Match DNS Resolution to CNAME Record Domain Policy and Reporting

Contents

Introduction

This document describes how to match your DNS solution to your CNAME record domain policy and reporting.

Problem

While using a Domain Name System (DNS) caching server such as BIND (with caching enabled) or Infoblox, your DNS resolution does not match the expected policy and reporting for your CNAME record domains. An allowed A-record request is answered by a CNAME reference to another A-record on a different, blocked domain.

For example, domain.com is allowed and blocked.com is blocked, while domain.com is a CNAME record pointing to blocked.com, which has an A-record. This issue presents itself as an **allowed domain being blocked with no such event logged on the dashboard.**

Solution

There are several methods to resolve this issue:

- Disable DNS caching for DNS forwarded to Umbrella. This prevents this issue from occurring.
- Allow the target CNAME in the Umbrella Dashboard as they arise.
- Avoid caching the CNAME record type or selectively not cache impacted domains reactively.

Cause

The root cause of this issue is DNS caching for CNAME records pointing to a different domain, where the target domain is blocked. Since the domain is allowed, the Umbrella resolvers flag the entire query as allowed, carrying down the CNAME chain. This results in an allowed query.

Since different domains vary in TTL, and Umbrella block records for malicious categories have a TTL of zero, caching interferes.

Here is a scenario where domain.com is allowed and blocked.com is blocked and domain.com is a CNAME record pointing to blocked.com which has an A-record.

Initial query:

A-record for domain.com: Allow list, CNAME for blocked.com -> A-record query for blocked.com, coming from a CNAME, allow bit passed inside Umbrella - A-record for blocked.com returned.
Analysis: Queries made to Umbrella: domain.com -> blocked.com. Result: Allowed. Umbrella logs domain.com as allowed, blocked.com as allowed.

Subsequent Query:

A-record for domain.com: CACHED - it is a CNAME for blocked.com -> A-record query for blocked.com: CACHED - A-record for blocked.com returned.
Analysis: Queries made to Umbrella: None. No Umbrella logs.

Future query (triggers the issue):

A-record for domain.com: CACHED - it is a CNAME for blocked.com -> A-record query for blocked.com (standalone query - CNAME was cached) - blocked.
Analysis: Queries made to Umbrella: blocked.com. Result: Blocked. Umbrella logs blocked.com as blocked.

Additional Information

- Umbrella Documentation: DNS Resolution