

Statement of Work and Scope for Effects and Mitigations of a Rogue Root Server Operator 7 April 2020

Background

Root Server Operators (RSOs) are dedicated to providing accurate and reliable service of the DNS Root Zone in accordance with the 11 principles outlined in RSSAC037¹. This work party will examine scenarios where an RSO, or someone acting as an RSO, serves incorrect zone data or otherwise violates any of those 11 principles. The purpose of this work is to understand the risks of potential rogue operators as well as prepare mitigations and proper responses to limit harm to the global Internet. The RSSAC Caucus will prepare a document detailing these risks and mitigations to the ICANN community.

Scope

The document will:

- Enumerate different types of rogue operations to include at least:
 - False announcements of an RSOs address space (route hijacking) or other impersonation of a legitimate root server
 - Non-IANA root zone data being served where authentic IANA data is expected (either by a legitimate or non-legitimate root server operator)
 - Alterations to root zone data
 - Threats to a local root service² that could render such a service as “rogue”.
- Outline the types of damage that could be done to different resolver configurations. A configuration of specific interest is the set of DNSSEC-validating resolvers versus non-validating resolvers.
- Describe potential detection strategies of rogue operations
- Describe mitigations for rogue operators and servers
- Recommend appropriate responses by other Root Server Operators or ICANN entities (for example: The Root Server Operator Review Panel³ aka DRF)
- Recommend *general* actions to be taken by RSS stakeholders
- Consider alterations of the root zone data before publication by the Root Zone Maintainer as out of scope

Deliverables

A final draft of the document will be delivered to RSSAC for approval and publication.

¹ RSSAC037 <https://www.icann.org/en/system/files/files/rssac-037-15jun18-en.pdf>

² RFC 7706 <https://tools.ietf.org/html/rfc7706>

³ A New Cooperation and Governance Model for the Root Server System
<https://www.icann.org/en/system/files/files/rss-governance-model-concept-paper-23apr19-en.pdf>

Date of Delivery

The work party shall submit a first draft to the RSSAC prior to December 2020. The work party shall submit the final draft to the RSSAC no later than April 2021. Submission prior to the deadline is welcome.

Guidelines

The RSSAC requests that this work party adhere to RSSAC operational procedures in its work. The work party should choose a work party leader. The work party leader will report progress on this work to RSSAC as appropriate. In the event that the deadline will not be realized, the work party leader should inform RSSAC immediately and provide details of the work that cannot be completed by the deadline.

RSSAC support staff will assist the work party deliberation of the work, including setting up a mailing list for the work party, arranging and supporting regular teleconference calls, taking notes of meetings, and drafting background materials, as needed.

Prior Relevant Work

RSSAC037 -- <https://www.icann.org/en/system/files/files/rssac-037-15jun18-en.pdf>