DNS-Auflösung an CNAME-Datensatzdomänenrichtlinie und Berichterstellung anpassen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Ihre DNS-Lösung mit Ihrer CNAME-Datensatzdomänenrichtlinie und der entsprechenden Berichterstellung abgleichen.

Problem

Bei Verwendung eines DNS-Caching-Servers (Domain Name System) wie BIND (bei aktivierter Caching-Funktion) oder Infoblox entspricht die DNS-Auflösung nicht den erwarteten Richtlinien und Berichten für Ihre CNAME-Eintragsdomänen. Eine zulässige A-Datensatz-Anforderung wird durch einen CNAME-Verweis auf einen anderen A-Datensatz in einer anderen, blockierten Domäne beantwortet.

Beispielsweise ist domain.com zulässig, und blocked.com ist gesperrt, während domain.com ein CNAME-Datensatz ist, der auf blocked.com verweist und einen A-Datensatz hat. Dieses Problem stellt sich als zulässige Domäne dar, die blockiert wird, ohne dass ein solches Ereignis auf dem Dashboard angemeldet ist.

Lösung

Es gibt mehrere Möglichkeiten, dieses Problem zu beheben:

- Deaktivieren Sie die DNS-Zwischenspeicherung für DNS, das an Umbrella weitergeleitet wird. Dadurch wird verhindert, dass dieses Problem auftritt.
- Lassen Sie das Ziel-CNAME im Umbrella Dashboard zu, sobald diese auftreten.
- Vermeiden Sie das Zwischenspeichern des CNAME-Datensatztyps, oder legen Sie die betroffenen Domänen nicht reaktiv im Cache ab.

Ursache

Die Ursache dieses Problems liegt in der DNS-Zwischenspeicherung für CNAME-Einträge, die auf eine andere Domäne verweisen, in der die Zieldomäne blockiert ist. Da die Domäne zulässig ist, kennzeichnen die Umbrella-Resolver die gesamte Abfrage als zulässig, wobei die CNAME-Kette nach unten getragen wird. Dies führt zu einer zulässigen Abfrage.

Da die TTL verschiedener Domänen variiert und Umbrella Block-Datensätze für bösartige Kategorien einen TTL-Wert von Null aufweisen, greift der Caching-Vorgang ein.

In diesem Szenario ist domain.com zulässig, und blocked.com ist blockiert, und domain.com ist ein CNAME-Eintrag, der auf blocked.com verweist und einen A-Eintrag hat.

Anfängliche Abfrage:

A-Eintrag für domain.com: Zulassungsliste, CNAME für blocked.com -> A-Record-Abfrage für blocked.com, von einem CNAME kommend, in Umbrella übergebenes Zulassungsbit - A-Record für blocked.com zurückgegeben.
Analyse: An Umbrella gestellte Fragen: domain.com -> blocked.com. Ergebnis: ZUGELASSEN. Umbrella protokolliert domain.com als zulässig, blocked.com als zulässig.

Nachfolgende Abfrage:

A-Eintrag für domain.com: CACHED - CNAME für blocked.com -> A-Record-Abfrage für blocked.com: CACHED - Ein Datensatz für blocked.com wurde zurückgegeben.
Analyse: An Umbrella gestellte Fragen: None. Keine Umbrella-Protokolle.

Zukünftige Abfrage (löst das Problem aus):

A-Eintrag für domain.com: CACHED - CNAME für blocked.com -> A-Record-Abfrage für blocked.com (eigenständige Abfrage - CNAME wurde zwischengespeichert) - blockiert.
Analyse: An Umbrella gestellte Fragen: blocked.com. Ergebnis: Gesperrt. Umbrella protokolliert blocked.com als blockiert.

Zusätzliche Informationen

- Umbrella-Dokumentation: DNS-Auflösung

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.