June 2026 Traffic Increase

Root Server Operators
July 2026

Overview

Starting on June 29, 2026, all DNS root server identities observed an increase in DNS query traffic to approximately double normal levels. A group of related autonomous systems were identified as responsible. Traffic remained elevated for approximately one week and returned to normal on July 7, 2026.

Timeline

Starting close to 12:00 UTC on June 29, traffic approximately doubled for all root server operators. Prior to the increase, the root server system received approximately 1.6M queries per second on average. During the increase, the RSS received 3.2M queries per second on average.

Elevated traffic was reported at several different metro locations, particularly on the U.S. East coast and in Europe, with some variation among individual root server identities.

Early investigation identified several related autonomous systems as the apparent source of elevated traffic. Further inspection revealed the traffic to be well-formed, query-name-minimized queries from tens of thousands of source IP addresses, and primarily for .com, .net, .org, .info, and .uk TLDs.

After several attempts to contact the autonomous system originating the traffic, a representative from the AS responded on July 3rd. They confirmed that the traffic originated from their networks (i.e., was not spoofed) and was the unintentional result of recent recursive resolver software updates. Traffic levels dropped briefly on July 3rd, for about two hours, but then returned to elevated levels. Following further outreach on July 6th, traffic levels returned to normal starting on July 7th.

Impacts

While the traffic increase was significant, it did not impact the service availability or performance of any root server operator in any measurable way. As stated in expectation E.3.4-A of RSSAC001[1], "Each RSO is expected to make all reasonable efforts to ensure that sufficient capacity exists in their deployed infrastructure to allow for substantial fluctuations in traffic loads." The RSOs did not consider the traffic to be an intentional attack, nor a hazard to their operations, and did not take any measures to mitigate it.

[1] https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-001-root-service-expectations-01aug23-en.pdf