Verständnis von Umbrella DNS mit QNAME-Minimierung

Inhalt

Einleitung

In diesem Dokument wird die Verwendung des Cisco Umbrella Domain Name System (DNS) mit QNAME-Minimierung beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Im Juni 2019 hat Cisco Umbrella die Unterstützung für die Namensminimierung (RFC7816) hinzugefügt. QNAME-Minimierung ist eine datenschutzorientierte Funktion in DNS, die darauf abzielt, das Senden des vollständigen Domänenziels an die Root-Namenserver zu beschränken. Dadurch wird der Fluss der DNS-Abfragen zur Bestimmung der DNS-Abfrageantwort geändert.

QNAME Minimierung ist ein weltweites Thema. Das Internet Systems Consortium hat einen Einführungsartikel zur QNAME Minimization veröffentlicht. Mozilla Firefox erfordert, dass Resolver

QNAME Minimization für DNS über HTTPS-Implementierungen verwenden, und hat einen Artikel zu diesem Thema.

Minimierung von Abfragen verstehen

Bei der Abfrageminimierung handelt es sich um einen neuen datenschutzorientierten Ansatz für autoritative DNS-Abfragen. Um herauszufinden, wie Abfragen minimiert werden können, beginnen Sie mit einer Erläuterung, wie eine DNS-Anforderung derzeit funktioniert.

Da der Großteil der menschlichen Interaktion mit dem Internet mit einer DNS-Abfrage beginnt, sind Big Data-Daten über den Standort der Benutzer wertvolle Informationen, die als private Daten betrachtet werden können.

Für dieses Beispiel besuchen Sie umbrella.cisco.com. Sie benötigen eine DNS-Abfrage, um festzustellen, wo sich dieser Server befindet. Umbrella sendet diese Abfrage daher an einen rekursiven DNS-Server, um die Antwort der Behörde zu finden. Gehen Sie dazu wie folgt vor:

1. Benutzerabfrage zum rekursiven DNS-Resolver: umbrella.cisco.com

2. Rekursiver DNS-Server fragt die Antwort von den Root-Namenservern ab: Wo kann ich umbrella.cisco.com finden, um zu root > antworten für .com

3. Abfragen auf den .com-Namenservern: umbrella.cisco.com auf .com > ruft den Speicherort von cisco.com auf.

4. Abfrage an cisco.com Namenserver: umbrella.cisco.com an cisco.com > Antwort bereitgestellt

In vielen Fällen kann dies mit mehreren weiteren Iterationen zu verschiedenen Namenservern fortgesetzt werden, bis ein A-Datensatz gefunden wird. In den Schritten 1-2 sucht Umbrella nur aktiv nach dem Speicherort der .com-Nameserver. Die vollständige umbrella.cisco.com-Domäne wird jedoch an den Root- und .com-Nameserver gesendet. Dasselbe gilt für den Namenserver cisco.com, der die vollständige Abfrage empfängt.

Bei der Minimierung von Abfragen wird der Algorithmus dahingehend geändert, dass nur die erforderliche Detailstufe in den Upstream-Abfragen abgefragt wird:

1. Benutzerabfrage zum rekursiven DNS-Resolver: umbrella.cisco.com

2. Rekursiver DNS-Server fragt die Root-Namenserver ab: Wo kann ich finden .com > Antwort für .com

3. Abfragen auf den .com-Namenservern: cisco.com von .com > cisco.com

4. Fragen Sie bei den cisco.com nach umbrella.cisco.com > Antwort

Dies funktioniert in den meisten Fällen hervorragend und ermöglicht es, die Antwort zu finden, ohne die eindeutige Abfrage preiszugeben, die an den Root- oder TLD-Namenservern durchgeführt wird.

Dieser Datenschutz ist umso wichtiger für Domänen, die das EDNS-Client-Subnetz nutzen, bei denen die DNS-Behörde bei der Abfrage über den C-Block der Quelle (/24) des Benutzers informiert wird. Ohne QNAME-Minimierung wissen die Root- und .com-Nameserver (in diesem Beispiel) Ihren allgemeinen Standort sowie Ihren genauen Zielort. Mit QNAME Minimization wissen die Wurzeln nur, dass jemand nach .com sucht und die Privatsphäre des Antragstellers gewahrt bleibt. Sie erfordern nicht die Detailgenauigkeit, die ihnen heute ohne QMIN-Datenschutz zur Verfügung gestellt wird.

Potenzielle Nebenwirkungen

QNAME Minimierung funktioniert in den meisten Fällen problemlos. Sie ist jedoch im Vergleich zu einer direkten Abfrage zusätzlichen Fehlerquellen unterworfen. Da das vollständige Ziel erst im letzten Schritt des Prozesses an den autoritativen Nameserver übermittelt wird, können Brüche in der DNS-Kette die Auflösung der Domäne unterbrechen. Hier ist zum Beispiel ein langer fiktionaler Name - umbrellas.in.the.rain.umbrella.cisco.com. Dies kann zu folgenden Abfragen führen:

1. Wie lauten die Namenserver für .com zu den Root-Servern .

2. Wie lauten die Namenserver für cisco.com auf die .com-Server?

3. Wie lauten die Namenserver für umbrella.cisco.com auf die Namenserver cisco.com

4. Wie lauten die Namenserver für rain.umbrella.cisco.com auf die Namenserver umbrella.cisco.com.

5. Wie lauten die Namenserver für the.rain.umbrella.cisco.com auf die Namenserver rain.umbrella.cisco.com

6. Wie lauten die Namenserver für in.the.rain.umbrella.cisco.com auf die Namenserver rain.umbrella.cisco.com: SERVFAIL

7. Wie lauten die Namenserver für umbrellas.in.the.rain.umbrella.cisco.com zu den Namenservern rain.umbrella.cisco.com (nicht abgefragt wegen SERVFAIL zuvor)?

8. Was ist die Antwort für umbrellas.in.the.rain.umbrella.cisco.com auf die umbrellas.in.the.rain.umbrella.cisco.com Namenserver, die früher gefunden wurden (nicht abgefragt wegen SERVFAIL früher)?

Da die Roots nicht die vollständige Abfrage erhalten, kann die Abfrage eine erfolgreiche autoritative Upstream-Antwort nicht erhalten, wenn eine der Ebenen der Domäne eine NXDOMAIN, SERVFAIL, die IP eines internen RFC-1918-Namenservers oder eine andere schlechte Antwort zurückgibt. Wenn z. B. der sechste Schritt zuvor (fett, unterstrichen) fehlschlägt, kann die Abfrage für umbrellas.in.the.rain.umbrella.cisco.com nicht aufgelöst werden. Um diese Probleme zu beheben, muss der Domäneninhaber sicherstellen, dass jede Ebene über eine gültige öffentliche Antwort verfügt.

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.