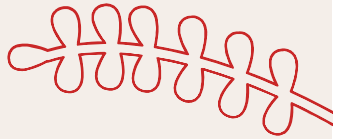
Negação de Serviço (DoS/DDoS)

Feito por:

- João Pedro de Oliveira Gibrail
- Luiz Henrique dos Santos Carneiro
- Matheus Ferreira Santos
- Murilo Rodrigues Fernandes Soares

Tópicos a serem abordados



01

O que é?

O que é, como funciona e principais diferenças

02

Fluxo do ataque

Como o ataque funciona passo a passo

03

Vulnerabilidades

Vulnerabilidades e ferramentas

04

Mitigação

Medidas técnicas e comportamentais

05

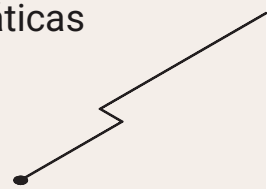
Exemplos

Exemplos reais

06

Conclusão

Conclusão e boas práticas



01
O que é?

O que é, como funciona e principais diferenças

O que é?

DoS

DoS (Denial of Service) ou Negação de Serviço, trata-se de um tipo de ataque cibernético em que um sistema, serviço ou rede é sobrecarregado com tráfego malicioso, tornando-o inacessível para usuários legítimos.

- Um único computador envia uma grande quantidade de requisições para um servidor-alvo.
- O servidor tenta responder, mas fica sobrecarregado e trava ou cai.
- Como resultado, o serviço fica indisponível para quem realmente precisa usá-lo.

DDoS

DDoS (Distributed Denial of Service) ou Negação de Serviço Distribuída, trata-se de uma variante mais avançada do DoS, sendo também um ataque com intenção de sobrecarregar determinado sistema, serviço ou rede.

- O ataque vem de múltiplos computadores simultaneamente (geralmente botnets).
- Esses dispositivos atacam simultaneamente um único alvo
- O volume de tráfego é muito maior do que no DoS, tornando o ataque mais difícil de parar e rastrear

Principais Diferenças

Característica	DoS	DDoS
Origem do ataque	Um único computador	Vários computadores (distribuídos)
Complexidade	Mais simples	Mais complexo
Intensidade	Menor	Maior (mais tráfego simultâneo)
Dificuldade de defesa	Mais fácil de bloquear	Mais difícil, pois vem de várias fontes
Uso comum de botnets	Raro	Muito comum

02
Fluxo do Ataque

Como o ataque funciona passo a passo

Fluxo do Ataque

1 Reconhecimento

O atacante identifica alvos potenciais (serviços, portas, servidores, serviços públicos vulneráveis) e avalia capacidade de rede e pontos fracos.

2 Comprometimento/Recrutamento

No caso de DDoS, o atacante compromete dispositivos (IoT, servidores mal protegidos) ou aluga botnets/serviços para reunir fontes de tráfego. Em DoS simples isso pode não ocorrer.

3 Preparação do vetor

O atacante escolhe a técnica (flood de rede, flood de aplicação, amplificação/reflexão) e configura parâmetros (volume desejado, duração aproximada, payloads conceituais).

Fluxo do Ataque

4 Lançamento

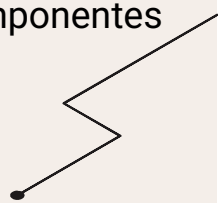
As fontes começam a enviar tráfego simultaneamente para o alvo, com o objetivo de esgotar recursos (banda, conexões, CPU, I/O da aplicação).

5 Persistência e adaptação

Durante o ataque, o atacante pode mudar vetores, IPs ou padrões para contornar filtros e prolongar o impacto.

6 Encerramento e limpeza

o atacante interrompe o envio; frequentemente há tentativas de apagar rastros em componentes controlados.



03 Vulnerabilidades

Vulnerabilidades e ferramentas

Vulnerabilidades exploradas

Serviços mal configurados

- Servidores DNS, NTP, SSDP, Memcached abertos na internet.
- Permitem ataques de amplificação e reflexão (resposta maior que a requisição).

Falta de controle de requisições

- APIs e sites sem rate limit permitem muitas chamadas simultâneas.
- Endpoints pesados (buscas, relatórios, loops) sobrecarregam o sistema.

Protocolos antigos e inseguros

- Versões antigas de NTP (monlist), Chargen, SNMP.
- Respondem a qualquer solicitação, facilitando abusos.

Falta de filtragem e firewall

- Tráfego suspeito não é bloqueado.
- Firewalls mal configurados deixam passar pacotes falsos (SYN, UDP flood).

Ferramentas utilizadas

LOIC (Low Orbit Ion Cannon)		Ferramenta open-source de stress que gera tráfego TCP/UDP em massa via interface simples. Muito usada por iniciantes e em ataques coordenados por voluntários.
HOIC (High Orbit Ion Cannon)		Evolução do LOIC focada em HTTP; mais poderosa e com opções de personalização para ataques direcionados em equipe.
Slowloris		Ataque “lento”: mantém muitas conexões HTTP abertas parcialmente para esgotar recursos do servidor sem gerar grande volume de tráfego. Eficaz com poucos recursos.
R.U.D.Y. (R-U-Dead-Yet)		Outro ataque de baixa intensidade que envia muitos POSTs lentos e mantém conexões abertas para degradar servidores web.

04
Mitigação

Medidas técnicas e comportamentais

Mitigação

Já que os ataques de DoS e DDoS assumem uma variedade de formas, mitigá-los requer uma variedade de táticas. As táticas mais comuns para parar os ataques DDoS incluem:

Limitação de taxa

Limita o número de solicitações que um servidor pode aceitar durante um determinado intervalo de tempo.

Firewalls de aplicativos web

Ferramentas que filtram o tráfego da web com base em uma série de regras.

Difusão da rede Anycast

Coloca uma ampla rede em nuvem distribuída entre um servidor e o tráfego de entrada, fornecendo recursos adicionais de computação com os quais responder às solicitações.

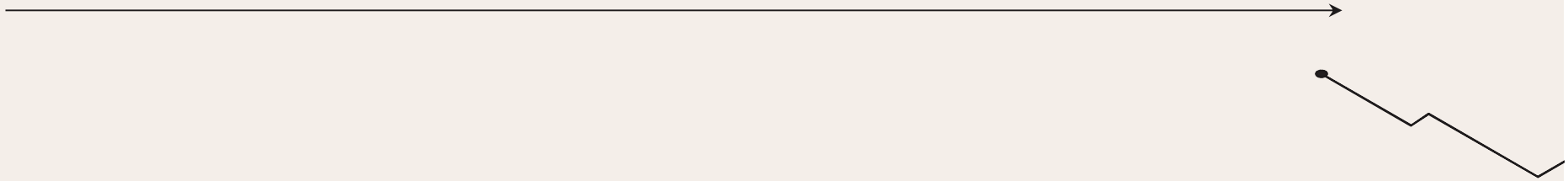
05 Exemplos

Exemplos reais

Exemplo real

Ataque DDoS à Azure, teve como alvo um único endpoint localizado na Austrália. Foi considerado o maior ataque de DDoS já registrado.

01	02	03
O incidente ocorreu em 24 de outubro de 2025.	Pico de 15,72 Tbps (terabits por segundo) de tráfego malicioso.	Aproximadamente 3,64 bilhões de pacotes por segundo (pps).



Exemplo real

04

Originou-se de mais de 500 mil endereços IP comprometidos.

05

Foi atribuído à botnet Aisuru, uma variante da família Turbo Mirai.

06

Segundo a Convergência Digital, o cliente alvo era da Cloudflare (empresa de infraestrutura e proteção contra DDoS).

07

A proteção DDoS da Azure foi ativada automaticamente.

08

O tráfego malicioso foi filtrado e redirecionado, evitando sobrecarga nos serviços do cliente.

09

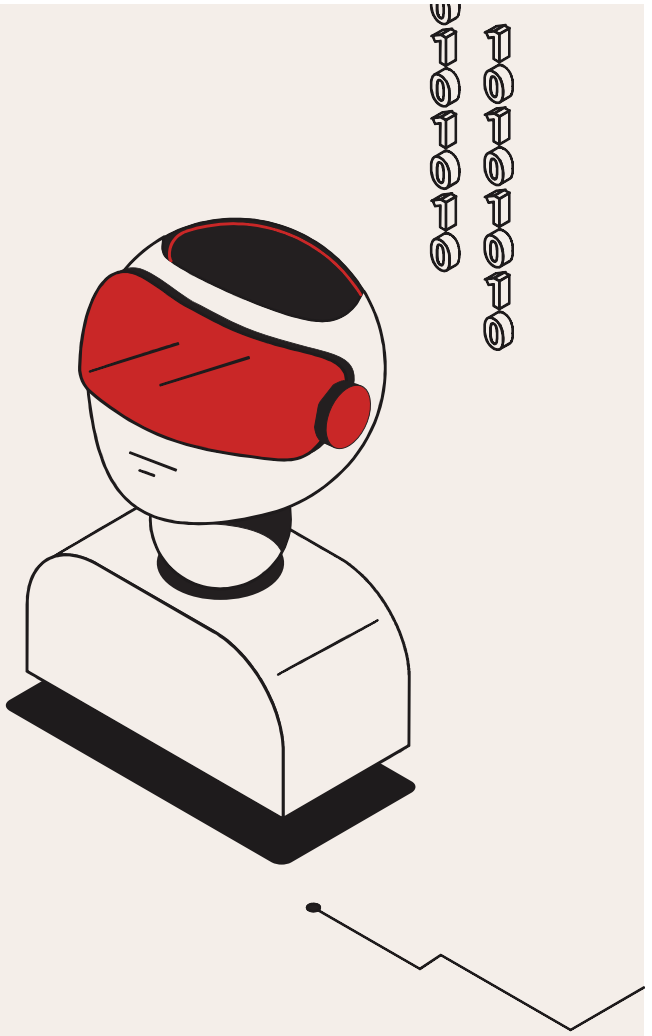
Não houve interrupção nos serviços dos clientes afetados (“disponibilidade ininterrupta”).

06
Conclusão

Conclusão e boas práticas

Conclusão

Os ataques DoS e, principalmente, DDoS representam uma das ameaças mais comuns e eficazes contra sistemas conectados à internet. A evolução dessas técnicas, como mostrado em ataques recentes que ultrapassam dezenas de terabits por segundo, demonstra que criminosos têm acesso a botnets cada vez maiores, muitas delas formadas por dispositivos IoT inseguros. Mesmo não explorando falhas de software, ataques DDoS podem interromper serviços críticos, gerar prejuízos financeiros, afetar a reputação das empresas e comprometer a disponibilidade de operações essenciais. Assim, defender-se não depende apenas de infraestrutura robusta, mas também de práticas preventivas, monitoramento constante e respostas rápidas. Em resumo: a prevenção é a principal defesa, e somente uma combinação de tecnologia, boas práticas e conscientização pode reduzir os impactos desse tipo de ataque.



Referências

•CONVERGÊNCIA DIGITAL. Azure da Microsoft sofreu ataque massivo de DDoS de 15,7 Tbps; cliente-alvo seria da Cloudflare. Convergência Digital, 24 out. 2025. Disponível em: https://convergenciadigital.com.br/governo/azure-da-microsoft-sofreu-ataque-massivo-de-ddos-de-157-tbps-cliente-alvo-seria-da-cloudflare/. Acesso em: 04 nov. 2025.
•TECMUNDO. Microsoft confirma ataque DDoS de quase 16 Tbps contra Azure. Tecmundo, 25 out. 2025. Disponível em: https://www.tecmundo.com.br/seguranca/408626-microsoft-confirma-ataque-ddos-de-quase-16-tbps-contra-azure.htm. Acesso em: 04 nov. 2025.
•ADRENALINE. Azure sofre maior ataque DDoS da história: 15,72 Tbps vindo de botnet IoT. Adrenaline, 25 out. 2025. Disponível em: https://www.adrenaline.com.br/seguranca/azure-maior-ataque-ddos-historia-15-72-tbps-iot-botnet/. Acesso em: 04 nov. 2025.
•CLOUDFLARE. What is a DDoS attack? Cloudflare. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/. Acesso em: 04 nov. 2025.
•CLOUDFLARE. How to DDoS. Cloudflare. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/ddos-attack-tools/how-to-ddos/. Acesso em: 11 nov. 2025.
•CLOUDFLARE. Learning DDoS. Cloudflare. Disponível em: https://www.cloudflare.com/learning/ddos/. Acesso em: 25 nov. 2025.
•OWASP. OWASP Top Ten. OWASP. Disponível em: https://owasp.org/www-project-top-ten/. Acesso em: 11 nov. 2025.
•KREBSONSECURITY. Krebs on Security. Disponível em: https://krebsonsecurity.com/. Acesso em: 11 nov. 2025.