Comprensión de Umbrella DNS con minimización de QNAME

Contenido

Introducción

Este documento describe cómo utilizar el Sistema de nombres de dominio (DNS) de Cisco Umbrella con la minimización de QNAME.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

En junio de 2019, Cisco Umbrella añadió compatibilidad con la minimización de nombres de consulta (RFC7816). La minimización de QNAME es una función orientada a la privacidad en DNS que tiene como objetivo limitar el envío del destino de dominio completo a los servidores de nombres raíz. Como resultado, se modifica el flujo de consultas DNS para determinar la respuesta a la consulta DNS.

La minimización de QNAME es un tema mundial. El Internet Systems Consortium tiene un artículo

de introducción sobre la minimización de QNAME. Mozilla Firefox requiere que los resolvers utilicen la minimización de QNAME para las implementaciones de DNS sobre HTTPS y tiene un artículo sobre este tema.

Comprender la minimización de consultas

La minimización de consultas es un nuevo enfoque centrado en la privacidad de los datos para las consultas autorizadas de DNS. Para explorar qué es la minimización de consultas, comience con una explicación de cómo funciona actualmente una solicitud DNS.

Dado que la mayor parte de la interacción humana con Internet comienza con una consulta de DNS, el big-data sobre a dónde van los usuarios es información inestimable, que se puede considerar datos privados.

En este ejemplo, está interesado en visitar umbrella.cisco.com. Necesita una consulta DNS para determinar dónde se encuentra este servidor, por lo que Umbrella envía esa consulta a un servidor DNS recursivo para encontrar la respuesta de la autoridad mediante estos pasos:

1. Consulta del usuario a la resolución DNS recursiva: umbrella.cisco.com

2. El servidor DNS recursivo consulta la respuesta desde los servidores de nombres raíz: ¿dónde puedo encontrar umbrella.cisco.com a raíz > respuesta para .com

3. Realice una consulta en los servidores de nombres .com: umbrella.cisco.com a .com > obtiene la ubicación de cisco.com nameservers

4. Consulte a los servidores de nombres cisco.com: umbrella.cisco.com a cisco.com > Respuesta proporcionada

En muchos casos, esto puede continuar con varias iteraciones más a diferentes nameservers hasta que se encuentre un registro A. En los pasos 1-2, Umbrella solo busca activamente la ubicación de los servidores de nombres .com. Sin embargo, el dominio umbrella.cisco.com completo se envía a la raíz y al servidor de nombres .com. Lo mismo ocurre con el servidor de nombres cisco.com que recibe la consulta completa.

Con la minimización de consultas, el algoritmo pasa a solicitar solamente el nivel de detalle requerido en las consultas ascendentes:

1. Consulta del usuario a la resolución DNS recursiva: umbrella.cisco.com

2. El servidor DNS recursivo consulta los servidores de nombres raíz: ¿dónde puedo encontrar .com > answer for .com?

3. Realice una consulta en los servidores de nombres .com: cisco.com a .com > ubicación de cisco.com

4. Consulte en cisco.com nameservers para umbrella.cisco.com > Answer

Esto funciona muy bien en la mayoría de los casos, y permite que la respuesta sea localizada sin

revelar la consulta única que se hace a los servidores de nombres root o TLD.

Esta privacidad es aún más importante para los dominios que utilizan la subred de clientes EDNS, donde se informa a la autoridad DNS del origen del bloqueo C del usuario (/24) al realizar consultas. Sin la minimización de QNAME, los servidores de nombres root y .com (en este ejemplo) conocen su ubicación general así como adónde va exactamente. Con la minimización de QNAME, las raíces solo saben que alguien está buscando .com y se mantiene la privacidad del solicitante. No requieren el nivel de detalle que se les proporciona actualmente sin las protecciones de privacidad de QMIN.

Posibles efectos adversos

La minimización de QNAME funciona sin problemas en la mayoría de los casos. Sin embargo, está sujeto a fuentes adicionales de error en comparación con una consulta directa. Dado que el destino completo no se revela hasta el último paso del proceso al servidor de nombres autorizado, las interrupciones en la cadena DNS pueden interrumpir la resolución del dominio. Por ejemplo, aquí hay un nombre ficticio largo: umbrellas.in.the.rain.umbrella.cisco.com. Esto puede dar lugar a las siguientes consultas:

1. ¿Cuáles son los servidores de nombres para .com a los servidores raíz .

2. ¿Cuáles son los servidores de nombres para cisco.com a los servidores .com

3. ¿Cuáles son los nameservers para umbrella.cisco.com a los nameservers cisco.com

4. ¿Cuáles son los nameservers para rain.umbrella.cisco.com a los nameservers umbrella.cisco.com.

5. ¿Cuáles son los nameservers para the.rain.umbrella.cisco.com a los nameservers rain.umbrella.cisco.com

6. ¿Cuáles son los nameservers para in.the.rain.umbrella.cisco.com a los nameservers rain.umbrella.cisco.com: SERVFAIL

7. ¿Cuáles son los nameservers para umbrellas.in.the.rain.umbrella.cisco.com a los nameservers rain.umbrella.cisco.com (no consultados debido a SERVFAIL anteriormente)

8. ¿Cuál es la respuesta para umbrellas.in.the.rain.umbrella.cisco.com a los servidores de nombres umbrellas.in.the.rain.umbrella.cisco.com que se encontraron anteriormente (no se consultó debido a SERVFAIL anteriormente)?

Dado que a las raíces no se les da la consulta completa, si uno de los niveles del dominio devuelve un NXDOMAIN, SERVFAIL, la IP de un servidor de nombres interno RFC-1918 u otra respuesta deficiente, la consulta puede fallar al recibir una respuesta autoritativa ascendente exitosa. Por ejemplo, si el sexto paso anterior (negrita, subrayado) fallara, la consulta de umbrellas.in.the.rain.umbrella.cisco.com podría fallar. Para resolver estos problemas, el propietario del dominio debe asegurarse de que cada nivel tenga una respuesta pública válida.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).