Ataques **DDoS** como ação anticompetitiva: prevenção, mitigação e reação

por T. Ayub

Quem é o **Ayub** e por que ele fala disso?

- Apaixonado pela internet desde **1995**.
- Services Admin e Ouvidor de irc.**BRASnet**.org.
- Gerente de **TI**.
- Diretor de **Redes**.
- **Chief** Technology Officer
- **Professor**, autor e **pesquisador** na área de Tecnologia da Informação e Comunicação.

@ayubio

@ayubio

YouTube: https://www.youtube.com/c/**ayubio**

Blog: https://medium.com/@**ayubio**

Twitter: https://twitter.com/**ayubio**

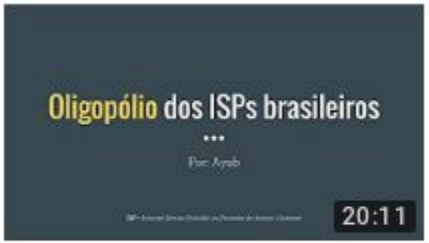
LinkedIn: https://www.linkedin.com/in/**ayubio**

E-mail: contato@ayub.net.br

https://www.youtube.com/c/**ayubio**

Franquia de tráfego na banda larga: faz sentido?...

15 mil visualizações •



Oligopólio dos provedores de internet brasileiros

12 mil visualizações •

SLA - tem certeza que você sabe o que significa?

17 mil visualizações •

8.8.8.8: vale a pena usar este número mágico no DNS?

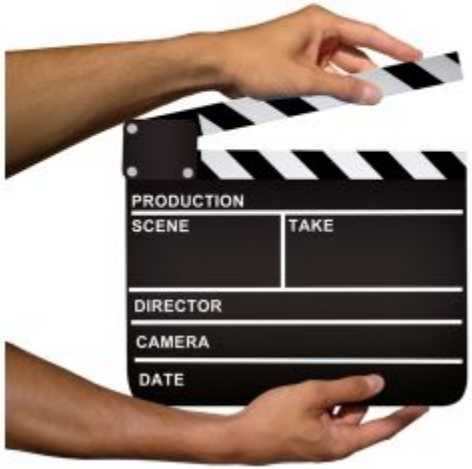
200 mil visualizações •

Ao vivo: um bate papo sobre neutralidade da rede

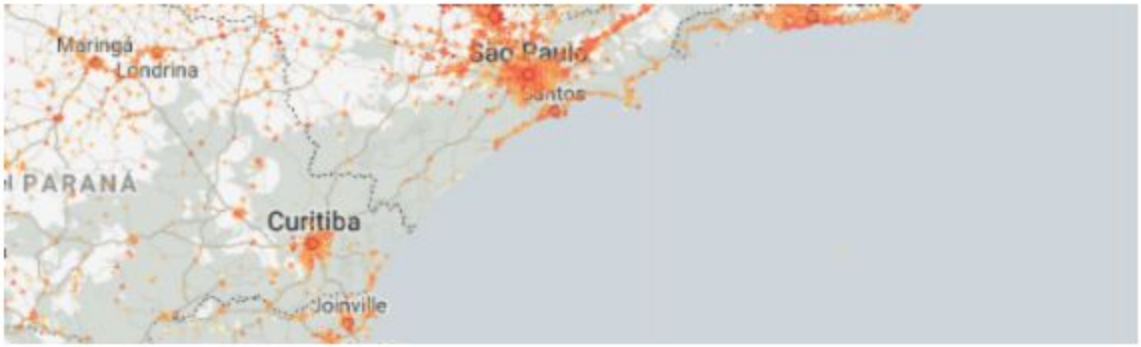
1,5 mil visualizações •

https://medium.com/@**ayubio**

Da claquete ao modem: como seria um futuro sem a neutralidade da rede?



https://medium.com/@**ayubio**



É possível um banco de dados nacional de cobertura de internet e telecomunicações?

O que são ataques **DDoS**?

Exaurir a
capacidade computacional
do alvo

Exaurir a
largura de banda
de internet
do alvo

Deixar o alvo **offline** ou com **performance degradada** severamente

Antes

Vandalismo

Games

Ciberativismo

Antes

Vandalismo

Games

Ciberativismo

Agora

Vandalismo

Games

Ciberativismo

Anticompetição

Empresas passaram realizar ataques **DDoS** contra concorrentes para causar **prejuízo financeiro**.

E por que esse **aumento**?

Diferentemente de antes, nos últimos 3 anos assistimos a **democratização** das ferramentas de ataque DDoS.

O eufemismo do *stress test*.

Best Plans for all your ip stresser needs

Sign up to get a full list of all available ddos packages along with concurrents and time limit!

1 Month Silver

$15.00

1 Concurrent
300 seconds boot time
250Gbps total booter network capacity
24/7 Dedicated Support
Access to DDOS tools

Sign Up

1 Month Gold

$20.00

1 Concurrent
1200 seconds boot time
250Gbps total booter network capacity
24/7 Dedicated Support
Access to DDOS tools

Sign Up

1 Month Ultimate

$55.00

1 Concurrent
3600 seconds boot time
250Gbps total booter network capacity
24/7 Dedicated Support
Access to DDOS tools

Sign Up

O ataque sob **encomenda.**

O ataque sob encomenda

- **Criminosos** ofertam o serviço de ataques DDoS contra concorrentes em **planos de duração** diária, semanal ou mensal.
- As ofertas são realizadas em grupos de **WhatsApp** ou **Telegram** de profissionais e empreendedores dos ramos de ISP, datacenter e áreas correlatas.

O ataque sob encomenda

- O ataque é especializado e **desenhado** para causar o maior prejuízo na empresa alvo através de uma escolha criteriosa:
  - **Dos horários dos ataques:**
  - **Dos IPs aos quais o ataque se destina:**
  - **O vetor de ataque:**

O ataque sob encomenda

- O ataque é especializado e **desenhado** para causar o maior prejuízo na empresa alvo através de uma escolha criteriosa:
  - **Dos horários dos ataques:** para causar o maior impacto na equipe ou no cliente.
  - **Dos IPs aos quais o ataque se destina**: derrubar os alvos mais frágeis ou mais importantes.
  - **O vetor de ataque**: para que se confunda ao máximo com tráfego legítimo.

O que torna um ataque DDoS **anticompetitivo**?

O que torna um DDoS anti-competitivo?

- Um ataque DDoS em si não costuma guardar **evidência forense** de sua autoria.
- A autoria pode ser **inferida** pelo *modus operandi* e as circunstâncias do ataque.
- Justamente estas **circunstâncias** caracterizam um ataque como anticompetitivo.

O que torna um DDoS anti-competitivo?

- Alguns exemplos:
  - 3 ISPs coexistem numa **região**, com a chegada do quarto os 3 iniciais passam a receber DDoS.
  - Ataque com **hora marcada**: ISP ganha RFP para link dedicado em feira agropecuária e recebe DDoS do início da feira até seu término.
  - Data center ganha **licitação pública** e é atacado no dia da homologação do serviço.

O que torna um DDoS anti-competitivo?

- Alguns exemplos:
  - A cada exibição/execução de **propaganda** na rádio e TV o anunciante recebe ataque DDoS.
  - Ataques durante **sorteio** de prêmios e brindes.
  - Todo **novo cliente** de um ISP ou datacenter é atacado assim que ativado o serviço.

O que torna um DDoS anti-competitivo?

- Alguns exemplos:
  - Os IPs públicos de um ISP alvo são **monitorados em tempo real** para que qualquer mudança nos IPs para evadir do ataque seja rapidamente detectada.
  - Um ISP alvo de DDoS contrata o serviço de ataque contra um concorrente do qual presume ser o mandante do ataque e uma **epidemia** de DDoS se inicia na região.

Como **prevenir** um ataque DDoS anticompetitivo?

Como prevenir?

- “Mantenha os amigos sempre **perto** de você e os inimigos mais **perto** ainda.”
- Conheça seus concorrentes, **visite-os.**
- Encontre pautas de **interesse comum** e os apoie nela.
- Participe de **associações** de setor, sindicatos patronais e similares.
- Mitigue imediatamente qualquer possível **desentendimento.**

Como mitigar?

- Se sua rede não tem **largura de banda maior que o ataque**, nada que você instale em sua infraestrutura irá protegê-lo do ataque.
- Mitigação de DDoS é um **serviço**, não é um produto.
- Para ISPs, o recomendável é adquirir o serviço de **trânsito IP** já com a mitigação de DDoS.
- Para sites, *web apps* e provedores de conteúdo, **CDNs** podem ser uma solução assim como o trânsito IP mitigado.

Como mitigar?

- Verifique se seu fornecedor de trânsito IP suporta o mecanismo de ***black hole*** e teste-o. Se não funcionar, exija o reparo do defeito. Se ele não suportar, troque de fornecedor.
- Atentem que ***black hole*** **não é mitigação**. Ataques populares se esquivam dele atacando simultaneamente todos os IPs de um sistema autônomo.

Como mitigar?

- Não seja pego de surpresa:
  - Contrate a proteção **antes do primeiro ataque**. Prevenir é mais barato e eficiente que remediar.
  - Crie e documente um **plano de ação** diante de um ataque DDoS.
  - Contrate os serviços de IP Stresser e **se ataque** para validar o treinamento de sua equipe e eficácia das soluções contratadas.

Como **reagir a** um ataque DDoS anti-competitivo?

Como reagir?

- DDoS é crime. Procure um advogado e faça uma **notícia-crime**.
  - Lei Nº 12.737/2012 (Lei Carolina Dieckman):
  - Art. 3º: “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública” - “Pena - **detenção, de um a três anos, e multa.**”

Como reagir?

- Prepare sua rede para fazer captura de pacotes dos ataques (.pcap), crie um mecanismo para coletá-los durante um ataque e nos ataques de amplificação, notifique todos os contatos de ***abuse*** de todos os IPs envolvidos. Mobilize a comunidade pela resolução de todas as vulnerabilidades exploradas.
- Pare de sofrer DDoS calado. Reaja!

Obrigado!

YouTube: https://www.youtube.com/c/**ayubio**

Blog: https://medium.com/@**ayubio**

Twitter: https://twitter.com/**ayubio**

LinkedIn: https://www.linkedin.com/in/**ayubio**

E-mail: contato@ayub.net.br