

DNS解決とCNAMEレコードドメインポリシーおよびレポートの照合

内容

[はじめに](#)

[問題](#)

[解決方法](#)

[原因](#)

[追加情報](#)

はじめに

このドキュメントでは、DNSソリューションをCNAMEレコードのドメインポリシーおよびレポートに一致させる方法について説明します。

問題

BIND（キャッシュを有効にした状態）やInfobloxなどのドメインネームシステム(DNS)キャッシュサーバーを使用している場合、DNS解決が、CNAMEレコードドメインの予期されたポリシーおよびレポートと一致しません。許可されたAレコード要求は、ブロックされた別のドメインの別のAレコードへのCNAME参照によって応答されます。

たとえば、domain.comは許可されblocked.comはブロックされますが、domain.comはAレコードを持つblocked.comを指すCNAMEレコードです。この問題は、許可されたドメインがブロックされ、そのようなイベントがダッシュボードに記録されないという症状を示します。

解決方法

この問題を解決するには、いくつかの方法があります。

- Umbrellaに転送されるDNSのDNSキャッシュを無効にします。これにより、この問題の発生が防止されます。
- Umbrellaダッシュボードで発生したターゲットCNAMEを許可します。
- CNAMEレコードタイプのキャッシュを回避するか、影響を受けるドメインを選択的にリアクティブにキャッシュしないようにします。

原因

この問題の根本原因は、ターゲットドメインがブロックされている別のドメインを指すCNAMEレコードのDNSキャッシュです。ドメインが許可されているため、Umbrellaリゾルバはクエリ全体に許可フラグを設定し、CNAMEチェーンを伝達します。この結果、許可されたクエリが生成されます。

TTLは異なるドメインによって異なり、悪意のあるカテゴリのUmbrellaブロックレコードのTTLはゼロであるため、キャッシュによる干渉が発生します。

次のシナリオでは、domain.comが許可され、blocked.comがブロックされています。
domain.comは、Aレコードを持つblocked.comを指すCNAMEレコードです。

最初のクエリ：

domain.comのAレコード：許可リスト、blocked.comのCNAME -> blocked.comのAレコードのクエリ。CNAMEから送信され、Umbrella内でビットを渡すことを許可します。blocked.comのAレコードが返されました。

分析：Umbrellaに対するクエリ：domain.com -> blocked.com結果：許可。Umbrellaは、domain.comを許可されているとおりに、blocked.comを許可されているとおりにログに記録します。

後続のクエリー：

domain.comのAレコード：CACHED - blocked.comのCNAME -> blocked.comのAレコードクエリ：CACHED - blocked.comのAレコードが返されました。

分析：Umbrellaに対するクエリ：なし。傘のログはありません。

今後のクエリ (問題のトリガー)：

domain.comのAレコード：キャッシュ済み - blocked.comのCNAME -> blocked.comのAレコードクエリ (スタンドアロンクエリ - CNAMEがキャッシュ済み) - ブロック済み

分析：Umbrellaに対するクエリ：blocked.com。結果：ブロックされました。Umbrellaがblocked.comをブロックとしてログに記録します。

追加情報

- [包括ドキュメント：DNS解決](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。