Operational Statement
on the
Integrity of the Root Server System

As of 2019-03-14

Introduction

During the past weeks, reports on incidents relating to the provisioning of DNS on the public internet have appeared. Two examples are

https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

and

https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

While some of the organisations that provide DNS service for the public DNS root are mentioned in these articles, the combined set of root server operators are issuing the following joint statement.

Statement

The events described in these articles were not related to the provisioning of DNS service for the global DNS root. The modus operandi of the attackers was to target domain names related to systems for managing domain delegation for domains well below the root level. The collective understanding is that these attacks were not targeted at the infrastructure used to serve the global DNS root zone.

To the best of the combined knowledge of all root-server operators, the events described in these articles have had no impact what so ever on the public root service or the integrity of the root zone they serve.

- There are no signs of lost integrity or compromise of the content of the root zone.
- There are no signs of lost integrity or compromise of the content of the root-servers.net zone.
- There are no signs of compromise of computer or network equipment related to the operation of the DNS root.
- There are no signs of unusual traffic or redirection of DNS traffic aimed at the root servers.
- There are no signs of clients having received unexpected responses from root servers.

While the events are disconcerting in several ways, they were, to the best of our knowledge, not related to the integrity or service of the root zone.

Should this situation materially change an additional Operational Statement will be made.