INSTITUTO DE INFORMÁTICA UFRGS

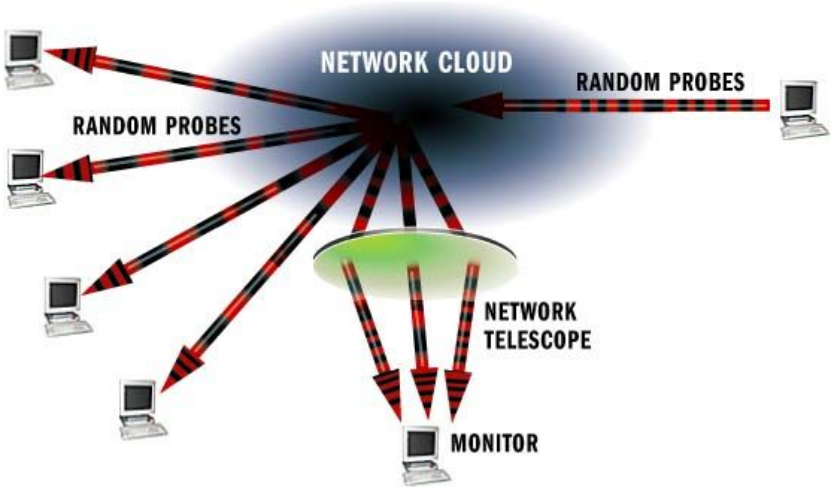
Além do tamanho: Investigando o Impacto de reduzir Network Telescopes da detecção de ameaças

Arthur Vinícius Cunha Camargo

UFRGS
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

Network Telescopes

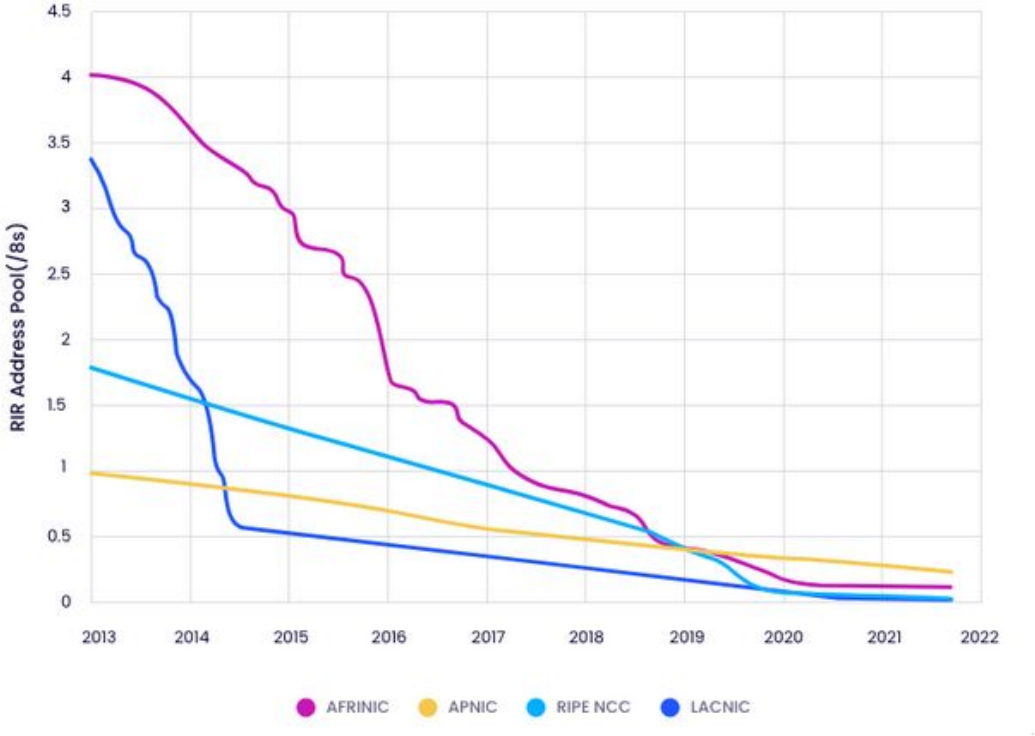
- Conceito
  - Método Passivo
  - Não Geram Tráfego
  - Simples de disponibilizar



Network Telescopes

- Ataques constantes no espaço de endereçamento IPv4
  - Scans
  - Botnets
  - Worms
  - Internet Backscatter Radiation

Situação do IPv4



Motivação

- Problemas
  - Grande utilização de endereçamentos
  - Escassez de IPv4 pode desestimular a utilização

- Objetivo
  - Diminuir o uso dos endereçamentos
  - Verificar o quanto se perde em detecção

Perguntas

- Qual a quantidade de endereços que tipicamente são utilizados em Network Telescopes ?

- Qual o impacto de reduzir o espaço de endereçamento na qualidade de detecção de ciberameaças ?

Investigando outros Telescopes

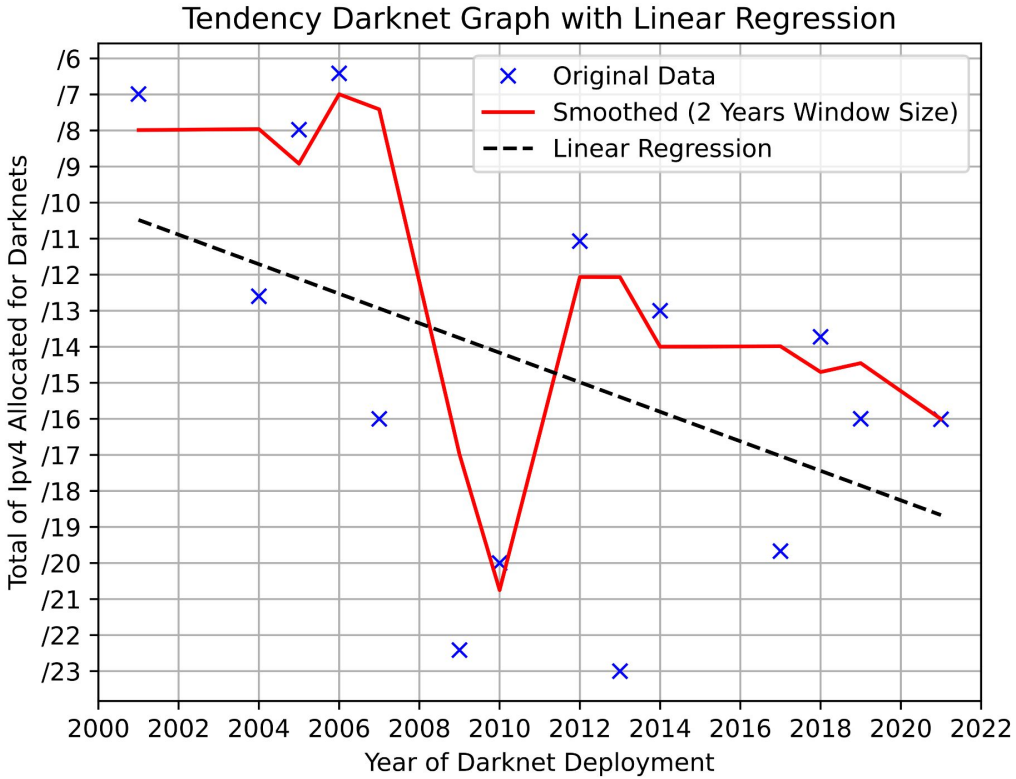
- Termos de pesquisa “Network Telescopes” OR “Darknets”
- Filtragem de 174 artigos
- 53 artigos relevantes
- 28 Network Telescopes

Resultados

IPv4 Addr.	Year	Name	Comments
50,331,648	2010	APNIC/ARIN	APNIC and ARIN collaborated on IBR research utilizing unallocated addresses 1/8, 50/8, and 107/8. This telescope had a lifespan of 1 week in 2006. (WUSTROW et al., 2010)
17,048,576	2001	Internet Motion Sensor	Arbor Networks and the University of Michigan project deploys sensors in diverse locations to enhance the diversity, sparsity, and size of a Network Telescope. The IMS initiative seems ending in 2004 and spanning into Merit Telescope. (COOKE et al., 2004b)
16,777,216	2005	MERIT	Merit Network Telescope used the 35/8 address from 2005 to 2018. After this date the Michigan University formalized the Orion telescope with a smallest address space. (Merit Network,)
16,777,216	2001	UCSD-CAIDA	The UCSD Network Telescope, a project from the University of San Diego/US was built on the globally routed 44/8 prefix (former AMPRNet) from 2001 to 2019. (CAIDA, 2024)
12,582,912	2019	UCSD-CAIDA	The UCSD Network Telescope reduced it size from a /8 to a /9 and /10 network. (CAIDA, 2024)
~2,000,000	2012	SWITCH	Collect data from the address space from multiple networks across Switzerland. (SWITCH,)
626,944	2004	Team Cymru	Multiple sensors deployed by the company Team Cymru. (CYMRU,)
524,288	2014	Farsight	Farsight's Network Telescope, now part of DomainTools, offers data through subscription. (Farsight Security,)
475,136	2018	ORION-MERIT	Michigan State University's project, known as the Observatory for Cyber-Risk Insights and Outages of Networks, focuses on Internet backscatter radiation. Designed and engineered with support from the US-NSF, it consists of 1,856 /24 subnets. (Merit Network,)

Resultados

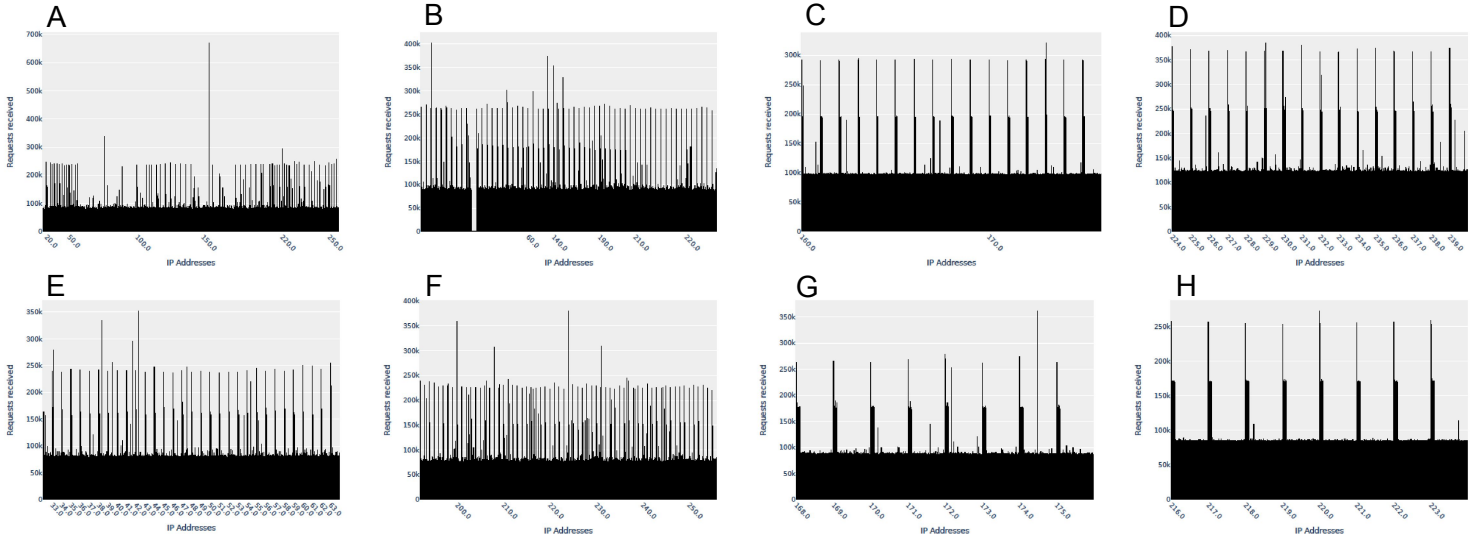
- Iniciativas novas são menores
- De uma média de um /8 para /16



Impacto na redução do Telescope

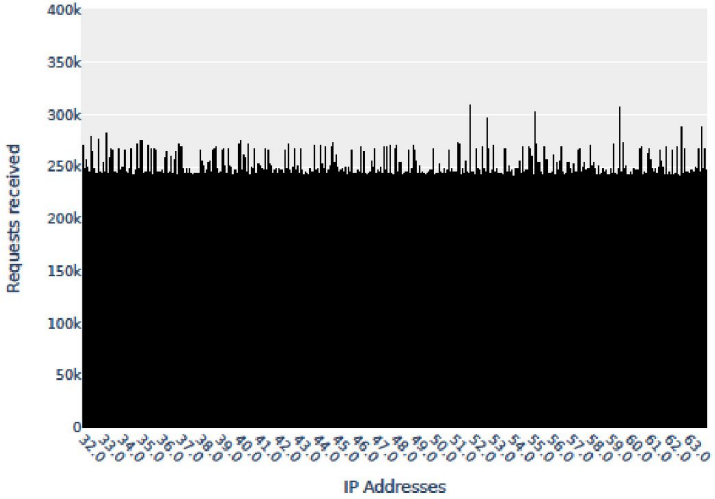
- ➔ Análise de 2 datasets NICTER-JP e Darknet-BR
- ➔ Quantidade de requisições recebidas por IPv4
- ➔ Quantidade de origens únicas por IPv4
- ➔ Análise de portas

NICTER - Distribuição de requisições IPv4

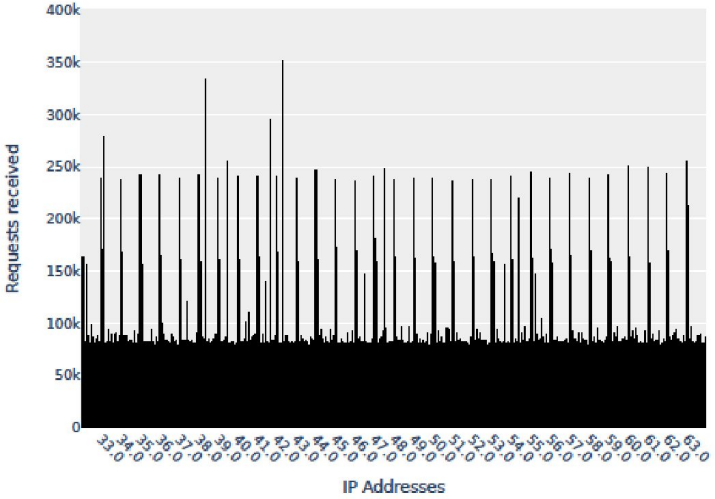


Comparação entre Telescopes

Darknet-BR



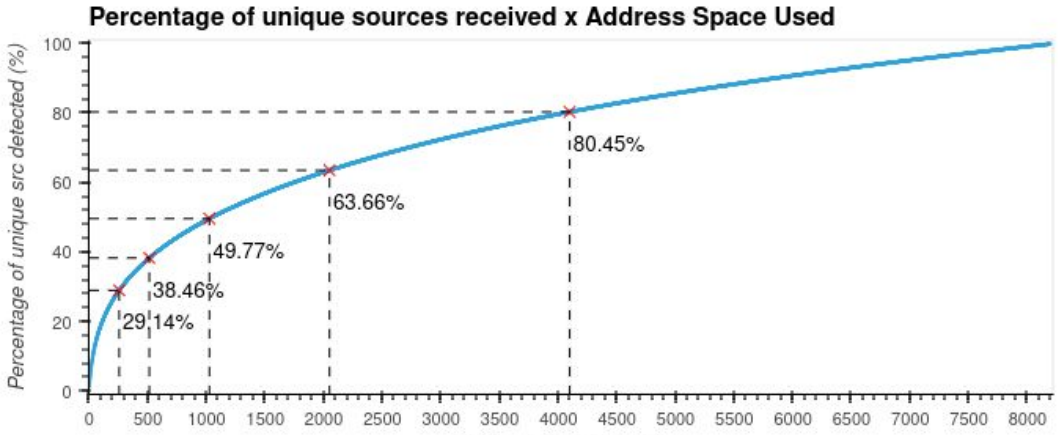
NICTER - E



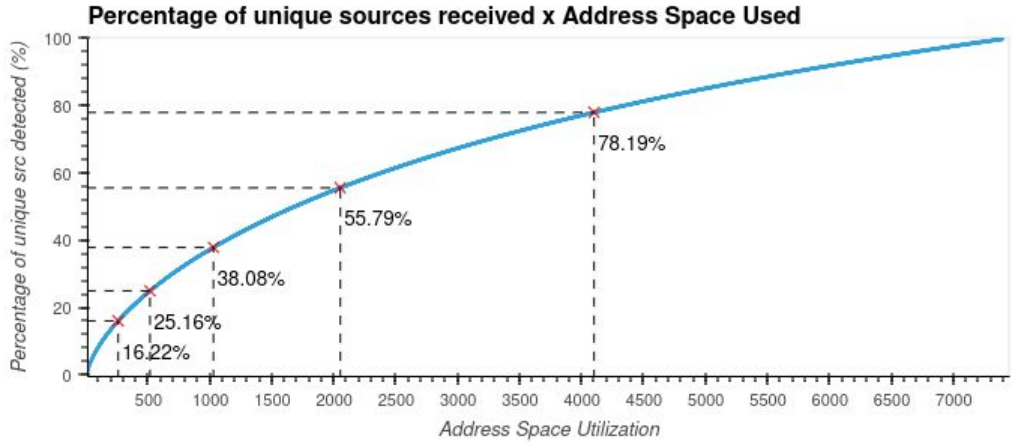
Existem valores preferíveis ?

- ➔ Número de origens únicas
- ➔ Quais tamanhos ainda nos permitem boas detecções ?
- ➔ Padrões de ataques ainda podem ser vistos ?

Darknet-BR



NICTER-E



Darknet-BR

TABLE 3 Number of unique sources and requests seem by different methods in Darknet-BR Telescope.

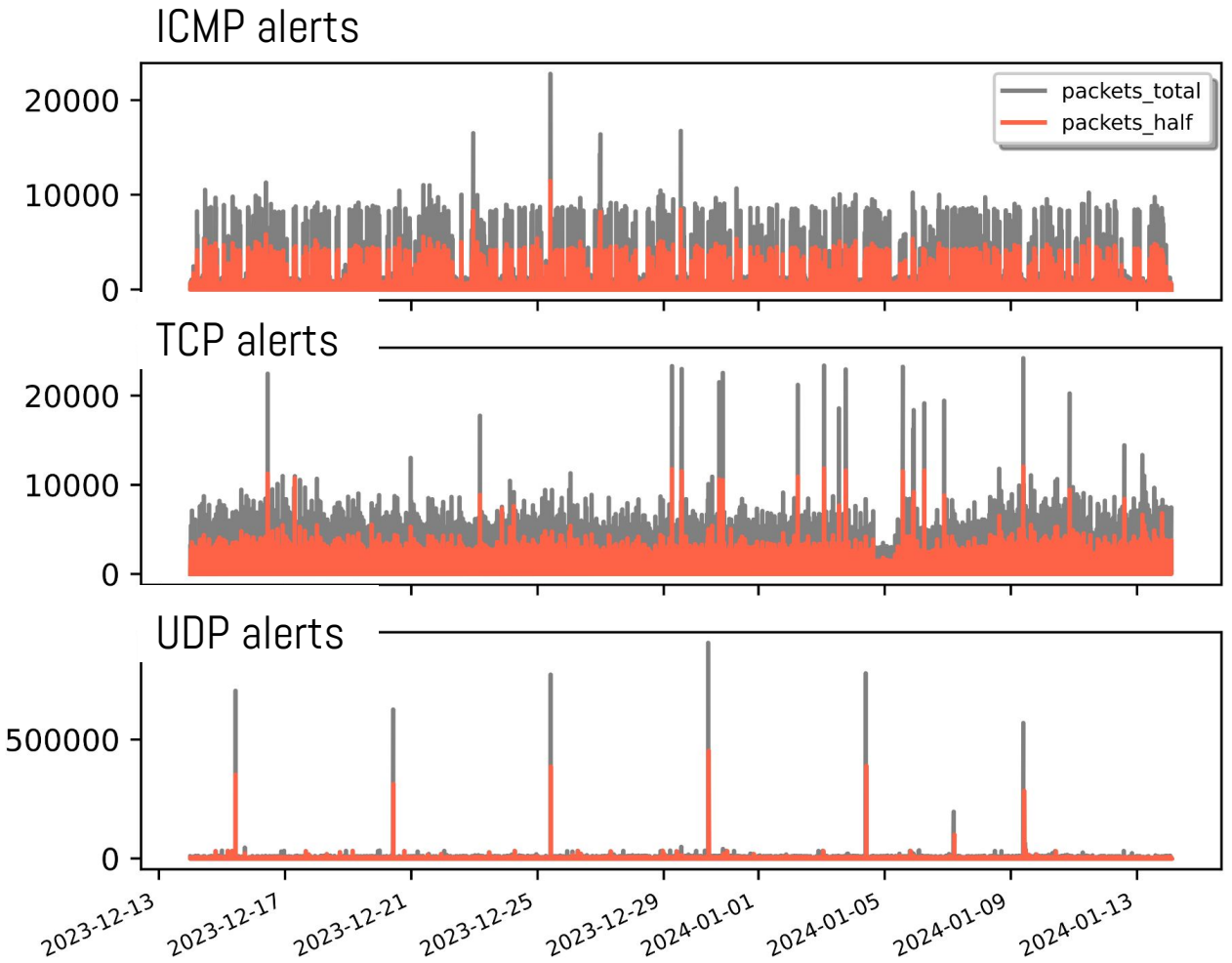
Method	Unique Sources (%)	Number requests (%)
Total	100.00	100.00
Low /20	80.30	50.03
High /20	80.26	49.97
Even /24 allocation	80.26	50.01
Odd /24 allocation	80.39	49.99

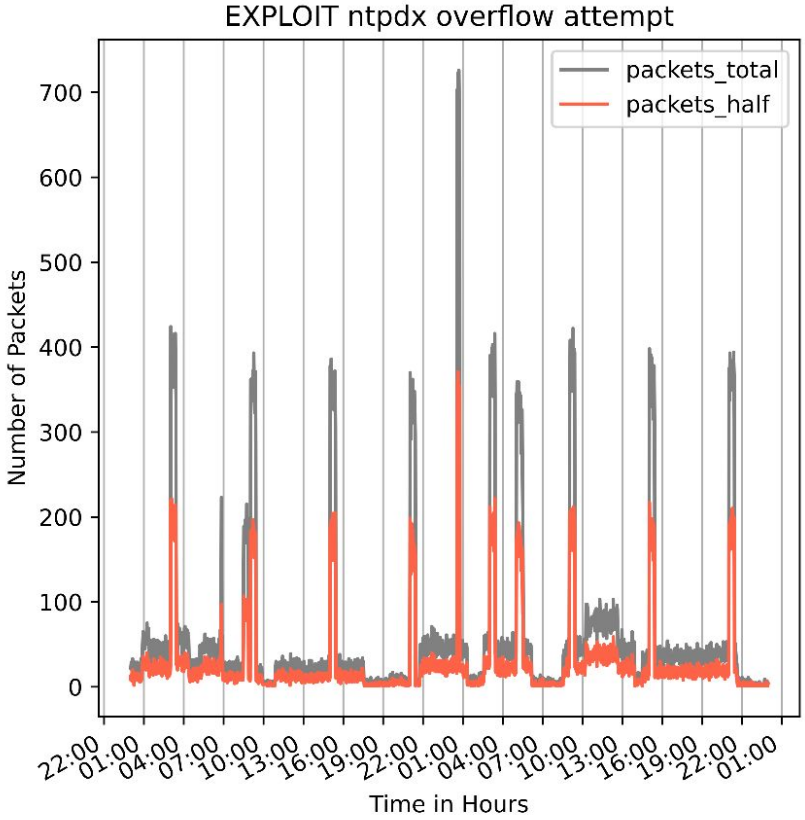
NICTER-E

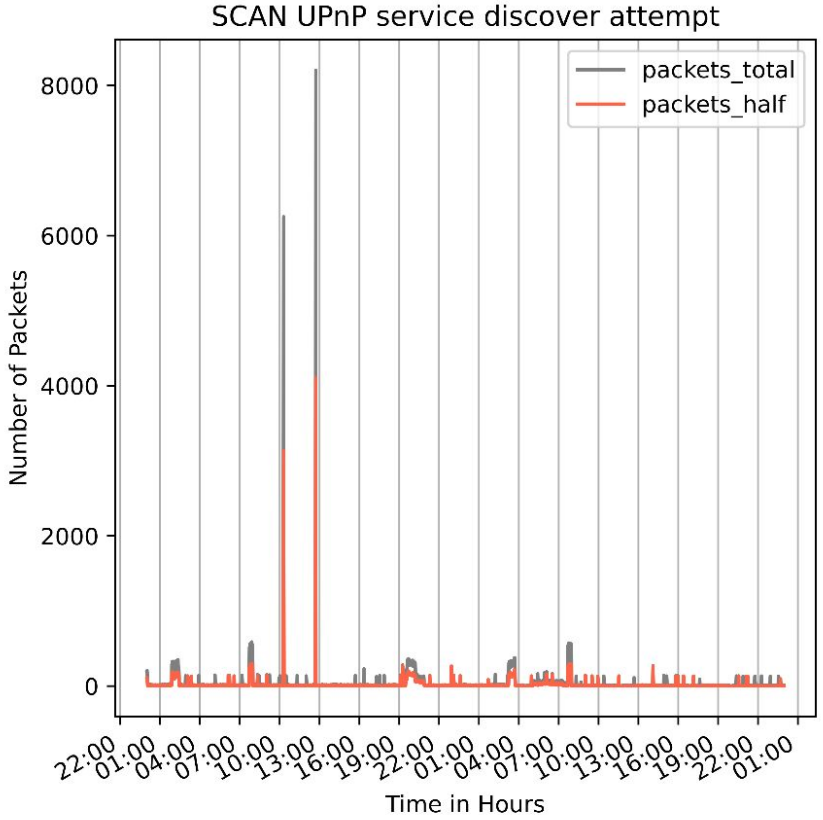
TABLE 4 Number of unique sources and requests seem by different methods in NICTER Telescope.

Method	Unique Sources (%)	Number requests (%)
Total	100.00	100.00
Low /20	74.73	50.01
High /20	74.46	49.98
Even /24 allocation	74.74	49.97
Odd /24 allocation	74.46	50.02

Alerts


ICMP alerts
packets_total
packets_half
20000
10000
0
TCP alerts
20000
10000
0
UDP alerts
500000
0
2023-12-13
2023-12-17
2023-12-21
2023-12-25
2023-12-29
2024-01-01
2024-01-05
2024-01-09
2024-01-13


EXPLOIT ntpdx overflow attempt
packets_total
packets_half
Number of Packets
0
100
200
300
400
500
600
700
22:00
01:00
04:00
07:00
10:00
13:00
16:00
19:00
22:00
01:00
04:00
07:00
10:00
13:00
16:00
19:00
22:00
01:00
Time in Hours


SCAN UPnP service discover attempt
packets_total
packets_half
Number of Packets
0
2000
4000
6000
8000
22:00
01:00
04:00
07:00
10:00
13:00
16:00
19:00
22:00
01:00
04:00
07:00
10:00
13:00
16:00
19:00
22:00
01:00
Time in Hours

Conclusão

- Reduzir na metade ainda permite ver 80% das origens
- Os métodos de amostragem não fizeram muita diferença
- Ainda é possível verificar padrões de ataques porém, em menor escala

E o IPv6 ?

Obrigado!

INSTITUTO DE INFORMÁTICA UFRGS

UFRGS UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL