Ataques DDoS em Outubro e Novembro

Análise e Recomendações Técnicas

made4it

MADE4IT
Quem Somos

CONECTAR É A NOSSA ESPECIALIDADE

*A **Made4it** nasceu com o conceito enraizado de consultoria de TI para atender todo porte de empresas, sempre com a filosofia de **ir até o fim na causa do cliente.***

Nossos Diferenciais

- *Suporte especializado*
- *Atendimento diferenciado*
- *Alta experiência no setor*
- *Principais certificações do mercado*

Notícias sobre os ataques

tiinside

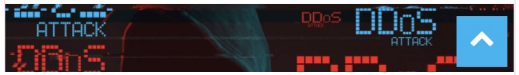
Publicidade

Início › Notícias › Comunicações › Em seis meses, volume de ataques DDOS aumenta cerca de 400% com...

Notícias | Comunicações | Gestão | Segurança

Em seis meses, volume de ataques DDOS aumenta cerca de 400% com foco em ISPs

Por Redação - 17 de novembro de 2023 0



InternetSul

Compartilhe:

Ciberataques afetam milhares de provedores no Brasil, causando interrupção nos serviços de Internet

ISH

GRUPO IROX TEAM AMEAÇA ATACAR O BRASIL. SAIBA COMO PROTEGER O SEU NEGÓCIO

Por ISH e SafeLabs: Um grupo de cyber ativistas denominado '**IRoX Team**' anunciou uma guerra cibernética contra Israel e os seus apoiadores, divulgando datas para seus ataques cibernéticos. Segundo a publicação em um grupo público de mensageria, o grupo

Daily Dark Web
@DailyDarkWeb
Follow

IRoX Team has declared cyber war against Israel and the countries supporting Israel

The group shared their target countries (scheduled ones):

Oct 20: Brazil, Canada, Poland, Spain
Oct 25: India, United Kingdom, Australia
Oct 30: France, Norway, Austria, Germany

#DarkWeb #IsraelPalestineWar

terra

TERRA FRIDAY | CENTRAL DO ASSINANTE | TERRA MAIL

Capa › Notícias

agora

BRASIL | MUNDO | LOTERIAS | PREVISÃO DO TEMP

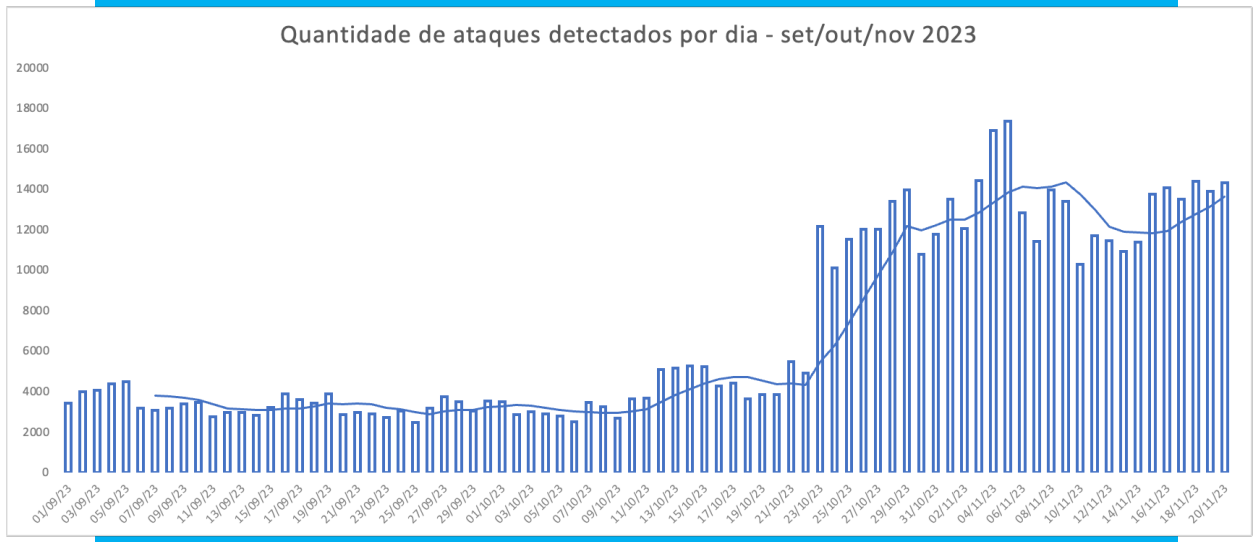
RS sob ataque! Ciberguerra abala provedores de internet no Estado

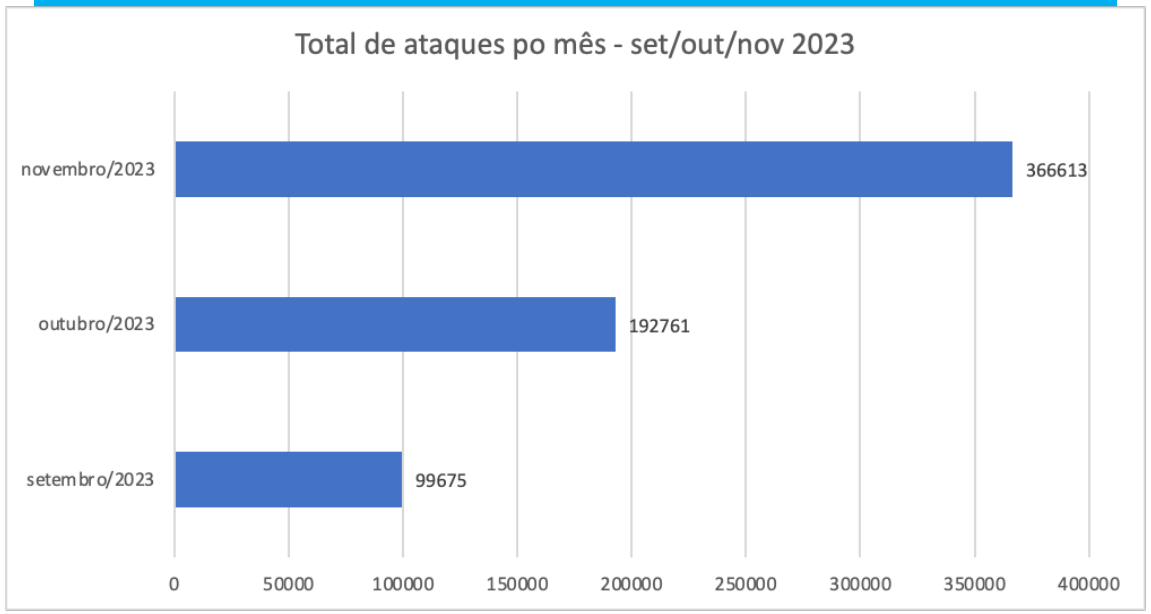
Milhares de provedores Brasileiros enfrentam ataques DDoS do grupo ciberativista e o Rio Grande do Sul é o mais atingido

Por: Juliano Haesbaert

24 out 2023 - 14h04 Compartilhar

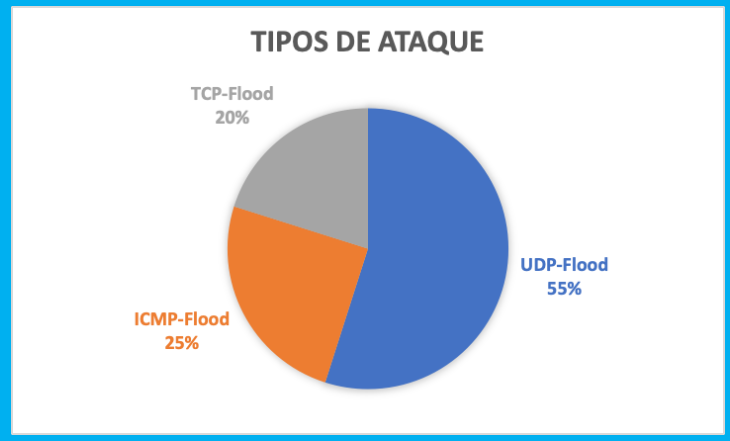
Histórico de Ataques - Sensores





made4 FLOW Anti-DDoS
Sua solução em Netflow

- *Aumento de aproximadamente **267%** no número de ataques detectados em novembro/23, comparado com setembro/23*
- *Pico de **17k ataques** no dia 05/11/2023*
- *Quase **367k ataques** só em novembro (até 20/11)*



Explorando os Ataques

ALINHAMENTO PRÉVIO

- *Os dados foram coletados de uma amostragem a partir dos sensores do Made4Flow;*
- *O período analisado foi de 20/10/2023 a 20/11/2023;*
- *Todos os dados são anônimos, e os dados originais analisados tiveram autorização prévia de serem analisados para o fim desta apresentação;*
- *Esta apresentação não pretende ser uma análise científica dos dados;*

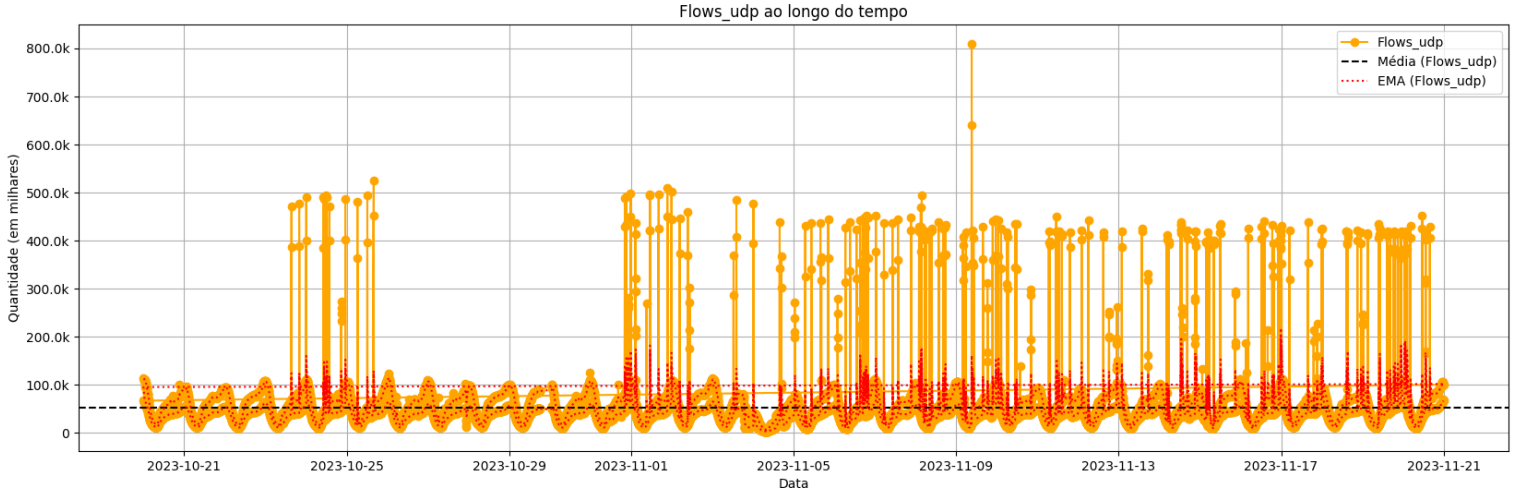
Estamos explorando os dados de maneira mais qualitativa, buscando embasar as recomendações que logo se seguem.

- *Por conta do tempo da apresentação, selecionamos alguns eventos, mas que refletem a grande maioria dos ataques;*
- *As análises contam com períodos sem ataque e com ataque;*

Para o período "sem ataque", consideramos um timeshift de 10 min anterior ao inicio do ataque.

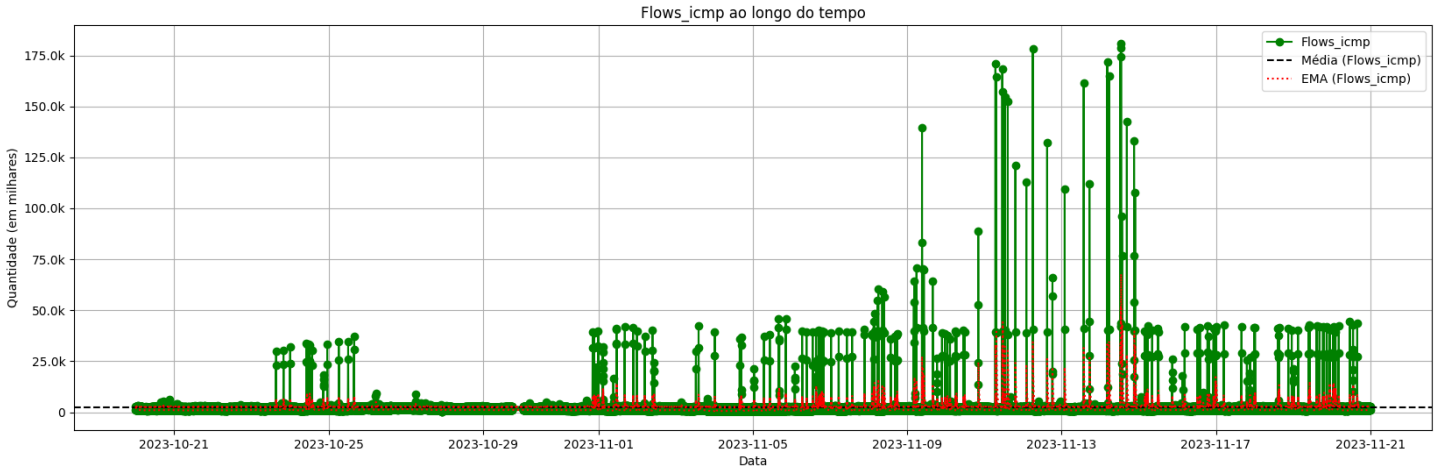
Explorando Ataque 01

Os fluxos TCP não tiveram uma alteração significativa no período!



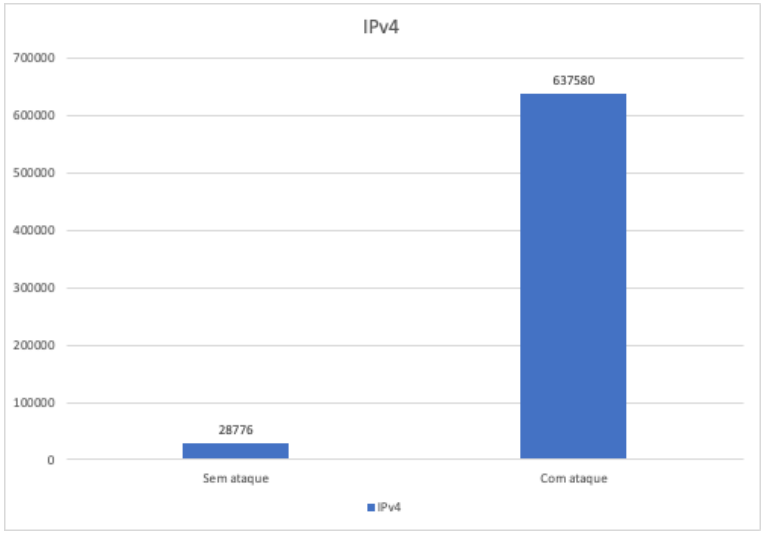
- ***Flows UDPs*** *ao longo do tempo*
- *Picos de* ***100k*** *fluxos/s em períodos sem ataque*
- *Diversas rajadas de até* ***800k*** *fluxos/s durante os ataques*

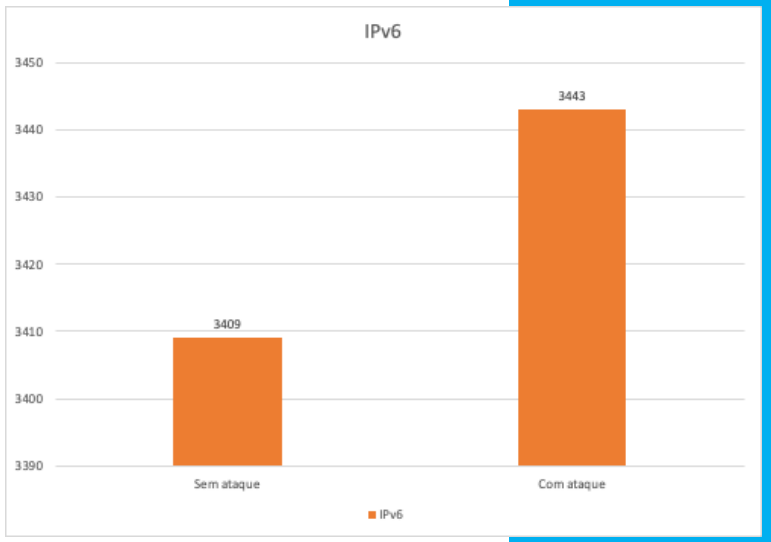
- ***Flows ICMP*** *ao longo do tempo*
- *Picos de* ***5k*** *fluxos/s em períodos sem ataque*
- *Diversas rajadas de até* ***175k*** *fluxos/s durante os ataques*



Ataque 01 - Quais protocolos?

Aumento em 22x o número de fluxos IPv4 !!!



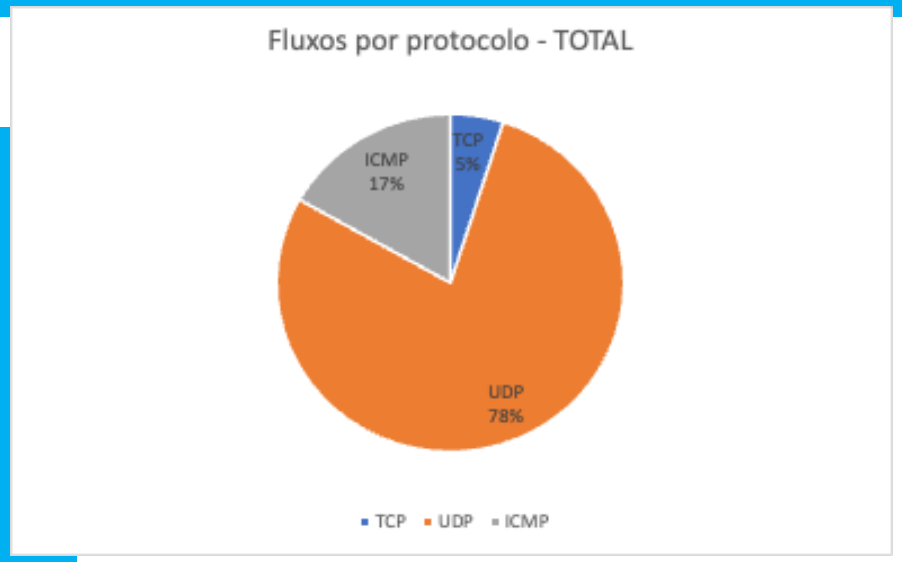


- ***IPv6*** *uma variação mínima*

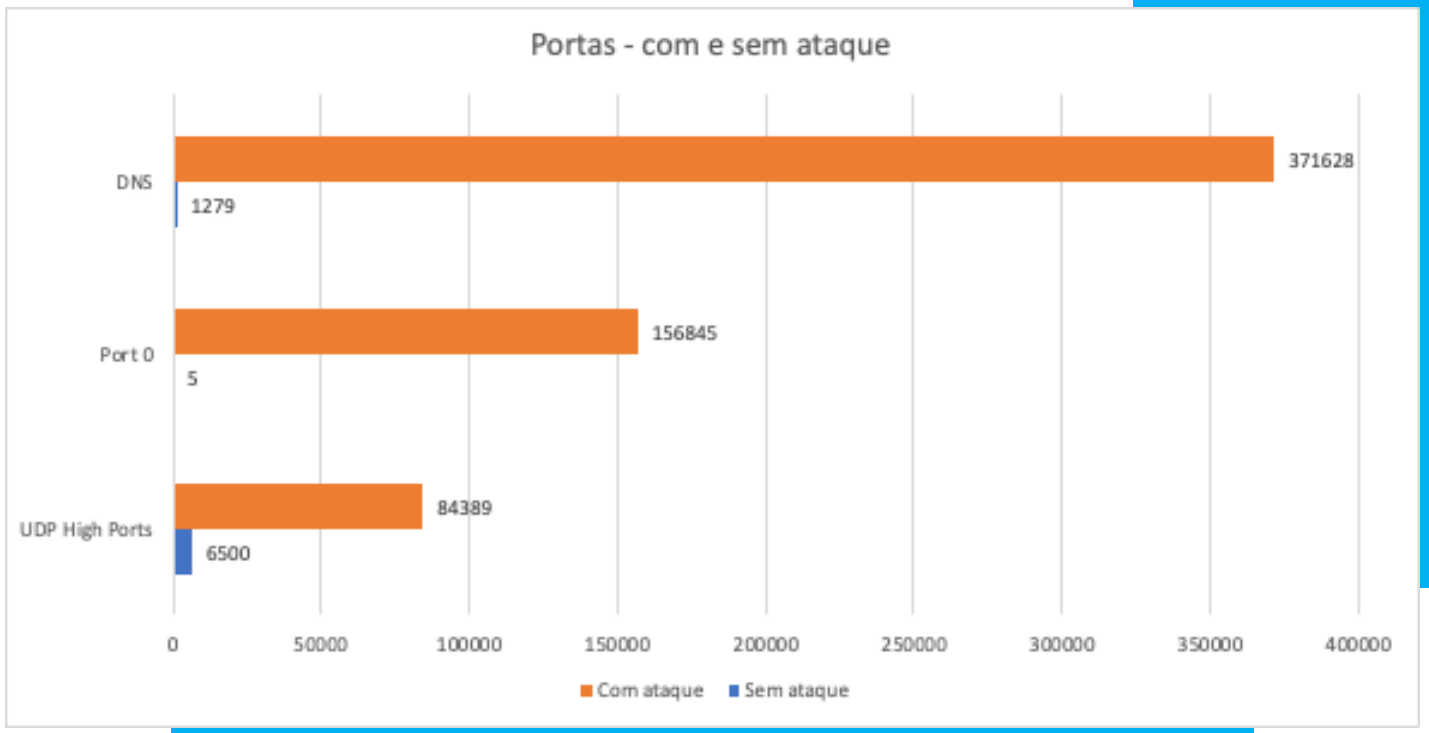
Resultado: ***Ataque volumétrico UDP ....***

- *78% UDP*
- *17% ICMP*
- *5% TCP*

Ok, ICMP também, mas em menor escala.



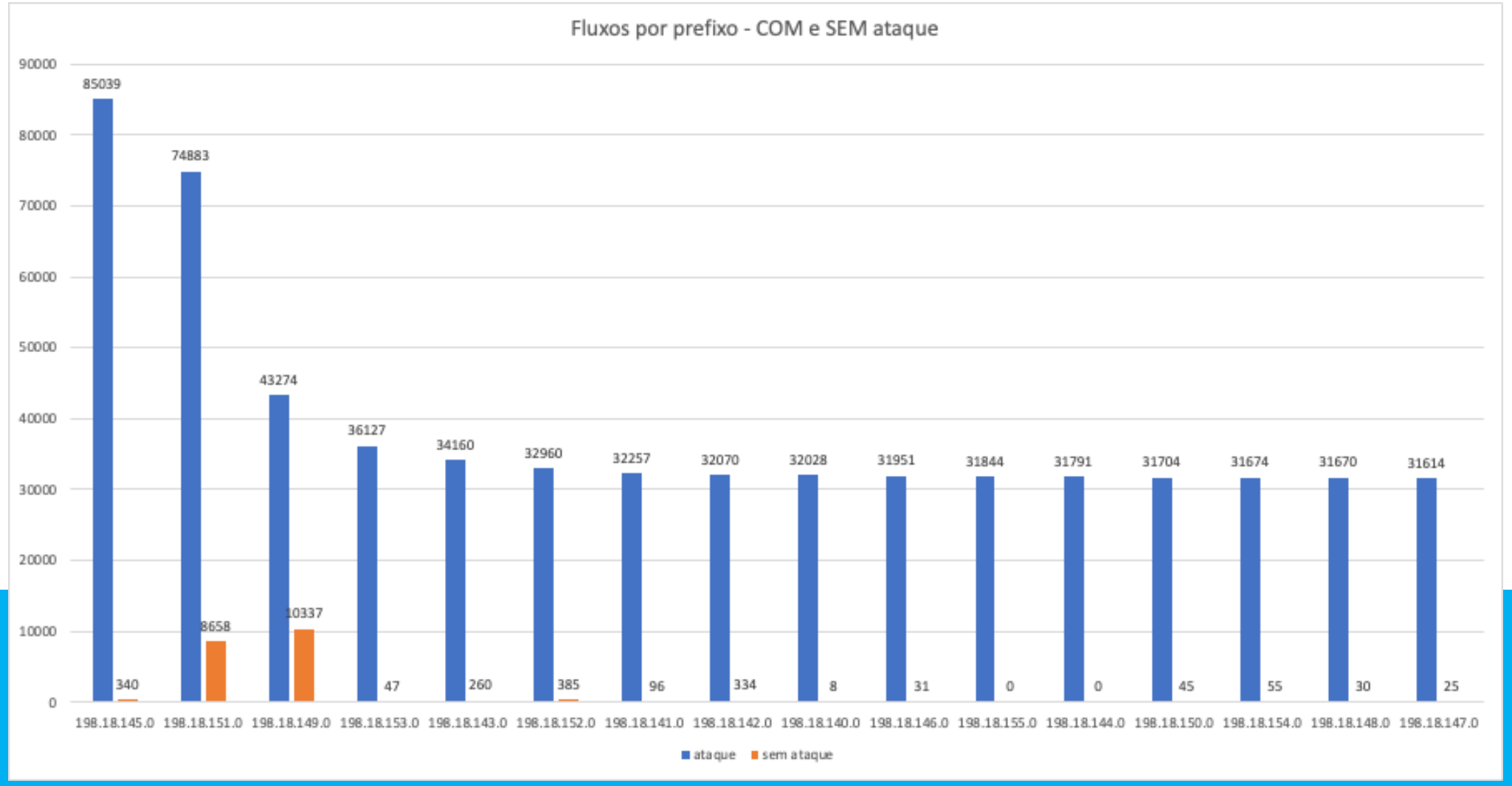
Ataque 01 - Avaliando o UDP



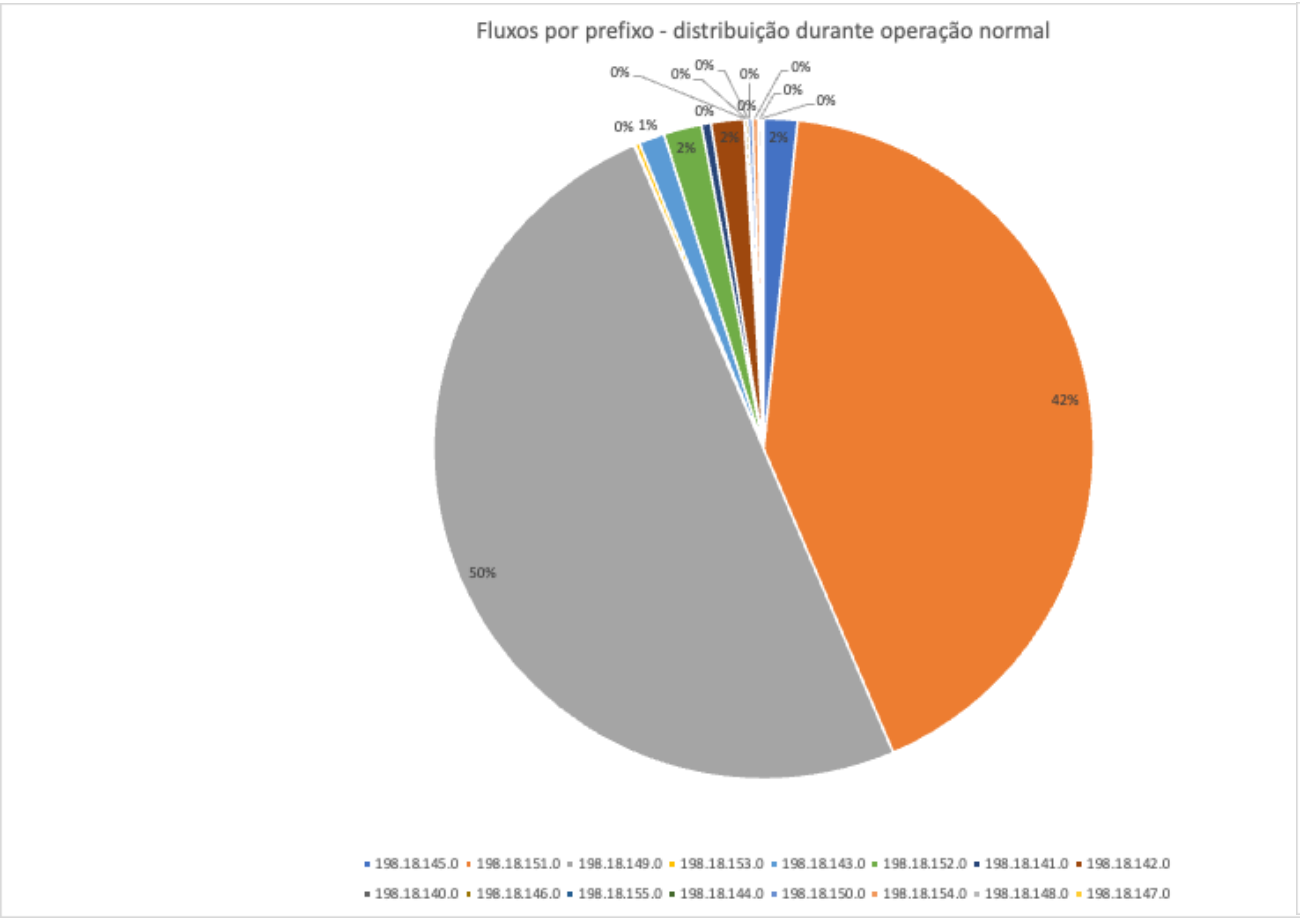
- *Aumento de **290x** no número de fluxos **DNS***
- *De **1.2k** para **371k***
- *Flood de porta 0*
- *De 5 fluxos para **156k***
- *Flood de portas altas*
- *De **6.5k** para **637k** (22x)*

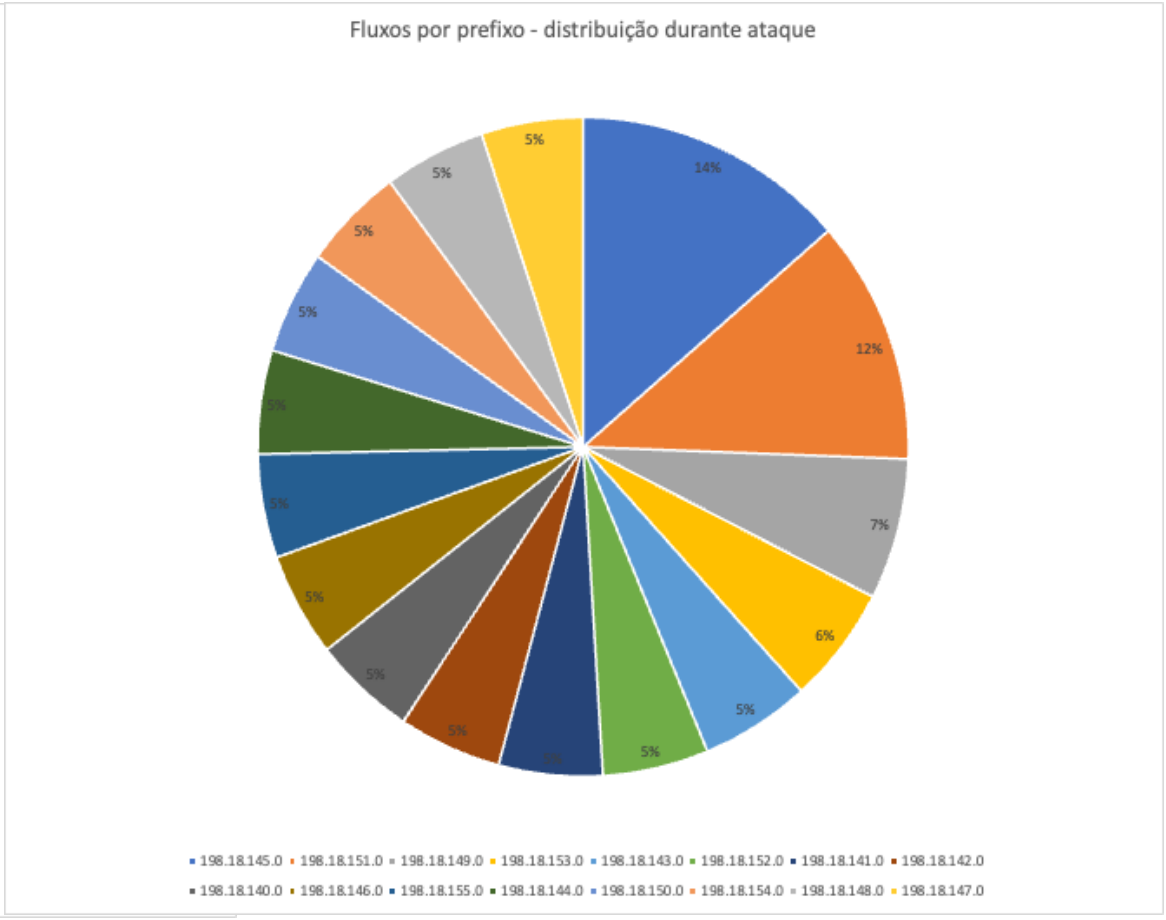
***Resultado**: Ataque volumétrico **UDP**, sendo o principal ofensor o tráfego **DNS** e de "porta 0" ....*

Ataque 01 - Direcionado a quem?



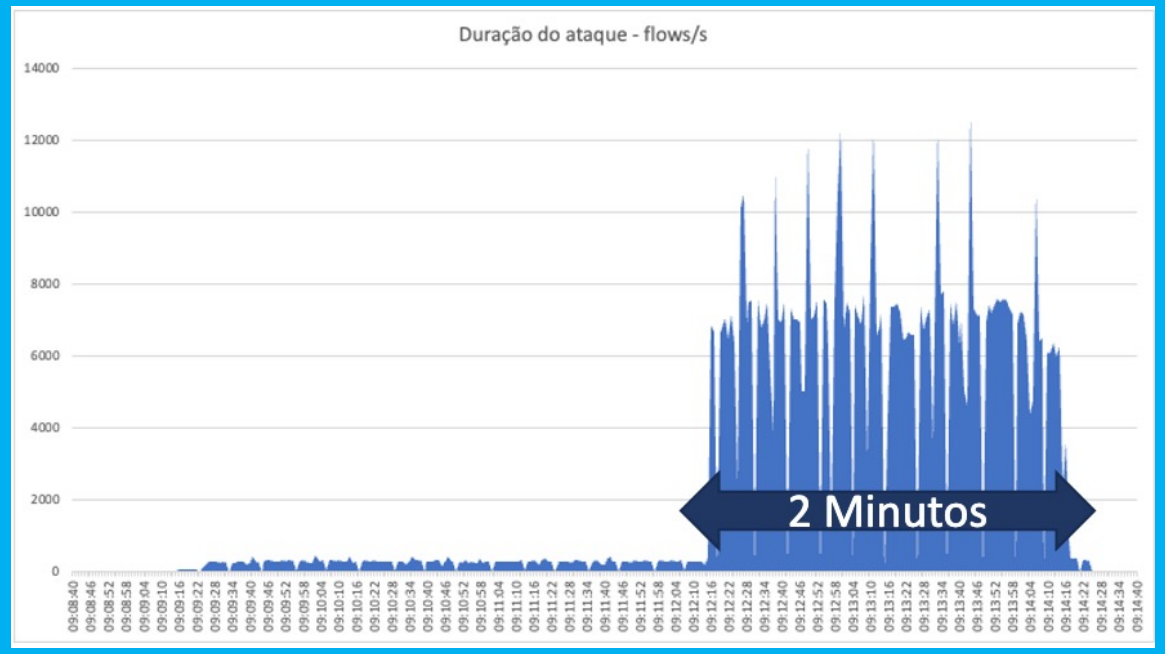
Ataque 01 - Direcionado a quem?

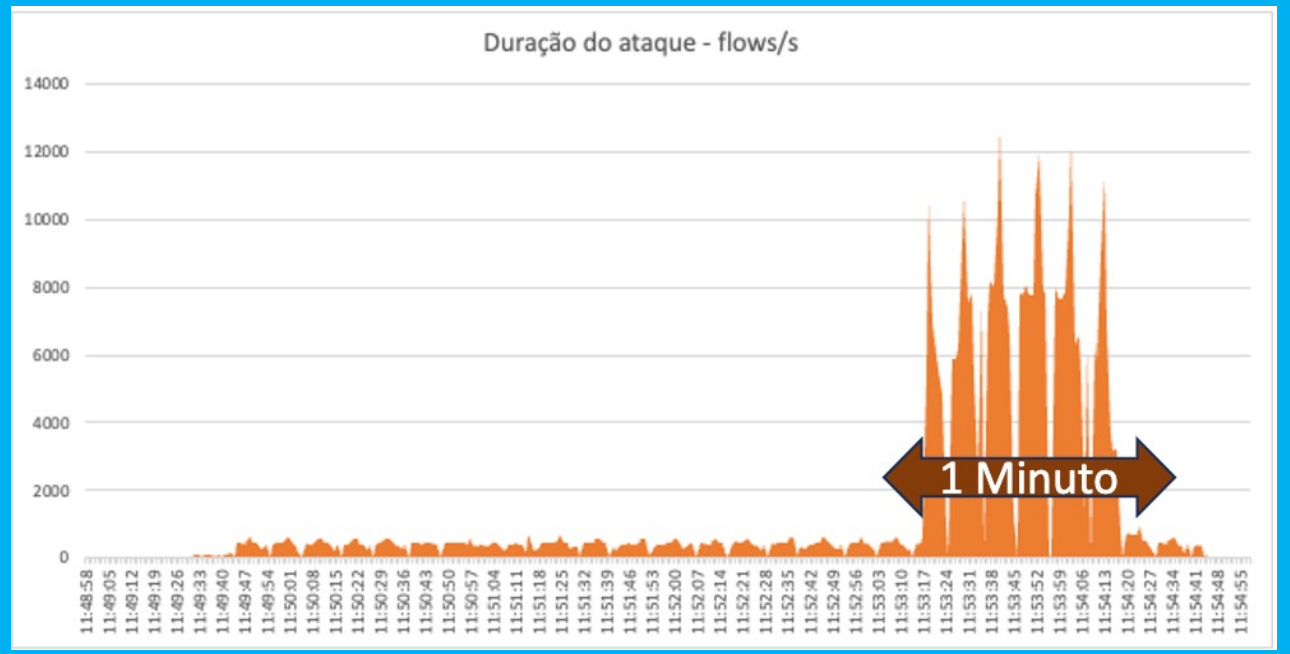




Resultado: *Ataque volumétrico UDP, sendo o principal ofensor o tráfego DNS e de "porta 0", destinado a todas as sub-redes do ASN ....*

Ataque 01 - Por quanto tempo?

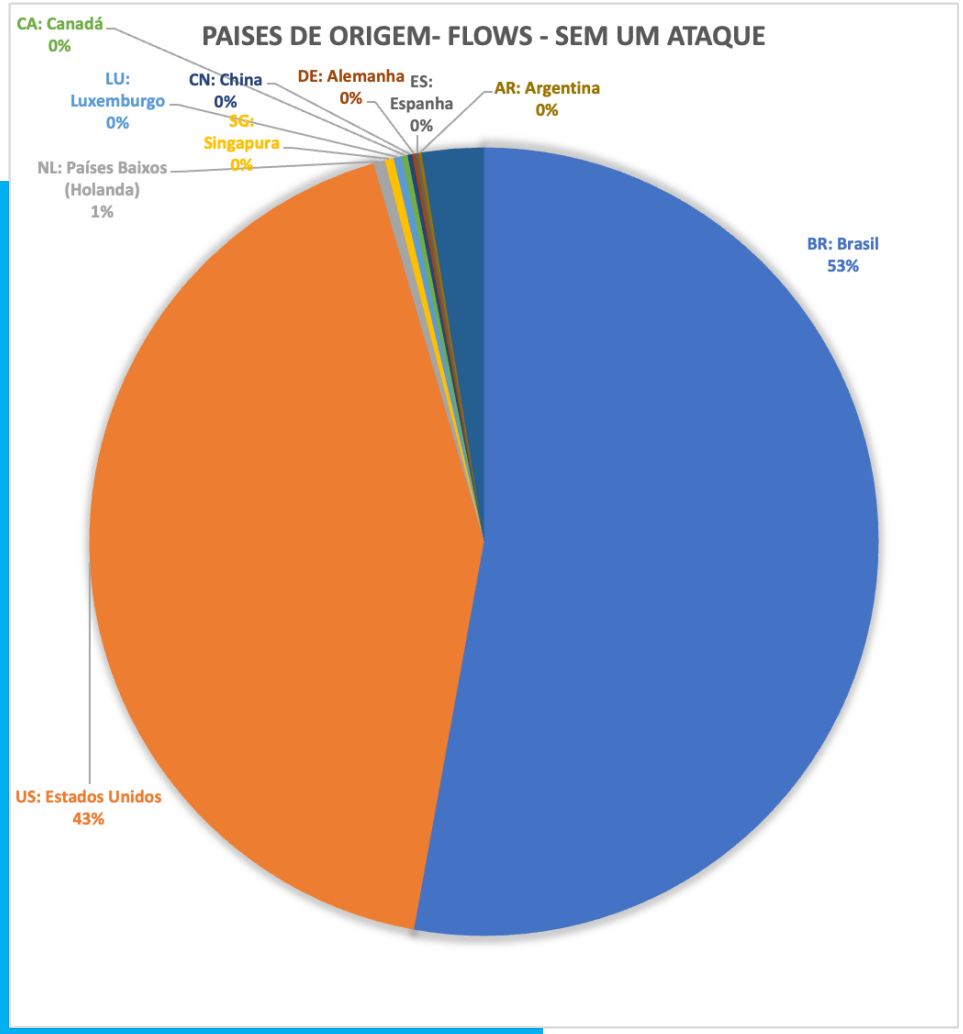




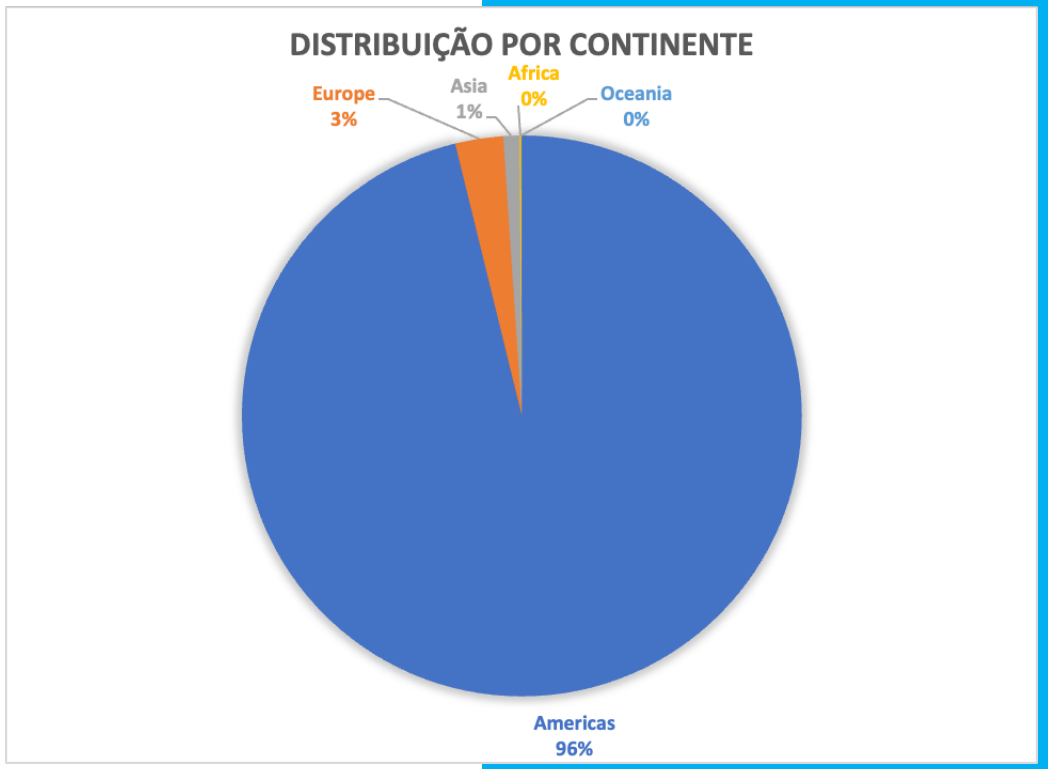
- *Os ataques do mesmo tipo/característica tem durado entre 40s e 120s*

***Resultado**: Ataque volumétrico UDP, sendo o principal ofensor o tráfego DNS e de "porta 0", destinado a todas as sub-redes do ASN, com duração de até 2 minutos, ...*

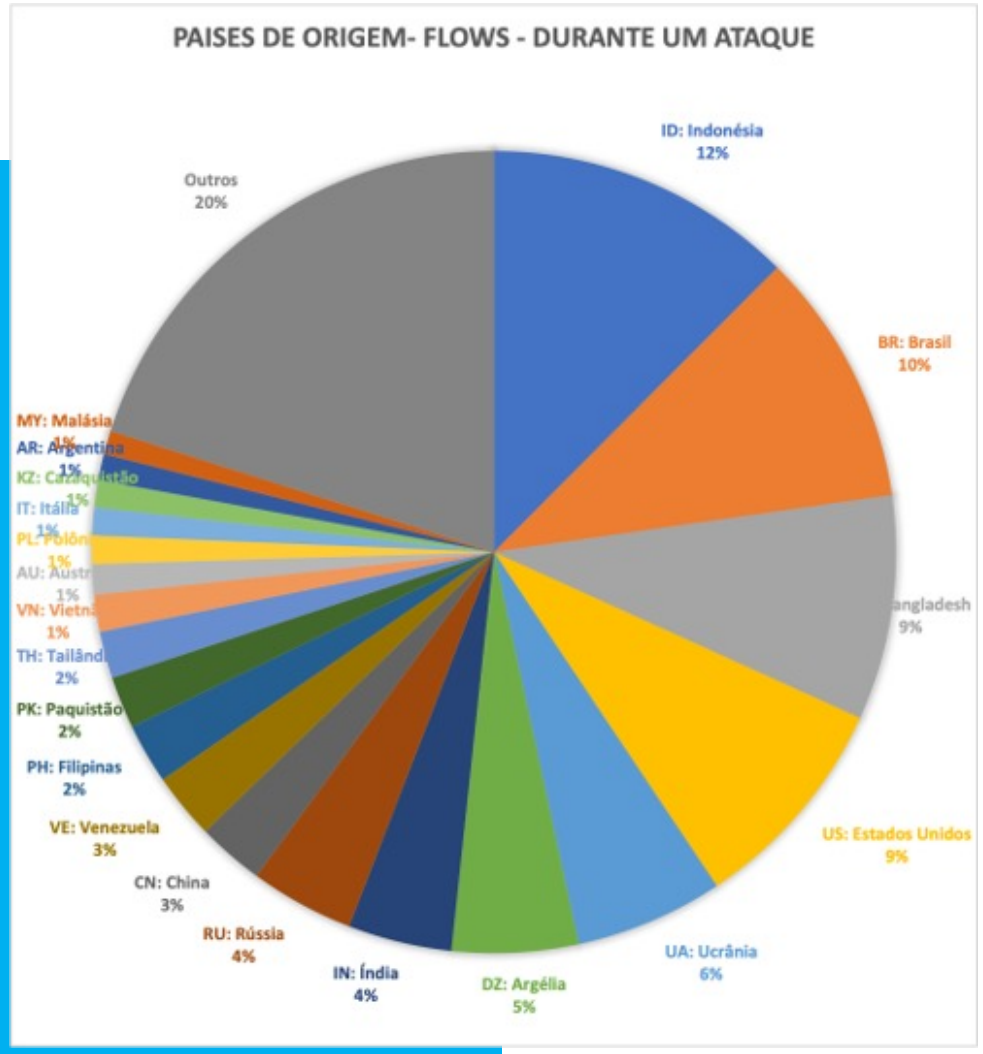
Ataque 01 - De quais Países?

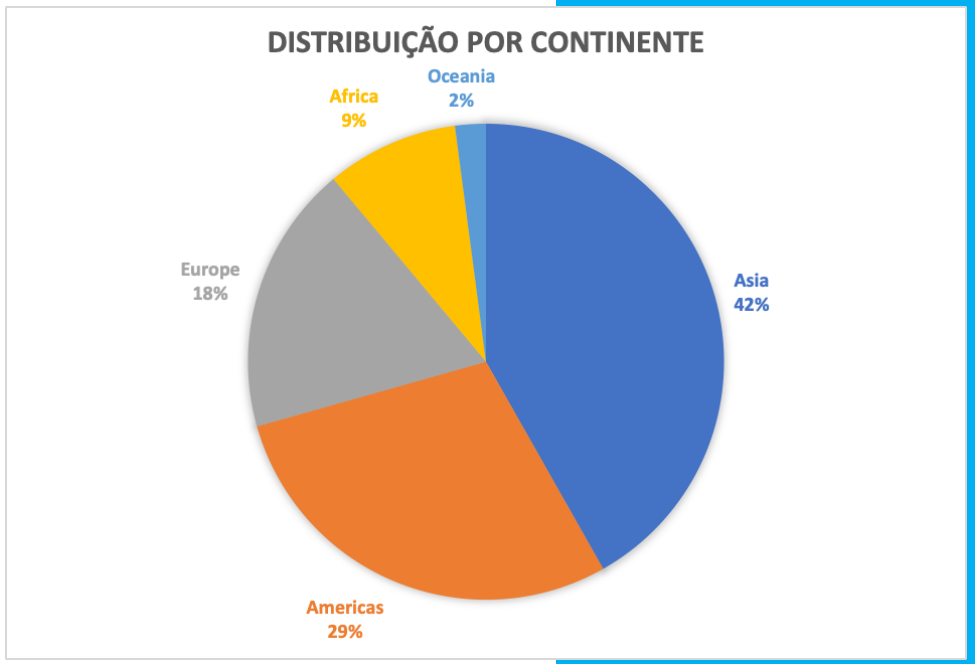


- *Durante a operação normal, mais de 90% do tráfego vindo de **ASNs BR/USA***



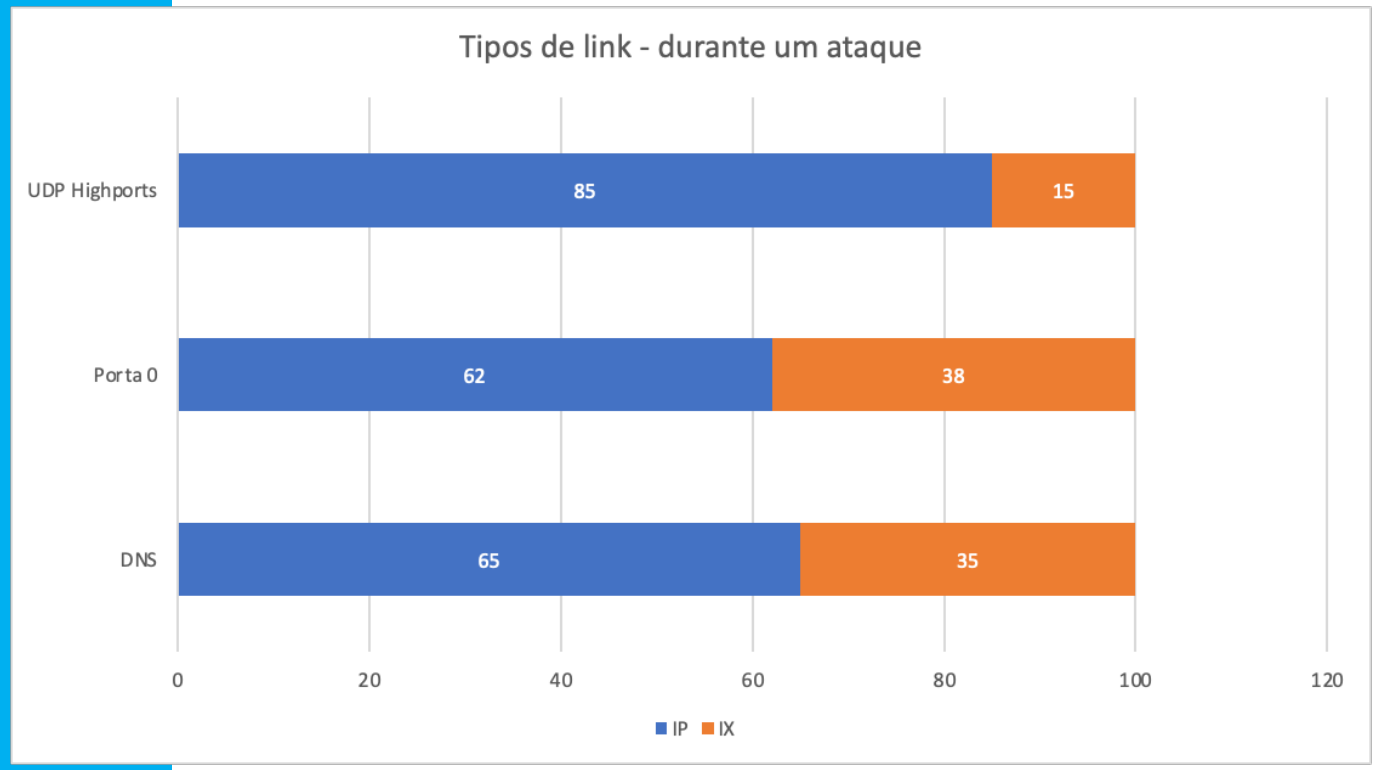
Ataque 01 - De quais Países?





Resultado: *Ataque volumétrico UDP, sendo o principal ofensor o tráfego DNS e de "porta 0", destinado a todas as sub-redes do ASN, com duração de até 2 minutos, com IPs de origem em todos os continentes, mas principalmente da região APNIC, ...*

Ataque 01 - Por quais links?



- *Até 38% do ataque entrando via IX.br*

***Resultado**: Ataque volumétrico UDP, sendo o principal ofensor o tráfego DNS e de "porta 0", destinado a todas as sub-redes do ASN, com duração de até 2 minutos, com IPs de origem em todos os continentes, mas principalmente da região APNIC, com cerca de 30% desse tráfego chegando através do IX São Paulo.*

Ataque 01 - Abrindo DNS e IX.br

***Tráfego DNS**, agregado por sub-rede /24 de origem, na interface do IX-SP*

Top 10 subnets origem IX-SP durante operacao normal - DNS		
Subnet	Anunciada ATM via IX.br?	Quem
8.8.8.0	Sim	Google
8.8.4.0	Sim	Google
212.102.32.0	Sim	CDN77
1.1.1.0	Não	CloudFlare
216.239.34.0	Sim	Google
216.239.32.0	Sim	Google
205.251.198.0	Não	Amazon
205.251.199.0	Não	Amazon
216.239.36.0	Sim	Google
108.59.161.0	Sim	Oracle

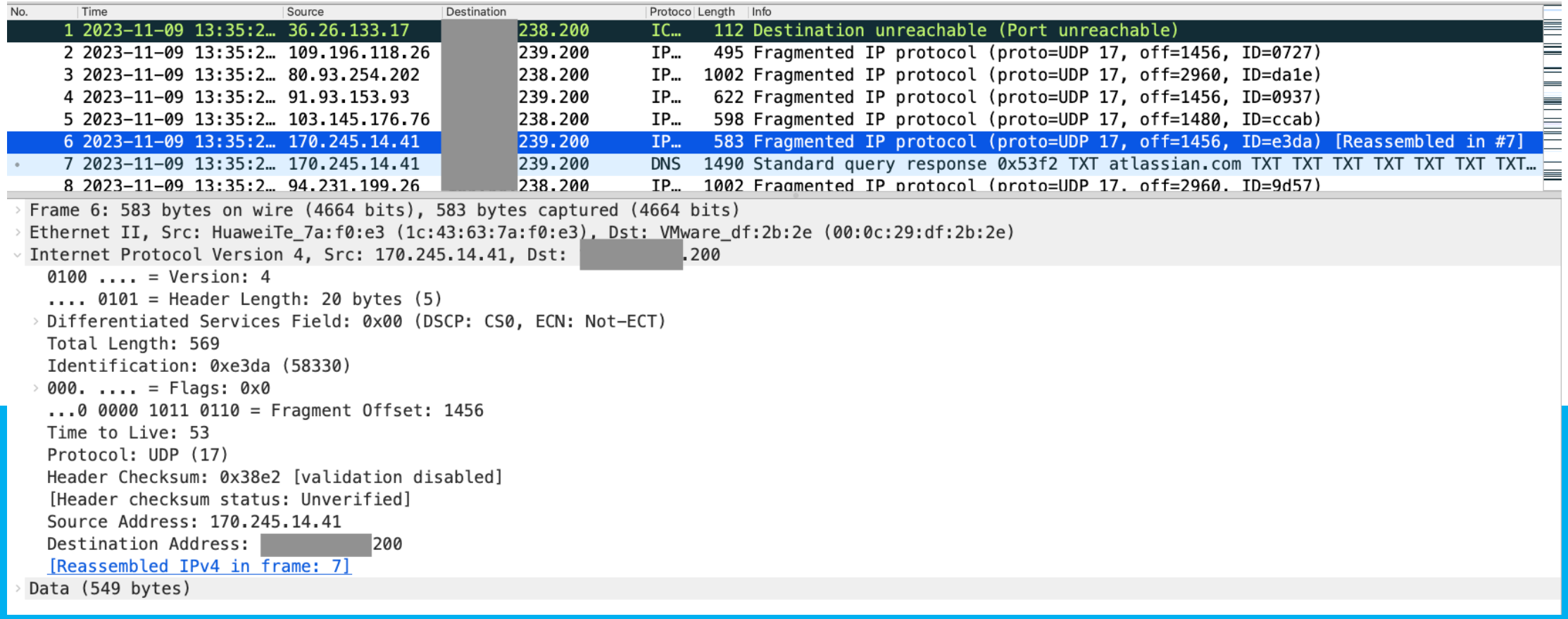
Top 10 subnets origem IX-SP durante ataque - DNS		
Subnet	Anunciada ATM via IX.br?	Quem
8.8.8.0	Sim	Google
103.102.247.0	Sim (via HE)	ATHOY CYBER NET (APNIC)
103.126.51.0	Sim (via HE)	City Net (APNIC)
103.97.206.0	Não	Mohammad Mahabub (APNIC)
103.186.52.0	Não	Wave Net (APNIC)
103.140.25.0	Sim (via HE)	Ali Akber (APNIC)
103.140.24.0	Sim (via HE)	Ali Akber (APNIC)
103.153.48.0	Sim (via HE)	MAYA SOFT (APNIC)
103.76.155.0	Sim (via HE)	Kurigram ISP (APNIC)
103.6.250.0	Não	Breeze Online (APNIC)

***Resultado**: Ataque volumétrico UDP, sendo o principal ofensor o tráfego DNS e de "porta 0", destinado a todas as sub-redes do ASN, com duração de até 2 minutos, com IPs de origem em todos os continentes, mas principalmente da região APNIC, com cerca de 30% desse tráfego chegando através do IX São Paulo, através de peers "internacionais" (ou spoofing).*

Ataque 01 – E a porta 0?

- *A porta 0 sempre esteve em evidência em todos os ataques que exploramos*
- *Ao analisar somente com netflow, perdemos alguns dados do tráfego, como por exemplo os mac-address envolvidos, se ele faz parte de um outro pacote fragmentado, etc*
- *Partimos então para uma captura de pacotes, e descobrimos que a porta 0 tão reportada nas análises eram na verdade fragmentos de uma resposta DNS grande*

Ataque 01 - Porta 0, agora fragmentos



No.	Time	Source	Destination	Protoco	Length	Info
1	2023-11-09 13:35:2…	36.26.133.17	[redacted]238.200	IC…	112	Destination unreachable (Port unreachable)
2	2023-11-09 13:35:2…	109.196.118.26	[redacted]239.200	IP…	495	Fragmented IP protocol (proto=UDP 17, off=1456, ID=0727)
3	2023-11-09 13:35:2…	80.93.254.202	[redacted]238.200	IP…	1002	Fragmented IP protocol (proto=UDP 17, off=2960, ID=da1e)
4	2023-11-09 13:35:2…	91.93.153.93	[redacted]239.200	IP…	622	Fragmented IP protocol (proto=UDP 17, off=1456, ID=0937)
5	2023-11-09 13:35:2…	103.145.176.76	[redacted]238.200	IP…	598	Fragmented IP protocol (proto=UDP 17, off=1480, ID=ccab)
6	2023-11-09 13:35:2…	170.245.14.41	[redacted]239.200	IP…	583	Fragmented IP protocol (proto=UDP 17, off=1456, ID=e3da) [Reassembled in #7]
7	2023-11-09 13:35:2…	170.245.14.41	[redacted]239.200	DNS	1490	Standard query response 0x53f2 TXT atlassian.com TXT TXT TXT TXT TXT TXT TXT…
8	2023-11-09 13:35:2…	94.231.199.26	[redacted]238.200	IP…	1002	Fragmented IP protocol (proto=UDP 17, off=2960, ID=9d57)

```
> Frame 6: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits)
> Ethernet II, Src: HuaweiTe_7a:f0:e3 (1c:43:63:7a:f0:e3), Dst: VMware_df:2b:2e (00:0c:29:df:2b:2e)
v Internet Protocol Version 4, Src: 170.245.14.41, Dst: [redacted].200
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 569
    Identification: 0xe3da (58330)
  > 000. .... = Flags: 0x0
    ...0 0000 1011 0110 = Fragment Offset: 1456
    Time to Live: 53
    Protocol: UDP (17)
    Header Checksum: 0x38e2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 170.245.14.41
    Destination Address: [redacted]200
    [Reassembled IPv4 in frame: 7]
> Data (549 bytes)
```

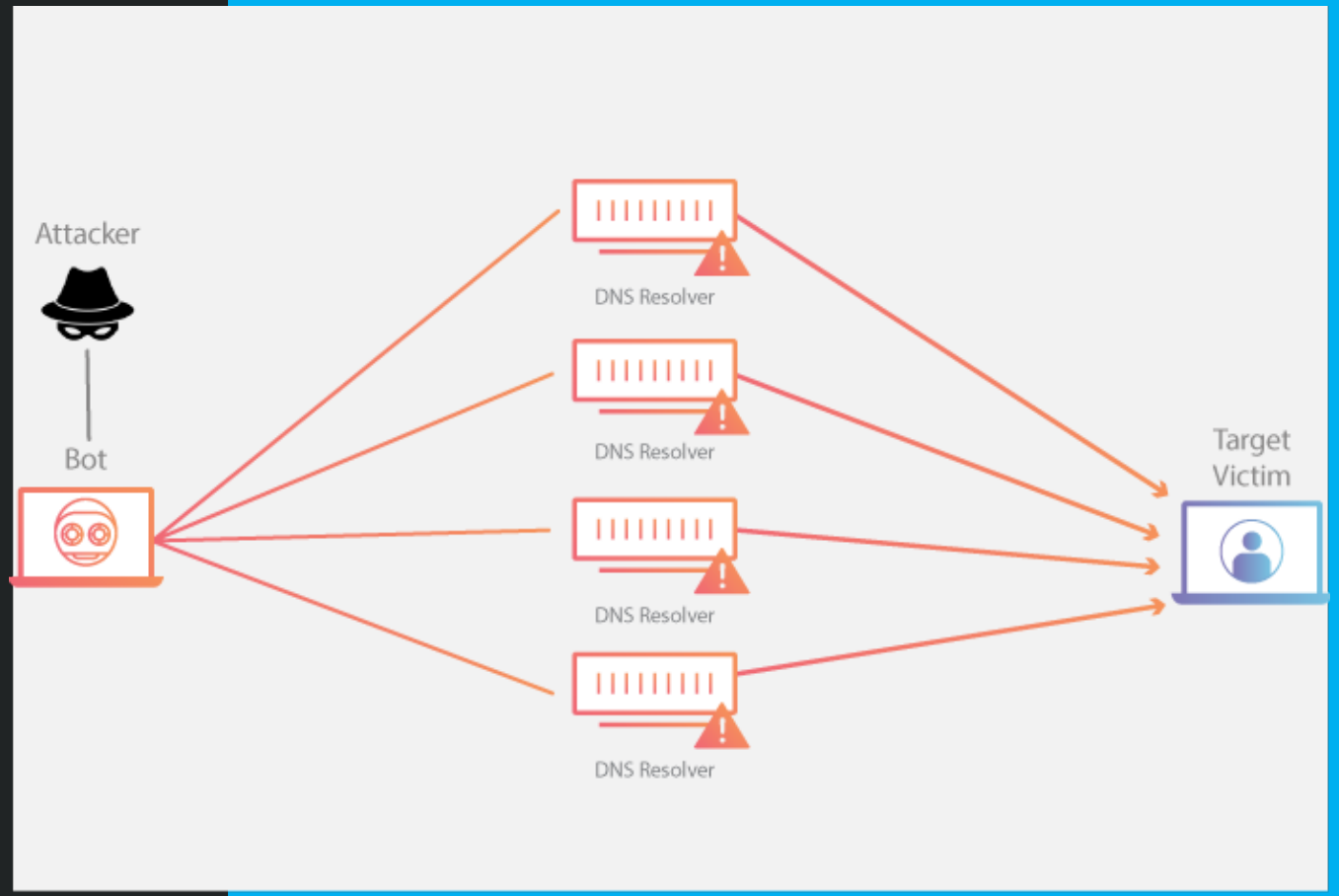
Ataque 01 - Amplificação DNS

- *Com a descoberta através da captura, podemos tipificar o ataque como de Negação de Serviço de Reflexão Distribuída (DRDoS) usando DNS*
  - *Amplificando respostas DNS grandes => tráfego porta 53*
    - *Fragmentando parte da resposta => tráfego porta 0*
    - *Gerando uma série de ICMP Port Unreachable => tráfego ICMP*
- *Utilizaram neste ataque o dominio atlassian.com, buscando o registro TXT (2084 bytes)*

***Resultado**: Ataque volumétrico UDP de amplificação DNS, destinado a todas as sub-redes do ASN, com duração de até 2 minutos, com IPs de origem em todos os continentes, mas principalmente da região APNIC, com cerca de 30% desse tráfego chegando através do IX São Paulo, através de peers "internacionais" (ou spoofing), causando o aumento no número de respostas DNS, fragmentos e o recebimento de ICMP port-unreachable.*

Para saber mais sobre este ataque

SAIBA MAIS



Para saber mais sobre este ataque

SAIBA MAIS

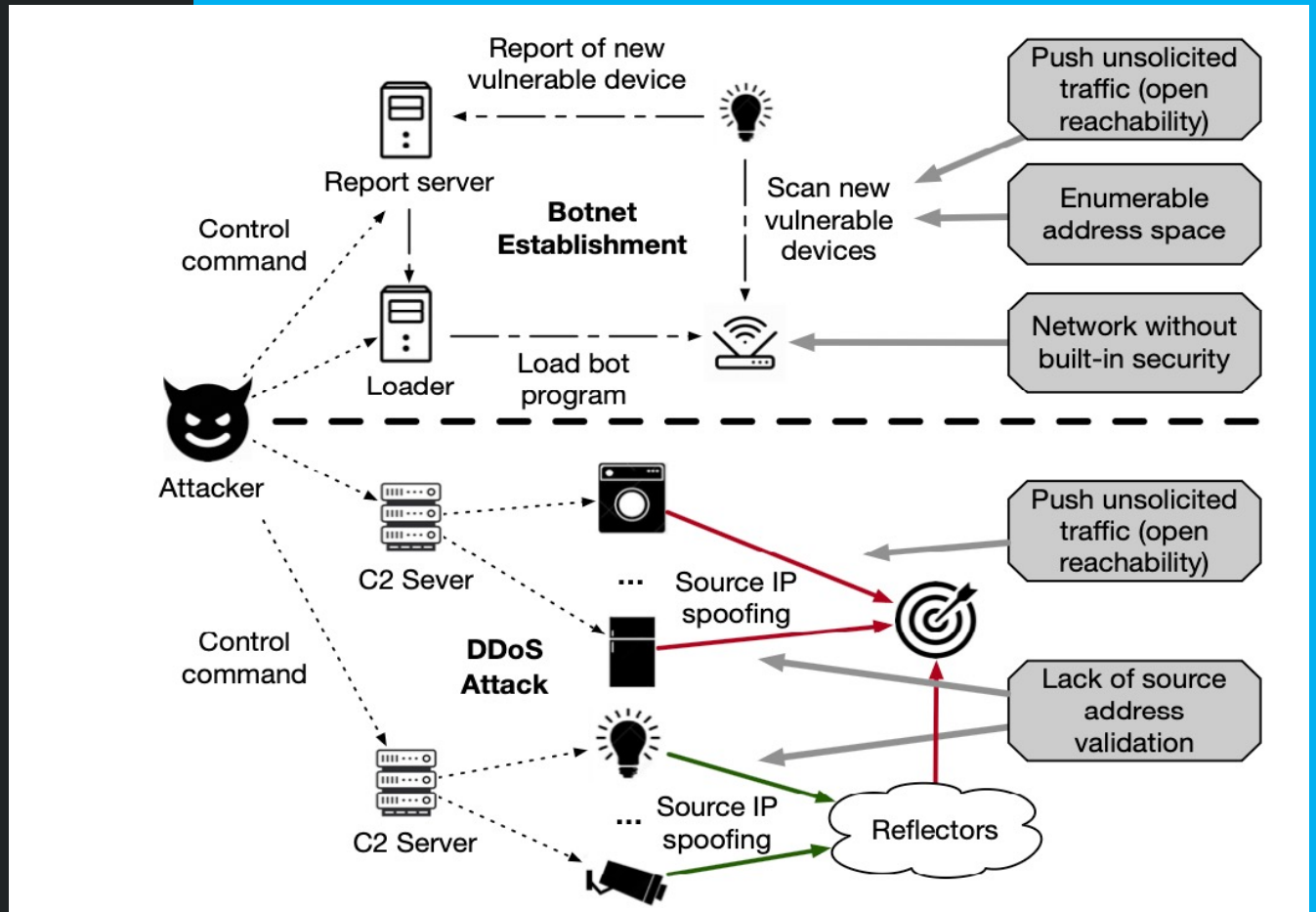


Fig. 2. IP design makes DDoS botnet establishment and attack easy

Resumo e pendencias

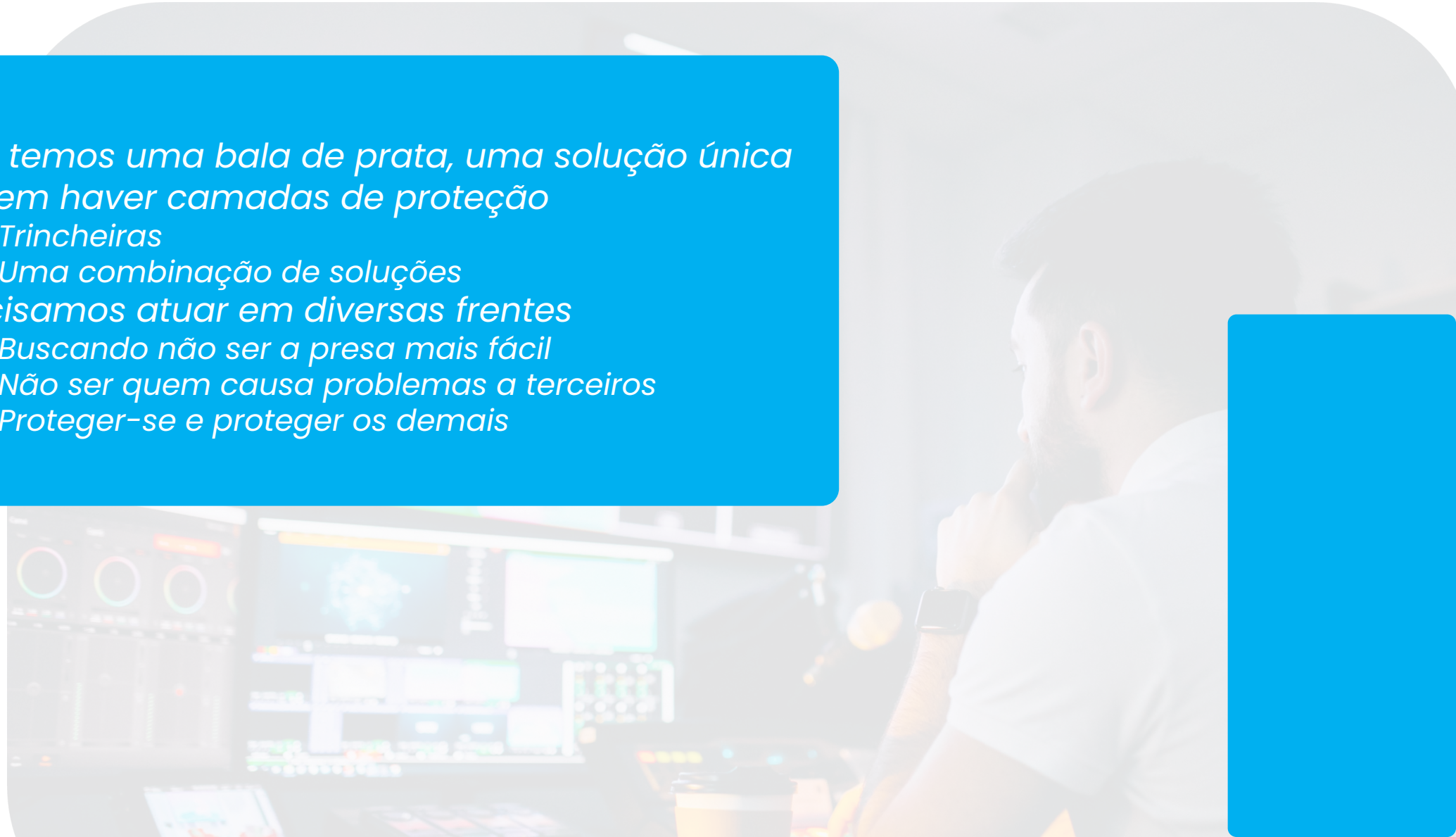
- *Este mesmo padrão de ataque apareceu em centenas de análises que fizemos*
- *Obviamente que alguns pontos oscilavam de rede para rede*
  - *Ex: países, continentes, o ratio entre IP:IX*
- *Porém a grande maioria analisada utilizou a amplificação DNS como técnica*
  - *Isto quer dizer que todos são assim? DEFINITIVAMENTE NÃO.*
- *A fazer:*
  - *Encontrar os participantes que encaminham estes ataques no IX.br (talvez via sflow)*
  - *Avançar na análise e consolidação de mais dados de outros tipos de ataque*

E AGORA, COMO SE PROTEGER?

E também como não ser o causador de problemas

Recomendações gerais

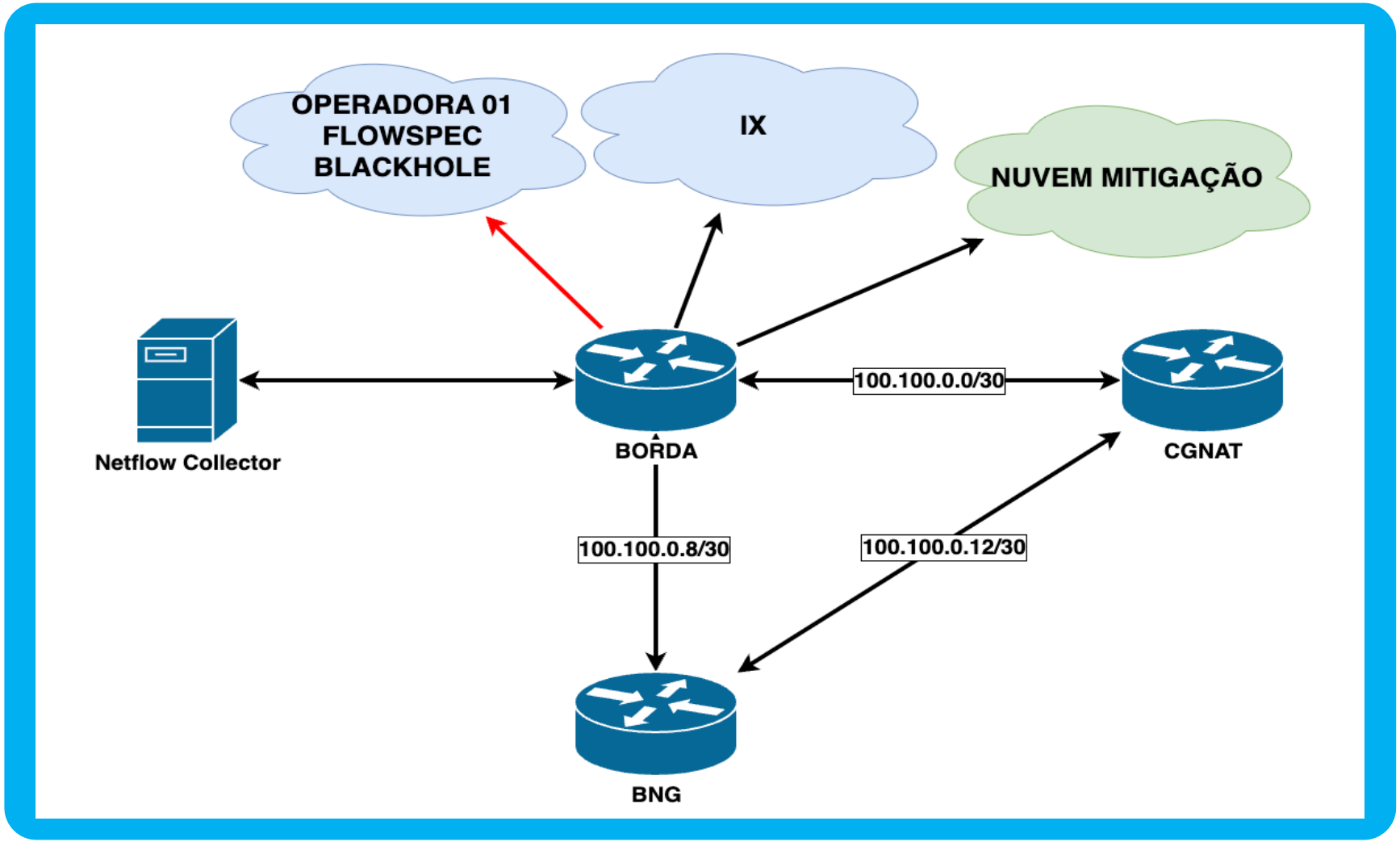
- *Não temos uma bala de prata, uma solução única*
- *Devem haver camadas de proteção*
  - *Trincheiras*
  - *Uma combinação de soluções*
- *Precisamos atuar em diversas frentes*
  - *Buscando não ser a presa mais fácil*
  - *Não ser quem causa problemas a terceiros*
  - *Proteger-se e proteger os demais*



Recomendações gerais

- ***Não se prepare durante o ataque. Esteja preparado!***
  - *Tenha sessão **BGP** com **RTBH** (**blackhole**) configurada;*
  - *Tenha sessão **BGP flowspec** com operadora configurada;*
  - *Tenha as **communities BGP** das operadoras em mãos;*
  - *Contrate operadoras que tenham suporte a **blackhole** e **flowspec**;*
  - ***Contrate links de mitigação**;*
  - ***Tenha uma ferramenta de deteção de ataques** alinhada com seu perfil de tráfego sem ataques;*
  - *Evite uso desnecessário **de IPv4 público**;*
  - *Evite uso de **Softrouters** nos principais serviços (**BGP, CGNAT, BNG**);*
  - ***Implemente IPv6**;*
  - *Implemente servidores **DNS Recursivos Anycast** escutando somente em IPs privados;*
  - ***Remova loops estáticos** de sua rede;*

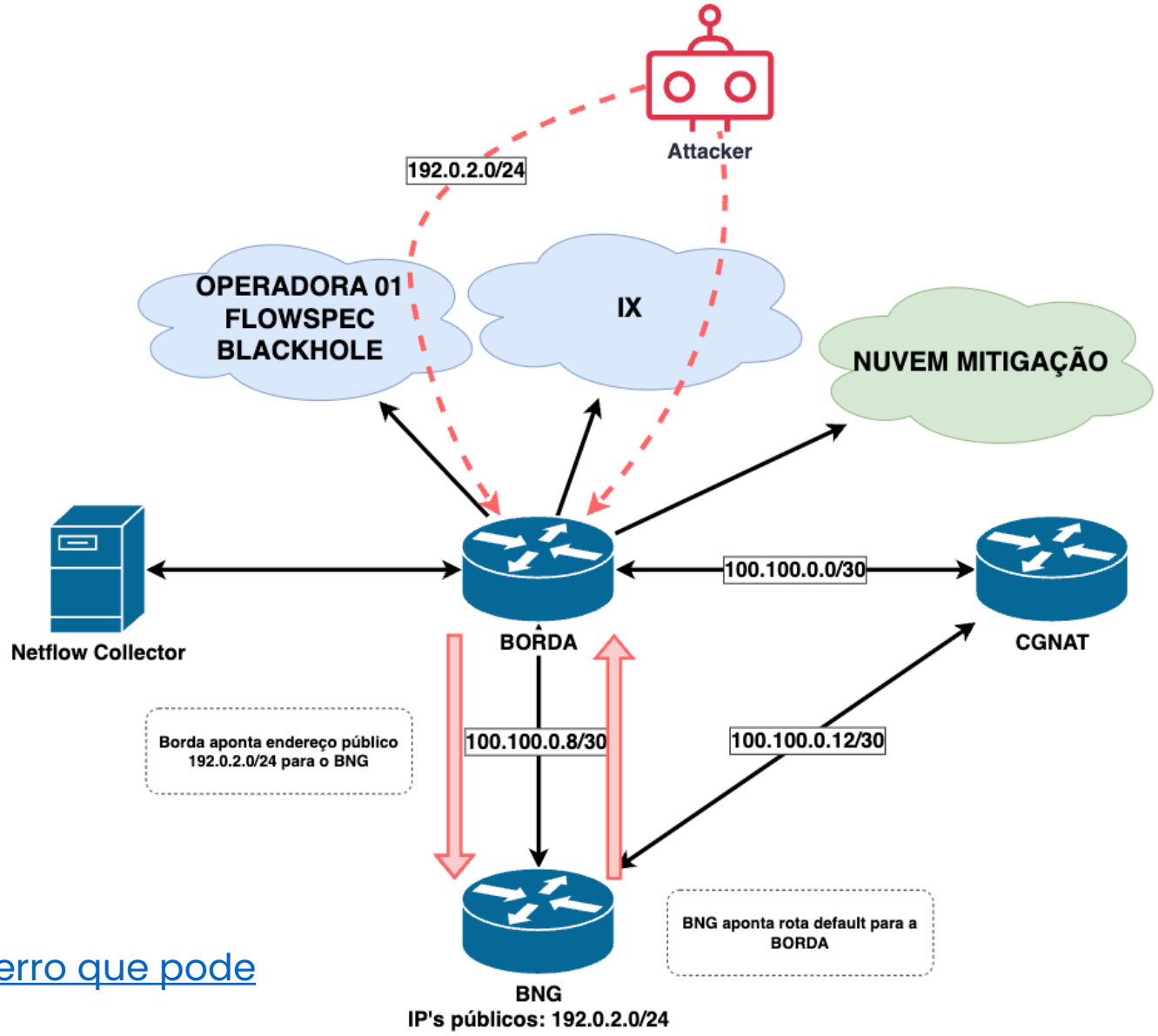
Sessão BGP com RTBH/Flowspec



Loops Estáticos

Entendendo o loop estático:

- *Atacante envia ataque para a rede 192.0.2.0/24*
- *Tráfego chega até a BORDA;*
- *BORDA encaminha para o BNG;*
- *BNG não possui a rota instalada e devolve o tráfego para a BORDA;*
- *Esse tráfego fica indo e voltando entre BORDA e BNG até estourar o TTL.*



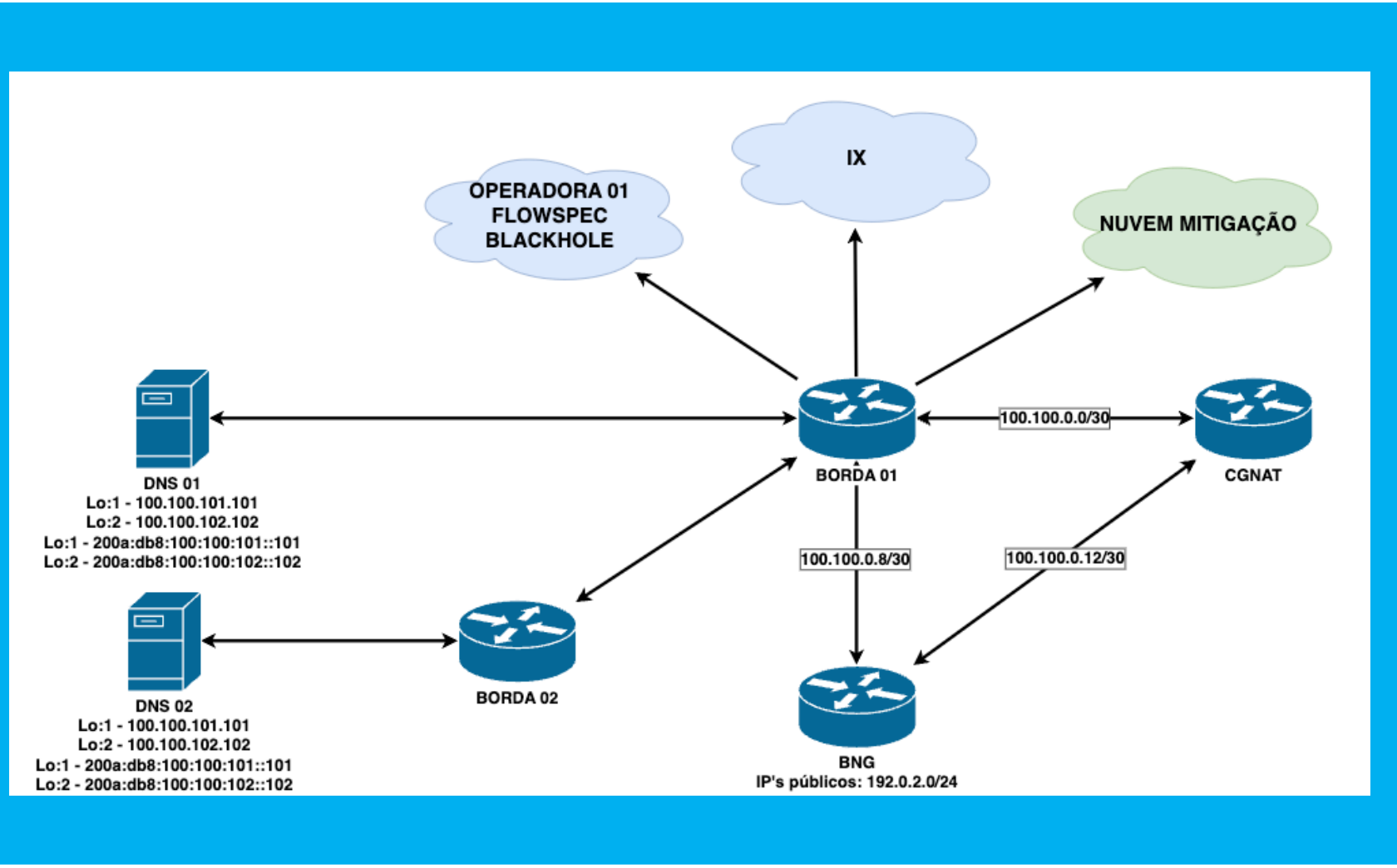
[Artigo BPF - Marcelo Gondim - Static Loop - Um erro que pode matar seu ISP/ITP]

Loops Estáticos

- *Validar loops estáticos no site [Radar by Qrator]*

DNS Recursivo Anycast

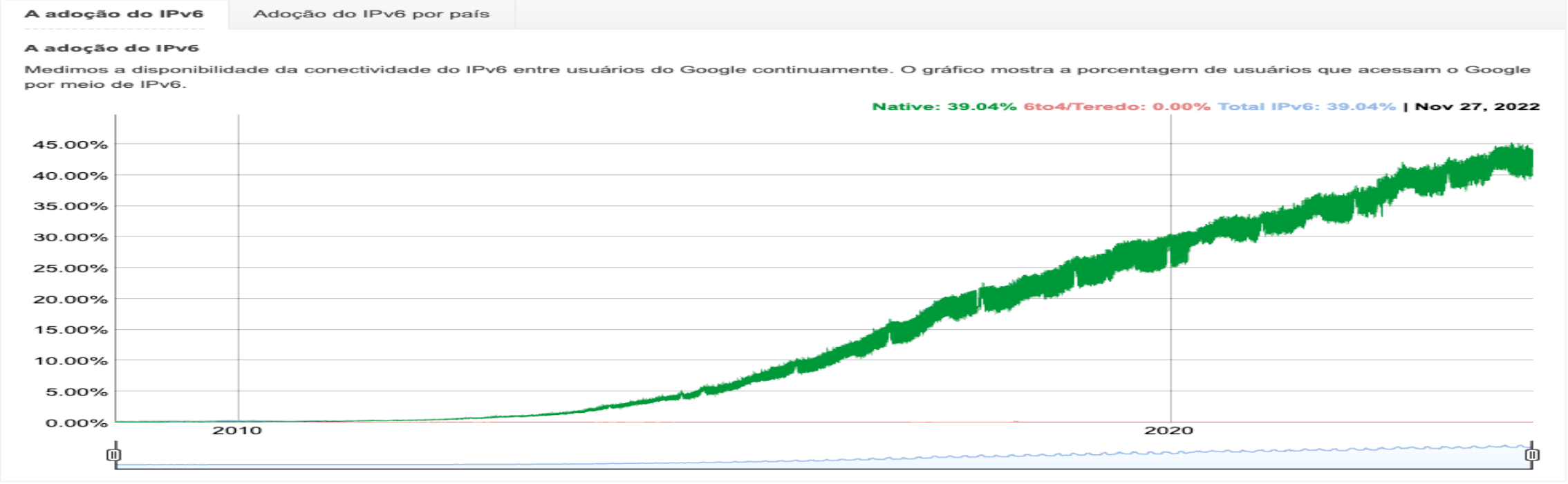
- *DNS escuta somente em IP's Privados;*
- *Mesmo IP responde em vários servidores(anycast);*
- *Servidores devem permitir somente rede do seu ISP;*
- ***NUNCA** deixar servidor DNS aberto para o mundo*



Implemente IPv6

Implemente IPv6 em massa

- *95% dos ataques são em IPv4;*
- *Quando estiver sob ataque, **IPv6** vai fazer grande diferença;*
- *45% do tráfego do Brasil está em **IPv6 –** Adoção IPv6 - Estatísticas Google*



Recomendações gerais

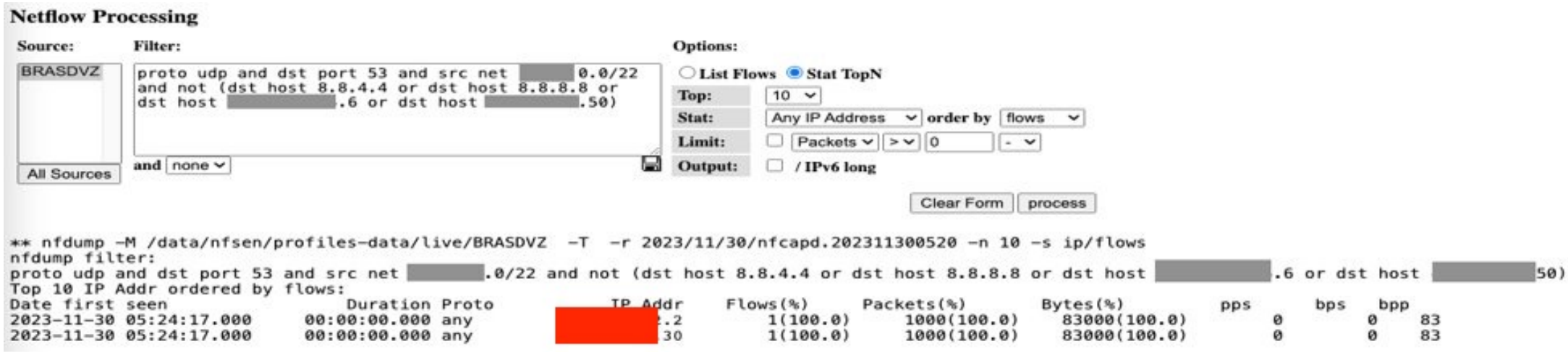
- ***Não seja o cara mau da história***
  - *Mantenha sua rede segura, faça scans regulares para encontrar falhas;*
  - *Feche portas de acesso à CPE's de clientes;*
  - *Não permita a comunicação entre clientes nas portas de gerência;*
  - *Permita que seu servidor DNS recursivo sirva somente à sua rede. JAMAIS deixe servidores DNS recursivo aberto para o mundo;*
  - *Garanta que seus equipamentos não estejam com portas sujeitas a amplificação sem controle de acesso (SNMP, NTP, DNS, Portmap, etc)*
  - *Monitore sua rede com NetFlow;*
  - *Mantenha seus registros whois/IRR/peeringDB atualizados;*
  - *Ingresse no projeto MANRS;*
  - *Responda ao CERT.br;*
  - *Implemente a BCP38 (Anti-Spoofing);*
  - *Identifique BOTNETS na sua rede e evite que esse tipo de tráfego malicioso saia da sua rede;*
  - *Bloqueie portas comumente utilizadas para ataques: https://wiki.brasilpeeringforum.org/w/Portas_de_Amplifica%C3%A7%C3%A3o_DDoS_e_Botnets*

Recomendações gerais

- **Identifique CPE's comprometidas na sua rede**

Exemplo de captura via netflow.
Dica: usar NFSEN para capturar flows do BNG. Tutorial instalação NFSEN - [Remontti - Guia Passo a Passo - Instalação NFDUMP, NFsen]

$ nfdump -R /var/log/flows/2017/12/06 'proto udp and dst port 53 and src net xx.xx.xx.xx/nn and not (dst host 8.8.4.4 or dst host 8.8.8.8 or dst host 1.1.1.1 or dst host 1.0.0.1 or dst host <SEU RECURSIVO>)'



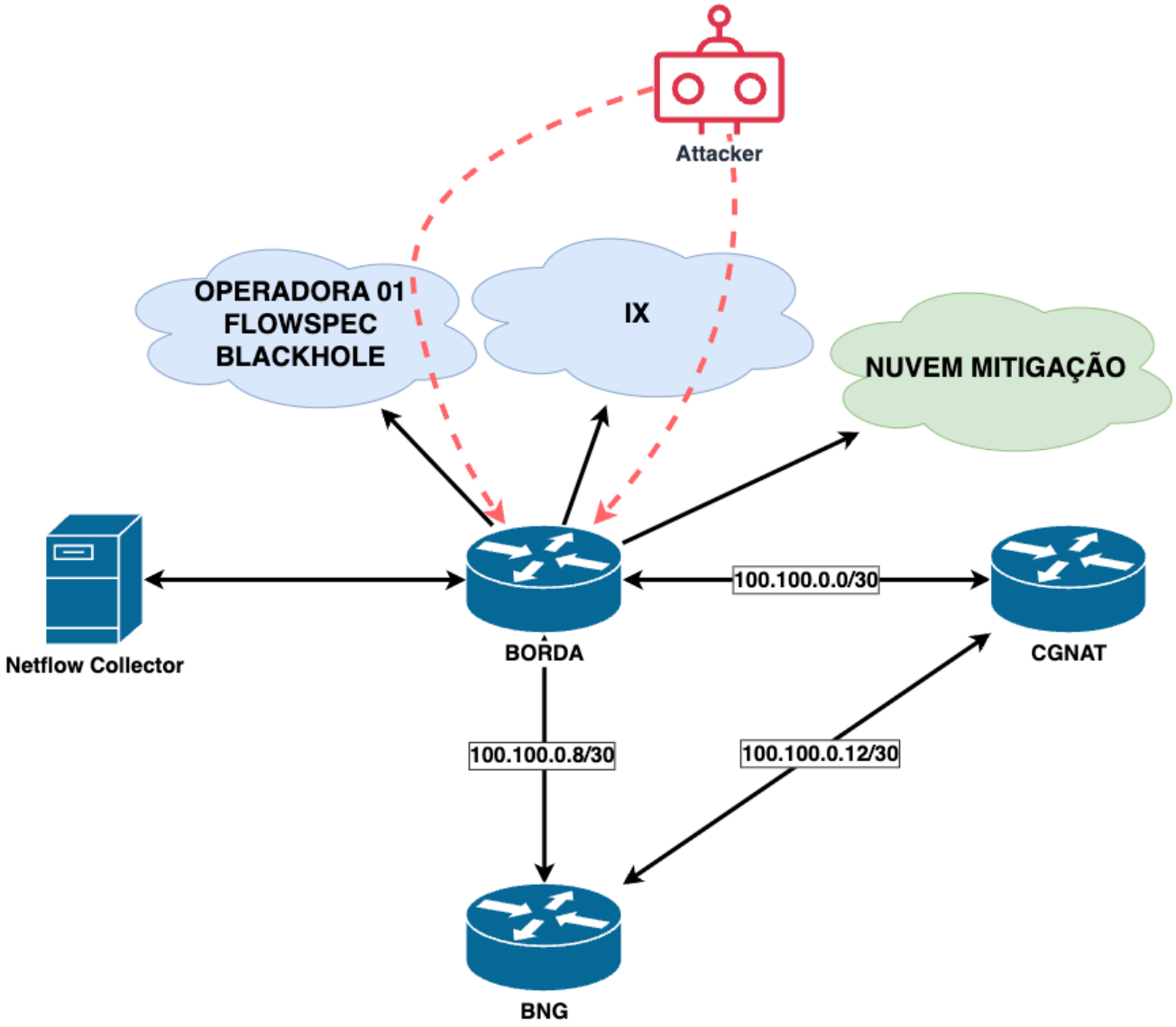
Fonte: https://www.cert.br/docs/palestras/certbr-semanacap2021.pdf

Recomendações gerais

- ***Durante o ataque***
  - *Monitore a rede com ferramentas SNMP e NetFlow;*
  - *Se o ataque estiver concentrado em poucos IP's, envie-os para blackhole;*
  - *Se possível, use bgp flowspec com as operadoras;*
  - *Se necessário, desvie todo tráfego para uma operadora de mitigação e:*
    - *Remova anúncios específicos do ATM dos IXs;*
    - *Envie apenas para peers "seguros" nos IXs (community 65001:peeras) - Communities IX;*
    - *Evite peers internacionais nos IXs;*
    - *Remova anúncios de outras operadoras que não fornecem mitigação;*
    - *Faça **rate-limit** para servidores DNS não seguros/conhecidos;*

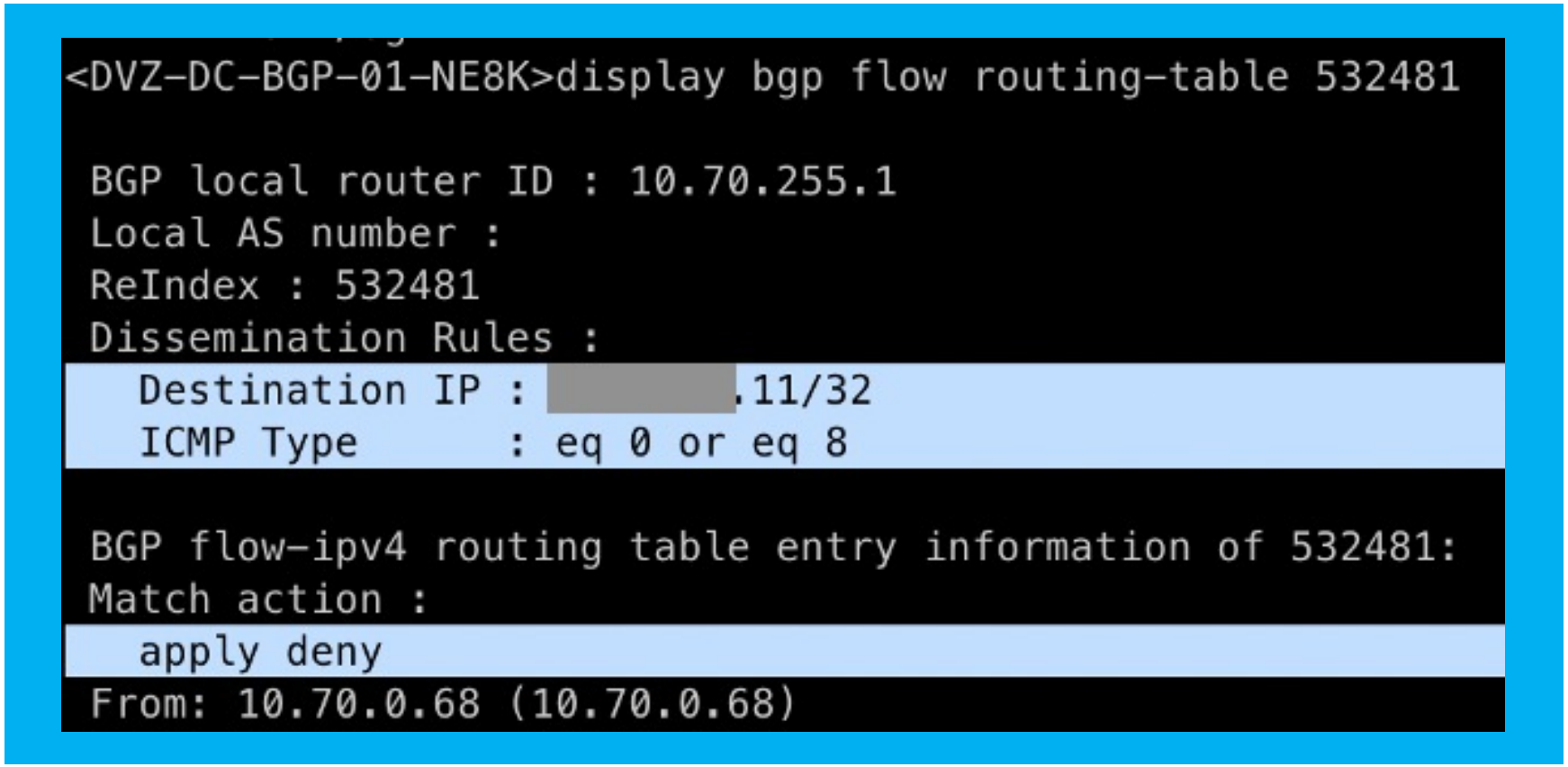
Mitigação

- Netflow collector detecta o ataque, gera as regras (blackhole, flowspec...) e envia para a **BORDA** que irá enviar as rotas atacadas para a **OPERADORA** ou para **NUVEM DE MITIGAÇÃO;**
- É possível mitigar dentro de casa, porém você precisa ter banda sobrando;



Mitigação

- Mitigação com bgp flowspec em Huawei;

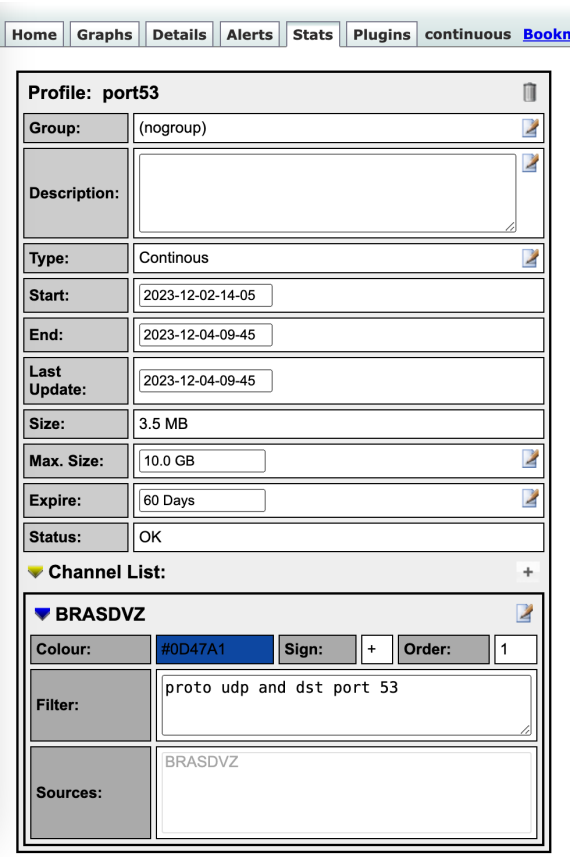


Monitoramento

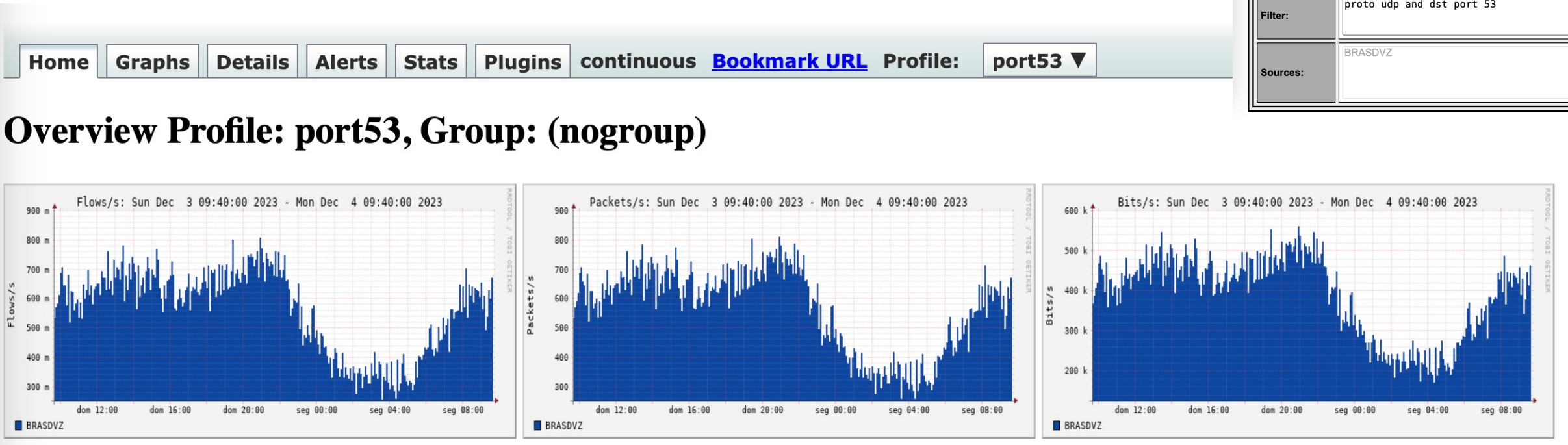
- *Entenda sua rede em detalhes!*
- *Monitore a rede com SNMP*
- *Monitore a rede com Netflow*
- *Monitore o perfil de tráfego de DNS*
  - *Quanto de tráfego de uso normal?*
  - *Quantos pacotes de uso normal?*
  - *Ajuste thresholds de DNS na ferramenta de detecção DDoS;*
- *Monitore o perfil de tráfego de porta 0*
  - *Quanto de tráfego de uso normal?*
  - *Quantos pacotes de uso normal?*
  - *Ajuste thresholds de Porta 0 na ferramenta de detecção DDoS;*

Monitoramento

Profile para monitoramento da porta 53 no NFSEN



Exemplo monitoramento perfil de tráfego porta 53 utilizando NFSEN



Sugestões para leitura

- Artigo Made4it - O que são ataques DDoS?
- Artigo Made4it - Ataques DDoS, como provedores devem se proteger?
- Artigo CERT.br - Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)
- CERT.br - Segurança para Provedores
- Artigo BPF - Marcelo Gondim - Recomendações sobre Mitigação DDoS
- Artigo BPF - Marcelo Gondim - Portas de Amplificação DDoS e Botnets
- Artigo BPF - Marcelo Gondim - Static Loop - um erro que pode matar seu ISP/ITP
- Artigo BPF - Marcelo Gondim - DNS Recursivo Anycast Hyperlocal
- Artigo BPF - Marcelo Gondim - MANRS
- Site oficial MANRS - Ações.
- BCP38 - Anti Spoofing - NIC.br

Dúvidas?

Contatos

Rafael Ganascim
www.made4it.com.br
ganascim.rafael@made4it.com.br
www.linkedin.com/in/rganascim

Gelso Baltazar
www.made4it.com.br
baltazar.gelso@made4it.com.br
www.linkedin.com/in/gelsobaltazar