DNS Observatory: Monitoring Global DNS Performance

Pawel Foremski, Paul Vixie
Farsight Security, Inc.
{pjf,vixie}@fsi.io

Abstract

DNS Observatory is a new research project by Farsight Security that aims at monitoring the performance, content, and security of the global DNS. We present a preliminary analysis of the world's top 10,000 authoritative DNS servers, responsible for ~87% of all DNS traffic we saw in January 2019. We found that just 500 top servers and 9 networks receive majority of all queries, that although most servers respond in <25ms, 20% need over 100ms, and that response delay is generally smaller for more popular DNS servers.

Methodology

1. We listen to SIE passive DNS channel 202, which streams ~200,000 DNS query-response transactions per second, seen above recursive DNS resolvers around the world.
2. We track the most popular values of a key feature, e.g. server IP, queried domain, or IP seen in answer.
3. We maintain an entry in cache for each popular key. Under each entry, we track several statistics, e.g. number of queries, successful responses, distinct FQDNs, SLDs, TLDs, qtypes, TTLs, IP addresses seen in answers, response delays, etc.
4. Every minute we reset all statistics and write the old values to a minutely file. We aggregate the files into larger time windows, and store all data as time-series.

Collected Data

Currently, we track the world's most popular:

1. authoritative DNS server IP addresses,
2. TLDs, effective SLDs, FQDNs,
3. IPv4 and IPv6 addresses seen in answers,
4. SLDs and FQDNs seen in NXDOMAIN responses.

For this poster, we focus on (**1**) as seen in January 2019, when we processed ~423 billion DNS transactions. We select just the top 10k servers, which corresponds to 87% of traffic.

Results

1. Huge portion of global DNS traffic is highly concentrated on a relatively small number of server IPs: 50% of traffic corresponds to roughly 500 servers. This highlights the possible negative impact on the Internet in case of a successful attack on a relatively small number of servers. More popular servers, likely higher in the DNS hierarchy, handle much more NXDOMAIN and "empty answer" traffic.
2. If we aggregate the traffic by the corresponding Autonomous System network name, we find that Amazon is the winner ahead of Verisign. The data suggests majority of world's DNS traffic is handled by only a dozen organizations.
3. The DNS is fast but with space for improvement. We found that ~10% of transactions finish in <10ms, 50% in <25ms, but as ~20% need >100ms, we suspect still many resolvers need to cross an ocean to reach a DNS zone authority.
4. The Internet engineers did their job right when it comes to *really* busy servers: generally they respond in <50ms.

Figures

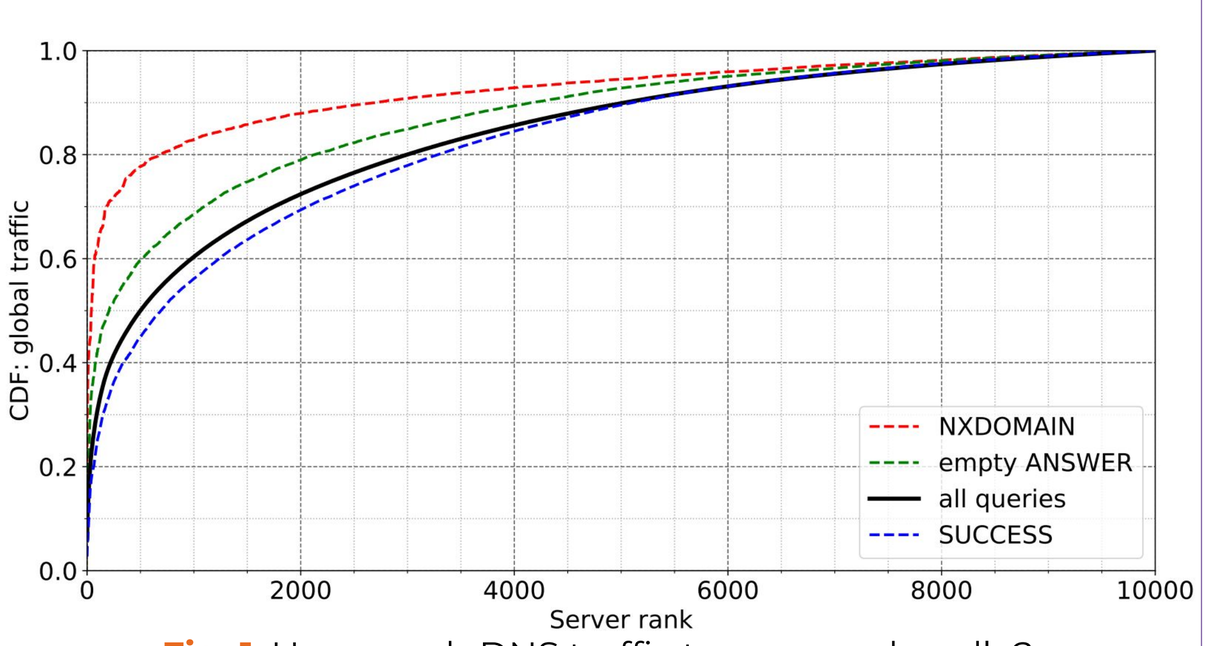

Fig. 1: How much DNS traffic top servers handle? Distribution of traffic vs. server popularity.

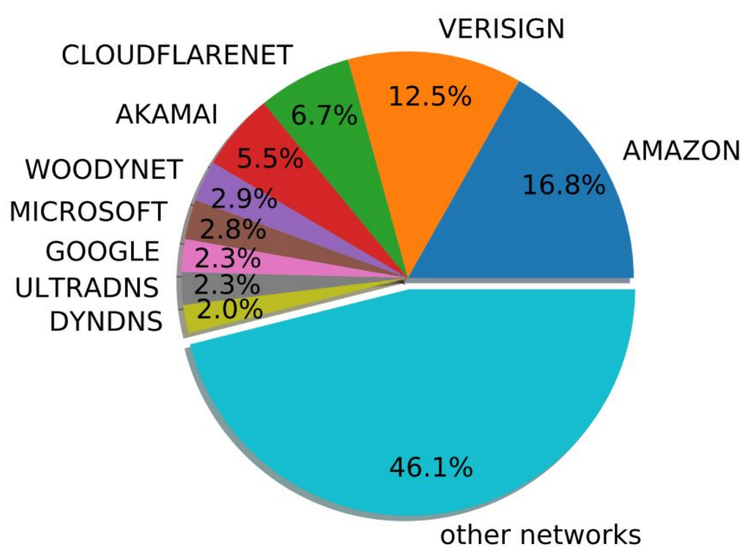

Fig. 2: Which networks handle most DNS traffic? Distribution of traffic vs. AS name

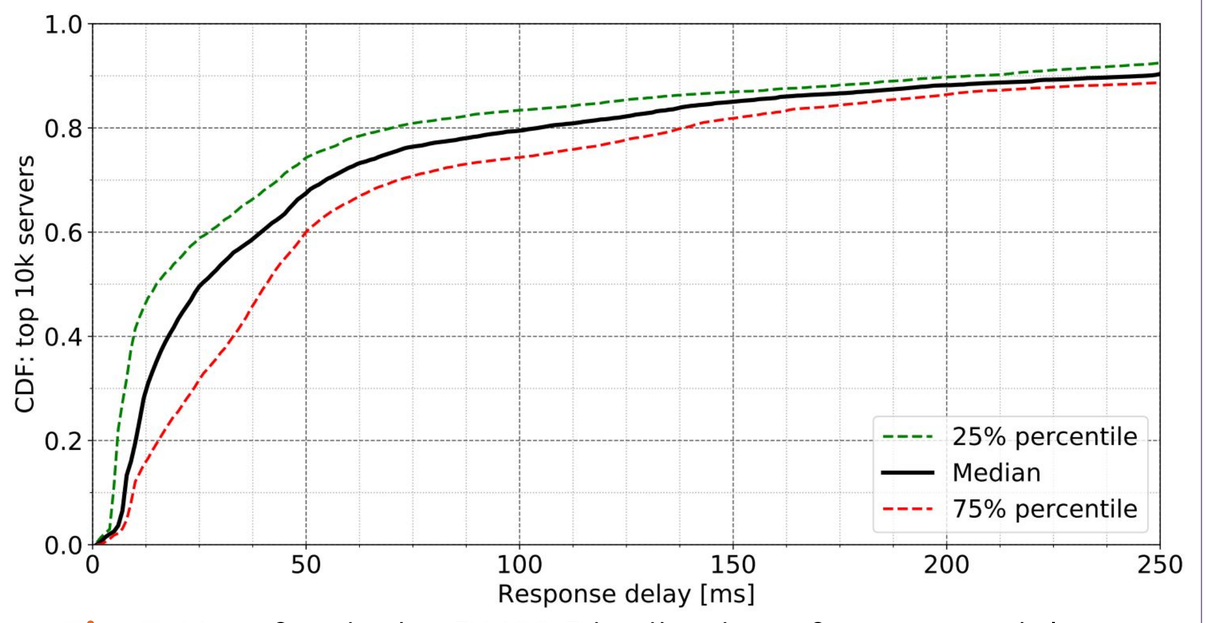

Fig. 3: How fast is the DNS? Distribution of response delays.

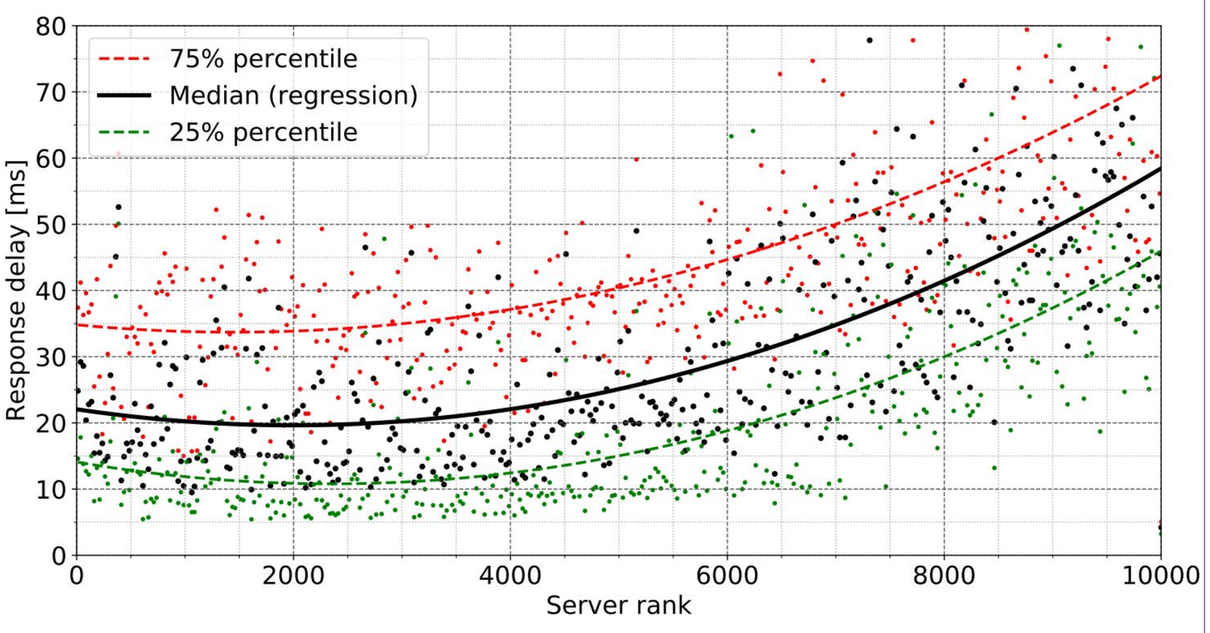

Fig. 4: Are more popular servers faster? Delay vs. server rank: measured data (point = 25 servers) and regression lines.

FARSIGHT SECURITY

WIDE Camp
March 5-7, 2019, Hamamatsu, Japan