Comprendere il DNS Umbrella con la riduzione al minimo di QNAME

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Panoramica](#)

[Informazioni sulla riduzione a icona delle query](#)

[Potenziali effetti collaterali](#)

Introduzione

In questo documento viene descritto come utilizzare il DNS (Domain Name System) Cisco Umbrella con la riduzione a icona di QNAME.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano su Cisco Umbrella

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

A giugno 2019, Cisco Umbrella ha aggiunto il supporto per la minimizzazione dei nomi di query (RFC7816). La minimizzazione di QNAME è una funzionalità orientata alla privacy in DNS che mira a limitare l'invio della destinazione del dominio completo ai server dei nomi radice. Di conseguenza, il flusso delle query DNS per determinare la risposta alla query DNS viene modificato.

QNAME Minimization è un argomento a livello mondiale. Internet Systems Consortium ha un

articolo introduttivo sulla minimizzazione di QNAME. Mozilla Firefox richiede ai resolver di utilizzare QNAME Minimization per le implementazioni DNS su HTTPS e ha un articolo su questo argomento.

Informazioni sulla riduzione a icona delle query

La riduzione al minimo delle query è un nuovo approccio basato sulla privacy dei dati per le query autorevoli DNS. Per scoprire che cos'è la riduzione a icona delle query, iniziare con una spiegazione del funzionamento corrente di una richiesta DNS.

Dal momento che la maggior parte dell'interazione umana con Internet inizia con una query DNS, i grandi dati su dove gli utenti stanno andando sono informazioni inestimabili, che possono essere considerate dati privati.

Per questo esempio, visitare il sito Web umbrella.cisco.com. Poiché è necessaria una query DNS per determinare la posizione del server, Umbrella invia la query a un server DNS ricorsivo per trovare la risposta dall'autorità tramite la procedura seguente:

1. Query utente sul resolver DNS ricorsivo: umbrella.cisco.com

2. Il server DNS ricorsivo esegue una query sulla risposta dai server dei nomi principali: dove posso trovare umbrella.cisco.com per radice > risposta per .com

3. Eseguire una query nei server dei nomi .com: umbrella.cisco.com to .com > ottiene la posizione di cisco.com server dei nomi

4. Eseguire una query su cisco.com server dei nomi: Da umbrella.cisco.com a cisco.com > Risposta fornita

In molti casi, questa operazione può continuare con diverse iterazioni su server dei nomi diversi fino a quando non viene individuato un record A. Nei passaggi 1-2, Umbrella sta cercando attivamente solo la posizione dei server dei nomi .com. Tuttavia, il dominio umbrella.cisco.com completo viene inviato al server dei nomi root e .com. Lo stesso vale per il server dei nomi cisco.com che riceve la query completa.

Con la riduzione a icona delle query, l'algoritmo passa alla sola richiesta del livello di dettaglio richiesto nelle query a monte:

1. Query utente sul resolver DNS ricorsivo: umbrella.cisco.com

2. Il server DNS ricorsivo esegue una query sui server dei nomi radice: dove posso trovare .com > risposta per .com

3. Eseguire una query nei server dei nomi .com: cisco.com to .com > percorso di cisco.com

4. Eseguire una query sui server dei nomi cisco.com per umbrella.cisco.com > Risposta

Nella maggior parte dei casi, questa procedura è efficace e consente di individuare la risposta senza rivelare la query univoca eseguita sui server dei nomi radice o TLD.

Questa privacy è ancora più importante per i domini che utilizzano la subnet del client EDNS, in cui l'autorità DNS viene informata del blocco C di origine dell'utente (/24) durante l'esecuzione di query. Senza la riduzione a icona di QNAME, i server dei nomi root e .com (in questo esempio) conoscono la posizione generale dell'utente e la posizione esatta in cui si sta andando. Con QNAME Minimization, le radici sanno solo che qualcuno sta cercando .com e la privacy del richiedente è mantenuta. Non richiedono il livello di dettaglio fornito oggi senza le protezioni per la privacy QMIN.

Potenziali effetti collaterali

Nella maggior parte dei casi, la minimizzazione di QNAME funziona senza problemi. Tuttavia, è soggetta a ulteriori cause di errore rispetto a una query diretta. Poiché la destinazione completa non viene rivelata fino all'ultimo passaggio del processo al server dei nomi autorevole, le interruzioni nella catena DNS possono interrompere la risoluzione del dominio. Ad esempio, qui è riportato il nome fittizio umbrellas.in.the.rain.umbrella.cisco.com. Di seguito sono riportate le possibili cause delle query:

1. Che cos'è il server dei nomi .com per i server radice?

2. Quali sono i server dei nomi per cisco.com ai server .com?

3. Quali sono i server dei nomi per umbrella.cisco.com nei server dei nomi cisco.com

4. Quali sono i server dei nomi per rain.umbrella.cisco.com nei server dei nomi umbrella.cisco.com?

5. Quali sono i server dei nomi per the.rain.umbrella.cisco.com nei server dei nomi rain.umbrella.cisco.com

6. Quali sono i server dei nomi per in.the.rain.umbrella.cisco.com per i server dei nomi rain.umbrella.cisco.com: SERVFAIL

7. Quali sono i server dei nomi per umbrellas.in.the.rain.umbrella.cisco.com nei server dei nomi rain.umbrella.cisco.com (query non eseguita a causa di SERVFAIL in precedenza)?

8. Qual è la risposta per umbrellas.in.the.rain.umbrella.cisco.com ai server dei nomi umbrellas.in.the.rain.umbrella.cisco.com trovati in precedenza (query non eseguita a causa di SERVFAIL in precedenza)?

Poiché alle directory principali non viene assegnata la query completa, se uno dei livelli del dominio restituisce un NXDOMAIN, SERVFAIL, l'indirizzo IP di un server dei nomi interno RFC-1918 o un'altra risposta inadeguata, la query potrebbe non ricevere una risposta autorevole upstream corretta. Ad esempio, se il sesto passaggio precedente (grassetto, sottolineato) non dovesse riuscire, la query per umbrellas.in.the.rain.umbrella.cisco.com potrebbe non riuscire a risolversi. Per risolvere questi problemi, il proprietario del dominio deve assicurarsi che ogni livello disponga di una risposta pubblica valida.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).