June 2025 Route Hijack of Root Server Address Prefixes

Overview

On June 20, 2025, routes for several root server address prefixes appeared in the global routing table originating from an unauthorized autonomous system, AS35168. This autonomous system number is registered to TNS-Plus, a network provider operating in Kazakstan. These bogus routes were advertised to its peer, AS28910 Uzbektelekom, and were present for approximately one hour and thirty minutes. During that time, DNS queries from some systems in the region where these networks operate were sent to unauthorized root name servers.

The following root server identifiers and prefixes were impacted by this route hijack:

Root Server Identifier	IPv4 Prefix
a.root-servers.net	198.41.0.0/24
b.root-servers.net	170.247.170.0/24
c.root-servers.net	192.33.4.0/24
f.root-servers.net	192.5.5.0/24
g.root-servers.net	192.112.36.0/24
h.root-servers.net	198.97.190.0/24
j.root-servers.net	192.58.128.0/24
m.root-servers.net	202.12.27.0/24

Timeline of Events

- 2025-06-20 19:40 bogus routes advertised
- 2025-06-20 19:42 RSO systems alert to the possibility of a route hijack[1]
- 2025-06-20 21:10 bogus routes withdrawn

Following the initial alert, the RSO identified a total of six root server prefixes impacted by the route hijack and all RSOs were notified. RSO representatives contacted both TNS-Plus and

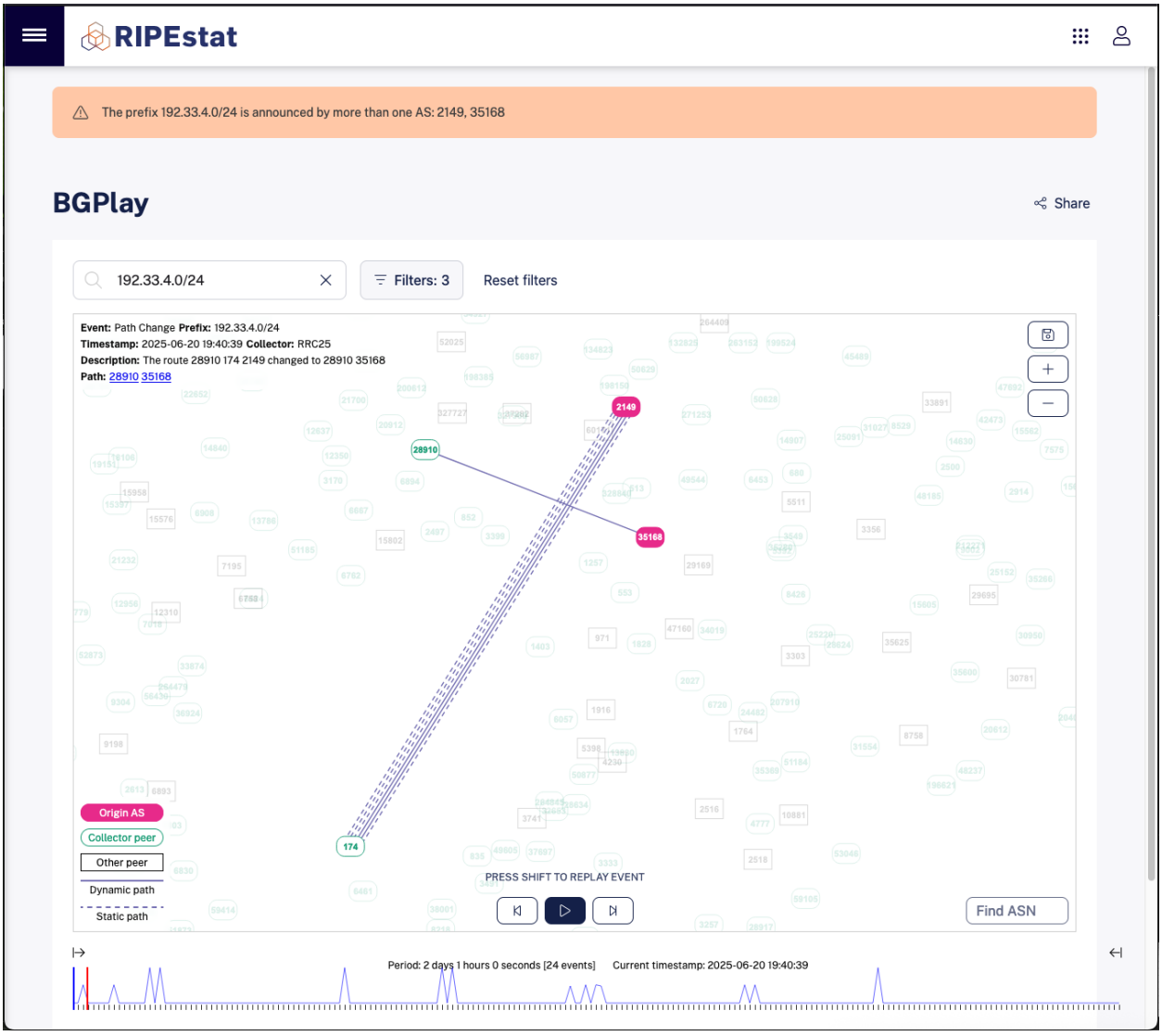
[1] The hijack was detected by a tool internally developed and operated by Verisign.

Uzbektelekom for an explanation, which has not yet been provided. If a meaningful explanation is provided, it will be shared with the community.

Subsequent analysis confirmed active instrumentation of the hijacked routes during the incident and two more impacted RSOs were identified.

Visibility

Evidence of the route hijacks for six root server identifiers are visible via RIPE NCC's BGPlay system. The screenshot below shows the data for c.root-servers.net, for example. The line connecting nodes 28910 and 35168 represents the bogus route advertisement. BGPlay URLs showing the route hijack for six root servers are provided as an appendix.



Context and Mitigations

There are multiple documented instances of middleboxes interfering with root server system traffic.[2,3] However, we believe this is the first documented case where routes to root server prefixes were hijacked using BGP.

The bogus routes had origin AS35168, suggesting they were not created by an RSO. RPKI is designed to detect route announcements made by unauthorized parties and would have caused these routes to be rejected by ISPs using RPKI Route Origin Validation.

Although three of the root server prefixes hijacked have covering Route Origin Authorizations published in RPKI, that did not prevent AS28910 from accepting the covered prefixes from AS35168 because apparently AS28910 does not implement Route Origin Validation at this time. Other policy, topology, and BGP route selection processes prevented any further propagation for all the hijacked prefixes in this incident.

Operators of recursive DNS services are encouraged to enable DNSSEC validation. While DNSSEC cannot prevent route hijacks and therefore cannot prevent DNS queries from being delivered to unauthorized root name servers, DNSSEC ensures the integrity of data and prevents acceptance of falsified responses from unauthorized name servers.

Appendix: BGPlay Links

a.root-servers.net:
https://stat.ripe.net/bgplay/198.41.0.0%2F24#starttime=1750446000&endtime=1750622400&rrcs=0%2C1%2C3%2C4%2C5%2C6%2C7%2C10%2C11%2C12%2C13%2C15%2C16%2C18%2C19%2C20%2C21%2C22%2C23%2C24%2C25%2C26&maxPathLength=1&showReannouncements=false&instant=469%2C1750448439

b.root-servers.net:
https://stat.ripe.net/bgplay/170.247.170.0%2F24#starttime=1750446000&endtime=1750622400&rrcs=0%2C1%2C3%2C4%2C5%2C6%2C7%2C10%2C11%2C12%2C13%2C15%2C16%2C18%2C19%2C20%2C21%2C22%2C23%2C24%2C25%2C26&maxPathLength=1&showReannouncements=false&instant=1%2C1750448439

c.root-servers.net:
https://stat.ripe.net/bgplay/192.33.4.0%2F24#starttime=1750446000&endtime=1750622400&rrcs=0%2C1%2C3%2C4%2C5%2C6%2C7%2C10%2C11%2C12%2C13%2C15%2C16%2C18%2C19%2C20%2C21%2C22%2C23%2C24%2C25%2C26&maxPathLength=1&showReannouncements=false&instant=1%2C1750448439

h.root-servers.net:
https://stat.ripe.net/bgplay/198.97.190.0%2F24#starttime=1750446000&endtime=1750622400&rrcs=0%2C1%2C3%2C4%2C5%2C6%2C7%2C10%2C11%2C12%2C13%2C15%2C16%2C18%2C19%2C20%2C21%2C22%2C23

[2] http://dx.doi.org/10.1109/INFCOM.2013.6566965
[3] http://www.icir.org/mallman/pubs/JFP+16/JFP+16.pdf

%2C24%2C25%2C26&maxPathLength=1&showReannouncements=false&instant=1%2C1750448439

j.root-servers.net:
https://stat.ripe.net/bgplay/192.58.128.0%2F24#starttime=1750446000&endtime=1750622400&rrcs=0%2C1%2C3%2C4%2C5%2C6%2C7%2C10%2C11%2C12%2C13%2C15%2C16%2C18%2C19%2C20%2C21%2C22%2C23%2C24%2C25%2C26&maxPathLength=1&showReannouncements=false&instant=299%2C1750448439

m.root-servers.net:
https://stat.ripe.net/bgplay/202.12.27.0%2F24#starttime=1750446000&endtime=1750622400&rrcs=0%2C1%2C3%2C4%2C5%2C6%2C7%2C10%2C11%2C12%2C13%2C15%2C16%2C18%2C19%2C20%2C21%2C22%2C23%2C24%2C25%2C26&maxPathLength=1&showReannouncements=false&instant=299%2C1750448439