ICANN NCAP Meeting #36 (2021-01-06) Report Recap

Introduction. The meeting opened with Jim Galvin noting that he will have to update his SOI due to Afilias being bought out by Donuts Inc. Study 2 has been delivered to SSAC for review. This bulk of the meeting summarized sources of collision-related data sources and relevant monitoring. This was intended to help kick start thinking about name collision analysis questions that could help develop guidance to provide to the ICANN board about the risks of collisions with new delegations. Summary data from ICANN, VeriSign, B-Root, SIDN Labs, and summaries from presentations on ISATAP and WPAD problems were covered.

Data Analysis. Matt Thomas took the group through a tour of some relevant data and analysis pertinent to studying name collisions. He first summarized existing reserved TLDs (e.g. *.test*, *.example*, *.invalid*, *.localhost*). Most reserved names accounted for a fraction of a percent as measured by ITHI. *.local* was the notable exception that led not only the reserved names, but also topped all unavailable names including *.home* and *.internal* which were 2nd and 3rd respectively. Notably, *.mail* was only in the top 200 undelegated TLDs.

A+J root have seen HTTPS query types rival others to place in the top six types recently. This appears to be affiliated with Apple device leakage, but it is not clear what is the root cause for them. An analysis of resolver distribution at B-root shows a widening disparity of influence popular open resolvers (e.g. Cloudflare, Google DNS, and OpenDNS) have.

[Editor's note: This suggests that mitigation strategies directed in coordination with public resolvers may be warranted.]

A+J root data as well as summary statistics from SIDN Labs are seeing qname minimization responsible for approximately 50% of all root queries. It was pointed out that modern resolvers are turning on qname minimization by default. This led to some consideration about what effect this ultimately will have on analysis, but the answer to which is currently unclear.

A few more graphs from SSAC reports and a slide each from independent ISATAP and WPAD presentations rounded out the analysis introduction. There was a brief discussion about the nature of the *.internal* graph which exhibited somewhat regular high spikes littered over the monitored period. Warrant suggested this may be a result of how some large public resolvers perform caching, while Matt suggested it may simply be an artifact of the long tail overlaid on top of some steady state base traffic that is anomalous and scheduled to be fixed by Amazon (EC2).

References

ICANN Identifier Technology Health Indicators (ITHI), https://ithi.research.icann.org

SSAC Advisory on Private-Use TLDs, https://www.icann.org/en/system/files/files/sac-113-en.pdf