Workgroup: dprive
Internet-Draft:
draft-schwartz-add-ddr-forwarders-00
Published: 21 September 2021
Intended Status: Informational
Expires: 25 March 2022
Authors: B. Schwartz
Google LLC

Discovery of Designated Resolvers in the Presence of Legacy Forwarders

Abstract

This draft describes how the Discovery of Designated Resolvers (DDR) standard interacts with legacy DNS forwarders, including potential incompatibilities and relevant mitigations.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the mailing list (add@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/add/.

Source for this draft and an issue tracker can be found at https://github.com/bemasc/ddr-forwarders.

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 25 March 2022.

Copyright Notice

Table of Contents

1. Conventions and Definitions

Legacy DNS Forwarder - An apparent DNS resolver, known to the client only by a non-public IP address, that forwards the client's queries to an upstream resolver, and has not been updated with any knowledge of DDR.

Cross-Forwarder Upgrade - Establishment of a direct, encrypted connection between the client and the upstream resolver.

2. Introduction

2.1. Background

The Discovery of Designated Resolvers specification [DDR] describes a mechanism for clients to learn about the encrypted protocols supported by a DNS server. It also describes a conservative client validation policy that has strong security properties and is unlikely to create compatibility problems.

On the topic of client validation of encrypted DNS transports, the DDR specification says:

> If the IP address of a Designated Resolver differs from that of an Unencrypted Resolver, clients MUST validate that the IP address of the Unencrypted Resolver is covered by the SubjectAlternativeName of the Encrypted Resolver's TLS certificate

As TLS certificates cannot cover non-public IP addresses, this prevents clients that are behind a legacy DNS forwarder from connecting directly to the upstream resolver ("cross-forwarder upgrade").

Recent estimates suggest that a large fraction, perhaps a majority, of residential internet users in the United States and Europe rely on local DNS forwarders that are not compatible with DDR.

2.2. Scope

This informational document describes the interaction between DDR and legacy DNS forwarders. It discusses possible client policies, problems that might arise, and relevant mitigations.

DNS forwarders and resolvers that are implemented with awareness of DDR are out of scope, as they are not affected by this discussion (although see Security Considerations, Section 6).

3. Relaxed Validation client policy

We define a "relaxed validation" client policy as a client behavior that removes the certificate validation requirement when the Unencrypted Resolver is identified by a non-public IP address, regardless of the Designated Resolver's IP address. This client policy is otherwise identical to the one described in [DDR].

4. Naturally compatible behaviors

The following network behaviors are naturally compatible with relaxed validation.

4.1. Malware and threat domain filtering

Certain DNS forwarders block access to domains associated with malware and other threats. Such threats rely on frequently changing domains, so these forwarders necessarily maintain an actively curated list of domains to block. To ensure that this service is not lost due to a cross-forwarder upgrade, the maintainers can simply add "resolver.arpa" to the list.

This pattern has been deployed by Mozilla, with the domain "use-application-dns.net" [MOZILLA-CANARY].

4.2. Service category restrictions

Certain DNS forwarders may block access to domains based on the category of service provided by those domains, e.g. domains hosting services that are not appropriate for a work or school environment. As in the previous section, this requires an actively curated list of domains, because the set of domains that offer a given type of service is constantly changing. An actively managed blocking list can easily be revised to include "resolver.arpa".

4.3. Time of use restrictions

Certain networks may impose restrictions on the time or duration of use by certain users. This behavior is necessarily implemented below the DNS layer, because DNS-based blocking would be ineffective due to stub resolver caching, so it is not affected by changes in the DNS resolver.

5. Privacy Considerations

The conservative validation policy results in no encryption when a legacy DNS forwarder is present. This leaves the user's query activity vulnerable to passive monitoring [RFC7258], either on the local network or between the user and the upstream resolver.

The relaxed validation policy allows the use of encrypted transport in these configurations, reducing exposure to a passive surveillance adversary.

6. Security Considerations

When the client uses the conservative validation policy described in [DDR], and a DDR-enabled resolver is identified by a non-public IP

address, the client can establish a secure DDR connection only in the absence of an active attacker. An on-path attacker can impersonate the resolver and intercept all queries, by preventing the DDR upgrade or advertising their own DDR endpoint.

These basic security properties also apply if the client uses the relaxed validation policy described in Section 3. Nonetheless, there are some subtle but important differences in the security properties of these two policies.

6.1. Transient attackers

With the conservative validation policy, a transient on-path attacker can only intercept queries for the duration of their active presence on the network, because the client will only send queries to the original (non-public) server IP address.

With the relaxed validation behavior, a transient on-path attacker could implant a long-lived DDR response in the client's cache, directing its queries to an attacker-controlled server on the public internet. This would allow the attack to continue long after the attacker has left the network.

6.1.1. Solution: DNR

This attack does not apply if the client and network implement support for Discovery of Network-designated Resolvers [DNR].

6.1.2. Mitigation: Frequent refresh

The client can choose to refresh the DDR record arbitrarily frequently, e.g. by limiting the TTL. For example, by limiting the TTL to 5 minutes, a client could ensure that any attacker can continue to monitor queries for at most 5 minutes after they have left the local network.

6.1.3. Mitigation: Resolver reputation

A relaxed-validation client might choose to accept a potential cross-forwarder upgrade only if the designated encrypted resolver has sufficient reputation, according to some proprietary reputation scheme (e.g. a locally stored list of respectable resolvers). This limits the ability of a DDR forgery attack to cause harm.

Major DoH client implementations already include lists of known resolvers [CHROME-DOH][MICROSOFT-DOH][MOZILLA-TRR].

6.2. Forensic logging

6.2.1. Network-layer logging

With the conservative validation policy, a random sample of IP packets is likely sufficient for manual retrospective detection of an active attack.

With the relaxed validation policy, forensic logs must capture a specific packet (the attacker's DDR designation response) to enable retrospective detection.

6.2.1.1. Mitigation: Log all DDR responses

Network-layer forensic logs that are not integrated with the resolver can enable detection of these attacks by logging all DDR responses, or more generally all DNS responses. This makes retrospective attack detection straightforward, as the attacker's DDR response will indicate an unexpected server.

6.2.2. DNS-layer logging

DNS-layer forensic logging conducted by a legacy DNS forwarder would be lost in a cross-forwarder upgrade.

6.2.2.1. Solution: Respond for resolver.arpa

Forwarders that want to observe all queries from relaxed validation clients will have to synthesize their own response for resolver.arpa, either implementing DDR or disabling it.

7. Compatibility Considerations

Using DDR with legacy DNS forwarders also raises several potential concerns related to loss of existing network services.

7.1. Split-horizon namespaces

Some network resolvers contain additional names that are not resolvable in the global DNS. If these local resolvers are also legacy DNS forwarders, a client that performs a cross-forwarder upgrade might lose access to these local names.

7.1.1. Mitigation: NXDOMAIN Fallback

In "NXDOMAIN Fallback", the client repeats a query to the unencrypted resolver if the encrypted resolver returns NXDOMAIN. This allows the resolution of local names, provided they do not collide with globally resolvable names (as required by [RFC2826]).

This is similar to the fallback behavior currently deployed in Mozilla Firefox [FIREFOX-FALLBACK].

NXDOMAIN Fallback results in slight changes to the security and privacy properties of encrypted DNS. Queries for nonexistent names no longer have protection against a local passive adversary, and local names are revealed to the upstream resolver.

NXDOMAIN Fallback is only applicable when a legacy DNS forwarder might be present, i.e. the unencrypted resolver has a non-public IP address, and the encrypted resolver has a different IP address. In the other DDR configurations, any local names are expected to resolve similarly on both resolvers.

7.2. Interposable domains

An "interposable domain" is a domain whose owner deliberately allows resolvers to forge certain responses. This arrangement is most common for search engines, which often support a configuration where resolvers forge a CNAME record to direct all clients to a child-appropriate instance of the search engine [DUCK-CNAME][BING-CNAME] [GOOGLE-CNAME].

Future deployments of interposable domains can instruct administrators to enable or disable DDR when adding the forged record, but forged records in legacy DNS forwarders could be lost due to a cross-forwarder upgrade.

7.2.1. Mitigation: Exemption list

There are a small number of pre-existing interposable domains, largely of interest only to web browsers. Clients can maintain a list of relevant interposable domains and resolve them only via the network's resolver.

7.3. Caching

Some legacy DNS forwarders also provide a shared cache for all network users. Cross-forwarder upgrades will bypass this cache, resulting in slower DNS resolution.

7.3.1. Mitigation: Stub caches

Clients can compensate partially for any loss of shared caching by implementing local DNS caches. This mitigation is already widely deployed in browsers and operating systems.

7.4. General mitigation: User controls

For these and other compatibility concerns, a possible mitigation is to provide users or administrators with the ability to control whether DDR is used with legacy forwarders. For example, this control could be provided via a general preference, or via a notification when connecting to a new network.

8. Informative References

[BING-CNAME] "Block adult content with SafeSearch - Map at a network level", n.d., <https://help.bing.microsoft.com/#apex/bing/en-us/10003/0>.

[CHROME-DOH] "DoH providers: criteria, process for Chrome", n.d., <https://docs.google.com/document/d/128i2YTV2C7T6Gr3I-81zlQ-_Lprnsp24qzy_20Z1Psw/edit>.

[DDR] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-ddr-02, 8 July 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-add-ddr-02>.

[DNR] Boucadair, M., Reddy, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", Work in Progress, Internet-Draft, draft-ietf-add-dnr-02, 17 May 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-02>.

[DUCK-CNAME] "Force Safe Search at a Network Level", n.d., <https://help.duckduckgo.com/duckduckgo-help-pages/features/safe-search/>.

[FIREFOX-FALLBACK] "About our rollout of DNS over HTTPS", n.d., <https://support.mozilla.org/en-US/kb/firefox-dns-over-https#w_about-our-rollout-of-dns-over-https>.

[GOOGLE-CNAME] "Keep SafeSearch turned on for your school, workplace, or home network", n.d., <https://support.google.com/websearch/answer/186669?hl=en>.

[MICROSOFT-DOH] "Determine which DoH servers are on the known server list", n.d., <https://docs.microsoft.com/en-us/windows-

server/networking/dns/doh-client-support#determine-which-doh-servers-are-on-the-known-server-list>.

[MOZILLA-CANARY] "Canary domain - use-application-dns.net", n.d., <https://support.mozilla.org/en-US/kb/canary-domain-use-application-dnsnet>.

[MOZILLA-TRR] "Mozilla Policy Requirements for DNS over HTTPs Partners", n.d., <https://wiki.mozilla.org/Security/DOH-resolver-policy#Mozilla_Policy_Requirements_for_DNS_over_HTTPs_Partners>.

[RFC2826] Internet Architecture Board, "IAB Technical Comment on the Unique DNS Root", RFC 2826, DOI 10.17487/RFC2826, May 2000, <https://www.rfc-editor.org/rfc/rfc2826>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/rfc/rfc7258>.

Acknowledgments

Thanks to Anthony Lieuallen and Eric Orth for early reviews.

Author's Address

Benjamin Schwartz
Google LLC

Email: bemasc@google.com