CycleHunter

Giovane Moura

January 22, 2021

1 Cyclic Dependency in the wild

`CycleHunter` goal is to detect cyclic dependencies within a zone. Figure 1 shows `CycleHunter`'s workflow. It is divided in four main parts, which we describe next:

1. Zone Parser: we start with this module, that reads and parses a DNS zone file, such as the the `.org` zone. Zone files contains delegations, and various types of records (A,AAA, NS, SOA, DNSSEC, and so forth). Zone parser reads the entire zone file and extract all NS records, outputing into a text file (NS List in Figure 1). Our goal is to determine *which* of these NS records are cyclic dependent, and, ultimately, what domains names in the zone file use those cyclic dependent NS records. Given many domain names are configured to use the same authoritative servers [2, 1], this step significantly reduces the search space. For example, the `.com` has 151M domain names, but only 2.19M unique NS records (**??**).

2. Resolve NS list: the next module is responsible for resolving each NS in NS list. To do that, this module asks its DNS resolver (such as BIND) for the start-of-authority (SOA) record [3], a record that every domain must have, for each NS in NS list. NS records which SOA records cannot be retrieved – that either time out or return SERVFAIL – are added to the output file *Timeout NSes*. The other NSes that have a SOA record are discarded, given they are properly delegated (otherwise the resolver could not retrieve the record).

3. Parent Check: this module is the one that ultimately detects cyclic dependent NS records. To do that, it does two main tasks: (i) determine which

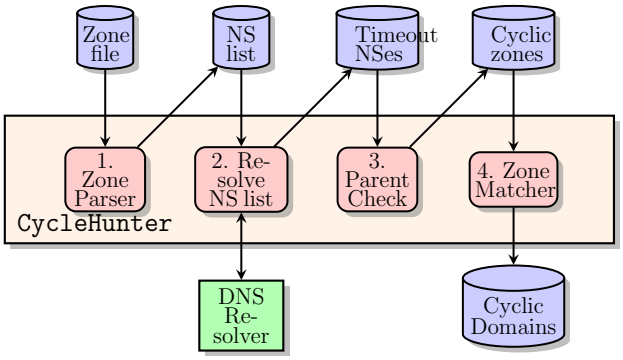

Figure 1: `CycleHunter` workflow

NS records from the Timeout NSes are *available* at the parent zone and (ii) evaluate which of them are ultimately cyclic dependent.

To do that, for each NS in *Timeout NSes*, this module asks the NS *parent* authoritative servers for their NS records. For example, consider that the NS record `ns1.example.org` has timed out. *Parent Check* then determines the parent zone of this record, which is `example.org`. Then, it determines what are the NS records of `example.org`, and ask them for the NS record of the timed out domain in question (`ns1.example.org`). (in DNS, there is some level of duplication of information in both parent and child authoritative servers [4, 5]). If a NS can be be retrieved from the parent, it is them marked for further investigation. This indicates that the timeout or error associated with this domain has to do with its *child* NS records, and not the parents. And it may as well be due to cyclic dependency.

To determine if it is indeed cyclic dependency, *Parent check* determines what DNS zones each NS depends. For example, the zone `example.org` has `[a,b].iana-servers.net` as NS records. In this example, we say that `example.org` depends on `iana-servers.net` zone to be resolvable. If `iana-servers.net` would, however, depend solely on `example.org`, then it would be *cyclic dependent*. These are marked as *Cyclic zones* and stored in a text file. (By definition, domains configured only in zone/in bailiwick cannot be cyclic dependent. However, in the wild, most second-level domains have out-of-zone NS records [4]).

Zone Matcher: the last module of `CycleHunter` consists in evaluating which domains the Zone File use NS records that are in cyclic dependency. Given multiple domains may use the same NS record, many domain names under the zone file (or even other zone files) may be cyclic dependent.

References

[1] Mark Allman. Comments on DNS Robustness. In *Proceedings of the Internet Measurement Conference 2018*, IMC '18, page 84–90, New York, NY, USA, 2018. Association for Computing Machinery.

[2] Aqsa Kashaf, Vyas Sekar, and Yuvraj Agarwal. Analyzing third party service dependencies in modern web services: Have we learned from the Mirai-Dyn incident? In *Proceedings of the ACM Internet Measurement Conference*, IMC '20, page 634–647, New York, NY, USA, 2020. Association for Computing Machinery.

[3] P.V. Mockapetris. Domain names - concepts and facilities. RFC 1034, IETF, November 1987.

[4] Giovane C. M. Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker. Cache me if you can: Effects of DNS Time-to-Live. In *Proceedings of the ACM Internet Measurement Conference*, pages 101–115, Amsterdam, the Netherlands, October 2019. ACM.

[5] Raffaele Sommese, Giovane CM Moura, Mattijs Jonker, Roland van Rijswijk-Deij, Alberto Dainotti, Kimberly C Claffy, and Anna Sperotto. When parents and children disagree: Diving into DNS delegation inconsistency. In *International Conference on Passive and Active Network Measurement*, pages 175–189. Springer, 2020.