

# DDOS



---

Trabalho Fatec

DSM - Noite



# **Introdução aos Ataques DDoS**

---

Tárcio Teles

# Definição:

DDoS (Distributed Denial of Service) é um tipo de ataque cibernético que tem como objetivo sobre carregar um sistema de computador ou rede, tornando-o inacessível para usuários legítimos.

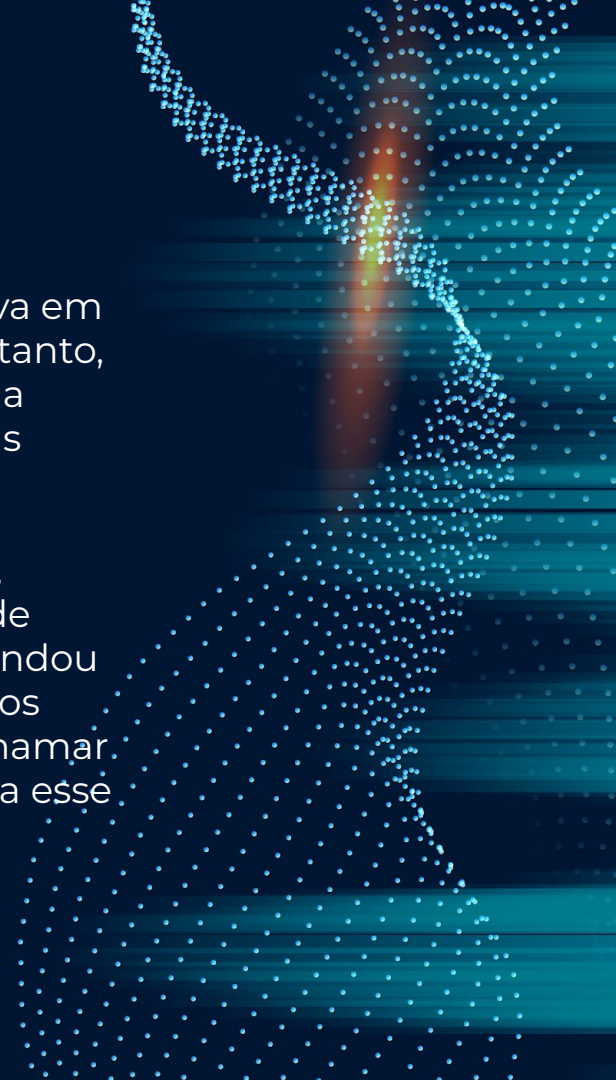
O objetivo primário de um ataque DDoS é interromper o funcionamento normal de um serviço online, como um site, aplicativo ou servidor, prejudicando a disponibilidade do serviço.



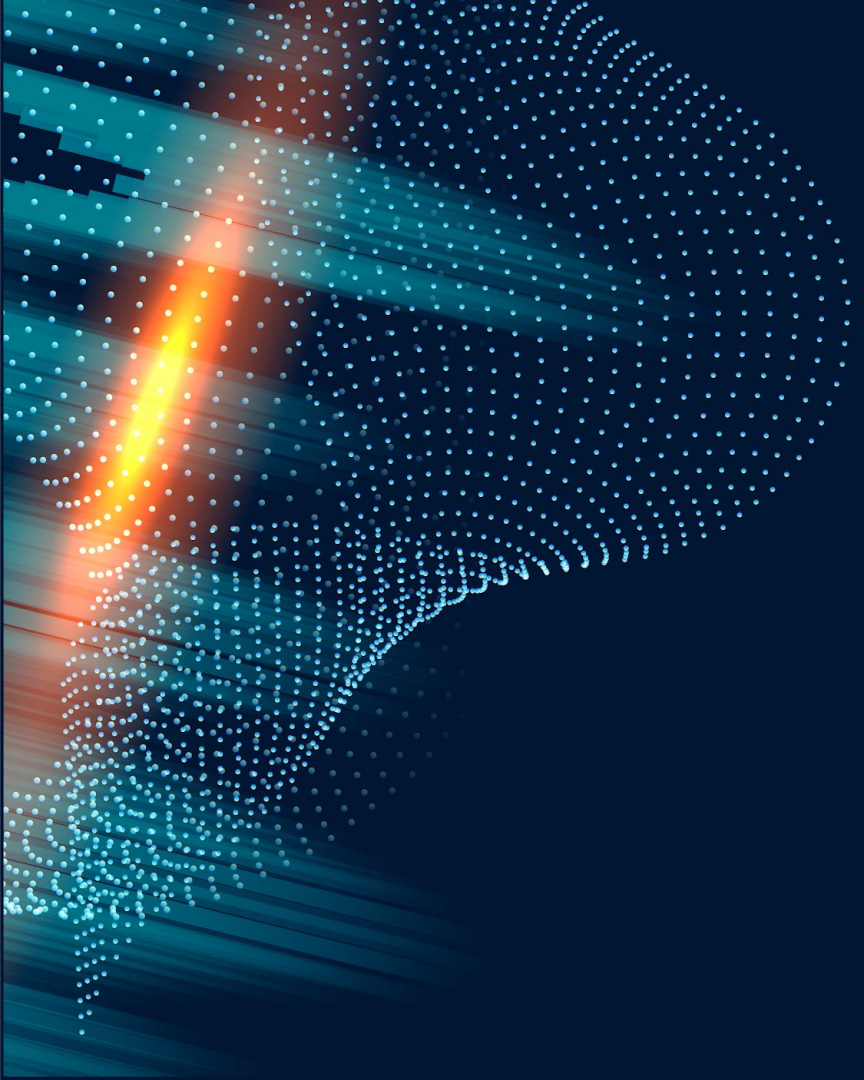
# Primeiros Ataques DDoS:

Os primeiros registros documentados de ataques DDoS remontam à década de 1990, quando a internet ainda estava em seus estágios iniciais de desenvolvimento comercial. No entanto, o conceito de ataques de negação de serviço remonta ainda mais, com formas mais simples de ataques sendo realizadas antes do advento da internet moderna.

Um dos primeiros ataques DDoS notáveis ocorreu em 1996, quando a Panix, um dos primeiros provedores de serviços de internet nos Estados Unidos, foi alvo de um ataque que inundou seus servidores com tráfego, tornando-os inacessíveis para os usuários legítimos. Esse incidente foi um dos primeiros a chamar a atenção para a vulnerabilidade das infraestruturas online a esse tipo de ataque.







# Tipos e Métodos de Ataques DDos

---

Lucas Ramos

---

# Tipos de Ataques DDoS

**Ataques de volume:** Sobrecarregam a largura de banda do alvo com tráfego massivo.

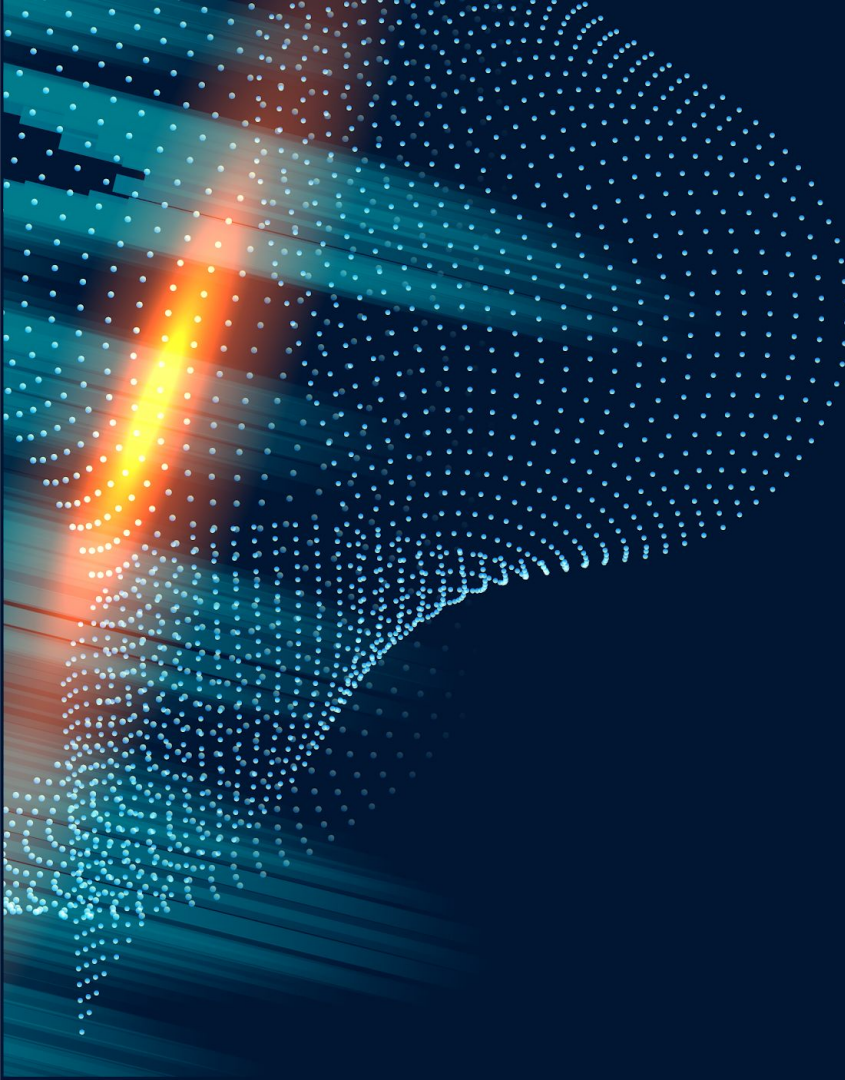
**Ataques de exaustão de recursos:** Esgotam os recursos computacionais do alvo, como CPU e memória.

**Ataques de aplicativos:** Exploram vulnerabilidades em aplicativos web ou serviços específicos.

**Ataques de protocolo:** Exploram vulnerabilidades em protocolos de rede.

**Ataques de camada de transporte:** Sobrecarrega a infraestrutura de rede subjacente.





# MOTIVAÇÕES E OBJETIVOS POR TRÁS DOS ATAQUES

---

Igor Fernandes

---

## Motivações obscuras

Os ataques DDoS (Distributed Denial of Service) representam uma ameaça persistente para a estabilidade e disponibilidade dos serviços online.

Por trás desses ataques, encontramos uma variedade de motivações obscuras, cada uma impulsionando diferentes grupos e indivíduos a lançarem esses ataques contra servidores e redes.

Além disso, é importante observar que esses ataques podem resultar em sérios prejuízos financeiros e de reputação para as organizações-alvo, bem como interrupções significativas dos serviços para os usuários finais, destacando a importância crítica de entender e mitigar essas ameaças de maneira eficaz.





# Motivações por trás dos ataques

As principais motivações são:

- Extorsão Financeira
- Concorrência Desleal
- Ativismo Político
- Hacktivismo
- Sabotagem
- Demonstração de Habilidade

---

# DNS Dyn

Um exemplo notável de ataque DDoS é o ataque ocorrido em outubro de 2016 contra a provedora de serviços de DNS Dyn, que resultou em interrupções significativas de acesso a muitos dos principais sites da internet, incluindo Twitter, Netflix, Amazon, e outros

Por trás desses ataques, encontramos uma variedade de motivações obscuras, cada uma impulsionando diferentes grupos e indivíduos a lançarem esses ataques contra servidores e redes.

- **Demonstração de Poder**
- **Exploração de Dispositivos IoT**
- **Impacto Financeiro e Reputacional**





# Consequências e Impactos dos ataques DDoS

---

Pedro Lacerda

---

# Efeitos dos Ataques DDoS

## 1. Tempo de Inatividade do Site

Seu site ficará indisponível e terá um impacto negativo no ranking de busca.

## 2. Questões de Servidor e Hospedagem

Se houver ataques regulares, o site terá problemas com o seu provedor de hospedagem.

## 3. Vulnerabilidade do Site

O site fica mais vulnerável ao hacking, pois todos os seus sistemas estão focados em colocar o site de volta online.

## 4. Tempo e Dinheiro Perdidos

Reparar um site leva um bom tempo. Tem um alto custo para reparar e em alguns casos você pode deixar de faturar com suas vendas.





# Estratégias de Mitigação e Prevenção

---

Davi Souza

---

# **Algumas maneiras De se proteger Contra ataques DDoS básicos:**

- Monitoramento de Tráfego
- Firewalls e Filtros de pacotes
- Proteção de DNS
- Colaboração com Provedores de Serviços de Internet (ISPs)

---

# Os Serviços de Proteção contra ataques DDoS mais utilizados do mundo:

1. Akamai
2. CloudFlare
3. GCore

Top 3 podendo variar de acordo com as preferências do contratante, porem, independente do escolhido, os 3 oferecem proteção utilizando o sistema de nuvem e muitas outras formas de mitigação.



---

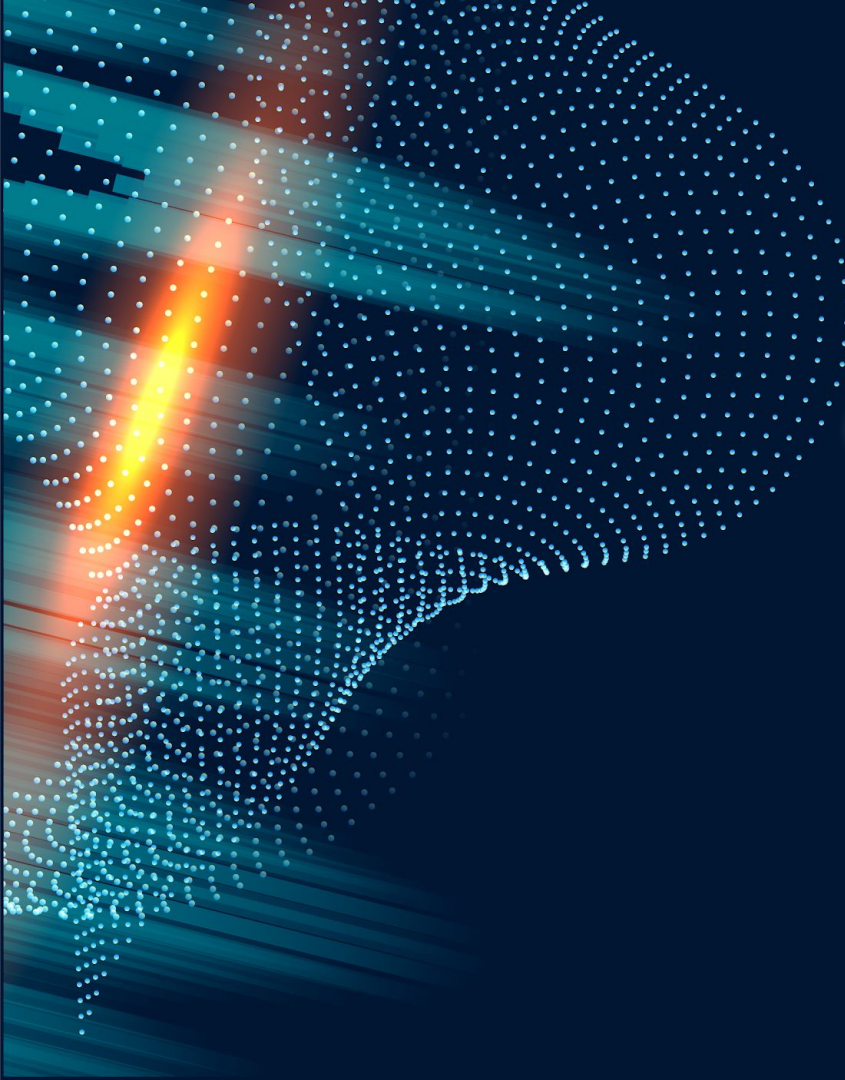
# Como funciona o serviço de proteção contra DDoS por nuvem?

Os serviços de proteção contra ataques DDoS baseados em nuvem são uma abordagem comum e eficaz para mitigar esses tipos de ataques. Funcionam com:

- **Redirecionamento de Tráfego**
- **Mitigação Ativa**
- **Relatórios e Análises**
- **Escalabilidade e Redundância**
- **Filtragem e Análise de Tráfego**







# **Desafios Futuros e Tendências em Ataques DDoS**

---

Robert Ruan

# Desafios futuros:

- **Diminuir a Vulnerabilidade da Internet das Coisas (IoT)**

Com mais dispositivos conectados à IoT, maior é a vulnerabilidade a invasões digitais

- **Otimizar o Armazenamento na Nuvem**

A adoção radical da nuvem, aumenta as chances de vazamento de dados e informações sensíveis.

- **Combater as ameaças em nível C (alto perfil)**

Ataques de alto perfil a empresas executivas

- **Implementar Defesa Multicamadas**

Otimização de soluções híbridas, que combatem os ataques

---

# Principais Tendencias

- **Colaboração e compartilhamento de ameaças**

Compartilhamento sobre ameaças cibernéticas entre organizações, resultando em respostas efetivas

- **Maior utilização de IA (Inteligência Artificial)**

Uso de IA para aprimorar a identificação de ameaças em tempo real

- **Abordagens Zero Trust**

Pressupõe que ninguém possa automaticamente ser considerado confiável

- **Aumento do investimento em Cybersegurança**

Garantir que os profissionais estejam atualizados, ciente dos riscos e mantendo a organização protegida



# Fim!

---

Obrigado!

