ICANN NCAP Meeting #39 (2021-01-27) Report Recap

Introduction. The meeting largely centered around an analysis of *.corp* and *.home* queries seen at A & J root, with some comparison to *.mail*, which was examined in a prior meeting. Matt Thomas led the analysis presentations noting the rise in volume in both names beginning in March 2020 coinciding with the COVID-19 pandemic. The usage patterns were noticeably different amongst the two, and different too from *.mail*. It was reported that Google's open source browser Chromium was changed in December 2020 that resulted in a significant drop in query traffic most noticeable in the *.home* analysis. The meeting concluded with a brief update From James Galvin on the Study 2 project. What follows is a technical summary of the *.corp* and *.mail* case studies.

.CORP Analysis. Matt Thomas provided a handful of graphs from A and J root showing query traffic patterns and trends over the past few years. There was marked increase in query volume and distinct source IP addresses beginning in March 2020 for `.corp` names, which was hypothesized to be related to the changing work patterns as a result of COVID-19. This hypothesis bore out as details were explored. Volume was somewhat concentrated in North America and Europe, but fairly widespread, particularly when grouped by source ASN. Examining the ASNs many of the largest contributors were residential ISPs, giving credence to the supposition that *.corp* was being used in work environments, but not at home.

Throughout this case study and later for *.home* a Venn diagram would show the relation of A, J, and old J root servers and the source ASN of query traffic. J-root consistently sinks a larger proportion of queries from different networks.

> *[Editor's note: This is most likely a result of J's much richer server deployment practice. J-root likely appears closer in the routing topology to a larger number of networks than A-root, with more resolver RTT estimates preferring J over A. Every root operator's traffic profile will differ according to each unique operator's unique server deployment model and BGP peering arrangements.]*

Label analysis provided further insight into source of *.corp* query activity including query names ending in *airbus.corp*, *sap.corp*, *zurich.corp*, and *bank.corp*. Many third-level labels often showed geographic structure such as *amer.zurich.corp* and *emea.zurich.corp*.

> *[Editor's note: There was an unexplained, but noticeable amount of PTR type traffic, particularly noticeable at old J-root, including a significant spike in 2019. It would have been interesting to know what was behind this traffic if possible.]*

.HOME Analysis. Like *.corp*, *.home* query volume rose significantly in March 2020, also attributed to the COVID-19 pandemic. The overall query volume of queries for *.home* is significantly larger than *.corp* and also much more widely distributed to the number of source ASNs. This point was highlighted to suggest that any remediation at the host or network level may require different strategies or more effort than in cases such as *.corp* where dispersion is less, or even *.mail* where diversity is further reduced still.

A sizable amount of query volume was reduced in December 2020, attributed to a change in Google's Chromium browser code. Before the change, Chromium would perform random name queries to test if a user was subjected to NXDOMAIN redirection or hijacking. Note, even though this change was noticeable, overall .home query volume still exceeds *.corp* query volume. Examining second and third labels show active TLD and popular second-level names prepending to *.home* (e.g. *com.home*, *google.com.home*). Warren Kumari suggested this may be a result of CPE or code such as that from dnsmasq poorly implementing QNAME minimization. Matt felt this was a very plausible and likely explanation for many queries. This idea is bolstered by the prevalence of queries with large volumes of queries including labels such as *hitronhub.com.home*, *fios-router.home*, and *unifi.home*.

Matt also pointed out the noticeable quantity of first labels starting with an underscore, suggesting that *.home* queries are often associated with service discovery protocols.

References

Chromium's impact on root DNS traffic - APNIC blog post by Matt Thomas

ICANN NCAP Meeting #39 page