BOLETIM DE SEGURANÇA

Novo ataque de zero day “HTTP/2 Rapid Reset” envolvido com DDoS.

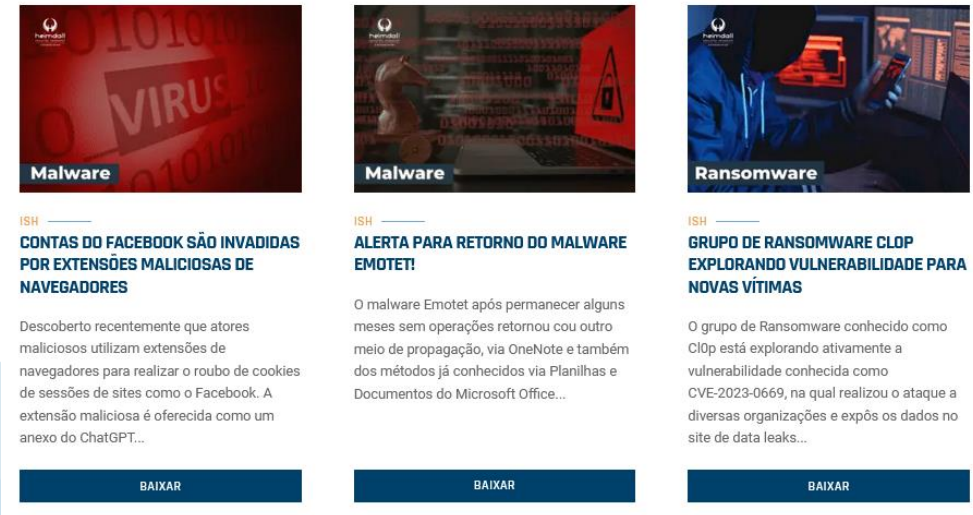
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



heimdall
security research

Sumário

Lista de Figuras

1 SOBRE O ATAQUE DDOS E VULNERABILIDADE

Uma nova técnica de DDoS (negação de serviço distribuída) chamada **"HTTP/2 Rapid Reset"** tem sido ativamente explorada como zero day desde agosto, quebrando todos os recordes anteriores.

A notícia do zero day foi entregue por meio de um anúncio coordenado entre a Amazon Web Services, Cloudflare e Google, as quais relataram a mitigação de ataques atingindo 155 milhões de solicitações por segundo (Amazon, 201 milhões de RPS (Cloudflare) e um recorde de 398 milhões de RPS (Google).

Este novo ataque explora uma vulnerabilidade de zero day rastreada como **CVE-2023-44487** (sem score definido), que abusa do recurso de cancelamento de fluxo do HTTP/2 para enviar e cancelar solicitações continuamente, sobrecarregando o servidor/aplicativo alvo e impondo um estado DoS.

O HTTP/2 apresenta uma proteção na forma de um parâmetro que limita o número de fluxos ativos simultaneamente para evitar ataques DoS, porém, nem sempre isso é eficaz.

Os desenvolvedores do protocolo introduziram uma medida mais eficiente chamado "cancelamento de solicitação", que não interrompe toda a conexão, mas que poderá ser abusada.

Atores maliciosos têm abusado deste recurso desde o final de agosto para enviar uma enxurrada de solicitações e redefinições HTTP/2 (quadros *RST_Stream*) em um servidor, solicitando que ele processe cada uma delas e execute redefinições rápidas, sobrecarregando sua capacidade de responder a novas solicitações recebidas.

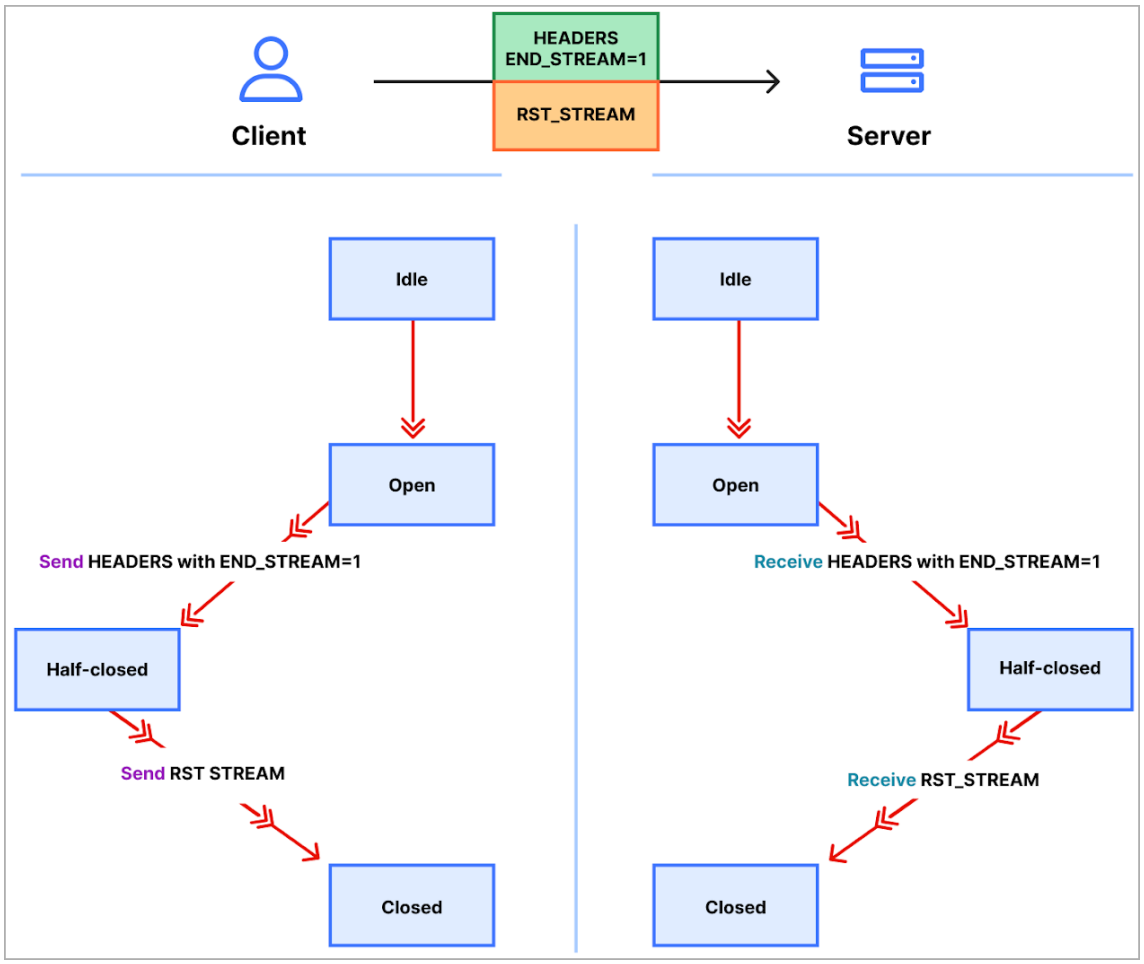


Figura 1 – Diagrama de fluxo de solicitações de acordo com a Cloudflare.

De acordo com a Google, o protocolo não exige que o cliente e servidor coordenem de forma alguma o cancelamento, o cliente pode fazê-lo unilateralmente, bem como pode presumir que o cancelamento terá efeito imediatamente quando o servidor receber o quadro *RST_STREAM*, antes que quaisquer outros dados dessa conexão TCP sejam processados.

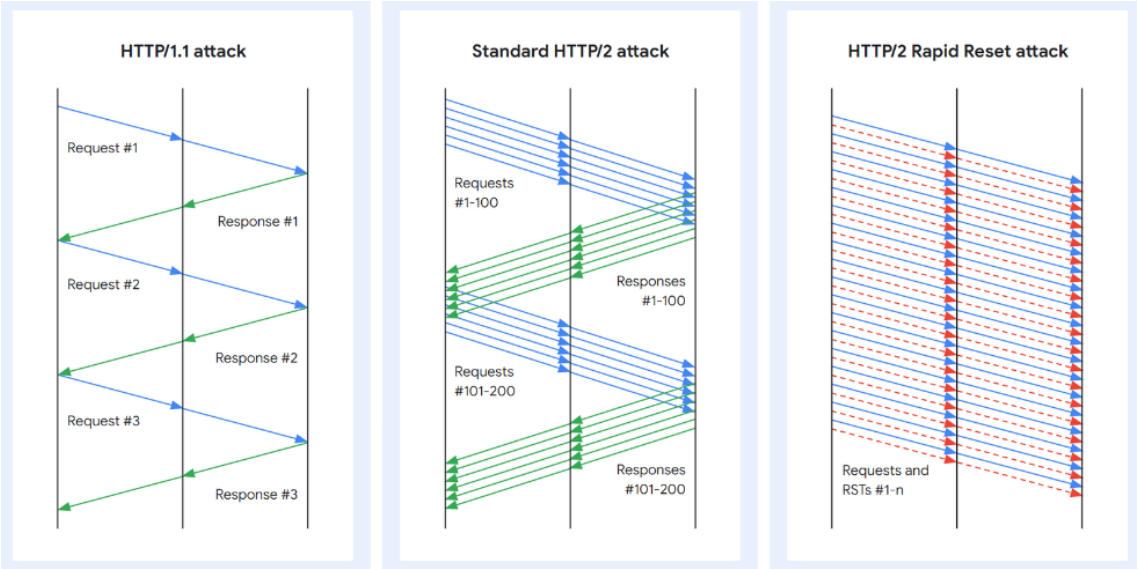


Figura 2 – Visão geral da lógica de redefinição rápida HTTP/2.

Para mitigar estes ataques, a Cloudflare afirmou que utilizou um sistema projetado para lidar com ataques hiper volumétricos chamado ***"IP Jail"***, que a empresa de Internet expandiu para cobrir toda a sua infraestrutura.

A Amazon afirmou que mitigou dezenas desses ataques sem fornecer detalhes sobre seu impacto, destacando que a disponibilidade de seus serviços ao cliente ofi mantida.

Por fim, as três empresas afirmaram que a melhor abordagem para os clientes combaterem ataques HTTP/2 Rapid Reset é utilizar todas as ferramentas de proteção contra inundação HTTP disponíveis e reforçar sua resiliência DDoS com mitigações multifacetadas.

Infelizmente, como esta tática abusa do protocolo HTTP/2, não existe uma solução geral que impeça totalmente os invasores de utilizá-la.

Diante disto, recomendamos que sejam acompanhados todos os serviços oferecidos pelas empresas de internet e hospedagem, como as três já mencionadas neste alerta, sendo necessário ativação de todos os recursos para que haja a mitigação dos ataques HTTP/2 Rapid Reset.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Comunicado HTTP/2 Zero Day – Cloudflare**
- **Comunicado HTTP/2 Zero Day – Google**
- **Comunicado HTTP/2 Zero Day - Amazon**

heimdall
security research
A DIVISION OF ISH