TLP: CLEAR

BOLETIM DE SEGURANÇA

Cloudflare mitiga o maior ataque DDoS de 3,8 Tbps já registrado

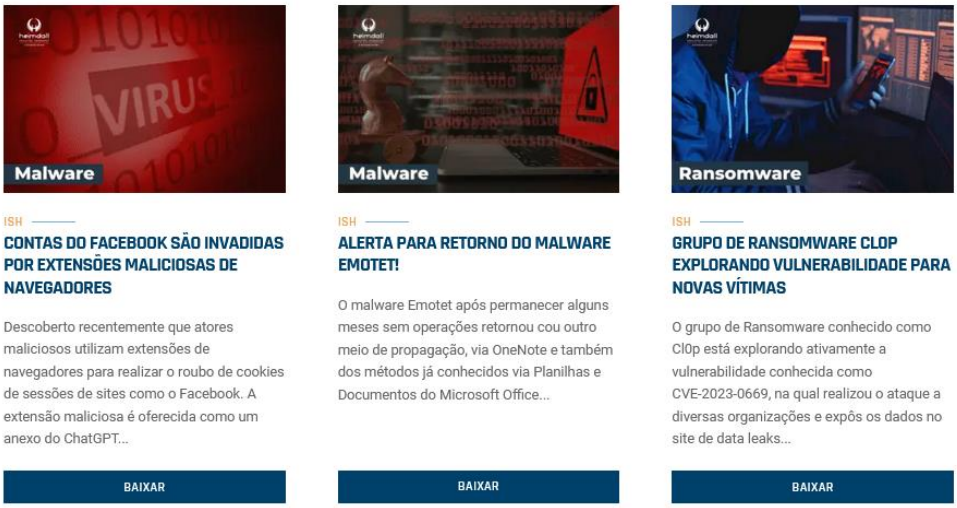
heimdall
security research
A DIVISION OF ISH

Acesse a nossa nova comunidade através do WhatsApp!

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



SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A **Cloudflare** anunciou a mitigação de um ataque **DDoS** recorde, que atingiu um pico de **3,8 terabytes por segundo (Tbps)** e durou **65 segundos**. Este ataque, o maior já registrado, foi completamente neutralizado pelos sistemas autônomos da Cloudflare, demonstrando a eficácia de suas defesas contra ameaças hipervolumétricas.

2 INFORMAÇÕES SOBRE A AMEAÇA

Desde o início de setembro, a Cloudflare tem enfrentado uma série de ataques DDoS L3/4 de alta intensidade. Ao longo do mês, a empresa mitigou mais de cem desses ataques, muitos dos quais ultrapassaram 2 bilhões de pacotes por segundo (Bpps) e 3 terabytes por segundo (Tbps).

O maior ataque registrado atingiu 3,8 Tbps, o maior já divulgado publicamente. A detecção e mitigação desses ataques foram realizadas de forma totalmente autônoma. Dois eventos de ataque distintos, direcionados ao mesmo cliente, foram neutralizados sem intervenção manual.

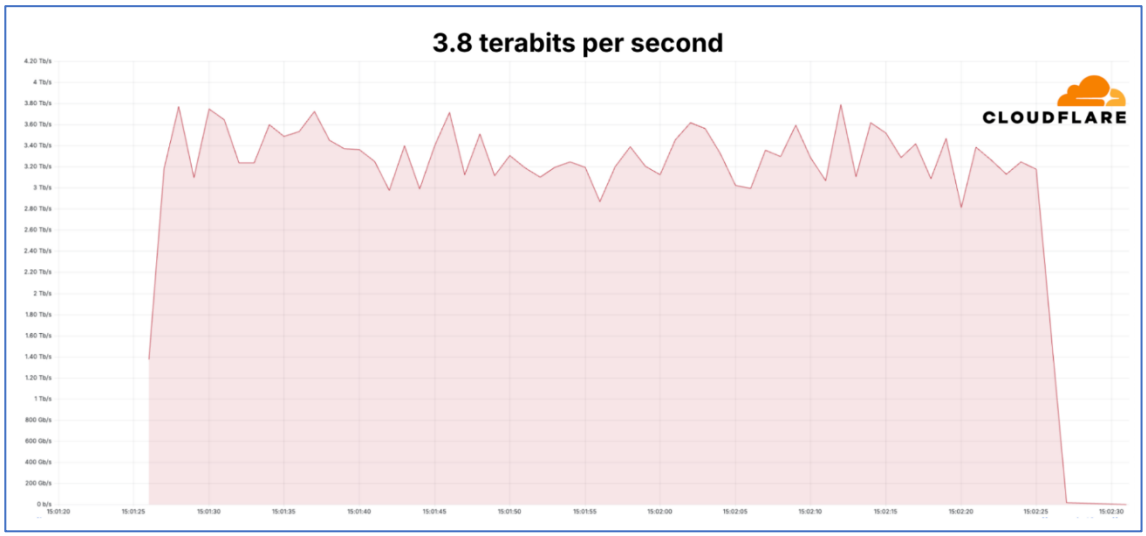


Figura 1 – Um ataque DDoS mitigado de 3,8 Terabytes por segundo que durou 65 segundos.

Clientes que utilizam os serviços de proxy reverso HTTP da Cloudflare, como o WAF e o CDN, bem como os serviços Spectrum e Magic Transit, estão automaticamente protegidos. Os clientes do Magic Transit podem aumentar ainda mais sua proteção com regras do Magic Firewall, implementando um modelo de segurança rigoroso. A escala e frequência desses ataques são sem precedentes, com potencial para derrubar propriedades da Internet desprotegidas ou protegidas por soluções insuficientes. No entanto, a Cloudflare possui a capacidade de rede, cobertura global e sistemas inteligentes necessários para mitigar esses ataques automaticamente.

Foi detectada uma campanha de ataque direcionada a diversos clientes nos setores de serviços financeiros, Internet e telecomunicações, entre outros. Essa campanha visa saturar a largura de banda e esgotar os recursos de aplicativos e dispositivos online. Os ataques utilizam principalmente UDP em uma porta fixa e têm origem global, com maiores volumes vindos do Vietnã, Rússia, Brasil, Espanha e EUA. Os ataques de alta taxa de pacotes parece ser originados de vários

dispositivos comprometidos, como dispositivos MikroTik, DVRs e servidores Web, que são coordenados para inundar o alvo com tráfego massivo. Já os ataques de alta taxa de bits parecem vir de muitos roteadores domésticos ASUS comprometidos, provavelmente explorados por uma vulnerabilidade CVE 9.8 (Crítica) descoberta recentemente pela Censys.

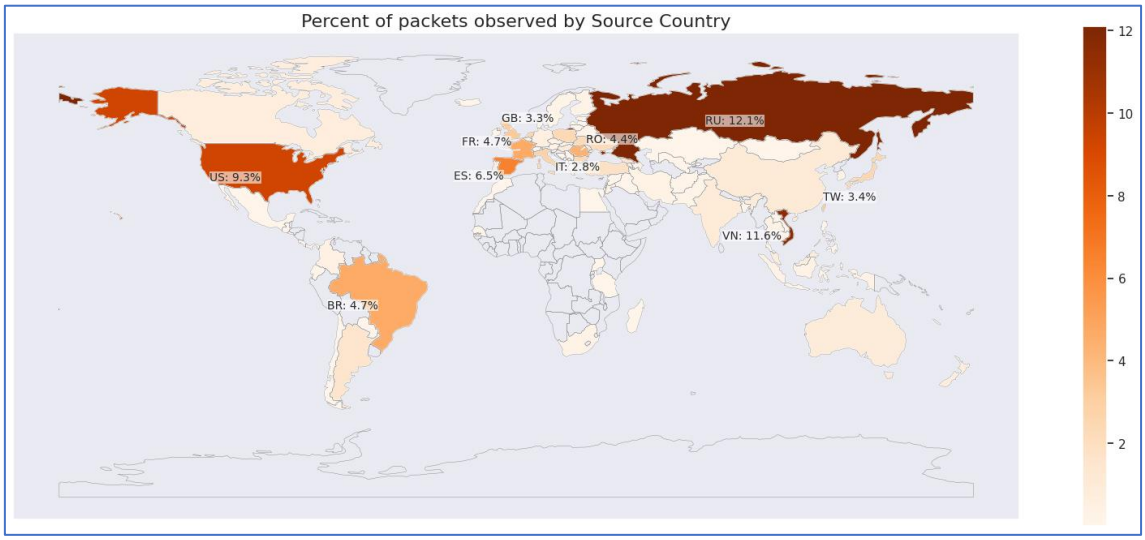


Figura 2 – Pacotes observados por países de orígem.

Para compreender como a Cloudflare identificou e neutralizou automaticamente os maiores ataques DDoS registrados, é essencial primeiro entender os fundamentos dos ataques DDoS.

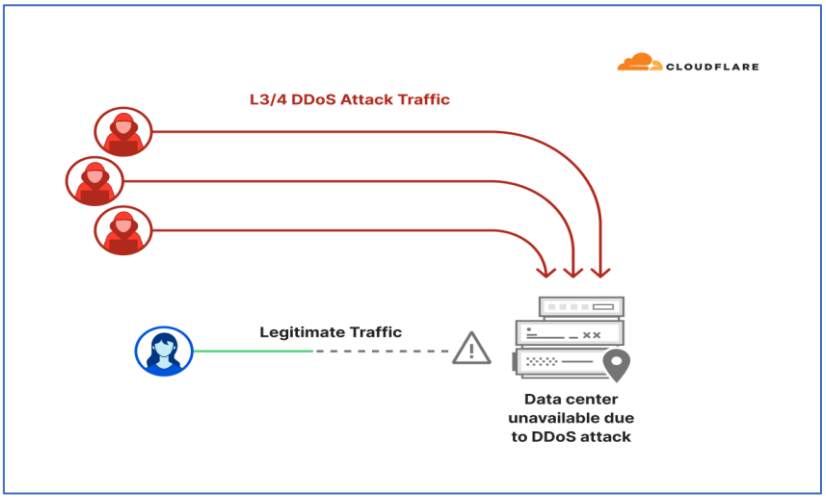


Figura 3 – Cadeia de ataque do DDOS.

Processar pacotes consome ciclos de CPU. Em tráfego normal (não ataque), um pacote legítimo faz com que o serviço execute uma ação, e diferentes ações

exigem diferentes quantidades de processamento. Antes de um pacote ser entregue a um serviço, há um trabalho inicial necessário. Os cabeçalhos de pacote da camada 3 precisam ser analisados e processados para entregar o pacote à máquina e interface corretas. Os cabeçalhos da camada 4 precisam ser processados e roteados para o soquete correto (se houver). Várias etapas adicionais podem inspecionar cada pacote. Se um invasor enviar pacotes em alta taxa, pode saturar os recursos de CPU, negando serviço a usuários legítimos.

Para se defender contra-ataques de alta taxa de pacotes, é necessário inspecionar e descartar pacotes ruins com o mínimo de ciclos de CPU, deixando CPU suficiente para pacotes bons. Adquirir mais CPUs ou mais rápidas pode ajudar, mas é um processo caro e demorado. A largura de banda da rede é a quantidade total de dados por tempo que pode ser entregue a um servidor. Pense na largura de banda como um cano de água. Se um invasor inserir mais dados inúteis, tanto dados ruins quanto bons serão descartados na entrada, tornando o DDoS bem-sucedido.

Figura 4 – Exemplo inserção alta quantidade de dados para ataque do DDOS.

Proteger-se contra-ataques que podem saturar a largura de banda da rede é desafiador, especialmente quando se está no lado downstream de um pipe saturado. As opções são limitadas como, aumentar a capacidade do pipe, redirecionar o tráfego legítimo para um pipe não saturado, ou solicitar ao **upstream** que reduza ou interrompa o envio de dados.

Do ponto de vista dos atacantes, há restrições semelhantes. Criar pacotes requer ciclos de CPU, assim como recebê-los. Se o custo de envio e recebimento fosse igual, o atacante precisaria de tanto poder de CPU quanto o defensor. No entanto, geralmente há uma assimetria de custo, com o atacante usando menos ciclos de CPU para gerar pacotes do que o defensor para os receber. Ainda assim, gerar ataques não é gratuito e pode demandar muito poder de CPU.

Para saturar a largura de banda, o invasor precisa gerar mais tráfego do que o serviço alvo pode suportar, superando sua capacidade. Isso é difícil, por isso ataques de reflexão/amplificação, como os de amplificação de DNS, são comuns. Nesses ataques, um pequeno pacote enviado a um serviço intermediário resulta em um grande pacote enviado à vítima.

Os invasores precisam de muitos dispositivos para gerar esses ataques, que podem ser servidores de nuvem, serviços de hospedagem ou dispositivos comprometidos como DVRs, roteadores e webcams infectados com malware, formando uma botnet. A rede da Cloudflare usa anycast, onde um único IP é anunciado por várias máquinas globalmente. Um pacote enviado a esse IP é atendido pela máquina mais próxima, distribuindo o ataque pela rede. Assim, um DVR infectado em Dallas envia pacotes para um servidor da Cloudflare em Dallas, enquanto uma webcam infectada em Londres envia pacotes para um servidor em Londres.

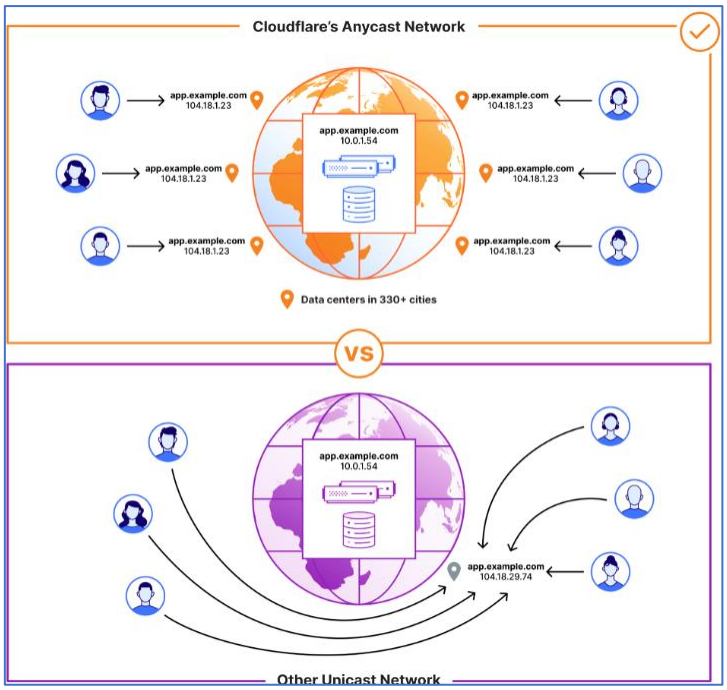


Figura 5 – Redes Anycast vs. Unicast.

A rede anycast da Cloudflare possibilita a alocação de recursos de computação e largura de banda mais próximos das regiões que mais necessitam. Em áreas densamente povoadas, onde o tráfego legítimo é maior, os data centers são equipados com mais largura de banda e recursos de CPU. Já em regiões menos povoadas, onde o tráfego é menor, os data centers são dimensionados de acordo. Como os ataques vêm principalmente de dispositivos comprometidos, eles tendem a seguir os padrões normais de tráfego, distribuindo o tráfego de ataque

proporcionalmente entre os data centers capazes de lidar com isso. Dentro dos data centers, o tráfego é ainda distribuído entre várias máquinas.

Para ataques de alta largura de banda, a rede da Cloudflare tem uma vantagem adicional. Grande parte do tráfego na rede não consome largura de banda de forma simétrica. Por exemplo, uma solicitação HTTP para uma página web gera um pequeno pacote de entrada, mas um grande volume de tráfego de saída. Isso significa que a Cloudflare ejetará mais tráfego legítimo do que recebe. Como os links de rede são simétricos, há largura de banda de entrada suficiente para receber tráfego de ataque volumétrico.

Quando o tráfego atinge um servidor dentro de um data center, a largura de banda do ataque já foi distribuída, evitando a saturação dos links upstream. No entanto, o ataque ainda não foi totalmente interrompido, pois os pacotes ruins ainda não foram descartados. Para isso, é necessário amostrar o tráfego, identificar o ataque e criar regras para bloquear os pacotes ruins.

A amostragem de tráfego e o descarte de pacotes ruins são realizados pelo componente l4drop, que utiliza XDP (**eXpress Data Path**) e eBPF (**extended Berkeley Packet Filter**). Isso permite a execução de código personalizado no kernel, processando cada pacote diretamente na placa de interface de rede (NIC), descartando pacotes de forma eficiente sem sobrecarregar a CPU.

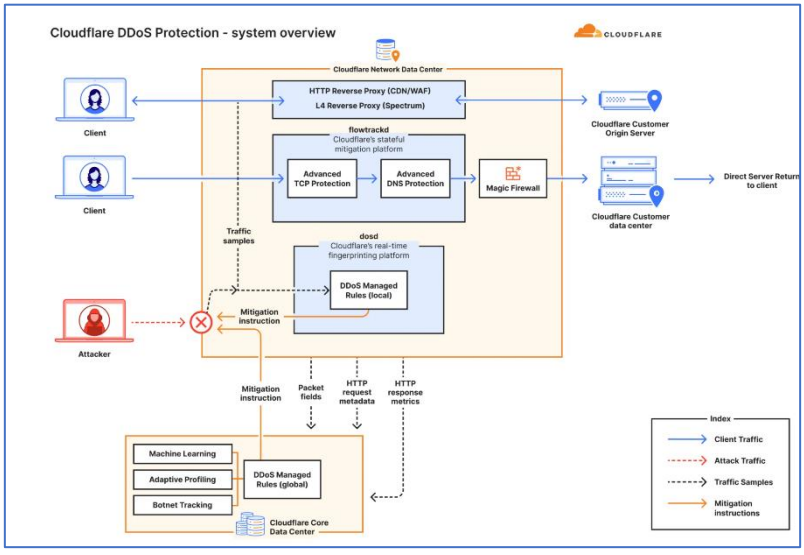


Figura 6 – Visão geral do sistema de proteção DDoS da Cloudflare.

Para detectar atributos suspeitos que possam indicar um ataque, foi utilizado o XDP para amostrar pacotes. Essas amostras incluem informações como IP de origem e destino, portas, protocolo, sinalizadores TCP, número de sequência, opções, taxa de pacotes, entre outros. A análise é realizada pelo daemon de negação de serviço (**dosd**), que contém filtros baseados em heurísticas para iniciar

a mitigação. Esses filtros são organizados por vetores de ataque e apresentados como Regras Gerenciadas de DDoS, permitindo personalização pelos clientes.

Ao receber amostras do XDP, o dosd gera várias impressões digitais de padrões de tráfego suspeitos. Utilizando um algoritmo de streaming de dados, ele identifica as impressões digitais mais eficazes para mitigar o ataque. Quando um ataque é identificado, o dosd envia uma regra de mitigação inline como um programa eBPF para eliminar o tráfego malicioso.

A detecção e mitigação de ataques pelo dosd ocorre no nível do servidor, data center e globalmente, tudo definido por software, garantindo uma rede resiliente e mitigação quase instantânea. Cada servidor executa a pilha completa de produtos Cloudflare, incluindo detecção e mitigação de DDoS, de forma autônoma. Servidores também compartilham instruções de mitigação dentro e entre data centers, assegurando proteção robusta contra-ataques localizados ou distribuídos globalmente.

Os sistemas autônomos de detecção e mitigação de DDoS operam em toda a nossa rede. Além da impressão digital dinâmica, contou-se com sistemas de proteção avançada para TCP e DNS, que utilizam análise estatística e inteligência de ameaças em tempo real. A **Adaptive DDoS Protection** incorpora aprendizado de máquina para mitigar anomalias de tráfego. Esses sistemas, integrados ao portfólio de segurança da Cloudflare, garantem proteção contra os maiores ataques do mundo, sustentados por uma das maiores redes globais.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Cludflare**
- **Thehackernews**

4 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH