The 2015 Root Server Operators' Exercise on Emergency Response

Introduction

In the 1st Quarter of 2015, the collective of Root Server Operators (RSOs), as a commitment to their ongoing performance of operating the 13 root servers, performed an exercise to test their processes and procedures in response to a simulated threat to the Root Server System. The exercise was facilitated by Delta Risk LLC[1], a reputable firm with prior experience in exercising disaster and continuity events.

This document summarises the activity and the recommendations from Delta Risk.

The exercise described above is not the first of these exercises, as several have been performed in the past, this is, however the first time the RSOs have collectively published the recommendations.

The RSOs would like to note that they have begun work on many of these items, and expect to extend, formalize, and document these existing procedures.

[1] www.delta-risk.net

Exercise Objectives

A Work Party made up of RSO staff and Delta Risk constructed the Root Server exercise. It embodied the following objectives.

1. Provide an opportunity for RSOs to collaborate on a response to a theoretical incident impacting multiple DNS root servers, their systems and operations.

2. Assess the effectiveness of emergency communications procedures between all of the DNS Root Server Operators

3. Provide an opportunity for RSOs to evaluate their organization's internal communications, escalation processes, and personnel dependencies

Impressions, Strengths & Areas for Improvement

At the conclusion of the event the following observations were made by Delta Risk.

Overall Impressions

- The Root Server Operators (RSOs) demonstrated excellent problem solving and creativity in responding to the presented threats in the exercise.
- Individual Root Server Operators are postured well to respond.
- Coordination between RSOs during an incident is helping Root Server Operators to respond effectively, further optimisations on their own response processes will further improve response capabilities

Strengths

- Each RSO contains passionate and technically sound staff able to diagnose and respond to incidents.
- Collectively the RSOs ability to use existing communication tools for rapidly sharing information is strong.
- The operational and technical diversity of the RSOs adds significant robustness to the Root System when faced with vulnerabilities in specific software or systems.

Areas for Improvement

- The Root Server Organizations could codify communication triggers and procedures between RSOs and external stakeholders.
- Coordination between RSOs could be improved by establishing an Incident Manager to help with information flow and coordination, between RSOs. This Incident Manager would be drawn from within the RSOs own ranks, and would be per-event.
- Pre-coordinated plans and procedures between the RSOs for community response would assist the Root Server Operators in communicating more effectively with the wider community in case of incidents.

Delta Risk Recommendations

The following ten recommendations were presented to the Root Server Operators at the culmination of the exercise. It is accepted that implementation of many of these recommendations were already in progress by the Root Server Operators prior to the exercise and as such the RSOs had already established a sound footing toward addressing these capabilities.

1. Develop well-formed communications protocols between the RSOs.
   - Define protocols for ongoing communications.
   - Define back-up procedures for any non-functioning capabilities.
   - Define and share "telephony etiquette" to facilitate effective communications.
   - Develop regular RSO communications and health checks.

2. Establish a role of an RSO incident “coordinator” to guide the overall incident response process.
   - Establish criteria and procedures for when to activate the incident coordinator.

3. Investigate and implement a real-time presence and instant messaging capability that is effective for all RSOs.

4. Develop automated process to update RSO contact information (including encryption details) and ensure communication systems are updated in a timely manner.

5. Develop and coordinate on pre-canned external communications templates to assist in community understanding.

6. Define terms of impact and build cohesive response and communications threshold references for the RSO community.

7. Implement monitoring thresholds that detect drops in traffic to provide visibility to a category of attacks that sink traffic as opposed to sourcing it.

8. Build relationships with local and regional law enforcement if relationships don't exist. Identify capabilities law enforcement can bring to assist with investigation and response activities.

9. Identify RSOs relationships with national or regional Computer Incident Response Teams (CIRT) / Computer Emergency Response Teams (CERT). Determine the best way to interact with CIRT / CERT in order to leverage their resources during response to a critical incident.

10. Conduct communication and coordination exercise at senior RSO manager level to understand if gaps in policies and procedures exist and improve communication and awareness throughout the individual organizations.

Conclusion

The individual Root Server Operators have accepted these recommendations and will prioritise appropriate resources to establishing a plan that responds to these recommendations.

The collective of Root Server Operators also commits to ongoing exercises to ensure that they maintain a sufficient level of readiness commensurate with the activities involved in performing the duties as a Root Server Operator.

This report was prepared by:

Jim Martin, F-Root
Terry Manderson, L-Root

This document has been endorsed by all 12 of the Root Server Operators (www.root-servers.org) .