Rapid Reset DDoS Attack

Ottobre 2023

Report Informativo SOC

Dettagli documento

Titolo attività
Rapid Reset DDoS Attack

Sintesi attività
Report contenente le evidenze relative all'attacco DDoS Rapid Reset che colpisce il protocollo HTTP/2

Destinatario pubblicazione
Referenti servizi SOC e SOC AdS

Livello di riservatezza (Clear/Green/Amber/Amber+Strict/Red)
CLEAR

Data pubblicazione
13/10/2023

Redatto da
Mirko Ioris

Revisionato da
Massimo Giaimo

Riservatezza della pubblicazione

Al documento viene applicato un livello di riservatezza, avvalorato dalla voce “Livello di riservatezza” presente in prima pagina. I valori utilizzabili (RED / AMBER / GREEN / CLEAR) hanno i seguenti significati:

TLP:RED = Riservato ai soli partecipanti.

> Le fonti possono utilizzare TLP:RED quando le informazioni non possono essere efficacemente utilizzate da altre parti e potrebbero avere un impatto sulla privacy, sulla reputazione o sulle operazioni di una parte se utilizzate in modo improprio. I destinatari non possono condividere le informazioni TLP:RED con parti al di fuori dello specifico scambio, riunione o conversazione in cui sono state originariamente divulgate. Nel contesto di una riunione, ad esempio, le informazioni di TLP:RED sono limitate ai presenti alla riunione. Nella maggior parte dei casi, TLP:RED dovrebbe essere scambiato verbalmente o di persona.

TLP:AMBER = Divulgazione limitata, riservata alle organizzazioni dei partecipanti.

TLP:AMBER+STRICT limita la condivisione solo all'*organizzazione*.

> Le fonti possono utilizzare TLP:AMBER quando le informazioni richiedono supporto per agire in modo efficace, ma comportano rischi per la privacy, la reputazione o le operazioni se condivise al di fuori delle organizzazioni coinvolte. I destinatari possono condividere le informazioni TLP:AMBER solo con i membri della propria organizzazione e con clienti o clienti che hanno bisogno di conoscere le informazioni per proteggersi o prevenire ulteriori danni.
>
> Nota: se la fonte desidera limitare la condivisione **solo** all'organizzazione, deve specificare TLP:AMBER+STRICT.

TLP:GREEN = Divulgazione limitata, riservata alla comunità.

> Le fonti possono utilizzare TLP:GREEN quando le informazioni sono utili per la consapevolezza di tutte le organizzazioni partecipanti, nonché con i colleghi all'interno della comunità o del settore più ampio. I destinatari possono condividere le informazioni TLP:GREEN con colleghi e organizzazioni partner all'interno del loro settore o comunità, ma non tramite canali pubblicamente accessibili. Le informazioni in questa categoria possono essere ampiamente diffuse all'interno di una particolare comunità. Le informazioni TLP:GREEN potrebbero non essere rilasciate al di fuori della community.

TLP:CLEAR = La divulgazione non è limitata.

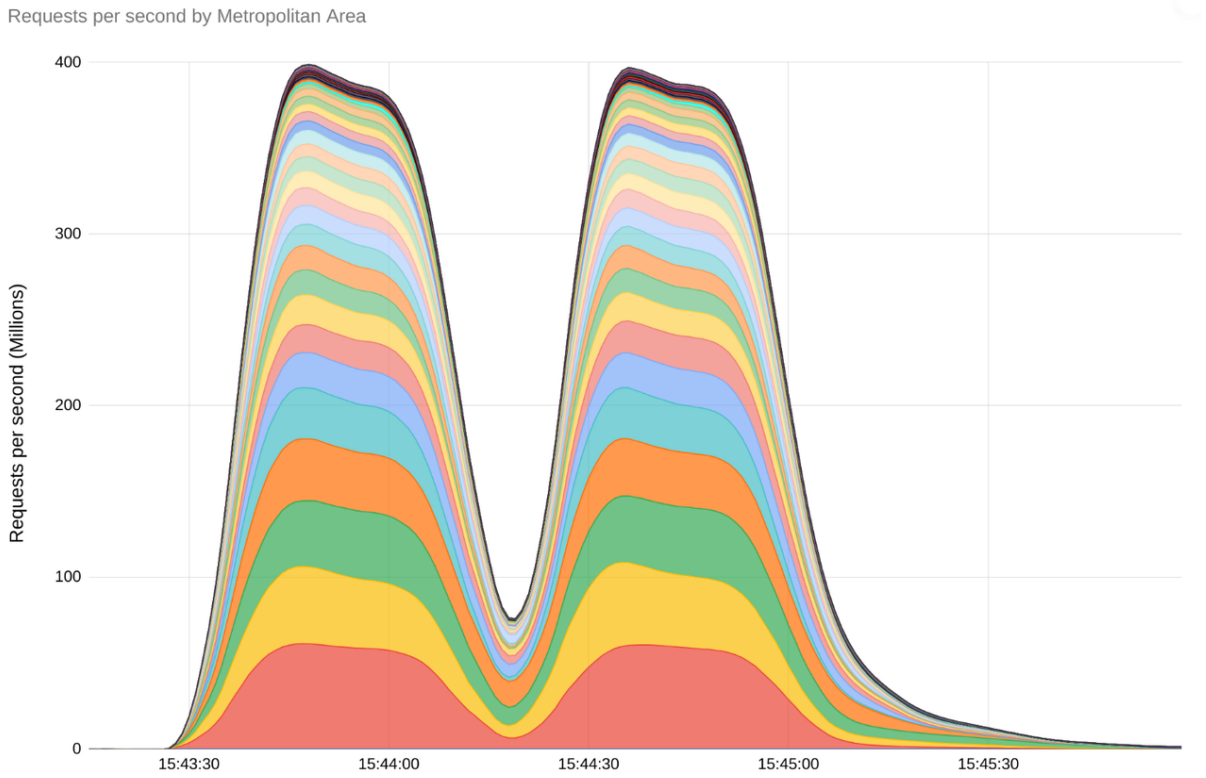
Le fonti possono utilizzare TLP:CLEAR quando le informazioni comportano un rischio minimo o prevedibile di uso improprio, in conformità con le regole e le procedure applicabili per il rilascio pubblico. Fatte salve le norme standard sul copyright, le informazioni TLP:CLEAR possono essere distribuite senza restrizioni.

Indice

Introduzione

Il giorno 10 ottobre 2023 Google Cloud, Amazon AWS e Cloudflare hanno mitigato l'attacco DDoS (Distributed Denial of Service) più grande mai registrato nella storia. Come descritto sul blog di Google Cloud [1], l'attacco ha raggiunto un picco di **398 milioni** di richieste al secondo (rps), superando di 7 volte e mezzo il record precedente di "sole" 46 milioni raggiunte da un attacco DDoS dell'anno scorso.

Per dare un'idea delle dimensioni, l'attacco (che è durato solo due minuti) ha generato più richieste del numero totale di visualizzazioni di articoli riportate da Wikipedia durante l'intero mese di settembre 2023.



Il grafico delle richieste per secondo (rps) ricevute da Google

Un attacco così imponente è stato possibile grazie allo sfruttamento di una vulnerabilità sul protocollo HTTP/2, usata per generare attacchi DDoS ipervolumetrici.

L'attacco è stato nominato **HTTP/2 Rapid Reset** e la vulnerabilità sfruttata è stata identificata come **CVE-2023-44487** [2], classificata di gravità elevata ricevendo un punteggio CVSS di 7,5 su 10.

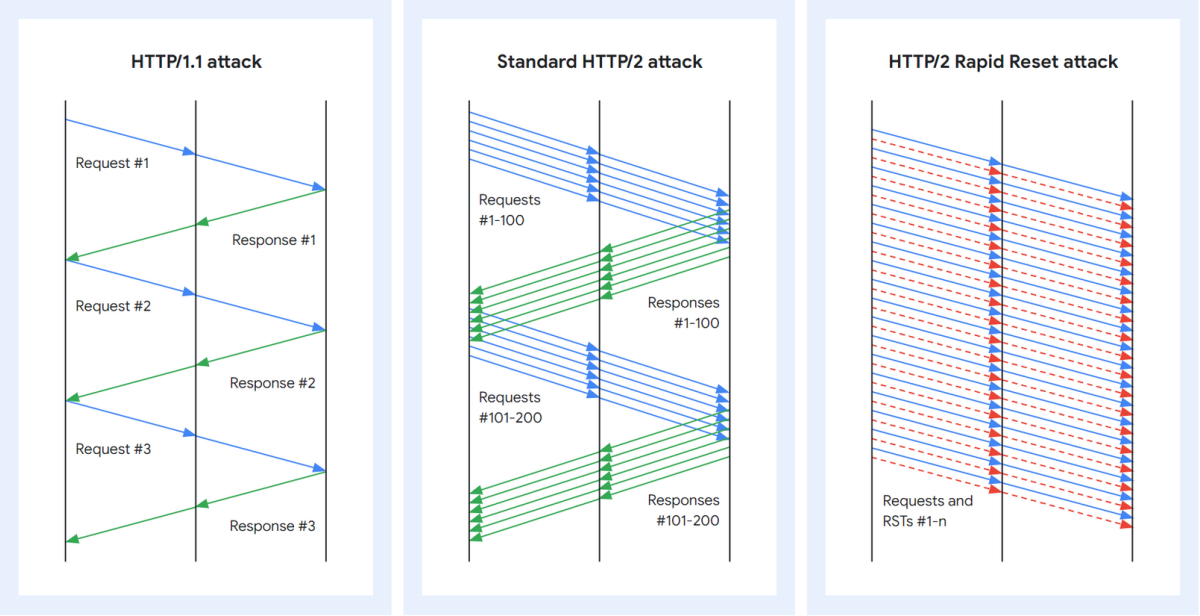
Panoramica sull'attacco

La grande differenza tra il protocollo HTTP/1.1 e HTTP/2 è il modo in cui le richieste vengono processate.

In HTTP/1.1 ogni richiesta viene elaborata in modo **seriale**, quindi il numero di richieste che possono essere inviate su una singola connessione TCP è di una richiesta per viaggio di andata e ritorno, dove un viaggio di andata e ritorno include la latenza di rete, il tempo di elaborazione del proxy e il tempo di elaborazione della richiesta di backend.

Con HTTP/2 le richieste vengono elaborate in **parallelo**. Grazie ad una funzionalità chiamata **Stream multiplexing**, ogni connessione TCP può essere utilizzata maggiormente, consentendo al client di aprire più flussi simultanei (fino a 100) su singola connessione. Facendo così si ottiene un throughput effettivo di 100 richieste per singolo viaggio di andata e ritorno, contro 1 richiesta per HTTP/1.1. Questo porta a un utilizzo quasi 100 volte superiore di ogni connessione.

L'attacco nasce perché il protocollo HTTP/2 consente ai client di indicare al server che un flusso precedente deve essere annullato inviando un frame di tipo RST_STREAM. Il protocollo non richiede che il client e il server coordinino la cancellazione in alcun modo e il client può farlo unilateralmente.



Il funzionamento dei protocolli HTTP/1.1 e HTTP/2 e dell'attacco

La capacità di un endpoint di inviare un frame RST_STREAM subito dopo l'invio di una richiesta, fa sì che l'altro endpoint inizi a lavorare e poi ripristini rapidamente la richiesta. Da qui il nome **Rapid Reset Attack**. La richiesta viene annullata, ma la connessione HTTP/2 rimane aperta.

Annullando esplicitamente le richieste, l'attaccante non supera mai il limite del numero di flussi aperti contemporanei. Il server però dovrà comunque svolgere una quantità significativa di lavoro per le richieste annullate, come l'allocazione di nuove strutture di dati di flusso, l'analisi della query e la decompressione dell'intestazione e la mappatura dell'URL a una risorsa. E' dunque intuibile come sia possibile saturare la capacità del server di destinazione con una grande quantità di richieste.

Riproduzione della vulnerabilità

Su GitHub è già stata resa disponibile una PoC (Proof of Concept) della vulnerabilità che può essere usata per testare i propri sistemi.

E' possibile scaricarla da qui: https://github.com/imabee101/CVE-2023-44487

Superficie d'attacco

Come menzionato da blackhatethicalhacking.com [4] il protocollo HTTP/2 è ampiamente adottato. Viene infatti utilizzato dal 35,6% di tutti i siti web secondo W3Techs, e nel 77% delle richieste http secondo i dati di Web Almanac.

La superficie d'attacco è dunque a livello globale. Le organizzazioni che possiedono servizi online e non hanno una protezione contro attacchi DDoS sono quelle più a rischio.

Come proteggersi

Sono già molti i vendor che stanno affrontando questa problematica, con patch di sicurezza, bollettini e mitigazioni [5].

- Cloudflare: HTTP/2 Rapid Reset: deconstructing the record-breaking attack
- Google: How it works: The novel HTTP/2 'Rapid Reset' DDoS attack
- AWS: CVE-2023-44487 - HTTP/2 Rapid Reset Attack
- NGINX: HTTP/2 Rapid Reset Attack Impacting NGINX Products
- Microsoft Response to Distributed Denial of Service (DDoS) Attacks against HTTP/2

Bibliografia

[1]https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps

[2]https://nvd.nist.gov/vuln/detail/CVE-2023-44487

[3]https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack

[4]https://www.blackhatethicalhacking.com/news/massive-ddos-attacks-exploiting-http-2-rapid-reset-zero-day-vulnerability/

[5]https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487