and improper values in EDNS0 fields.

The following is an non-exhaustive list of subjective observations that could be considered "rogue", based on the guiding principles from RSSAC037.

1. *Intentionally degraded service:* An RSO purposely degrades service to queries based on the source of the queries, except in the case where 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 outside of normal traffic engineering.

Note that this document is primarily discussing rogue operators in the form of rogue organizations. Because organizations hire many individuals to fulfill their root service obligations, it is possible that an individual of an organization may make statements or perform actions that are considered rogue by this document. An organization should generally not be considered rogue based on the behaviour 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 Acknowledgements 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 discussion of 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 review 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
Russ Mundy
Steve Crocker
Shinta Sato
Warren Kumari
Wes Hardaker
Yazid Akanho

ICANN Staff
Andrew McConachie
Danielle Rutherford
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.