WTR

WORKSHOP
DE TECNOLOGIA DE REDES DO POP-RS

> 2021

DDoS, Roteamento, anycast e DNS

Leandro Bertholdo

22 SET

Click to add text

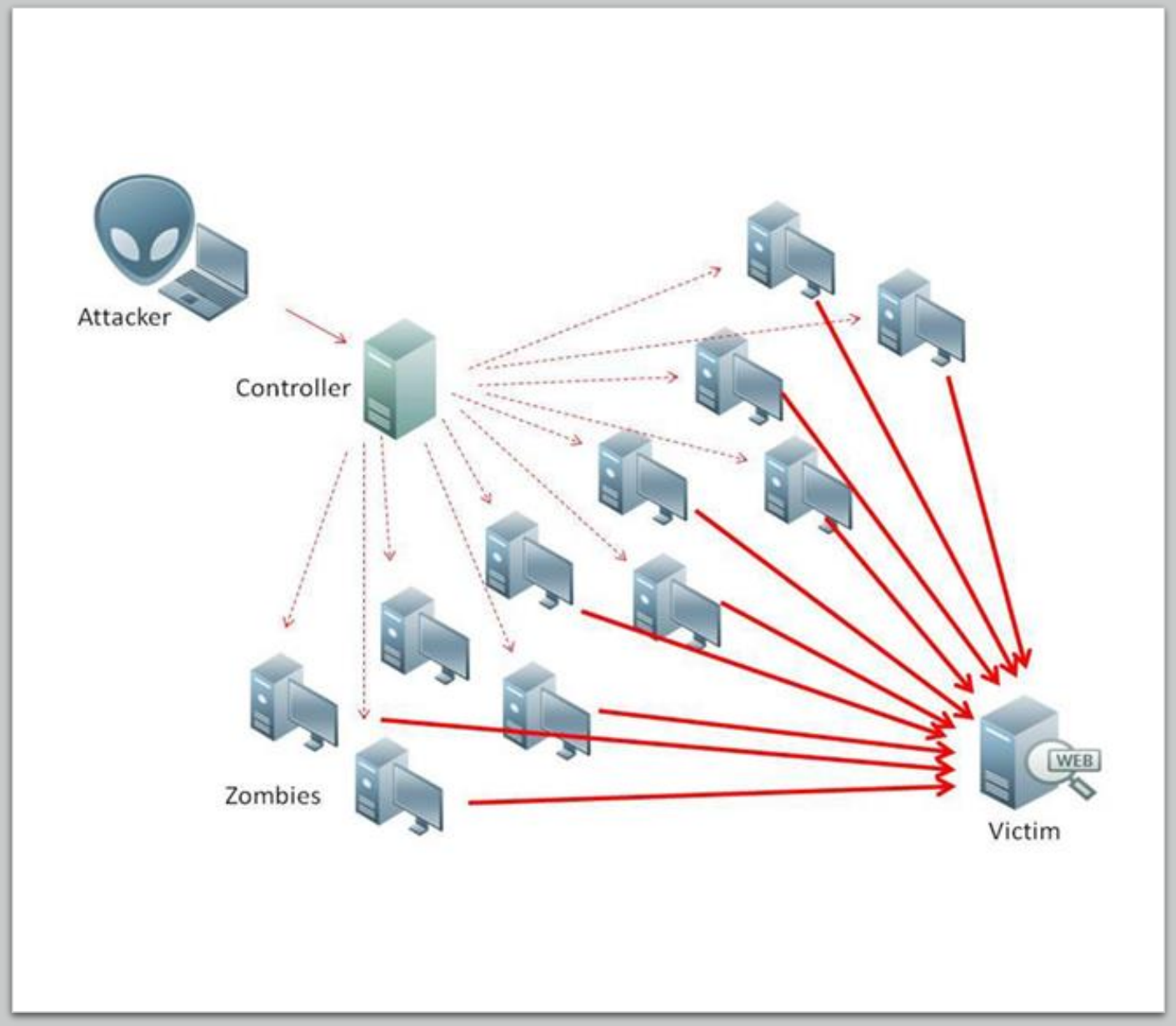
DDoS, Roteamento, anycast e DNS: Que tipo de mudanças a busca por segurança esta provocando na Internet?

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

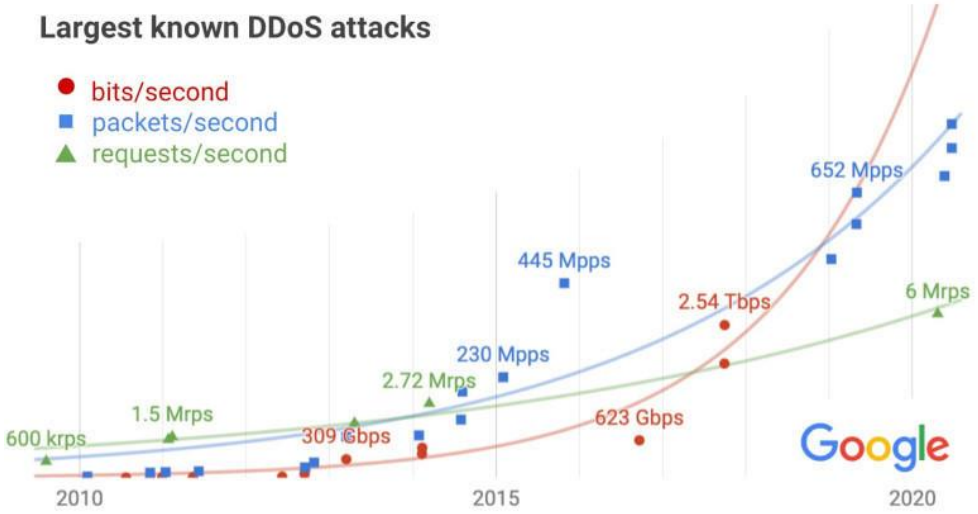
Sumário

- Os desafios de segurança de redes tem impulsionado várias mudanças na Internet que conhecemos.
  - No roteamento (RPKI)
  - No DNS (DNSSEC)
  - Na busca por serviços de segurança
- Um do maiores problemas
  - DDoS – Distributed Denial of Service Attacks



Tipos de DDoS

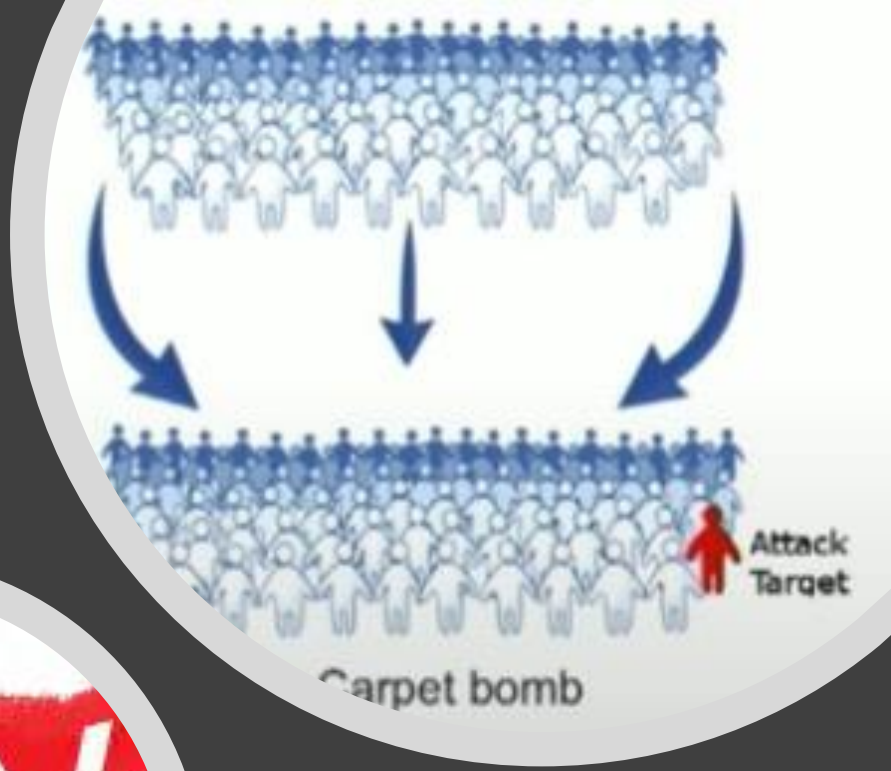
- DDoS Volumétrico (mais comum)
  - Ja registrados ataques acima de 1Tbps
    - 2,57 Tbps contra Google em 2017
    - 2,3 Tbps contra Amazon em 2020
    - Consume banda e capacidade de roteamento
- DDoS contra protocolos
  - Funciona exaurindo recursos
    - tabela de rotas e conexões
    - Alvo sao servidores, roteadores e firewalls
- DDoS contra Aplicações
  - Consume os recursos de um serviço
    - HTTP/HTTPS, DNS, etc.



https://www.zdnet.com/article/google-says-it-mitigated-a-2-54-tbps-ddos-attack-in-2017-largest-known-to-date/

Tipos de DDoS

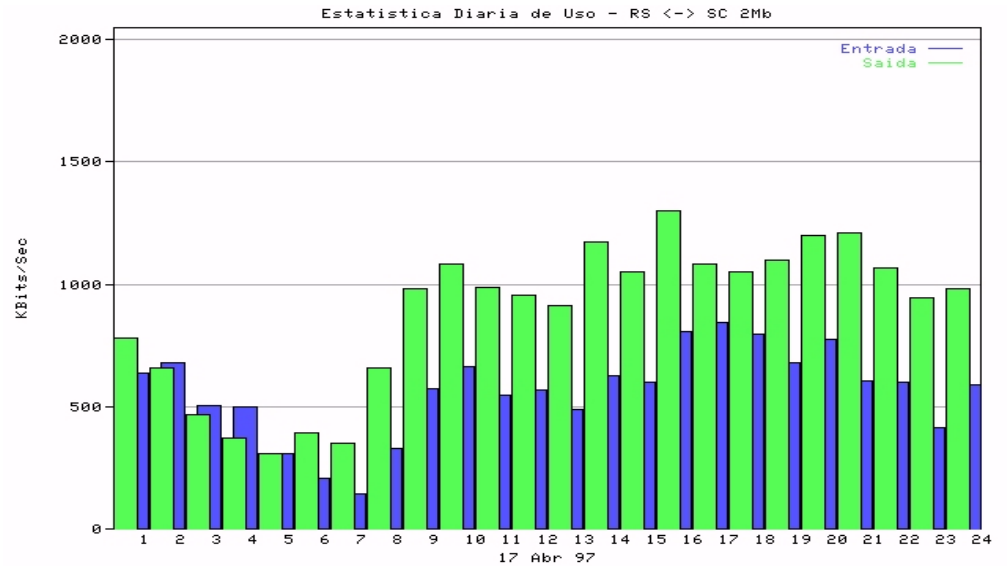
- DDos contra espaço de endereçamento (Carpet bombing)
  - DDoS volumétrico destinado a cada um dos IPs da empresa – não somente contra um servidor ou serviço



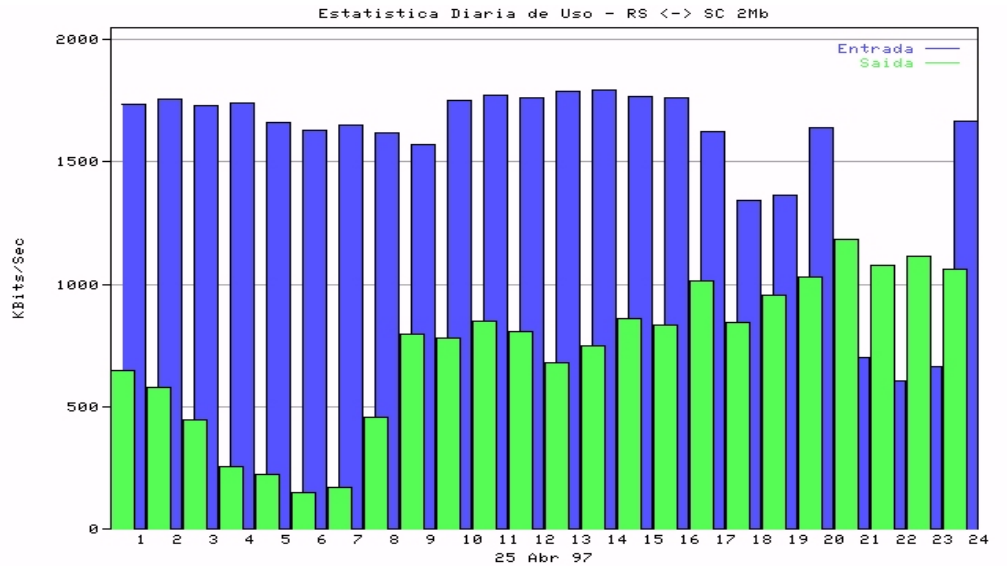
E o que mudou nos últimos anos?

O passado:
Primeiro DoS registrado no PoP-RS (1997)

Tráfego Normal (2Mbps)

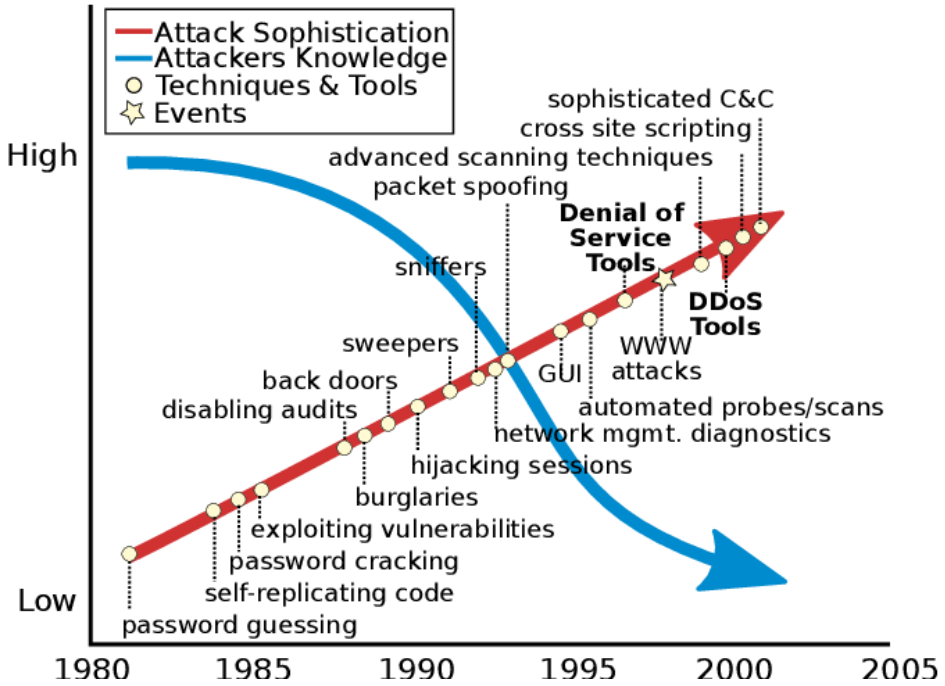


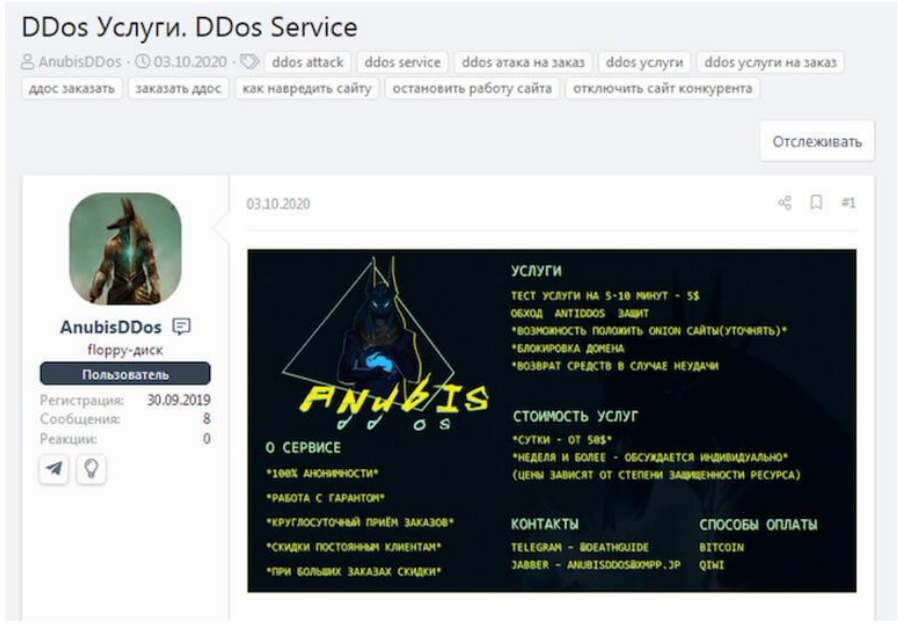
Tráfego durante o ataque (ICMP flooding)

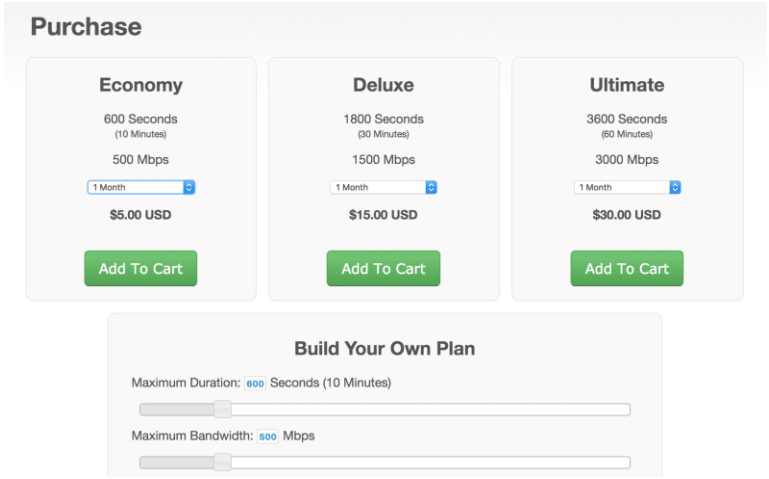


Ataques dependiam do conhecimento de detalhes de protocolos e implementações de sistemas operacionais

O presente: DDoS-as-a-service



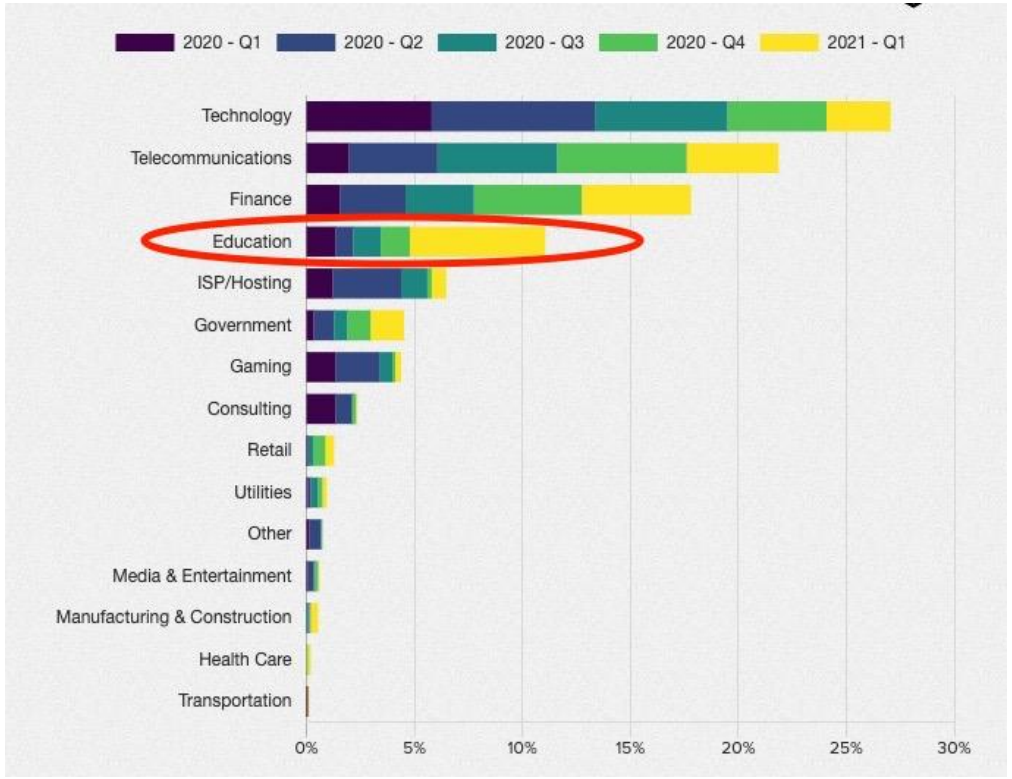




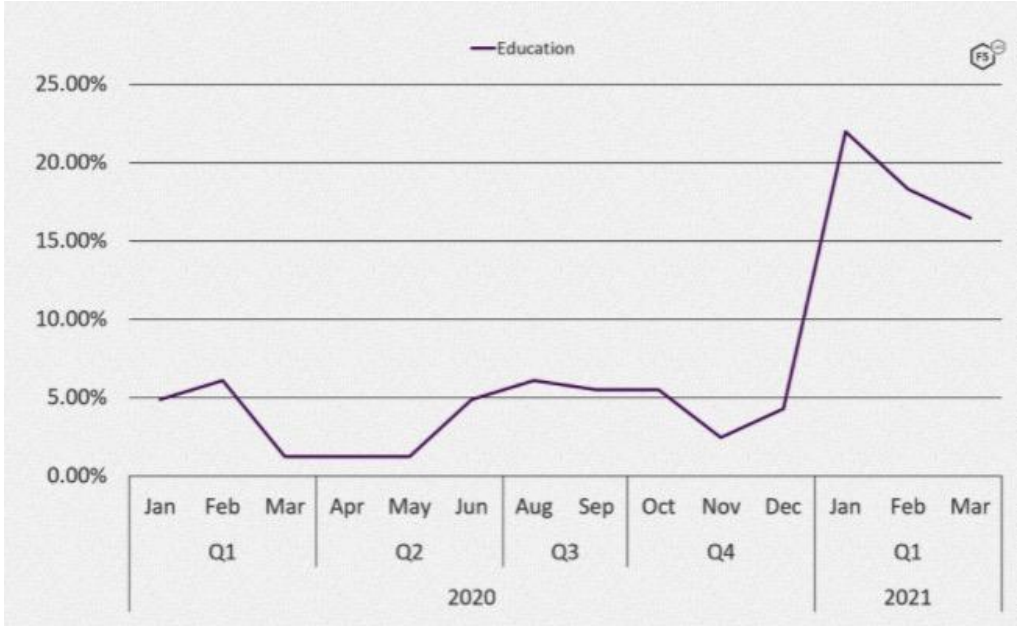
O conhecimento técnico não é mais necessário

Alvos dos ataques

Ataques por setor



Aumento no setor de educação em 2021



Fonte: https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020

Frequencia dos ataques (2020-2021)

- 90% dos ataques duram **menos** de 1 hora

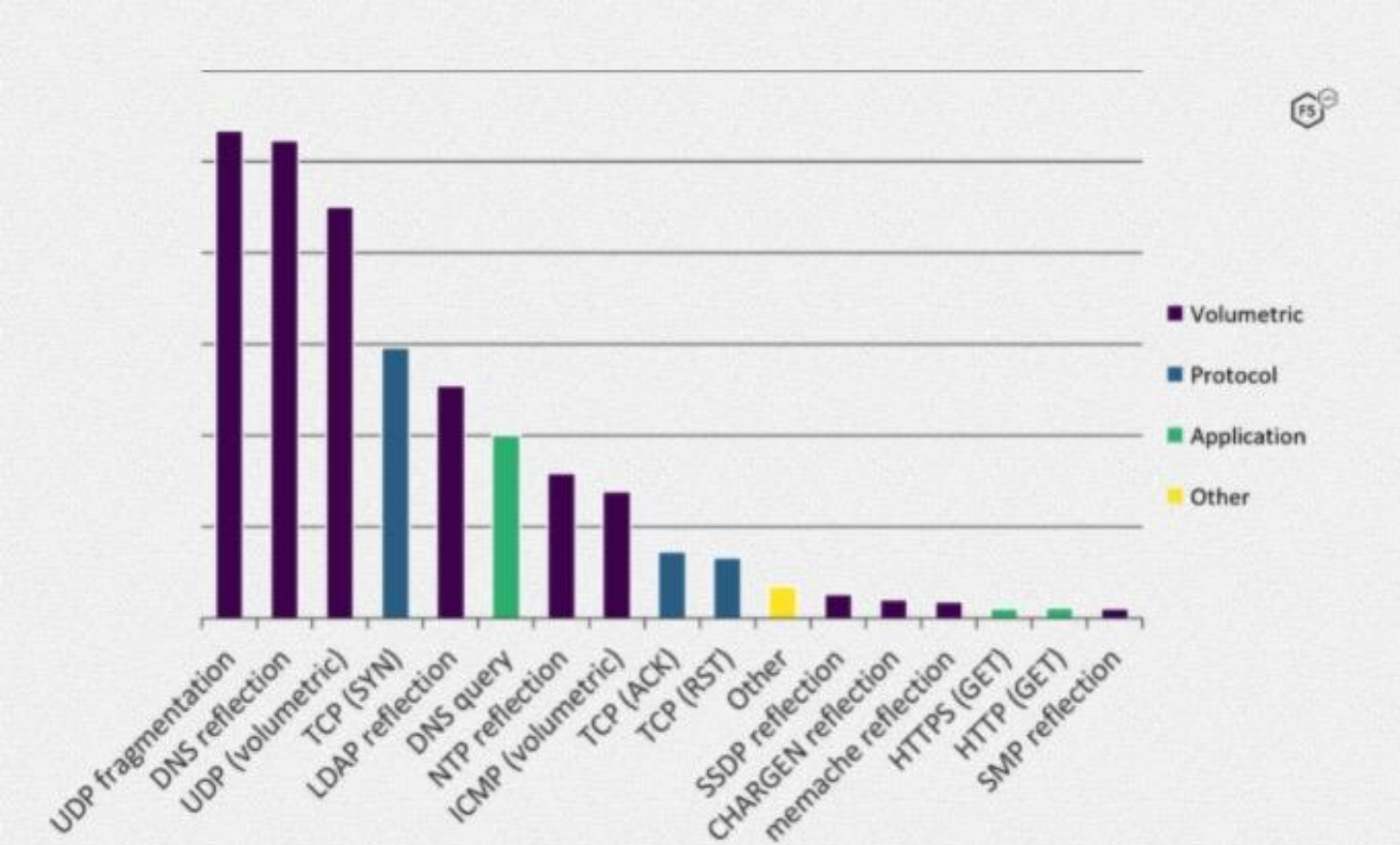


Figure 3. Frequency of different DDoS attack tactics, January 2020 through March 2021.

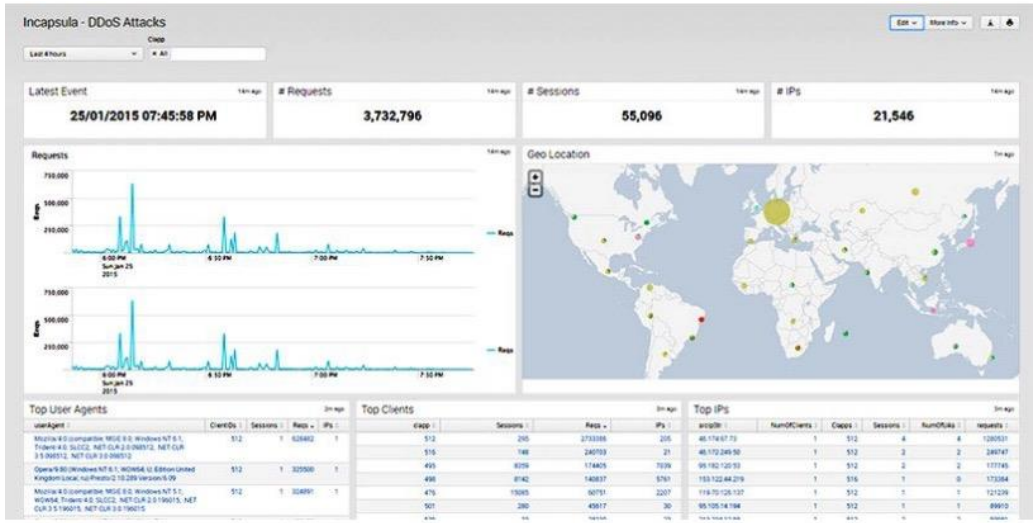
Fonte: https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020

Soluções para DDoS

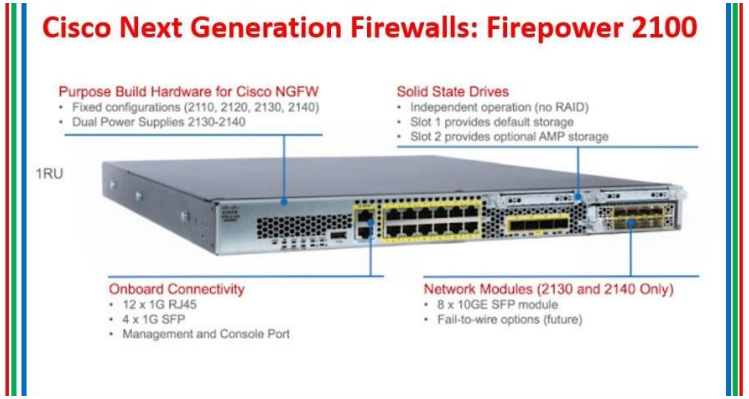
- **Mais banda passante**
  - Super-dimensionar enlaces
  - Prover capacidade excedente em routers e firewalls
- **Mais capacidade**
  - Multiplos datacenters geodistribuidos
  - Balanceamento e anycast
  - Elastic Compute Cloud
- **Configurar medidas anti-DDoS no hardware atual**
  - Taxa de pacotes/conexões por origem
  - Filtros (proativos) usados em ataque de amplificacao
    - ex: memcached (udp/11211), BCP38/84 (ingress filtering)

Soluções para DDoS

- Implementar **hardware e software anti-DDoS**
  - WAF – Web Application Firewall
  - NGFW - Next Generation Firewall
    - Geolocation filtering
    - Blacklists signature
  - SIEM - Security information and event management tools
    - ex: splunk
  - Analise de Flows!!! 



Imperva integrated with Splunk.

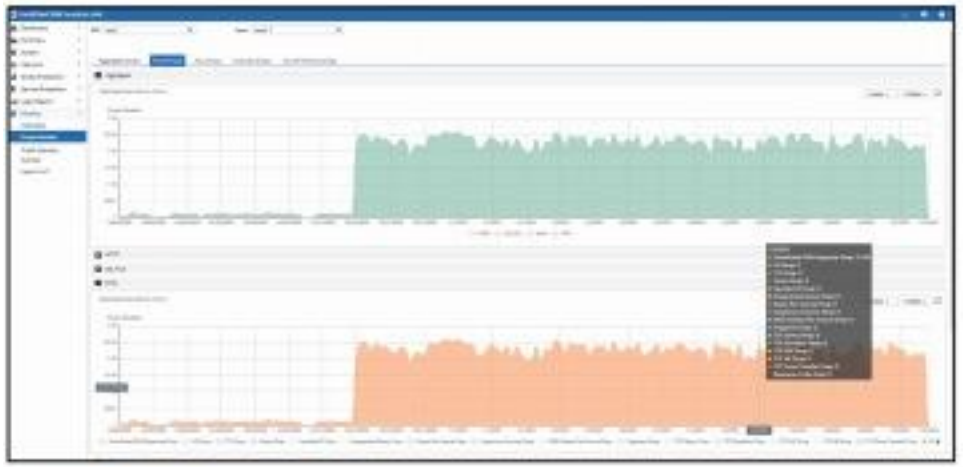


Soluções para DDoS

- Implementar um appliance anti-DDoS
  - DNS mitigation
  - Ex: Arbor Peakflow, FortiDDoS,..

FortiDDoS 200F, 400B, 1200B, 1500E, 1500F, 2000E and VM04/08/16

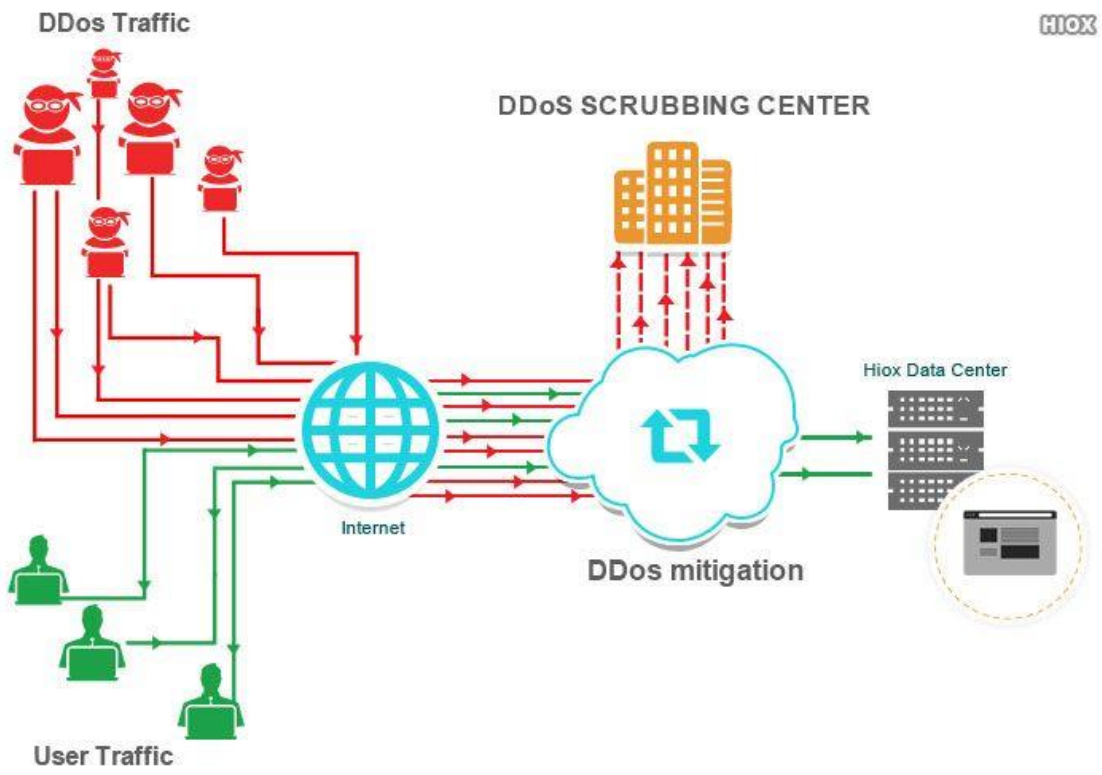
- **Proteger servidores DNS** IMPORTANT
  - Diferentes datacenters
  - Diferente espaço de endereçamento
  - Solução anycast



DNS Attacks (F)

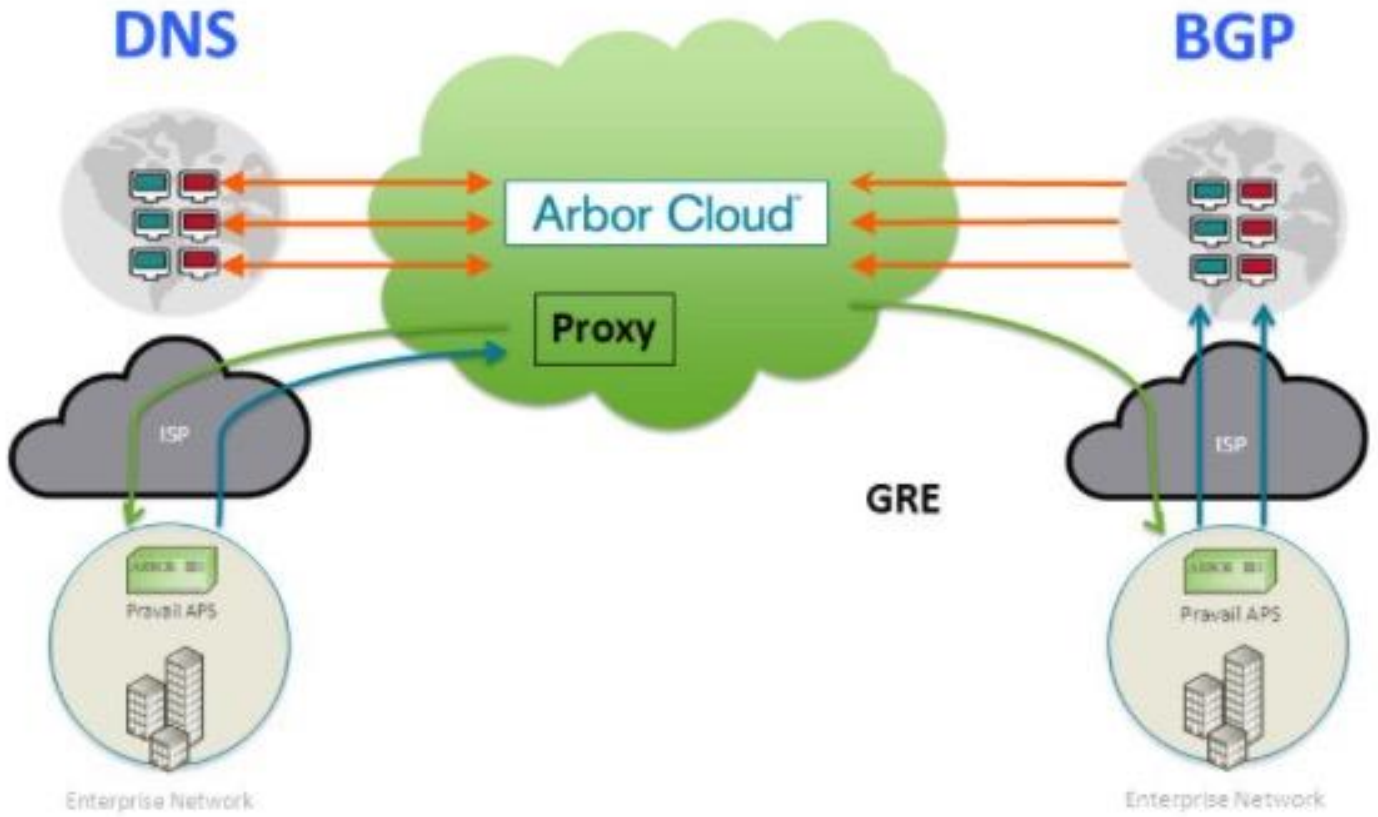
Soluções para DDoS

- Contratar proteção anti-DDoS:
  - Cloudflare
  - Radware
  - Akamai
  - Arbor Cloud / Netscout
  - Imperva
  - Neustart
  - Azure, Link11, …
  - F5, Oracle, Verizon, …



https://www.youtube.com/watch?v=z7ltWcN3mqk&t=130s

Como funciona um serviço anti-DDoS genérico?

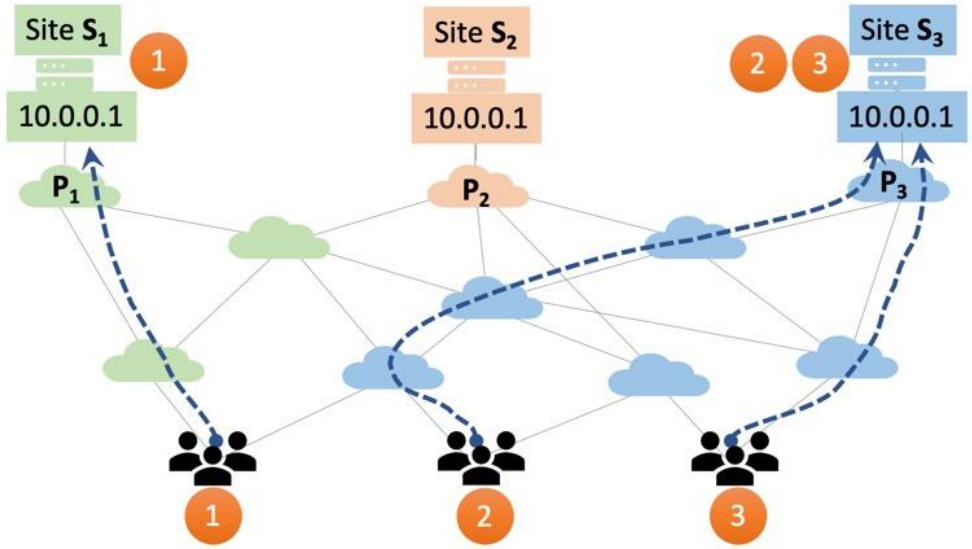


Que técnicas são utilizadas pelos serviços anti-DDoS

- **DNS**
  - Utilizado para redirecionar um site para um **proxy-cache**
  - Proxy-cache utiliza '**capchas**' para reconhecer uma conexão legitima
  - Permite melhor balaceamento
  - Servidor **DNS** prove uma resposta diferente baseado na **geolocalização** da origem
- **Roteamento BGP**
  - Redireciona o trafego da rede sob ataque para um "**scrubbing center**"
  - Retorna o trafego 'limpo' para o cliente
  - Utiliza **anuncios BGP** mais especificos para levar o trafego ate o scrubbing center

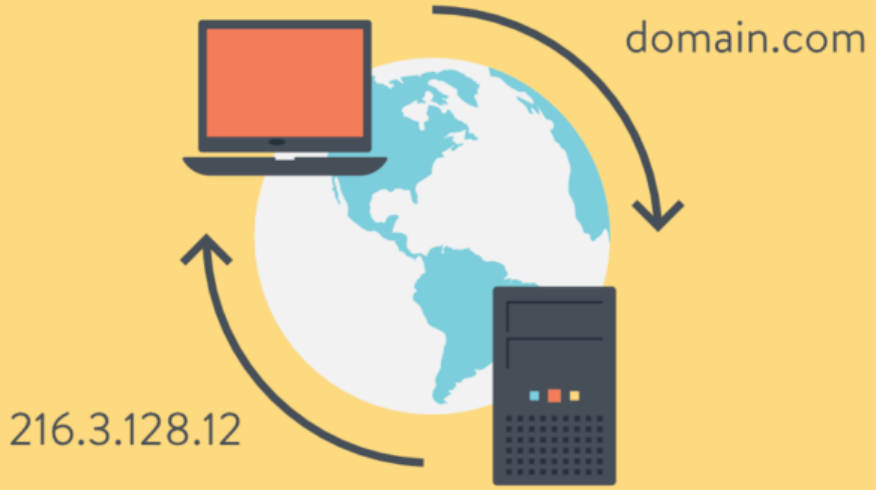
Que técnicas são utilizadas pelos serviços anti-DDoS e servidores de DNS

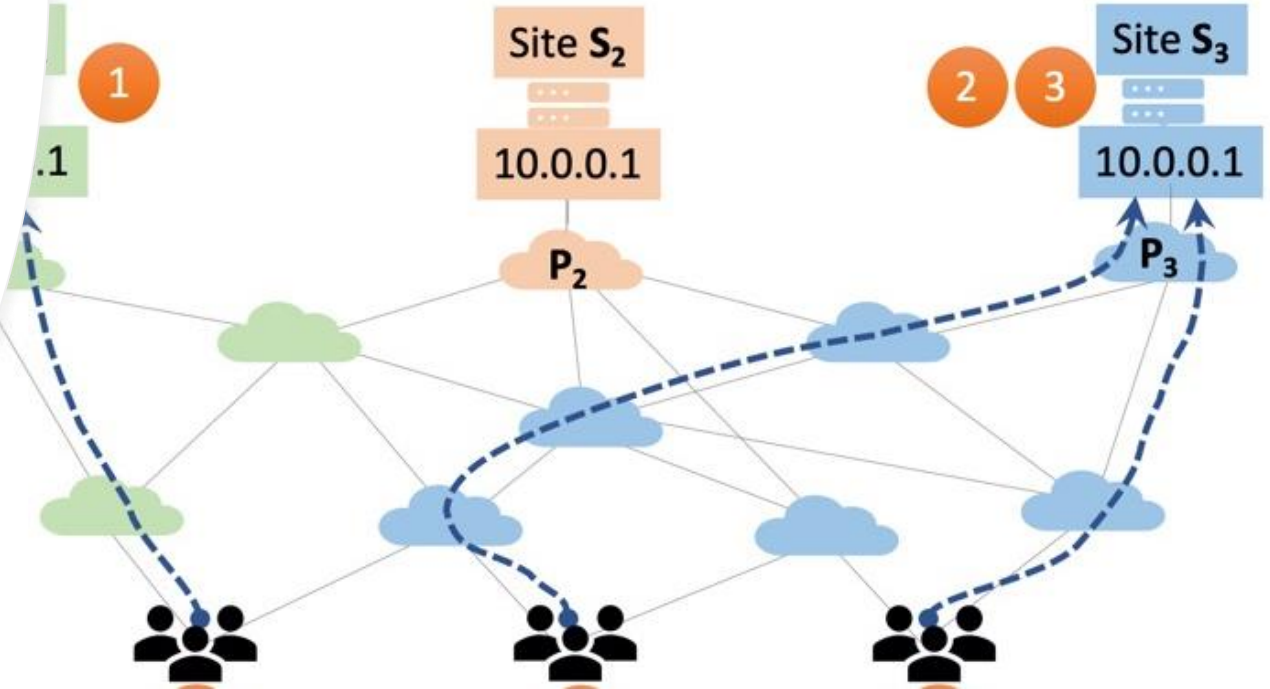
- **Anycast**
  - Utilizado pelos scrubbing centers e servidores de DNS
  - Mesmo IP em vários locais da internet



Que técnicas são utilizadas pelos serviços anti-DDoS e servidores de DNS

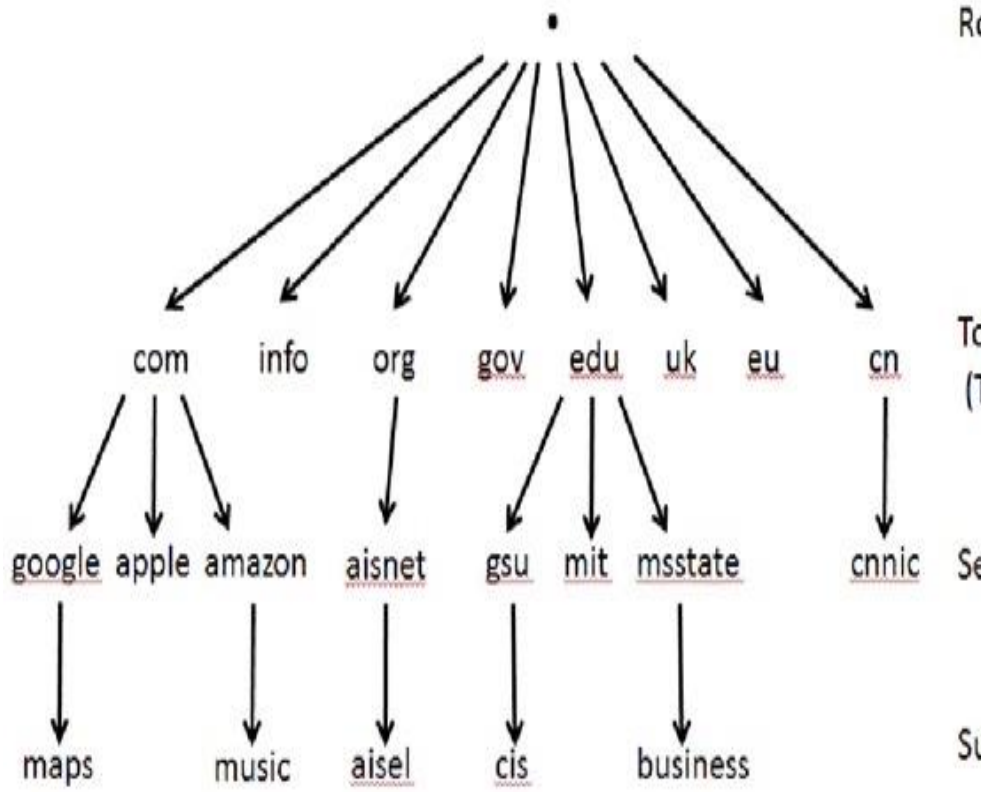
- **Anycast**
  - Utilizado pelos scrubbing centers e servidores de DNS
  - Mesmo IP em vários locais da internet



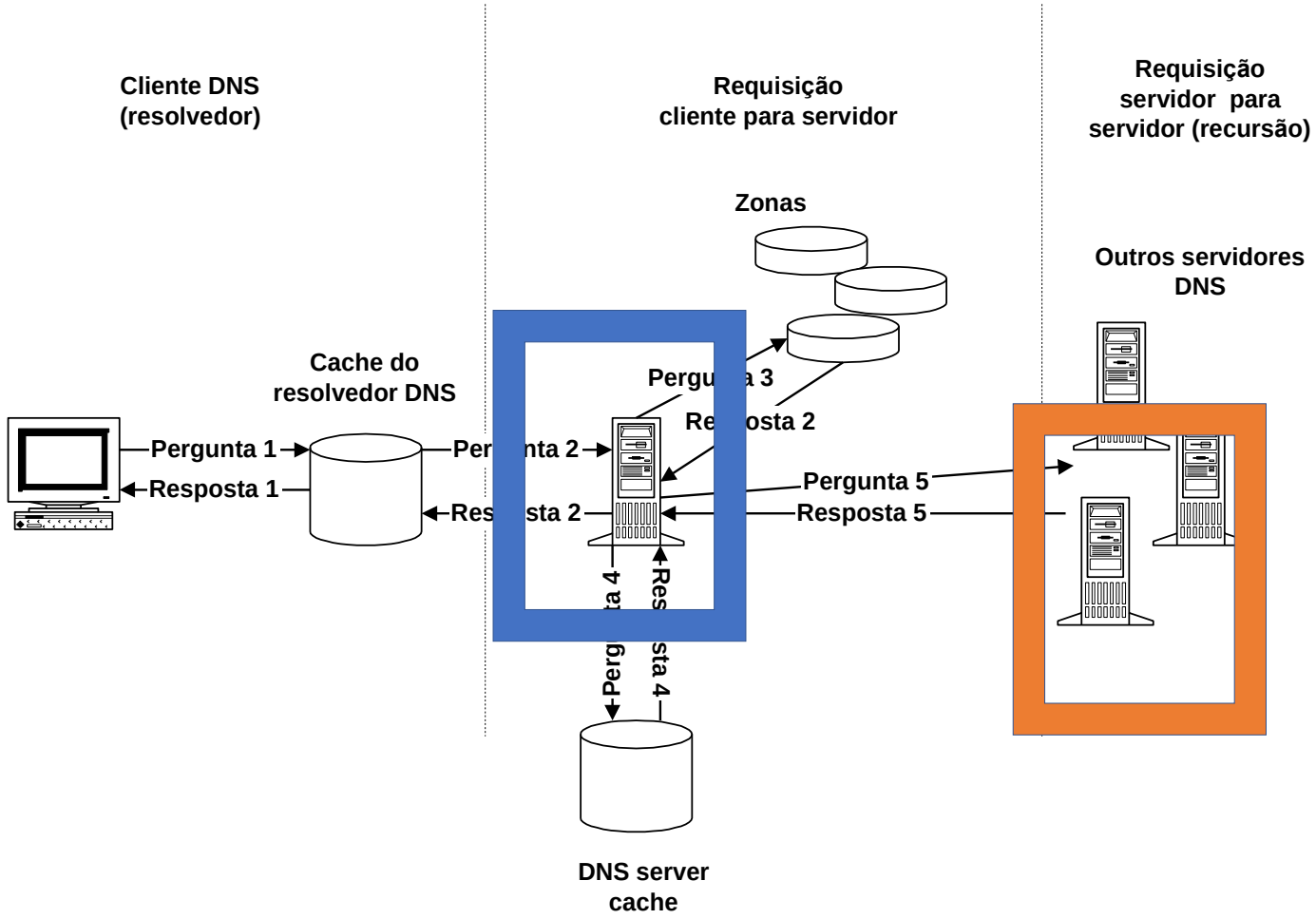


O Sistema de nomes da Internet

A hierarquia de nomes de dominios



A peças importantes da resolução de nomes



O que preocupa quanto a roteamento e DNS

Para pensar - DNS

- **Resolvers estao ficando concentrados**!
  - Usuarios geralmente sao orientados a usar 1.1.1.1 ou 8.8.8.8
  - Muitas empresas simplesmente encaminham a resolução para “open servers”

- **Servidores DNS primarios e secundarios estao ficando concentrados**!
  - 15% de todos os domínios .COM e .NL registram ambos os servidores DNS sobre o mesmo prefixo IPv4.
  - Incidente com DynDNS em 2016 (DDoS) afetou AirBnB, Amazon, Fox News, Xbox, governo da Suécia, BBC, CNN e muitos outros.
    - https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
  - Quantos usam redes diferentes mas estão no mesmo local físico?

Para pensar - DNS

- **Novo procolo DNS over HTTPS** concentrando no Google a resolução de nomes de todos os usuários de navegadores Chrome e Firefox.
- Porque devemos nos preocupar?
  - Google pode decidir não resolver o nome – poder de **censura**
  - Google pode mapear para outro nome – poder de **distorcer noticias**
  - Google ocultar informações de localização de DNS para concorrentes
    - Os servicos de CDN usam as informacoes do DNS para geolocalizar seus usuarios.
    - Concorrente sempre serao mais ineficazes para entregar conteudo.
    - Impede a concorrencia de melhorar os servicos
    - Resultado: **monopolio privado**.
  - A Internet depende de uma empresa!

Para pensar - Roteamento

- Provedores não tem **infraestrutura para suportar outage** de um IXP ou de um datacenter
  - Falha no AMS-IX em 2015 afetou o DE-CIX negativamente.
  - Falha do DE-CIX 2018: blackout na Internet na Alemanha.
  - Falha no IX.br/SPO 2018: vários usuários e sites com problema de acesso
  - Falha no DC-Commcorp Porto Alegre

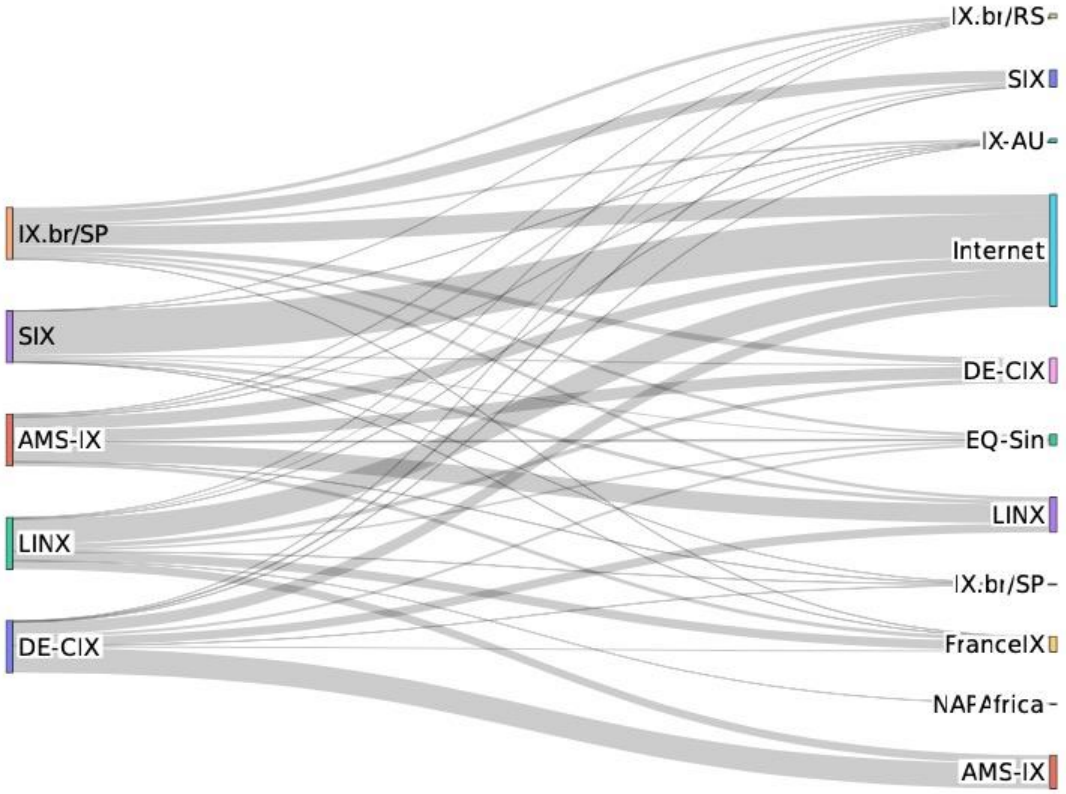
- **Qual o impacto de desastre afetando datacenters em uma região**?
  - Cyber Resilience of Systems and Networks – 2019 – book
  - Analise da região de **Ashburn/US**
  - Potencial de **perdas na Cyber economia** dos US com impacto global
  - Identificada a necessidade de analise de riscos para IXPs, indicando que hoje não há forma de prever o impacto na Internet.
  - Vários serviços de governos hospedados na região.

Para pensar - Roteamento

- Qual o impacto de uma falha do **IX.br/SP**?
  - 37% das redes sobrecarregarão do circuitos dos provedores de transito para chegar em redes como amazon.
  - 23% das redes indo para Seatlle/US (SIX)
    - Alguns Ases nacionais trocarão tráfego em US.
  - 12% indo parar em Frankfurt/DE (DE-CIX)
  - 8% indo para IX.br/RS (ex. Akamai e Netflix)
  - 6% para LINX/UK

Para pensar - Roteamento

- Qual o impacto de uma falha do IX.br/SP?
  - 37% das redes sobrecarregarão provedores de transito
  - 23% indo para Seatlle/US (SIX)
    - Alguns Ases nacionais trocarão tráfego em US.
  - 12% indo parar em Frankfurt/DE
  - 8% indo para IX.br/RS (ex. Akamai e Netflix)
  - 6% para Londres/UK



Para pensar - Resumo

- Resolvers estao concentrados em poucas redes (cloud)
  - Usuarios geralmente sao orientados a usar 1.1.1.1 8.8.8.8 em falhas
- Blocos IP de DNSs primarios e secundarios no mesmo datacenter fisico ou mesmo provedor de serviço.
  - 15% de todos os domínios .COM e .NL registram ambos os servidores DNS sobre o mesmo prefixo IPv4.
- Provedores não tem infraestrutura para suportar outage de um IXP
  - Falha do DE-CIX 2018: blackout na Internet Alemã

Perguntas ?