2024

Analisando e contendo um ataque DDoS de amplificação DNS

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

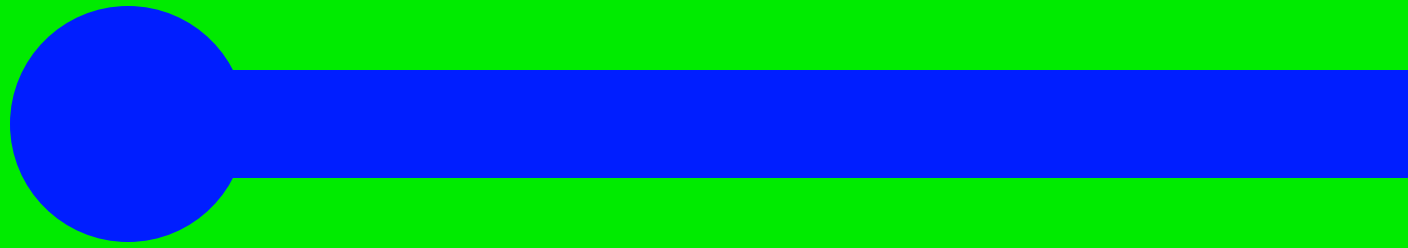
Educação, Pesquisa e Inovação em Rede

Palestrante: Antonio Silverio Montagner

PoP SC
PONTO DE PRESENÇA DA RNP SANTA CATARINA

REMEP
Florianópolis

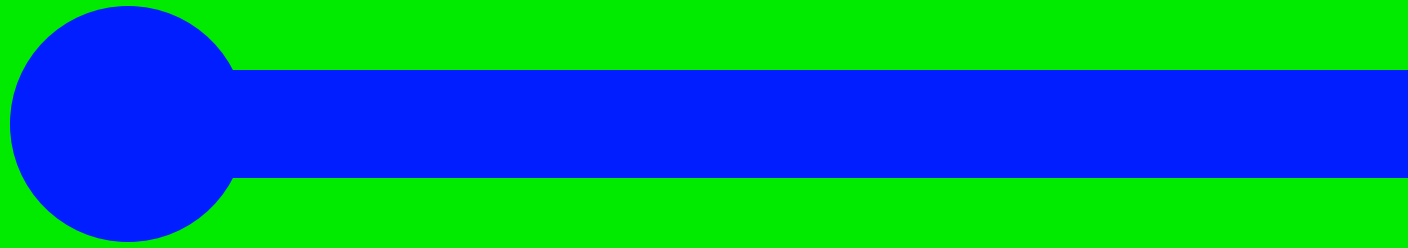
Whoami



Antonio Silverio Montagner

- Interior de SP ⇔ Florianópolis - SC
- Graduação em Ciência da Computação | UFSC
- Mestrado em andamento | UFSC
- Analista de Tecnologia da Informação | REMEP-FLN/PoP-SC/RNP
- Entusiasta em cibersegurança (since i was born)
- Algumas certificações e alguns artigos
- Café lover

Motivação



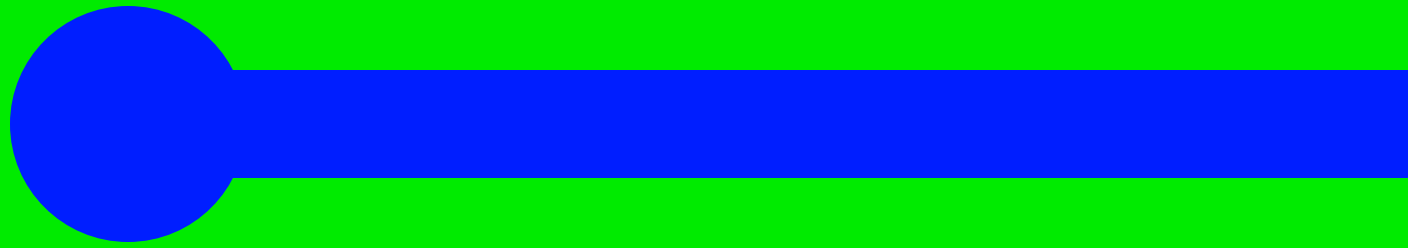
Motivação

- Características de um ataque DDoS utilizando a técnica de amplificação DNS
- Contenção do ataque
- Monitoramento do ataque
- Demonstrar uma análise dos dados coletados
- Educação e conscientização
- Incentivar a colaboração

Sumário

Sumário

DDoS



DDoS

- DDoS (Distributed Denial of Service)
  - Ataque cibernético em que múltiplos sistemas comprometidos enviam tráfego massivo para sobrecarregar um serviço ou site, tornando-o inacessível para usuários legítimos.
  - Consomem largura de banda, recursos do servidor e capacidade de resposta, deixando o serviço lento ou inoperante.
- Amplificação DNS
  - Um tipo de DDoS em que o atacante explora servidores DNS abertos para amplificar o tráfego direcionado para a vítima.
  - O atacante envia pequenas requisições DNS forjadas para servidores DNS, que respondem com respostas significativamente maior para o endereço IP da vítima, causando sobrecarga.

Os Eventos

Os Eventos : O que aconteceu, como aconteceu, a "cena do crime"

- Perfil
  - Ataque de amplificação DNS
- Fases do ataque
  - **Fase 1** (grosseria = volumetria + duração)
    - Primeiros dias
    - Mitigado com controles no acesso, borda e solução AntiDDoS no backbone
    - Entendendo o perfil do ataque...
  - **Fase 2** (já atrapalhei e continuo te perturbando)
    - Próximas semanas
    - Ataques com menor volumetria e duração, mas suficiente para degradar o enlace
    - AntiDDoS conseguia filtrar parte do ataque
  - **Fase 3** (Já posso remover as proteções?)
    - Próximos meses
    - Rajadas curtas (menor que 1m)
    - Ajustes no AntiDDoS

Análise do perfil da amplificação DNS

Análise - Sistema de Fluxos:

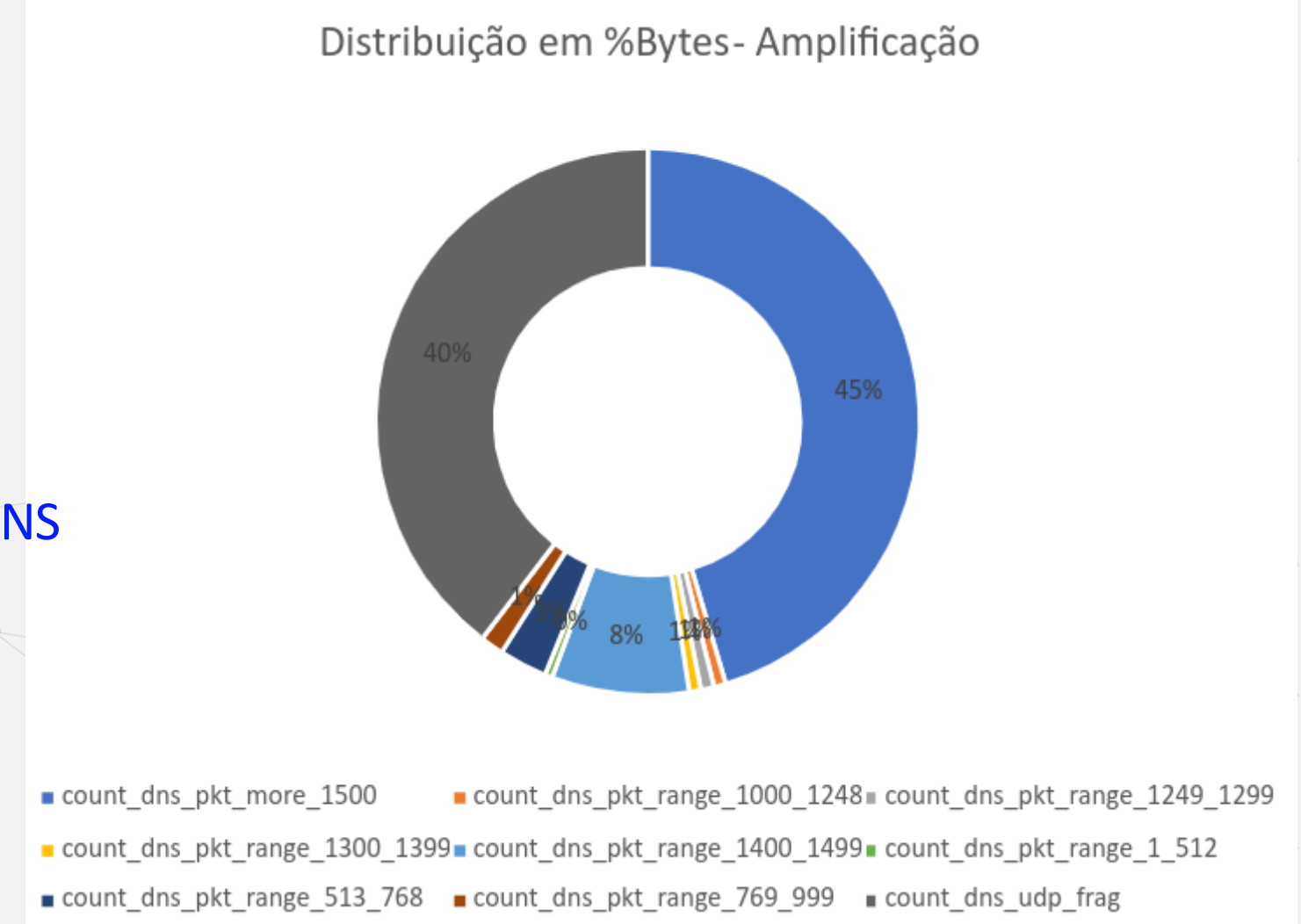
- Análise inicial através de sistema flows
- Identificou alta volumetria para:
  - Protocolo UDP
    - Porta 53 (DNS)
    - Porta 0 (Opa, fragmentação!)
  - Destino: 100% destino IP do cliente X
  - Traços de ICMP
    - (Flood icmp?)
- IPSpoofing clássico?
- Ao realizar a análise dos IPs atacantes, eram hosts respondendo a requisições DNS (inclusive recursores públicos), **BINGO --> DDoS utilizando Amplificação DNS**

Análise do perfil da amplificação DNS

Análise quantitativa até roteadores de borda:

Tráfego UDP

- ~ 45% > 1500 Bytes
  - Rede em jumbo frame
- ~ 40% UDP fragmentado
  - Porta 0 origem/destino
- ~ 8% <=512 Bytes
  - Tamanho usual de resposta DNS



Análise do perfil da amplificação DNS (2)

Análise tráfego legítimo x ataque:

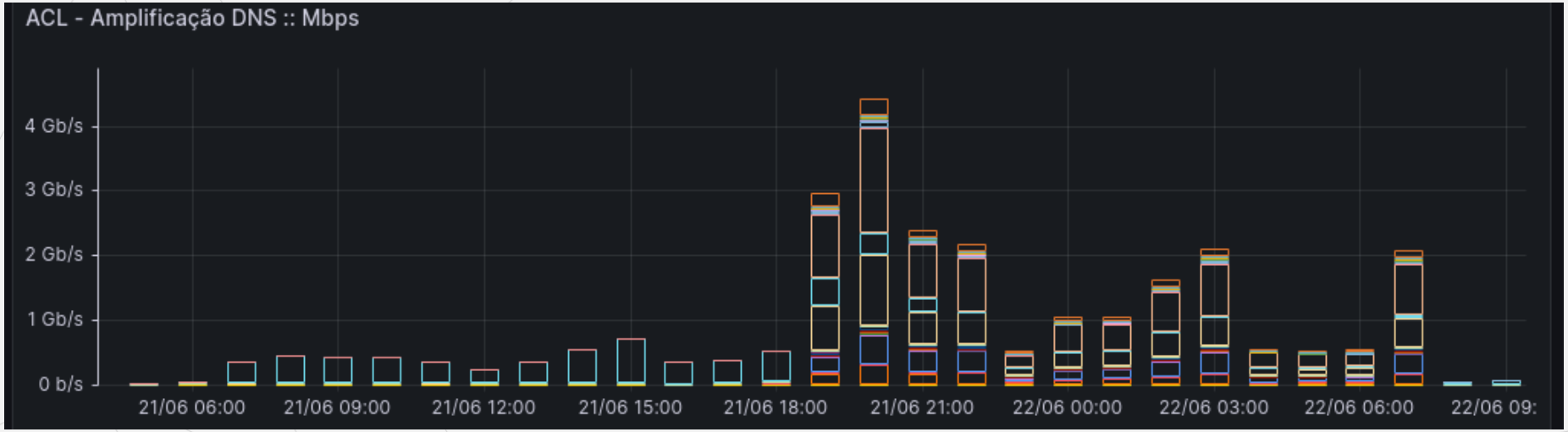
Contador - dia 07/12 - 8:30	% bytes	% pacotes	Ataque % Bytes	GB	Ação atual ACL
count_default_permit	82,75	83,25		33910,00	accept
count_dns_firewall	0,00	0,00		0,01	accept
count_dns_client_ok	0,02	0,06		6,49	accept
count_dns_pkt_more_1500	7,82	5,43	45,38	3203,64	discard
count_dns_pkt_range_1000_1248	0,12	0,11	0,70	49,55	discard
count_dns_pkt_range_1249_1299	0,14	0,11	0,79	55,95	discard
count_dns_pkt_range_1300_1399	0,12	0,09	0,69	48,67	discard
count_dns_pkt_range_1400_1499	1,41	1,00	8,17	576,84	discard
count_dns_pkt_range_1_512	0,08	0,41	0,45	31,55	discard
count_dns_pkt_range_513_768	0,49	0,77	2,85	201,33	discard
count_dns_pkt_range_769_999	0,24	0,29	1,39	98,38	discard
count_dns_recursivo_publico	0,000269771	0,001159281	0,00027	0,110543578	accept
count_dns_udp_frag	6,82	8,49	39,58	2794,27	discard
count_icmp	0,06	0,71		25,71	accept
TOTAL	**100,00**	**100,00**	**100,00**	**40976,78**	

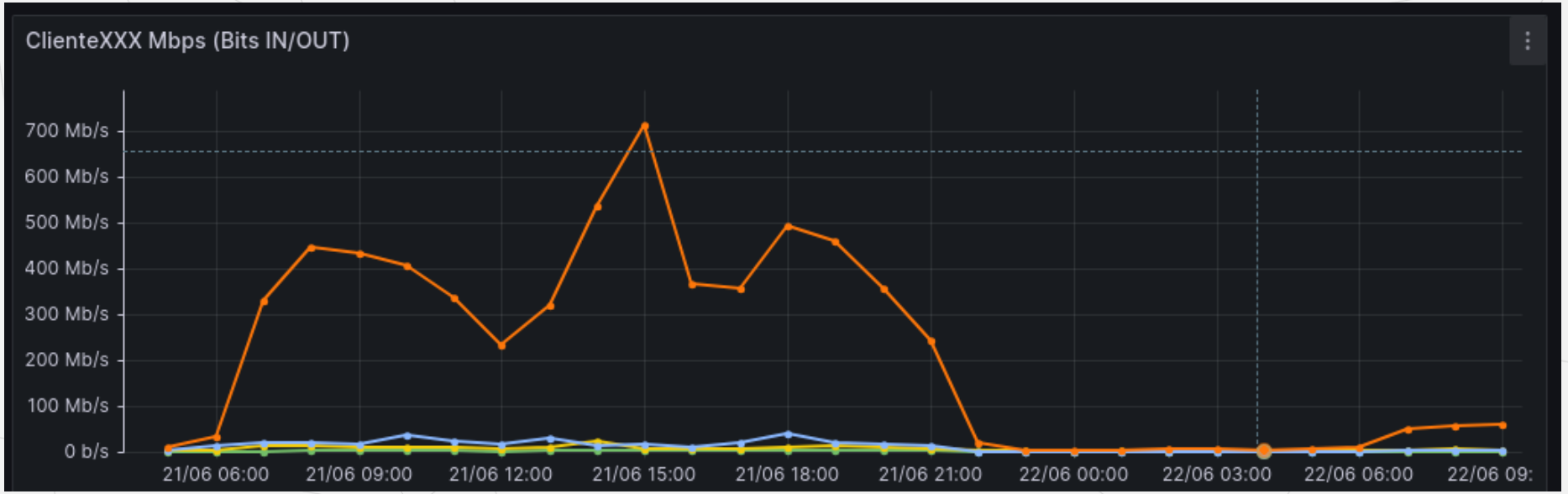
Bloqueio na borda PoP-SC (discard)

%	GB
100,00	**7060,17**

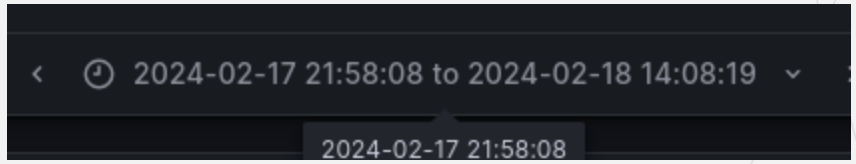
Contador - dia 07/12 - 8:30		
Total tráfego	40976,78	GB
Tráfego Ataque:	**7060,17**	GB
Tráfego entregue limpo pro Cliente:	33916,60	GB
Ataque x Tráfego Total	17,23	%

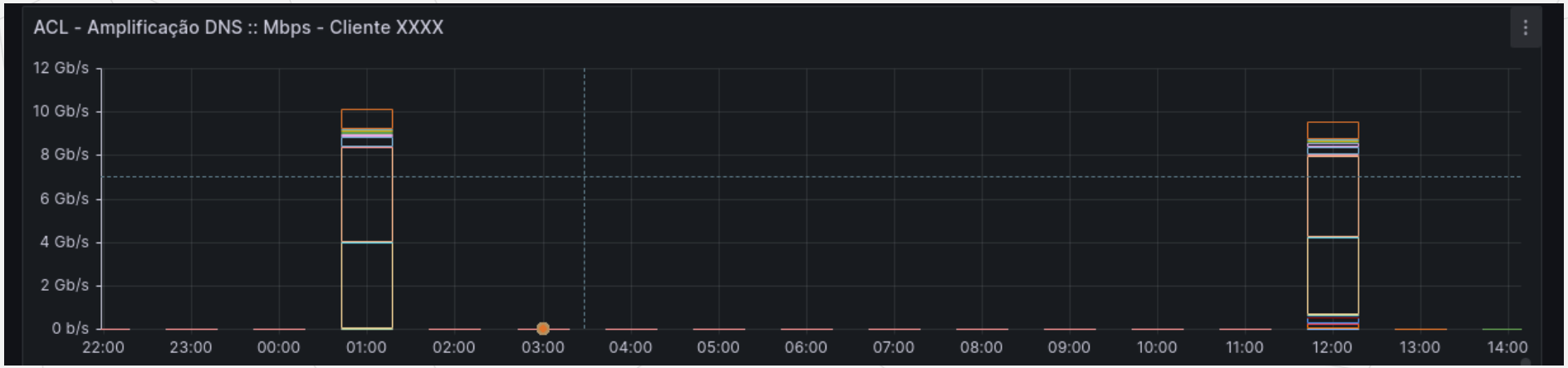
Ataque contido X Tráfego entregue no cliente



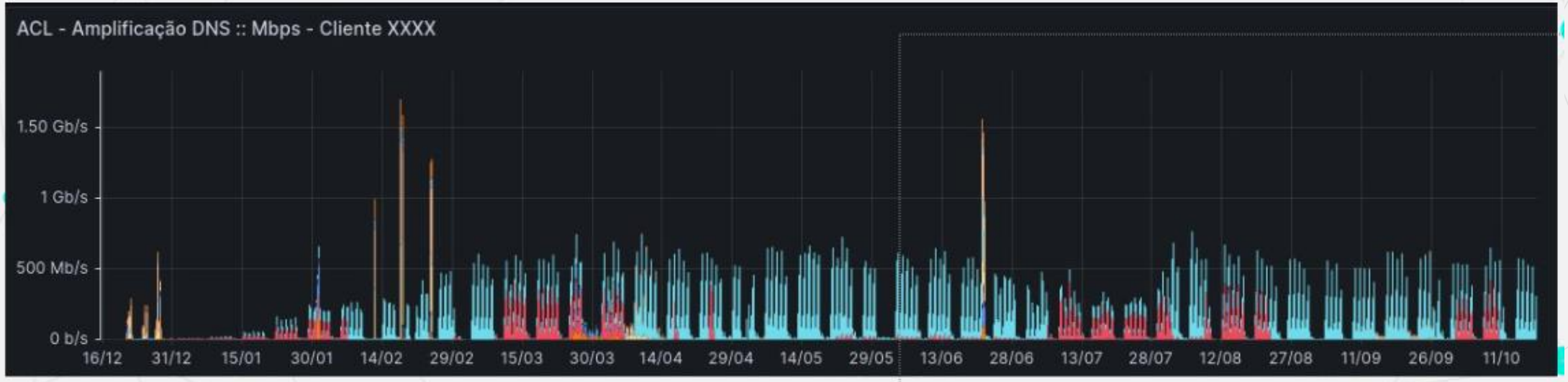


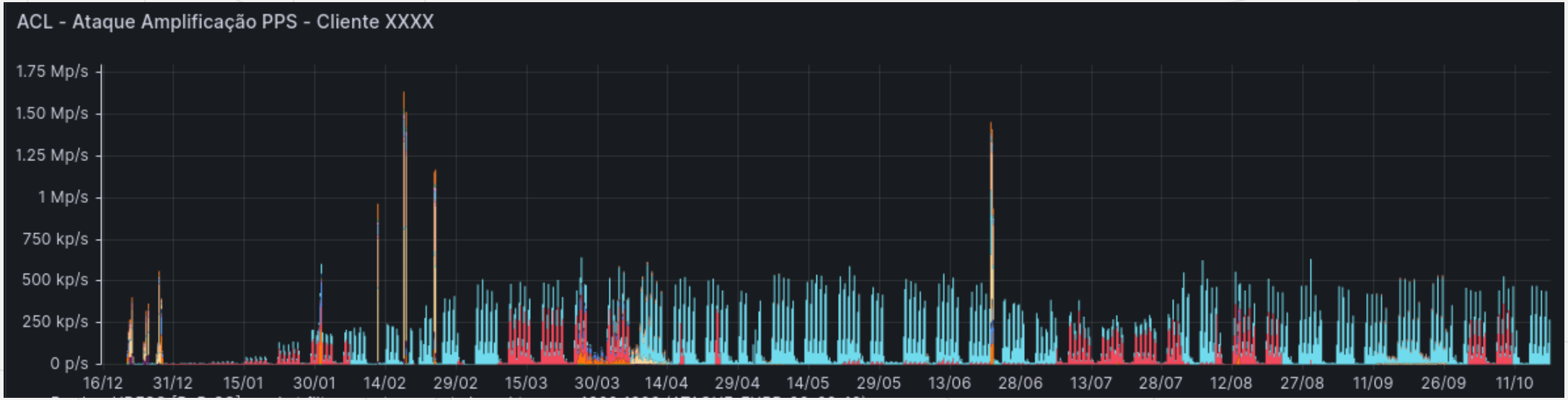
Rajadas superiores a 10Gbps





Histórico do volume e persistência do ataque





Gráficos e análises

Gráficos e análises

Como foi feito a análise?

- O trafego capturado pelo Firewall do cliente
- Scripts em Python para tratar e analisar os dados
  - Por que scripts Python?
    - Conforto com a linguagem
    - Grande quantidade de dados
- Os IPs abusados no ataque foram separados em uma lista (IPv4 e IPv6).
  - Separado em (ativos /não ativos) e DNS recursivo (habilitado/desabilitado)
- Lista de IPs foi enviado para o CENTRO DE ATENDIMENTO A INCIDENTE DE SEGURANÇA (CAIS) da RNP.

Gráficos e análises

- Dados capturados no intervalo de 10 meses.

  (dias iniciais do ataque teve mais volume, posterior foi foi mantido alguns IPs para monitoramento)

  Total de dias com ataques de volume considerável (IPv4): 84

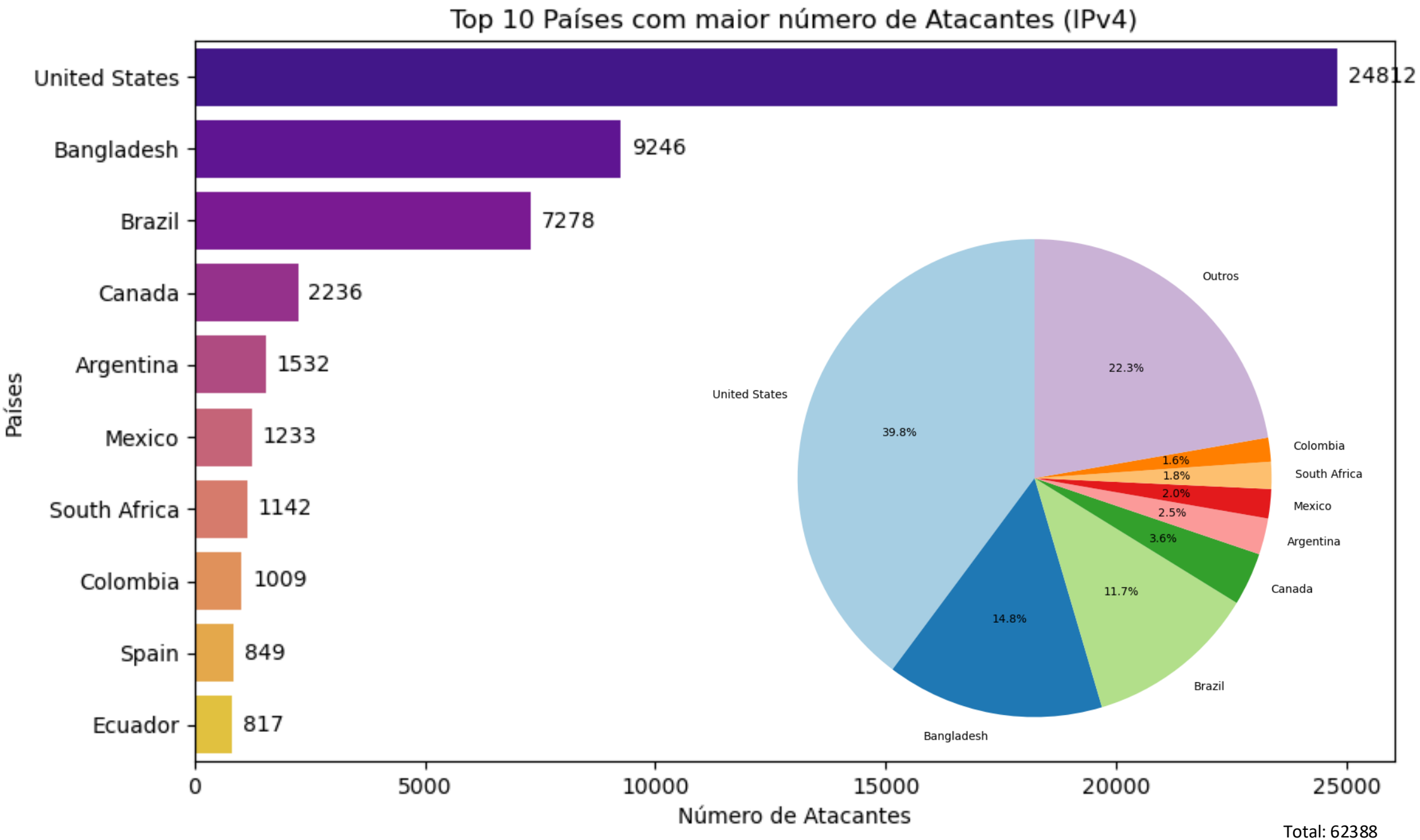
  Total de dias com ataques de volume considerável (IPv6): 71

- Total de IPs atacantes no período: 64973
  - IPv4: 62388
  - IPv6 : 2585
- Total de eventos no período: 113738024

  IPv4: 106.299.401

  IPv6: 7.438.623

- Total de países e regiões (segue a ISO 3166-1): 215 países

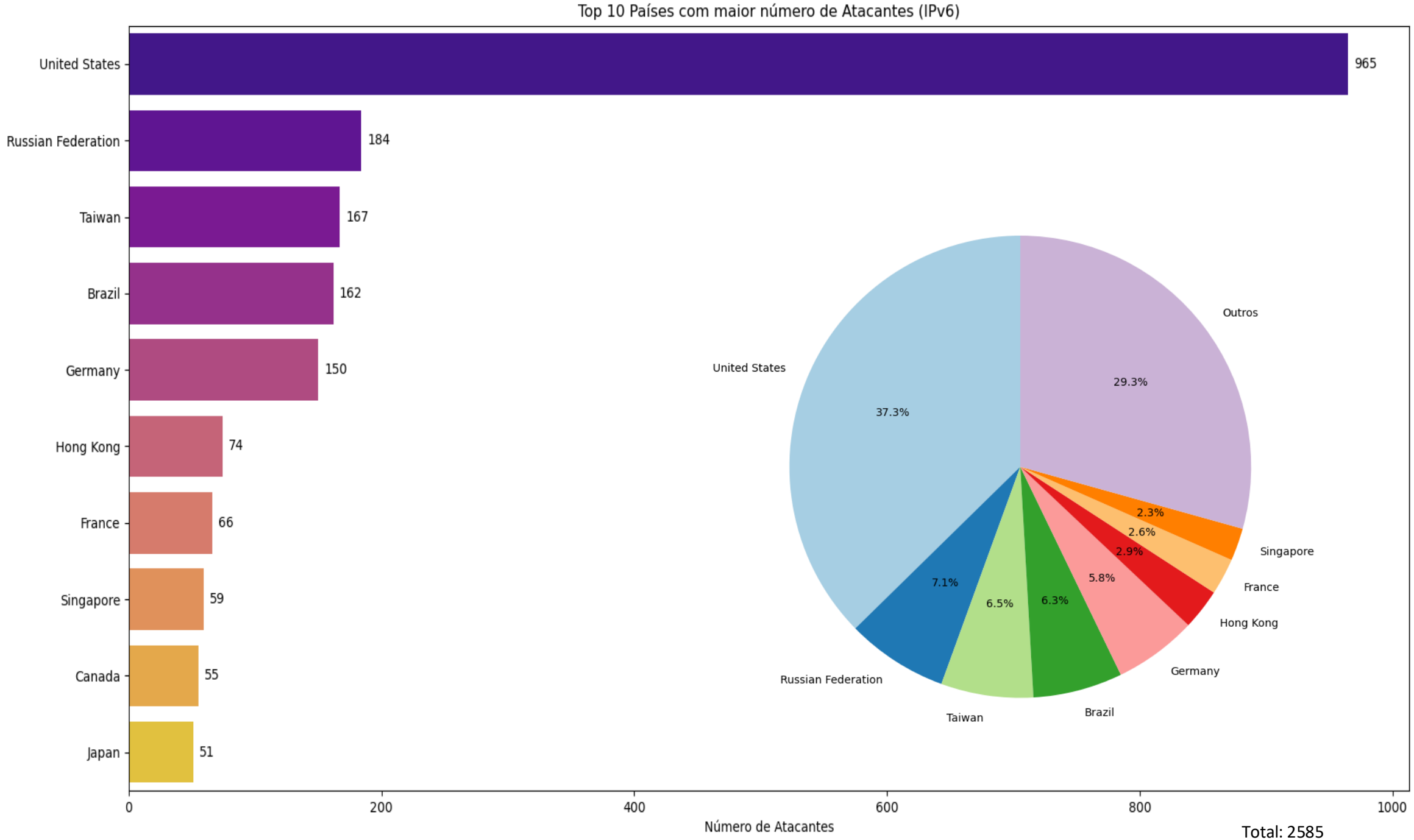

Top 10 Países com maior número de Atacantes (IPv4)
United States
Bangladesh
Brazil
Canada
Argentina
Mexico
South Africa
Colombia
Spain
Ecuador
24812
9246
7278
2236
1532
1233
1142
1009
849
817
Países
0
5000
10000
15000
20000
25000
Número de Atacantes
Outros
22.3%
United States
39.8%
Colombia
1.6%
South Africa
1.8%
Mexico
2.0%
Argentina
2.5%
Canada
3.6%
Brazil
11.7%
Bangladesh
14.8%

Total: 62388

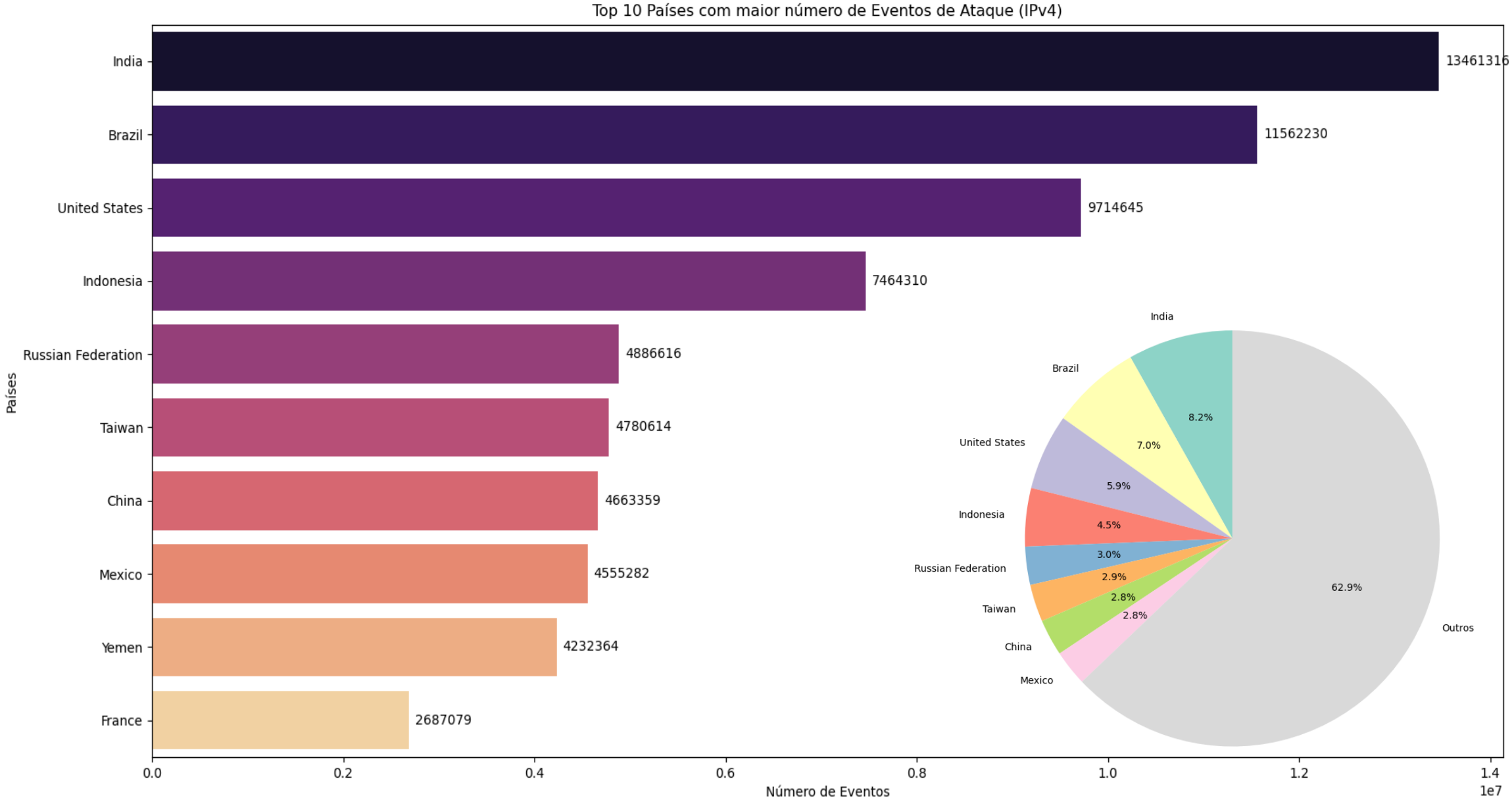
Gráficos e análises

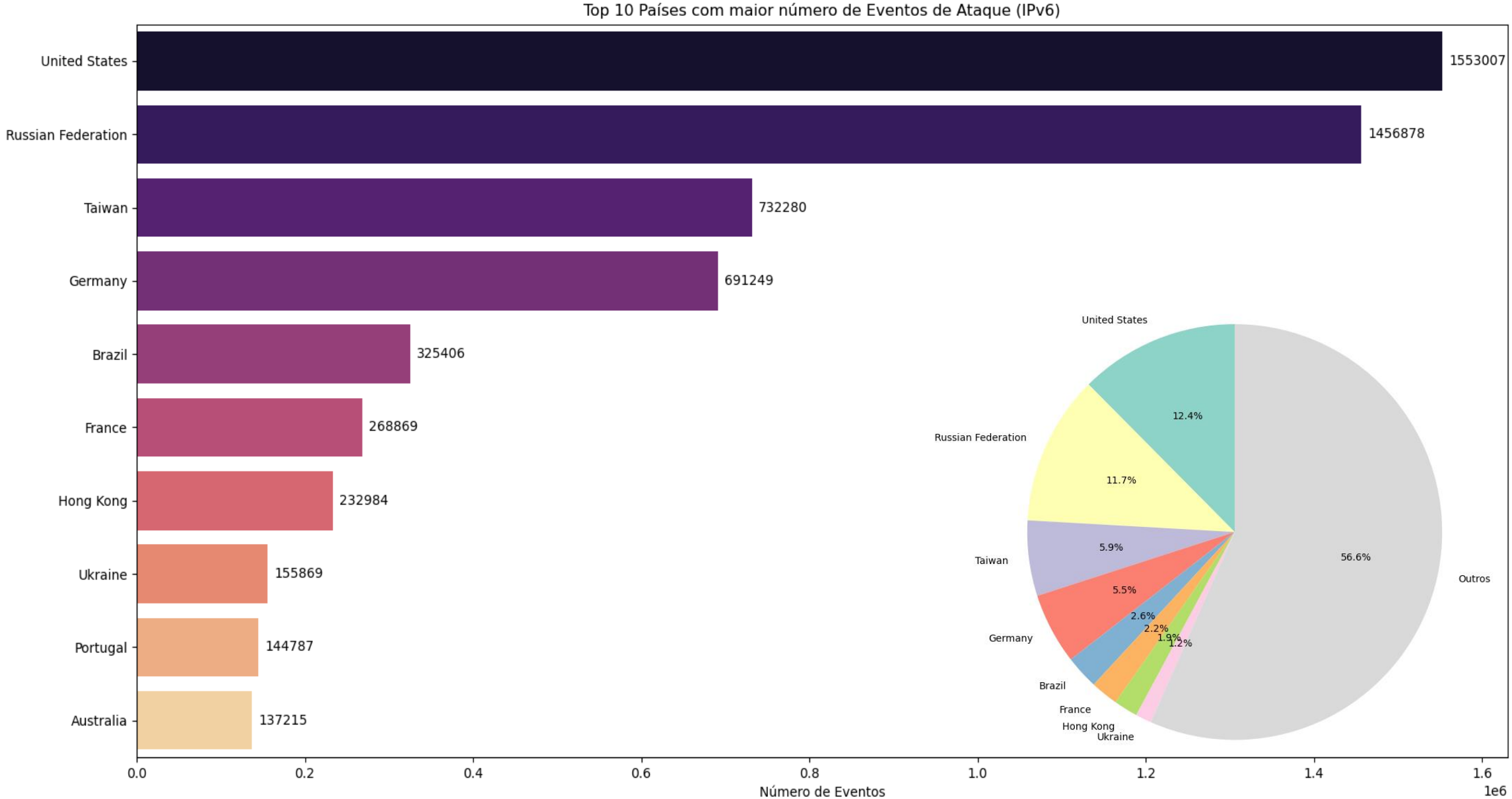
- **Quantidade de IPv4 por País do TOP 5 participantes do ataque:**
  1. **Estados Unidos** possui um total de ~1,2 bilhões de alocações IPv4 oficiais feitas pela ARIN
     - 35% do total global de 4,3 bilhões (1º no ranking global)
  2. **Bangladesh** possui um total de ~1,9 milhões de alocações IPv4 oficiais feitas pela APNIC
     - 0,08% do total global de 4,3 bilhões (72ª no ranking global)
  3. **Brasil** possui um total de ~90 milhões de alocações IPv4 oficiais feitas pela LACNIC
     - 1,39% do total global de 4,3 bilhões (7ª no ranking global)
  4. **Canada** possui um total de ~74 milhões de alocações IPv4 oficiais feitas pela ARIN
     - 2,2% do total global de 4,3 bilhões (9ª no ranking global)
  5. **Argentina** possui um total de ~19,5 milhões de alocações IPv4 oficiais feitas pela LACNIC
     - 0,26% do total global de 4,3 bilhões (26ª no ranking global)

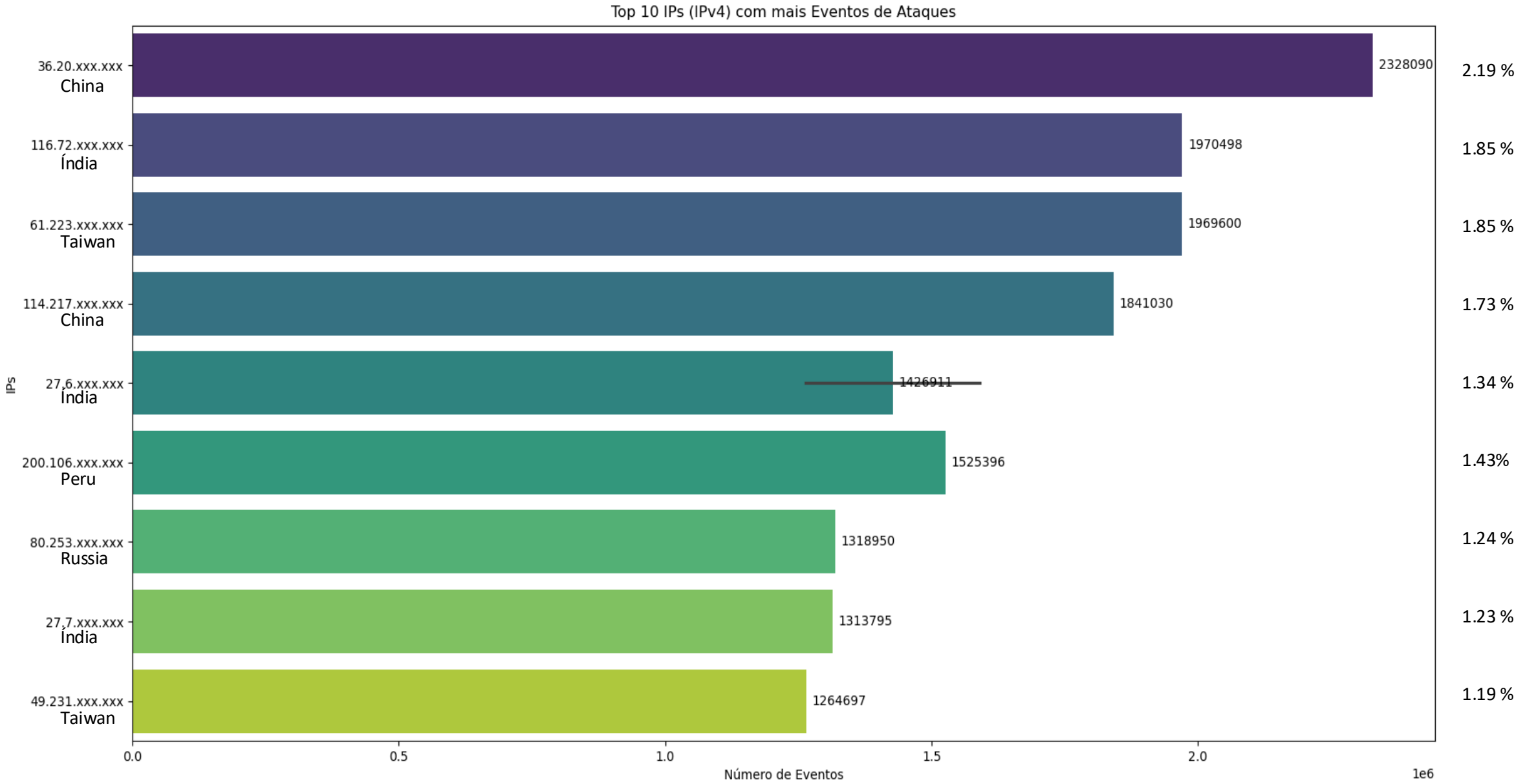
Dados de 2024- https://worldpopulationreview.com/country-rankings/ip-address-by-country


Top 10 Países com maior número de Atacantes (IPv6)
United States
Russian Federation
Taiwan
Brazil
Germany
Hong Kong
France
Singapore
Canada
Japan
965
184
167
162
150
74
66
59
55
51
0
200
400
600
800
1000
Número de Atacantes
Outros
29.3%
United States
37.3%
Singapore
2.3%
France
2.6%
Hong Kong
2.9%
Germany
5.8%
Brazil
6.3%
Taiwan
6.5%
Russian Federation
7.1%

Total: 2585


Top 10 Países com maior número de Eventos de Ataque (IPv4)
India
Brazil
United States
Indonesia
Russian Federation
Taiwan
China
Mexico
Yemen
France
13461316
11562230
9714645
7464310
4886616
4780614
4663359
4555282
4232364
2687079
Países
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
1e7
Número de Eventos
India
Brazil
United States
Indonesia
Russian Federation
Taiwan
China
Mexico
Outros
8.2%
7.0%
5.9%
4.5%
3.0%
2.9%
2.8%
2.8%
62.9%


Top 10 Países com maior número de Eventos de Ataque (IPv6)
United States
Russian Federation
Taiwan
Germany
Brazil
France
Hong Kong
Ukraine
Portugal
Australia
1553007
1456878
732280
691249
325406
268869
232984
155869
144787
137215
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
1.6
1e6
Número de Eventos
United States
12.4%
Russian Federation
11.7%
Taiwan
5.9%
Germany
5.5%
Brazil
2.6%
France
2.2%
Hong Kong
1.9%
Ukraine
1.2%
Outros
56.6%


Top 10 IPs (IPv4) com mais Eventos de Ataques
IPs
36.20.xxx.xxx
China
116.72.xxx.xxx
Índia
61.223.xxx.xxx
Taiwan
114.217.xxx.xxx
China
27.6.xxx.xxx
Índia
200.106.xxx.xxx
Peru
80.253.xxx.xxx
Russia
27.7.xxx.xxx
Índia
49.231.xxx.xxx
Taiwan
2328090
1970498
1969600
1841030
1426911
1525396
1318950
1313795
1264697
2.19 %
1.85 %
1.85 %
1.73 %
1.34 %
1.43%
1.24 %
1.23 %
1.19 %
0.0
0.5
1.0
1.5
2.0
1e6
Número de Eventos

Outros: 85.95 %

Shodan

General Information

Hostnames	[redacted].com
Domains	[redacted].COM
Country	India
City	Sambhaji Nagar
Organization	[redacted]
ISP	[redacted]
ASN	AS[redacted]

// LAST SEEN: 2024-11-16

Open Ports

53 161 7547

// 53 / UDP

-1360646303 | 2024-11-16T05:38:16.763720

```
dnsmasq-2.87
Recursion: enabled
```

// 161 / UDP

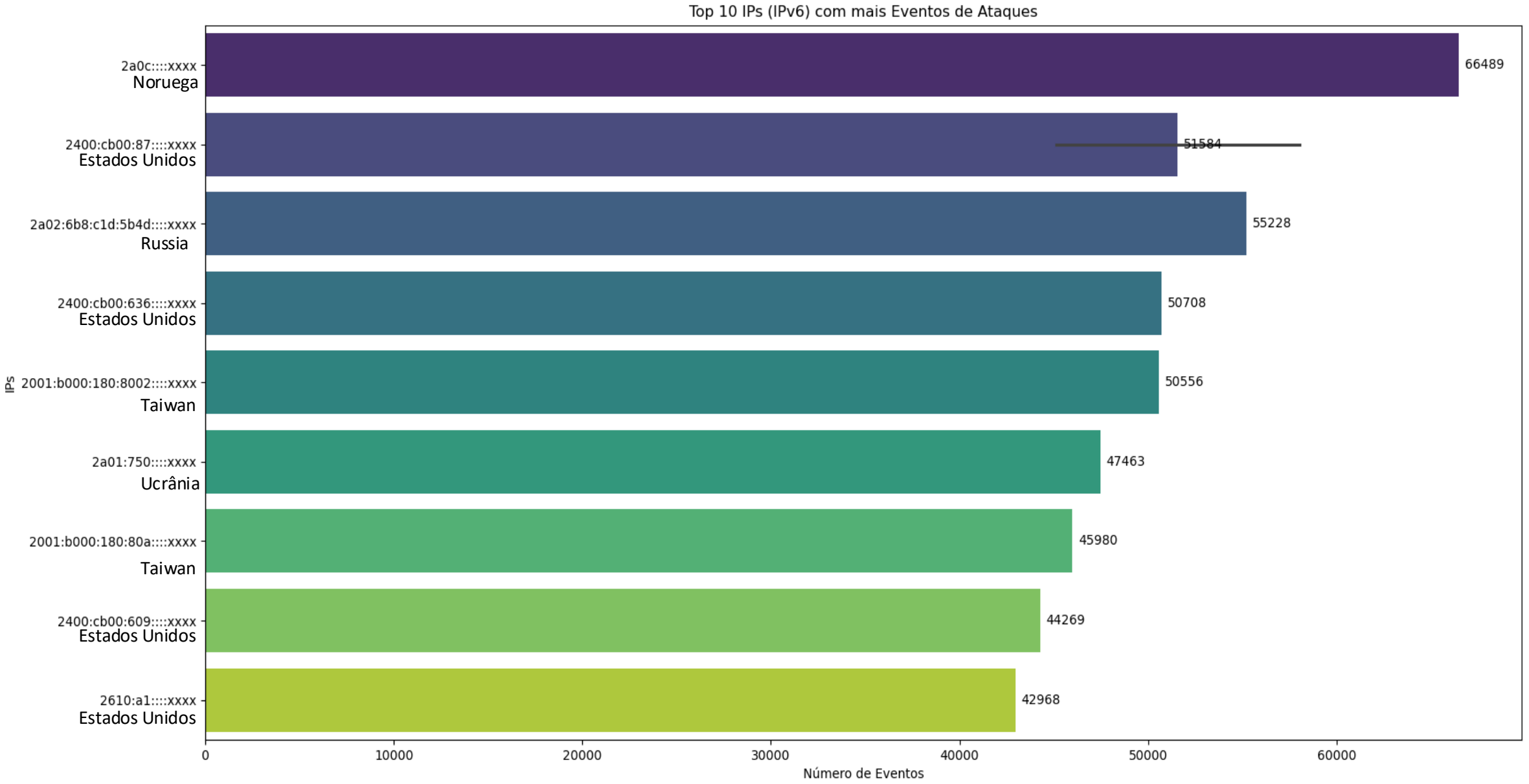
-1445766947 | 2024-11-15T12:56:34.906186

```
SNMP:
  Uptime: 15979100
  Description: System Description
  Service: 6
  Versions:
    1
  Contact: System Contact
  Location: System Location
  Objectid: 1.3.6.1.4.1.16972
  Name: EARTH-2022
```

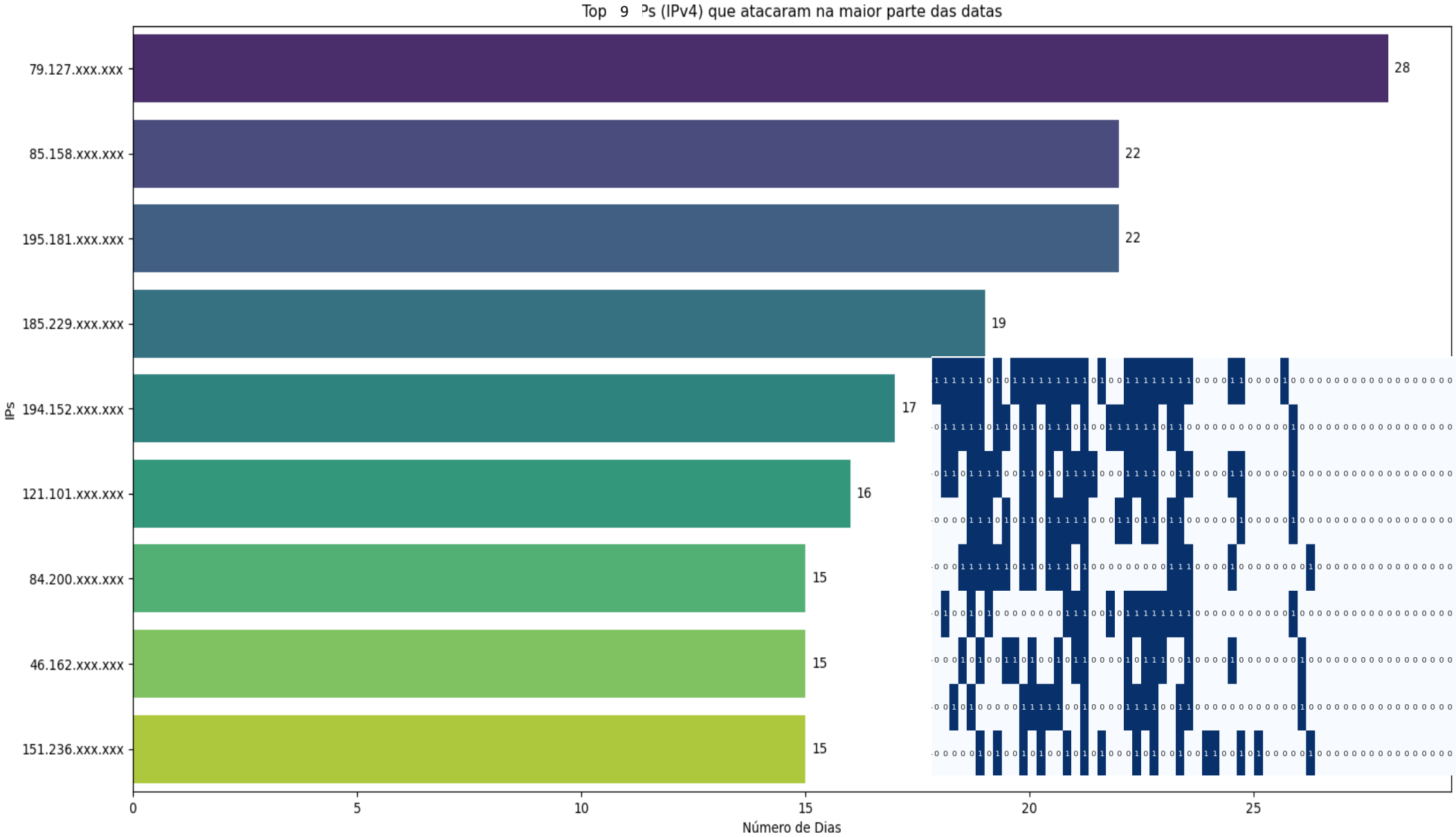
// 7547 / TCP

-2006410025 | 2024-11-13T07:04:00.946544

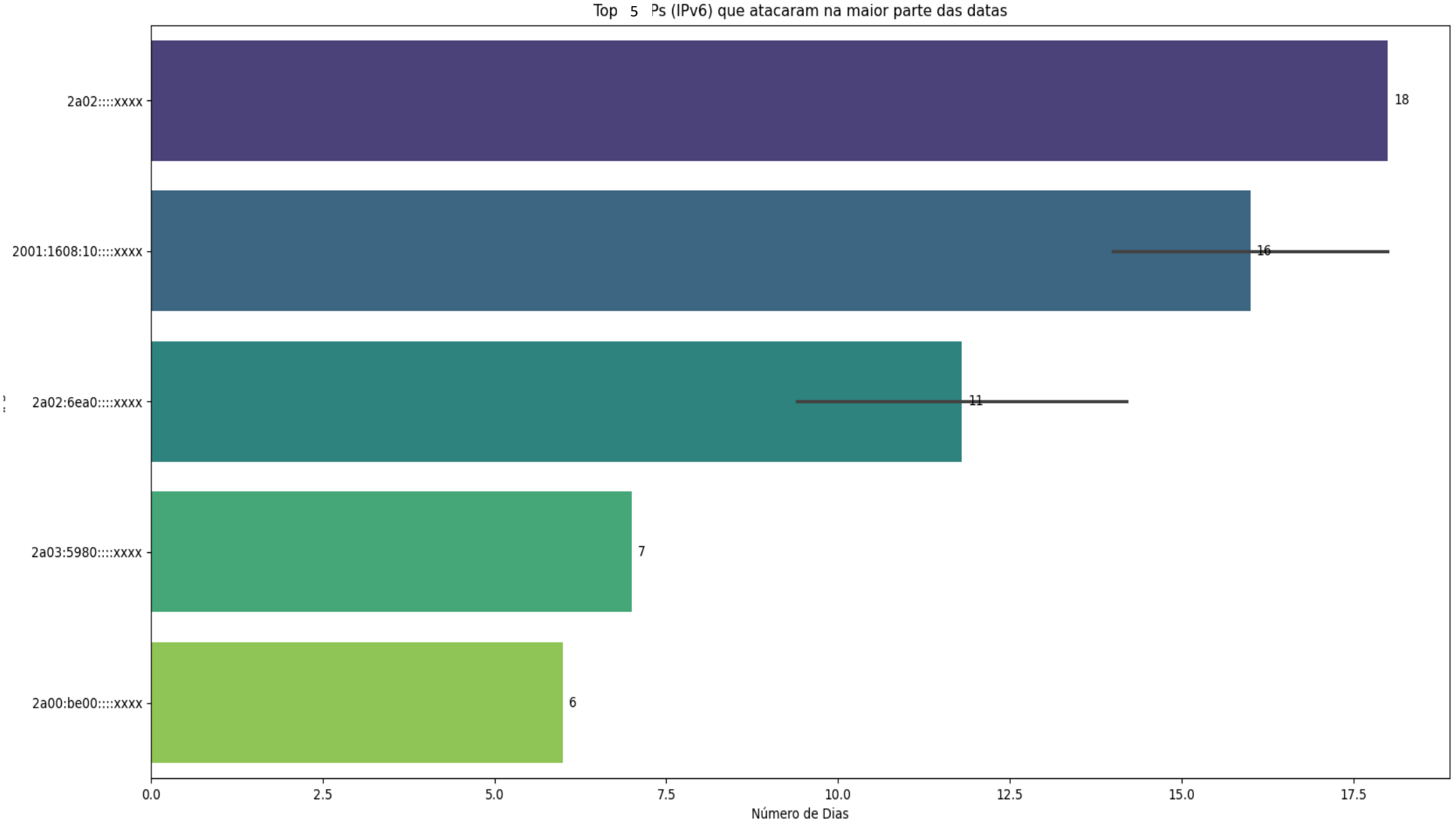
```
HTTP/1.1 404 Not Found
Server: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 460
Connection: close
```


Top 10 IPs (IPv6) com mais Eventos de Ataques
IPs
2a0c::::xxxx
Noruega
66489
0.89 %
2400:cb00:87::::xxxx
Estados Unidos
51584
0.69 %
2a02:6b8:c1d:5b4d::::xxxx
Russia
55228
0.74 %
2400:cb00:636::::xxxx
Estados Unidos
50708
0.68 %
2001:b000:180:8002::::xxxx
Taiwan
50556
0.68 %
2a01:750::::xxxx
Ucrânia
47463
0.63 %
2001:b000:180:80a::::xxxx
Taiwan
45980
0.61 %
2400:cb00:609::::xxxx
Estados Unidos
44269
0.59 %
2610:a1::::xxxx
Estados Unidos
42968
0.57 %
0
10000
20000
30000
40000
50000
60000
Número de Eventos

Outros: 93.92 %



Total de dias com ataques (IPv4): 84



Total de dias com ataques (IPv6): 71

Clientes sob a gerência do PoP-SC/RNP

Número de eventos que possuem algum vinculo com o PoP-SC (IPv4): 467

Número de eventos que possuem algum vinculo com o PoP-SC (IPv6): 207

Número de IPs IPv4 de clientes sob a gerência do PoP-SC/RNP : 5

Número de IPs IPv6 de clientes sob a gerência do PoP-SC/RNP : 2

Falsos positivos

Provável host interno da unidade infectado

Gráficos e análises

- Total de IPv4 atacantes: 62388
  - Ativos (Ping): 31430
  - 50.38%
- Total de IPv6 atacantes: 2585
  - Ativos (Ping): 1975
  - 76.40%

- Total de IPv4 atacantes: 62388
  - Respondendo DNS: 16227
  - 26.01%
- Total de IPv6 atacantes: 2585
  - Respondendo DNS: 33
  - 1.28%

Verificado em: 10/10/2024

Conclusão

Conclusão: Gráficos e análises

O que cada gráfico pode nos ajudar a entender?

- Fornecem percepções importantes sobre um ataque DDoS
- Espalhados globalmente, com uma concentração significativa em algumas regiões
- Pode ajudar a implementar bloqueios/monitoramento referente a geolocalização
- Auxílio em medidas de contenção para regiões específicas
  - Importante ter um histórico para saber quais regiões é de seu interesse
- Uso de IPv6 para ataques, mas ainda não tanto quando IPv4
- Vida útil de um host atacante
- Importante a colaboração internacional, uma vez que o ataque é "Distributed"

Conclusão

Com isso, demonstra que um tipo de ataque existente há décadas ainda é tão expressivo. Sendo importante ter profissionais treinados para responder a esse tipo de evento.

Aprendizado:

- Estar preparado para responder a esse tipo de evento e contar com as parcerias.
- Analise:
  - Analisar para ajuste nos métodos de contenção para melhor eficiência
  - Preparação para caso ocorra eventos similares
  - Ajuda para a comunidade notificando os IPs participantes
- Algumas recomendações:
  - Meios de prevenção
  - Meios de mitigação
  - Monitoramento
  - Profissionais preparados
  - Grupos de segurança/CSIRTs

Contato:

- **LinkedIn:** www.linkedin.com/in/antonio-s-montagner
- **Email:** antonio.montagner@pop-sc.rnp.br

LinkedIn

OBRIGADO(A)!

Elaborado por:
Antonio Silverio Montagner
Guilherme Eliseu Rhoden

RNP ORGANIZAÇÃO SOCIAL DO MCTI
MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

Dúvidas?