December 2025 DDoS against multiple DNS root servers

Root Server Operators
July 2026

Overview

On December 23, 2025, multiple DNS root server identities were targeted with a volumetric DDoS attack. The attack came in multiple waves, was highly distributed, peaked at over one terabit per second of attack traffic across all root server identities, and lasted just under ten minutes.

Timeline & Targets

Different RSOs reported the attack starting and ending at slightly different times, perhaps indicating that attacks to each root server identity were not launched exactly simultaneously. Starting times varied between 15:37—15:39 UTC and ending times between 15:41—15:48 UTC.

The table below indicates which root server identities were targeted by this attack.

a.root-servers.net	Yes
b.root-servers.net	Yes
c.root-servers.net	Yes
d.root-servers.net	Yes
e.root-servers.net	Yes
f.root-servers.net	No
g.root-servers.net	No
h.root-servers.net	No
i.root-servers.net	Yes
j.root-servers.net	Yes
k.root-servers.net	Yes
l.root-servers.net	Yes
m.root-servers.net	Yes

Impacts

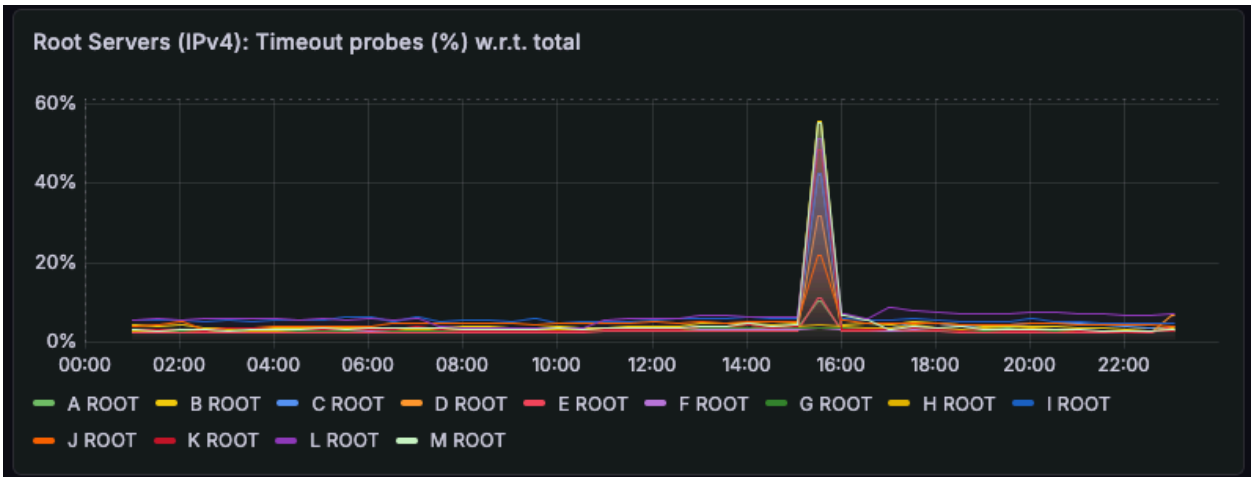
The RIPE NCC DNS Monitoring Service (DNSMON) regularly monitors latency and availability of all root server identities from numerous RIPE Atlas Anchor vantage points. DNSMON indicates that the attack did have an impact on several root server identities, to varying degrees.

This DNSMON screenshot[1] covers the period from 15:00 to 16:10 UTC. Note the color range slider is set so that intervals with 0% unanswered queries are shown in green and 35% or greater unanswered queries are shown in red, with a color gradient in between.

The “RootViz” dashboard from SIDN Labs, also based on RIPE Atlas measurements, captured the event as well.[2]

[1] https://dnsmon.ripe.net/?start=2025-12-23T15:00:00.000Z&end=2025-12-23T16:10:00.000Z&zone=root&protocol=udp&ipVersion=both&viewpoint=unanswered-queries&autoRefresh=false&rt_color_range=60-722&rrt_color_range=125-200&uq_color_range=0-35&level=servers

[2] https://rootviz.sidnlabs.nl/public-dashboards/f81c02c68d7a4986ba1674fd7eb87b74?from=2025-12-23T00:00:00.000Z&to=2025-12-23T23:59:59.000Z&timezone=utc



RSO representatives quickly coordinated efforts, shared pertinent attack forensics for analysis, and continued to monitor traffic levels for recurrence. No mitigation actions were taken due to the short time span of the attack (10 minutes).

The root server system remained available for DNS clients despite the varying degrees of impact across the service footprint. There are no known reports of end-user visible error conditions during this incident. Because the DNS protocol is designed to cope with partial reachability among a set of name servers, the impact was, to our knowledge, limited to minor delays for some name lookups when a recursive name server needed to query a DNS root name server (e.g. a cache miss concerning a TLD). One aspect of DNS resilience is the diversity of root systems and continuing with independent operations has proven to be an effective approach to ensuring service availability.

The DNS Root Server Operators continue their work to increase the resilience and capacity of the Root Server system.