A Study of Unexpected DNS Queries at B-Root

Dipsy Desai, Jelena Mirkovic
USC/ISI

Domain Name System (DNS) lies at the core of the Internet to translate human-readable domain names into machine-friendly Internet Protocol (IP) addresses so that web browsers can access Internet resources requested by the users. B-Root server is one of the 13 DNS root servers across the world, which are authoritative for queries to different Top-Level-Domains (TLDs). Root servers receive billions of queries every year mainly for address resolution. Among these, there are a huge number of unexpected queries (queries that occur frequently or occur with no valid request), accounting for more than half of the total incoming queries. As such, there is a clear need to identify the reason for such high density of queries. In this work, we perform a comprehensive and longitudinal analysis to find the source and probable cause of such millions of unexpected, repetitive, and malformed incoming queries hitting B-root server. Finding the root cause of these queries will assist to classify them based on the cause, such as being malicious or accidental. One of the aims of this project is to improve the efficiency of the B-root server by comprehensively dealing with unexpected queries.

In addition to the unexpected queries, we find that a major type of invalid queries are those requests arriving with an invalid TLD. For example *internal*, *local*, *lan*, *localhost*, etc. are the most common and highly queried ones among the list. Chromium, an open source web browser project accepts user inputs to search terms, website names, etc. It's probing process involves sending three randomly generated DNS queries of 7-15 lowercase characters (such as *banananinа*) to determine the presence of captive portals. These random characters usually appear as TLDs (although occasionally have a domain name search at the end [Thomas(2020)]) and hence add to the total density of invalid TLDs reaching B-root.

Another type of queries arriving at B-root are Empty queries, which are of the form $QNAME = .$. They account for more than 3.5% of all incoming queries only behind invalid TLDs like *internal* and *local*. One of the major contributors to the empty query category are the Priming Queries which are of type Name Sever (NS), as defined in [Koch et al.(2017)]. Introduced in 2017, priming queries are used the find the list of IP addresses of some or all of the root servers. One word queries are also among the popular queries at B-root, which have one word TLD, either valid or invalid. We hypothesize the recent increase in their count to the introduction of QNAME Minimization [Bortzmeyer(2016)] in 2017. This is a technique aimed at enhancing the privacy offered by DNS resolver, by clipping the query and only sending the full QNAME to the name server for resolution. Minimized Queries account for more than 31% of the one word queries at B-root.

We observe an unusual behaviour at B-root as some IP addresses repeatedly send queries for the same type of Resource Record (RR). If the DNS resolver on these IP addresses is configured correctly, it should be able to cache the results for a certain period of time before making another request for the same RR, making them unexpected queries. Another large set of queries are the ones from Bogon IP address ranges (private IP addresses such as 10.0.0.0/8). We find that these addresses most likely belong to IoT devices configured inside a home network. We classify these queries as unexpected as such queries should not leave their local network in the first place.

References

[Bortzmeyer(2016)] Stéphane Bortzmeyer. 2016. DNS Query Name Minimisation to Improve Privacy. RFC 7816. https://doi.org/10.17487/RFC7816

[Koch et al.(2017)] Peter Koch, Matt Larson, and Paul E. Hoffman. 2017. Initializing a DNS Resolver with Priming Queries. RFC 8109. https://doi.org/10.17487/RFC8109

[Thomas(2020)] Matthew Thomas. 2020. *Chromium's impact on root DNS traffic.* Verisign Inc. Retrieved Feb 26, 2024 from https://blog.apnic.net/2020/08/21/chromiums-impact-on-root-dns-traffic/