empty.as112.arpa

Wheee…

What is AS112?

The AS112 project provides a distributed sink for queries sent to non-unique IP address (such as private addresses defined in RFC 1918) in order to reduce the load on the in-addr.arpa authoritative servers in answering such queries. The AS112 project is named after the Autonomous System Number (ASN) that was assigned to it. This is defined in RFC 6304, "AS112 Nameserver Operations".

– https://www.ripe.net/analyse/dns/as112

The AS112 project is a community effort to run an important network service intended to handle reverse DNS lookup queries for private-only use addresses that should never appear in the public DNS system. In the seven days leading up to publication of this blog post, for example, Cloudflare's 1.1.1.1 resolver received more than 98 billion of these queries -- all of which have no useful answer in the Domain Name System.

– Cloudflare

Great! Who runs AS112?

The AS112 project encompasses a loosely coordinated collection of independently operated nameservers. Each nameserver functions as a single node in an AS112 anycast cloud [RFC4786] and is configured to answer authoritatively for a particular set of nominated zones.

– rfc7534

Server operators are volunteers who offer a route to the well known addresses of the AS112 servers, either to handle the queries generated by their local user populations, or to help carry the global traffic load.

– https://as112.net/ops-listing.html

Actual Answer: Nobody knows. “loosely coordinated volunteers” -> ¯_(ツ)_/¯

How does one become an AS112 operator?

The AS112 project encompasses a loosely coordinated collection of independently operated nameservers. Each nameserver functions as a single node in an AS112 anycast cloud [RFC4786] and is configured to answer authoritatively for a particular set of nominated zones.

– rfc7534

Server operators are volunteers who offer a route to the well known addresses of the AS112 servers, either to handle the queries generated by their local user populations, or to help carry the global traffic load.

– https://as112.net/ops-listing.html

Actual Answer: Nobody knows. “loosely coordinated volunteers” -> ¯_(ツ)_/¯

Why is this a bad idea…

There is no way to tell who is running an as112.net node (and so anyone can return anything for empty.as112.net).

Registry updates ns1.foo.com to empty.as112.arpa

Attack:
Step 1: Enter a wildcard for empty.as112.arpa pointing to my server
Step 2: ???
Step 3: Profit!

Questions?

Srsly?

```
$ dig +trace +nodnssec foo.empty.as112.arpa
.   76716   IN   NS   a.root-servers.net.
…
.   76716   IN   NS   m.root-servers.net.
;; Received 239 bytes from 8.8.8.8#53(8.8.8.8) in 91 ms

as112.arpa.     172800   IN   NS   a.iana-servers.net.
as112.arpa.     172800   IN   NS   b.iana-servers.net.
as112.arpa.     172800   IN   NS   c.iana-servers.net.
;; Received 113 bytes from 2001:7fd::1#53(k.root-servers.net) in 49 ms

empty.as112.arpa.  3600   IN   NS   blackhole.as112.arpa.
;; Received 117 bytes from 199.43.134.53#53(c.iana-servers.net) in 47 ms

empty.as112.arpa.  604800 IN SOA  blackhole.as112.arpa. noc.dns.icann.org. [...]
;; Received 112 bytes from 192.31.196.1#53(blackhole.as112.arpa) in 21 ms
```