DNS Resolver-Based Policy Detection Domain

draft-grover-add-policy-detection-00

Abstract

This document specifies the behavior that is expected from the Domain Name System with regard to DNS queries for the special-use domain name ‘TBD.arpa’ and designates this domain as a special-use domain name.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Content-control software can be used to filter (i.e., block) web requests that the user, the user’s guardian, or the network operator deems objectionable or outside the usage policy of the network. Blocked resource categories can include advertisements, explicit content, known malware, and government-unapproved material, along with many others.

One way to implement content control that does not rely on software or settings on the end-user’s computing device is DNS-based content filtering, which examines a client’s initial DNS request for the domain providing a resource and then either returns no result or returns an alternate result so that the user is presented with an explanation that filtering has taken place.

DNS-based policy such as content filtering is often built into a network’s configured DNS recursive resolver. In addition to blocking a request, the resolver may also log the request for use by the network administrators.

A network operator might wish to provide, or might be obligated to provide, a filtering policy to users of its network. Because such a policy is often enforced by the network operator’s default resolver, the use of a technology such as DNS over HTTPS (DoH) [RFC8484] or DNS over TLS (DoT) [RFC7858] can result in bypassing local policies. If the user agent can check for the presence of a policy, this could be used as a signal that the network operator wishes its resolver to be used as a condition of using the network, and that DoH or DoT should be disabled.

At present, there is no standardized mechanism for the user or user agent to identify the presence of a policy on a network’s default resolver.
resolver without making a request that could trigger the policy and logging thereof, which could have undesirable side-effects.

Therefore, this document defines such a mechanism by defining a so-called "canary domain" that is an instance of Special-Use Domain Names [RFC6761]. DNS requests for this domain would return different results when a DNS-based policy is in place, allowing for the detection of the policy in a consistent way by user agents.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Design Goals and Constraints

This canary domain has been defined with the following design goals and constraints in mind:

- Minimize the risk of exposing personal information
- Ensure that the canary request cannot be mistaken for a user-initiated DNS request
- Ensure that the technique is not specific to any given user agent, policy, or resolver service
- Ensure that the technique is easy to implement for user agents and resolvers

4. Behavior

Resolvers implementing a policy modify the result for the reserved domain 'TBD.arpa', which can be observed by clients to determine if a policy is present.

If a policy exists, the resolver MUST return NXDOMAIN [RFC1035]. If policy is not present, DNS lookup will be successful (i.e., not NXDOMAIN). (This could perhaps resolve to an actual host with a web page managed by IANA, similar to example.com [RFC6761].)
5. Domain Name Reservation Considerations

This section specifies considerations for systems involved in domain name resolution when resolving queries for the reserved domain ‘TBD.arpa’, in accordance with [RFC6761].

1. Users: Users may invoke command-line DNS lookup tools to resolve the domain, for the purposes of determining if a DNS-based policy is present.

2. Application Software: Application software doing automated lookups are the primary targets of this domain name reservation. Applications can attempt to resolve this name in order to determine if a DNS-based policy is present.

3. Name Resolution APIs and Libraries: Caching servers MUST NOT treat this name as special, unless they implement a policy, in which case they MUST return NXDOMAIN.

4. Caching DNS Servers: Caching servers MUST NOT treat this name as special, unless they implement a policy, in which case they MUST return NXDOMAIN.

5. Authoritative DNS Servers: Authoritative servers other than those supporting the ‘.arpa’ TLD MUST respond to queries for this name with NXDOMAIN.

6. DNS Server Operators: Operators SHOULD ensure that any caching DNS server with a policy on their network properly responds to this name with NXDOMAIN.

7. DNS Registries/Registrars: The defined name is a subdomain of the ‘.arpa’ top-level domain, which is operated by IANA under the authority of the Internet Architecture Board according to the rules established in [RFC3172]. There are no other registrars for ‘.arpa’.

6. IANA Considerations

IANA is requested to record the domain name ‘TBD.arpa’ in the "Special-Use Domain Names" registry. See Section 5 for the completed registration template.

[[NOTE TO RFC EDITOR: please change ‘TBD’ to the name assigned by IANA. The name ‘dns-content-policy-detection’ is suggested.]]
7. Security Considerations

Although a DNS resolution request for the ‘TBD.arpa’ domain can reveal whether the user or application wishes to detect the presence of DNS-based policy, such a request is relatively neutral compared to a request for a domain that might be subject to a policy.

8. References

8.1. Normative References


8.2. Informative References


Appendix A. Acknowledgements

Thanks to Martin Thomson for his feedback.

Authors’ Addresses

Andy Grover
Mozilla
Email: agrover@mozilla.com
URI: https://mozilla.com/

Peter Saint-Andre
Mozilla
Phone: +1 720 256 6756
Email: stpeter@mozilla.com
URI: https://mozilla.com/