GOAL
Find name servers that move from IP address to IP address too much.

METHOD
Using a passive DNS Database, detect changes in IP addresses from A records three or more times in a month.

CAVEAT
Organizations may have valid use cases for moving name servers (e.g., content distribution networks [CDN]).

FILTER
Select name servers whose IPs are in different ASNs (according to BGP, using available routing data); treat ASNs as different only when they have different owners (according to WHOIS).

RESULT
Name servers that move without a valid reason are probably malicious.