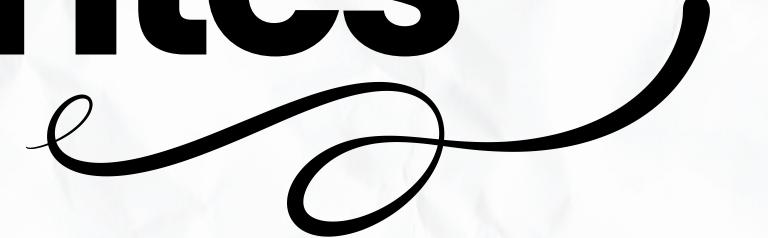


*Segurança em  
ambientes de nuvem:*

# **OCASO DO ATAQUE DDOS À AMAZON WEB SERVICES**

# Integrantes



Francisco Freitas Rodrigues

Ciência da computação  
2º semestre



Leandro de Souza da Rosa

Ciência da computação  
1º semestre



Gustavo Bergmann Reckziegel

Análise e desenvolvimento de sistemas  
1º semestre



Philippe da Rosa Lopes

Ciência da computação  
2º semestre

# Tópicos de Abordagem

**01** Introdução

**02** Ataques DDoS

**03** O caso do ataque  
à AWS

**04** Estratégias de mitigação

**05** Conclusão

**06** Pesquisas

# \* Introdução \*

- O que são ataques DDoS:
  - Negação de serviço distribuído
  - Sobrecarga de tráfego malicioso
- Impactos gerais:
  - Prejuízos financeiros e operacionais
- Objetivo do trabalho:
  - Analisar o ataque DDoS à AWS em 2020

# Ataques DDoS



## *Definição:*

- Interrupção de serviços com tráfego excessivo.

## *Métodos de ataque:*

- Amplificação (ex.: CLDAP)

## *Efeitos:*

- Danos à reputação
- Perda de disponibilidade

## *Prevenção geral:*

- Ferramentas de monitoramento e firewalls robustos.

# O caso AWS



## Descrição:

- Fevereiro de 2020, 2,3 Tbps de tráfego
- Técnica: CLDAP Reflection
- Três dias de "status de ameaça elevada"



## Impactos:

- Sem grandes interrupções
- Serviços mantiveram disponibilidade

# Dados Violados

- *Este caso específico:*
  - Não houve violação de dados.
  - Alvo: Disponibilidade dos serviços.



# Identificação e Resolução

- Monitoramento (NetFlow, logs de serviço).
- AWS Shield e sistemas de inspeção.

- Scrubbing systems (remoção de tráfego malicioso).
- Proteção em tempo real com AWS Shield.

# Como poderia ser evitado?

Arquitetura de rede resiliente

Monitoramento contínuo.

Educação sobre segurança e redundância

Rate limiting e firewalls configurados.



# Princípios de Segurança

## Disponibilidade:

- Alvo principal do ataque

## Integridade:

- Garantia contra modificações

## Confidencialidade:

- Proteção dos dados

## Autenticidade:

- Ações rápidas garantiram legitimidade dos serviços

## Não-repúdio:

- AWS forneceu evidências de medidas adequadas

## Serviços de Segurança Nativos na AWS

Gestão de Identidades e Acessos	Controles de Detecção	Segurança em Infraestrutura	Proteção de Dados	Resposta a Incidentes
AWS Identity & Access Management (IAM) AWS Organizations AWS Control Tower AWS Cognito AWS Directory Service AWS Single Sign-On AWS Secrets Manager IAM Access Analyzer	AWS CloudTrail AWS Security Hub AWS Config Amazon CloudWatch Amazon GuardDuty VPC Flow Logs Traffic Mirroring Trusted Advisor	AWS Systems Manager AWS Shield (Standard) AWS Web Application Firewall (WAF) AWS Firewall Manager Amazon Inspector Amazon Virtual Private Cloud (VPC) EC2 Image Builder Amazon Fraud Detector	AWS Key Management Service (KMS) AWS CloudHSM Amazon Macie AWS Certificate Manager Server Side Encryption S3 Block Public Access	AWS Config Rules AWS Lambda Amazon Detective Step Functions CloudEndure DR AWS SSM Automations

© 2021, Amazon Web Services, Inc. or its Affiliates.

Mais de 1000 soluções e imagens no AWS Marketplace. Com preço sob demanda, SaaS ou BYOL



# Conclusão

## *Licções aprendidas:*

- Preparação e mitigação robusta são essenciais.
- Ferramentas como AWS Shield são críticas.

## *Importância:*

- Adotar boas práticas de segurança cibernética.
- Planejar resposta a incidentes para minimizar impactos.

# Referências



## **BBC NEWS. (2020). AMAZON 'THWARTS LARGEST EVER DDOS CYBER-ATTACK'.**

Disponível em: <https://www.bbc.com/news/technology-53093611>. Acesso em: 06 dez. 2024.

## **ATAQUE DDOS À AMAZON WEB SERVICE. AMAZON SAYS IT MITIGATED THE LARGEST DDOS ATTACK EVER RECORDED.**

Disponível em: <https://www.youtube.com/watch?v=qxH4FyBqHjw>. Acesso em: 18 nov. 2024.

## **AMAZON WEB SERVICES (AWS). MANAGED DDOS PROTECTION – AWS SHIELD.**

Disponível em: <https://aws.amazon.com/shield/ddos-attack-protection/>.  
Acesso em: 06 dez. 2024.

## **AMAZON WEB SERVICES (AWS). DDOS PROTECTION OVERVIEW.**

Disponível em: <https://aws.amazon.com/developer/application-security-performance/articles/ddos-protection/>. Acesso em: 06 dez. 2024.