Authority Robustness Scoring Via Glue Cycle Detection (Abstract)

Panagiotis Kintis*, David Dagon*, and Manos Antonakakis*

*Georgia Institute of Technology,
{kintis,manos}@gatech.edu, dagon@sudo.sh

I. Introduction

In preparation for DNSSEC, changes were made in 2010 to TLD nameserver operations [1]. Indirectly, these changes may have created a new class of zone fragility, which DNS architects may wish to avoid. In 2010 the `.com`, `.net`, and `.edu` zones were modified to no longer promote glue to authoritative status, and to respond to glue queries with referrals rather than non-authoritative answers.

In some cases, these changes made mutually dependent zones non-resolvable. The canonical example is a pair of mutually dependent zones that look to each other for glue:

```
example.com. NS ns1.example.net.
example.com. NS ns2.example.net.
example.net. NS ns1.example.com.
example.net. NS ns2.example.com.
```

Figure 1 shows the cycle created by this arrangement. If no record exists in cache, the resolution of `example.net` depends on finding `ns1.example.com`, which is a child label of the zone `example.com`. In turn, the successful discovery of the `example.com` authorities requires the resolution of `ns1` or `ns2.example.net`, and so on.

Such cycles were permitted in the past, and were somewhat common in various TLDs. Companies would purchase a pair of domains (e.g., a `.com` and `.net` version of their branded domain), and have the glue in one point to the other. A host resolving `example.com` child labels would be given a referral to `ns1` and `ns2.example.net`, but the answer always included glue in the *ADDITIONAL* record field of the DNS answer. The glue was "promoted to authoritative status", and allowed the resolver to use the Additional records and find the cousin nameservers.

To protect against poisoning attacks, these additional records are discarded by many modern resolvers. In such case, the resolvers would suspend resolution of the `example.com` child label, and restart a query for `ns1` or `ns2.example.com`. Such a lookup potentially experiences two failures, n for each unreachable DNS authority under the `example.com` zone. In any event, such cycles rendered some zones unreachable.

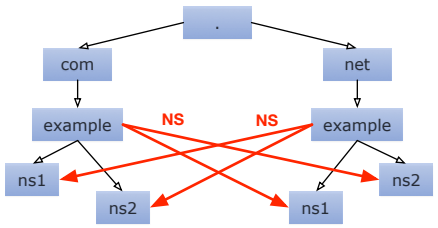

Fig. 1. DNS Glue Cycle Creation

.

II. Analysis

Several thousand domains were affected by the March 1^{st}, 2010 change in TLD operation. While the effort to fix those zones took some time, they are all now reachable and simple cycles have been removed from the `com` and `net` zones. However, a question remains open: are there zones which contain subgraphs that *are* cycles, but as a whole remain resolvable by virtue of one or a few additional nameservers? Conceptually, there could be zones with numerous cyclic authorities, but remain resolvable because of a single NS record. Thus, instead of a half dozen NS, the zone might only have one functional host, if glue is not promoted or is absent.

These "almost cyclic" zones would be an interesting group to identify and measure. While they appear robust and appear to have geographic and power diverse authorities, their resolution really depends on the operation of a single DNS server. In other words, we ask: "are there cliques of glue records, such that the loss of that single DNS server would induce a cycle?"

We propose:

- The creation of auditing resources to collect and organize TLD zones, and provide ongoing meta-data describing their referral behavior. Are there authorities at the TLD level or lower that still rely on glue promotion strategies?
- Census work to identify the number of actual vs cyclic DNS records. That is, measure the number of actual cycles that occur between multiple TLDs. For example, glue cycles across not just `.com` and `.net` but also more TLDs, including `.org`, or others with similar referral behavior.
- We will further measure the number of "induced" cycles that can occur, with the removal of one NS, or two, and so on, from the set of authorities for a given zone. How "fragile" are some zones, compared to others, should a single NS become unavailable or attacked?
- The creation of a scoring standard, and simple command line tools, so that DNS auditors and DNS secondaries can determine whether the resources they offer companies really contribute to the robustness of the zone.

References

[1] Verisign, "Changes to .com/.net/.edu Name Servers in Preparation for DNSSEC," 2010. [Online]. Available: https://www.verisign.com/en_US/domain-names/dnssec/dns-behavior-changes/index.xhtml