瞭解使用QNAME最小化的Umbrella DNS

目錄

簡介

本檔案介紹如何透過QNAME最小化使用思科傘狀網域名稱系統(DNS)。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據思科資安防護傘

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

2019年6月，Cisco Umbrella增加了查詢名稱最小化支援(RFC7816)。QNAME最小化是DNS中面向隱私的功能，旨在限制將整個域目標傳送到根名稱伺服器。結果，用於確定DNS查詢響應的DNS查詢流被修改。

QNAME最小化是一個全球性的主題。Internet Systems Consortium有一篇關於QNAME最小化的介紹文章。Mozilla Firefox要求解析程式對通過HTTPS實現的DNS使用QNAME最小化，並有一篇關於此主題的文章。

瞭解查詢最小化

查詢最小化是一種以資料隱私為中心的新型DNS權威查詢方法。要瞭解什麼是查詢最小化，首先要解釋當前DNS請求的工作方式。

由於大多數人類與Internet的互動都從DNS查詢開始，使用者去往何處的大資料是無價的資訊，可以視為私有資料。

在本例中，您希望訪問umbrella.cisco.com。您需要使用DNS查詢來確定此伺服器所在的位置，因此Umbrella將該查詢傳送到遞迴DNS伺服器，以使用以下步驟從機構查詢答案：

1.遞迴DNS解析器的使用者查詢：umbrella.cisco.com

2.遞迴DNS伺服器從根名稱伺服器查詢答案：在哪裡可以找到umbrella.cisco.com到root > answer for .com

3.在.com名稱伺服器上查詢：umbrella.cisco.com to .com >獲取cisco.com nameservers的位置

4.查詢cisco.com域名伺服器：umbrella.cisco.com到cisco.com >提供答案

在許多情況下，這可以繼續對不同的名稱伺服器進行多次迭代，直到找到A記錄。在步驟1-2中，Umbrella只主動尋找.com名稱伺服器的位置。但是，完整的umbrella.cisco.com域將傳送到根目錄和.com名稱伺服器。接收完整查詢的cisco.com nameserver也一樣。

使用查詢最小化，演算法將轉向僅請求上游查詢中所需的詳細程度：

1.遞迴DNS解析器的使用者查詢：umbrella.cisco.com

2.遞迴DNS伺服器查詢根名稱伺服器：在哪裡可以找到.com > answer for .com

3.在.com名稱伺服器上查詢：cisco.com到.com > cisco.com的位置

4.在cisco.com nameservers中查詢umbrella.cisco.com >答案

這在大多數情況下都非常有效，並且可以在不向根或TLD名稱伺服器顯示唯一查詢的情況下找到答案。

對於使用EDNS客戶端子網的域而言，這種隱私更為重要，因為查詢時會向DNS主管機構通知使用者的源C塊(/24)。如果沒有QNAME最小化，則根目錄和.com（在本例中）名稱伺服器會知道您的一般位置以及您確切的位置。通過QNAME最小化，根節點只知道有人正在查詢.com，且請求者的隱私得以維護。如果沒有QMIN隱私保護，它們不需要提供當前所需的詳細程度。

潛在的副作用

在大多數情況下，QNAME最小化工作沒有問題。但是，與直接查詢相比，它可能會受到其他失敗源的影響。由於直到進程的最後一步才向授權名稱伺服器顯示完整目標，因此DNS鏈中的中斷可能會中斷域的解析。例如，這裡有一個長長的虛構名稱 — umbrellas.in.the.rain.umbrella.cisco.com。這可能會導致以下查詢：

1. .com到根伺服器的名稱伺服器是什麼。

2. cisco.com到.com伺服器的名稱伺服器是什麼

3. umbrella.cisco.com到cisco.com nameserver的名稱伺服器是什麼

4. rain.umbrella.cisco.com到umbrella.cisco.com nameserver的名稱伺服器是什麼？

5. the.rain.umbrella.cisco.com到rain.umbrella.cisco.com nameserver的名稱伺服器是什麼

6. in.the.rain.umbrella.cisco.com到rain.umbrella.cisco.com nameserver的名稱伺服器是什麼：SERVFAIL

7. umbrellas.in.the.rain.umbrella.cisco.com的名稱伺服器與rain.umbrella.cisco.com名稱伺服器之間的名稱伺服器是什麼（未查詢，因為以前有SERVFAIL）

8. umbrellas.in.the.rain.umbrella.cisco.com對於先前發現的umbrellas.in.the.rain.umbrella.cisco.com名稱伺服器（由於較早的SERVFAIL而未查詢）的答案是什麼

由於根沒有給出完整的查詢，如果域的一個級別返回NXDOMAIN、SERVFAIL、RFC-1918內部名稱伺服器的IP或其他不良響應，查詢可能無法收到成功的上游授權響應。例如，如果前面的第六步（加下劃線）失敗，則無法解析umbrellas.in.the.rain.umbrella.cisco.com的查詢。要解決這些問題，域所有者必須確保每個級別都有有效的公共響應。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。