Understanding and Quantifying Aggressive Resolver Behaviors

Natália G. Knob[1], Ricardo de O. Schmidt[1], Marco A. S. Trentin[1], Jelena Mirkovic[2], Wes Hardaker[2], and John Heidemann[2]

[1]University of Passo Fundo, Brazil
[2]USC Information Sciences Institute, USA

While prior research has investigated DNS servers [12, 9, 10, 15, 2] and some DNS use patterns [1, 8, 3, 11, 7] in great detail, little is known about the diversity of DNS recursive resolvers implementations and behaviors. Yet, recursive resolvers are the linchpin of the DNS infrastructure; their (mis)behavior can affect both DNS clients and authoritative servers. Misconfigured recursives can be misused in attacks [13], or introduce delays in responses to clients [1, 4]. Recursives that generate excessive queries to the DNS infrastructure [6, 5, 14] misuse precious resources of authoritative nameservers, possibly for no useful purpose. In part, the lack of insight and understanding into diversity of recursive resolver behaviors have led communities to take leap-of-faith efforts like the DNS Flag Day, which did not go according to plans. Our research seeks to understand, quantify and characterize recursive resolver behaviors, specifically for those that aggressively send DNS queries.

As example of the abusive recursive problem, Fig 1 shows the CDF of number of requests received by the root DNS servers from unique IP addresses. This plot has been generated from DNS-OARC DITL 2018 and 2019 datasets[1]. We can see from this figure that 99% of all recursives send moderate amount of queries. However, the 1% that send aggressively were responsible for sending up to 98% and 93% of all traffic in 2018 and 2019 respectively. Moreover, the 1% of abusive recursives correspond to around 8.3k recursives in 2018 and over 14k in 2019; which might indicate a growing number of abusive recursives in the Internet, misusing the DNS infrastructure. Within the huge amount of queries sent by these abusive recursives, there is the potentially useless DNS traffic wasting, some times critical, resources of the DNS root infrastructure.

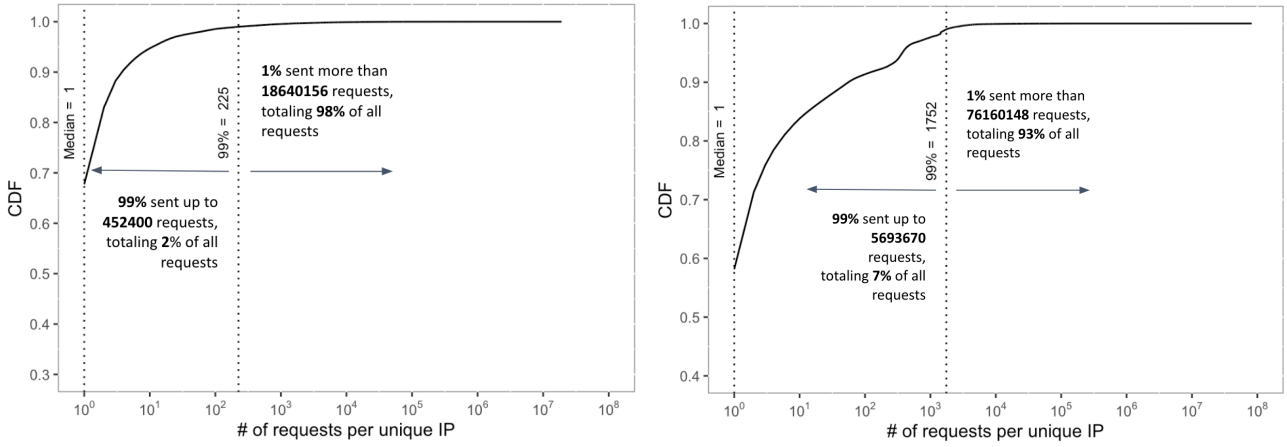

Figure 1: CDF of number of requests in 2018 (left) and 2019 (right); data from DITL datasets

We seek to understand: (1) individual behavior of aggressive recursive resolvers, e.g. are they aggressive all the time or only occasionally and to specific targets; (2) ownership of aggressive recursives; (3) nature of aggressive recursives, e.g., if they are home or cloud machines, or recursive resolvers for multiple users; and (4) root causes of aggressive behavior, e.g. improper caching, misconfiguration, malicious application, etc. Our ultimate goal is to provide insights and guidance for improved recursive software and configuration, as well as the development of tools to detect aggressive recursives and minimize their impact on the DNS infrastructure.

References

[1] Rami Al-Dalky, Michael Rabinovich, and Kyle Schomp. A Look at the ECS Behavior of DNS Resolvers. In *Internet Measurement Conference*, 2019.

[2] Mark Allman. Comments on dns robustness. In *Proceedings of the Internet Measurement Conference 2018*, IMC '18, pages 84–90, New York, NY, USA, 2018. ACM.

[3] Timm Böttger, Felix Cuadrado, Gianni Antichi, Eder Leão Fernandes, Gareth Tyson, Ignacio Castro, and Steve Uhlig. An Empirical Study of the Cost of DNS-over-HTTPS. In *Internet Measurement Conference*, 2019.

[4] Tom Callahan, Mark Allman, and Michael Rabinovich. On Modern DNS Behavior and Properties. *ACM Computer Communication Review*, 43(3), July 2013.

[5] Sebastian Castro, Duane Wessels, Marina Fomenkov, and Kimberly C. Claffy. A day at the root of the internet. *Computer Communication Review*, 38(5):41–46, 2008.

[6] Sebastian Castro, Min Zhang, Wolfgang John, Duane Wessels, and Kimberly C. Claffy. Understanding and preparing for DNS evolution. In *Traffic Monitoring and Analysis, Second International Workshop, TMA 2010, Zurich, Switzerland, April 7, 2010, Proceedings*, pages 1–16, 2010.

[1]https://www.dns-oarc.net/oarc/data/ditl

[7] Wouter B. de Vries, Ricardo de O. Schmidt, Wes Hardaker, John Heidemann, Pieter-Tjerk de Boer, and Aiko Pras. Verfploeter: Broad and load-aware anycast mapping. In *Proceedings of the ACM Internet Measurement Conference*, London, UK, 2017.

[8] Pawel Foremski, Oliver Gasser, and Giovane Moura. DNS Observatory: The Big Picture of the DNS. In *Internet Measurement Conference*, 2019.

[9] Andrew Kalafut, Minaxi Gupta, Pairoj Rattadilok, and Pragneshkumar Patel. Surveying dns wildcard usage among the good, the bad, and the ugly. In Sushil Jajodia and Jianying Zhou, editors, *Security and Privacy in Communication Networks*, pages 448–465, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[10] Daiping Liu, Shuai Hao, and Haining Wang. All your dns records point to us: Understanding the security threats of dangling dns records. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 1414–1425, New York, NY, USA, 2016. ACM.

[11] Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang, and Jianping Wu. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? In *Internet Measurement Conference*, 2019.

[12] Giovane C. M. Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker. Cache me if you can: Effects of DNS Time-to-Live (extended). Technical Report ISI-TR-734b, USC/Information Sciences Institute, July 2019. Released May 2019, updated Sept. 2019.

[13] Christian Rossow. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In *In Proceedings of the 2014 Network and Distributed System Security Symposium, NDSS*, 2014.

[14] Duane Wessels and Marina Fomenkov. Wow, that's a lot of packets. In *Proc. of Passive and Active Measurement Workshop*, 2003.

[15] Ming Zhang, Yaoping Ruan, Vivek Pai, and Jennifer Rexford. How dns misnaming distorts internet topology mapping. In *Proceedings of the Annual Conference on USENIX '06 Annual Technical Conference*, ATEC '06, pages 34–34, Berkeley, CA, USA, 2006. USENIX Association.