

Spoofers

Délio Alves A94557
Diogo Miranda A100839
João Rodrigues A100598

Índice

01

O que é o Spoofer?

02

Importância do Spoofer

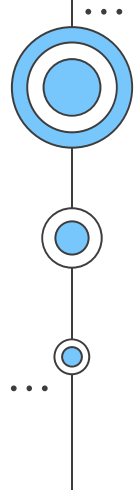
03

Metodologia utilizada

04

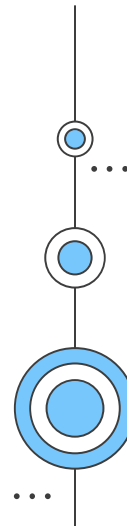
Resultados





01

O que é o Spoofer



O que é o Spoofer?



Projeto desenvolvido pela
organização CAIDA

Fundada em 1997, o Centro de Análise de Dados da Internet Aplicada (CAIDA) realiza pesquisas de rede e constrói infraestruturas de pesquisa para apoiar a coleta, curadoria e distribuição de dados em larga escala para a comunidade científica de pesquisa.



O que é o Spoofer?

-O Spoofing é a prática de mascarar ou falsificar informações de indentificação, como o endereço IP, de modo a enganar sistemas, dispositivos ou utilizadores;

-O Spoofer é um projeto de pesquisa e desenvolvimento focado em compreender e mitigar estes ataques de Spoofing na internet;

-Visa o desenvolvimento de métodos para detetar, prevenir e atenuar estes ataques;

-Tem como objetivo criar um ambiente online mais seguro e confiável, para todos os utilizadores da internet;

...

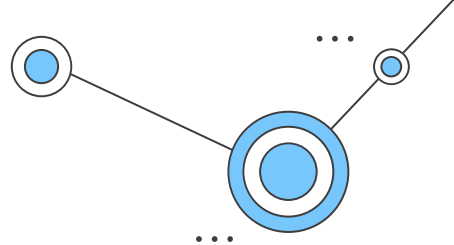


02

Importância do Spoofer



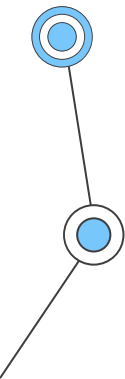
Importância do Spoofer



A vulnerabilidade que o protocolo TCP/IP apresenta a ataques de Spoofing permite que os mesmos sejam facilmente escaláveis e persistentes. Apesar de anos de grandes esforços para a prevenção destes ataques, novos ataques deste tipo continuam a surgir, incluindo contra arquiteturas DNS.

- As limitações apresentadas pelos mecanismos atuais reforçam a necessidade do desenvolvimento de novos métodos para prevenir e mitigar estes ataques.

Desta forma nasceu o projeto Spoofer.



Importância do Spoofer

NEWS AND ANNOUNCEMENTS

CAIDA Spoofer Project Improves Routing Security by Publicizing Spoofed Source Address Packets

By Megan Kruse • 9 May 2018

BGP

CAIDA

-Notícia do site Manrs sobre o projeto Spoofer

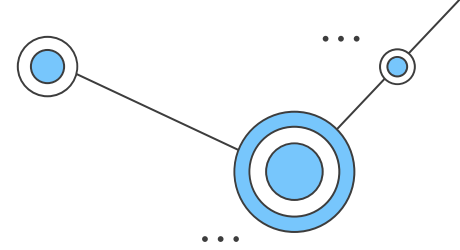


03

Metodologia utilizada



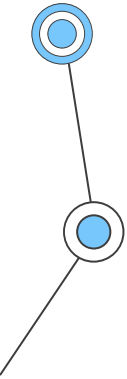
Metodologia utilizada

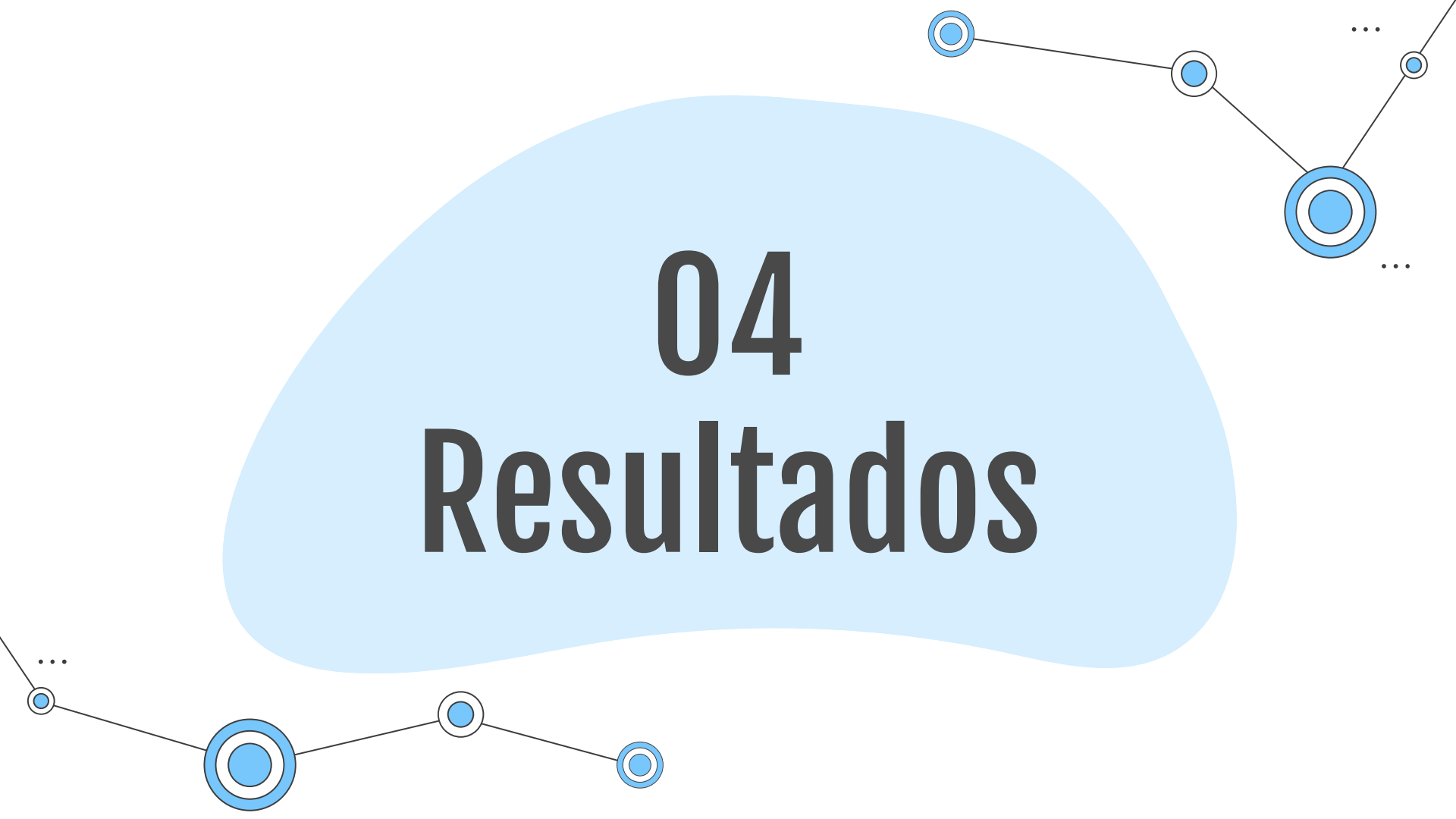


O programa spoofer envia uma série de pacotes UDP falsificados para servidores distribuídos em todo o mundo.

Esses pacotes são projetados para testar:

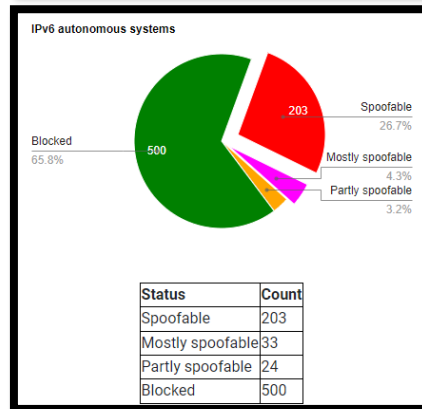
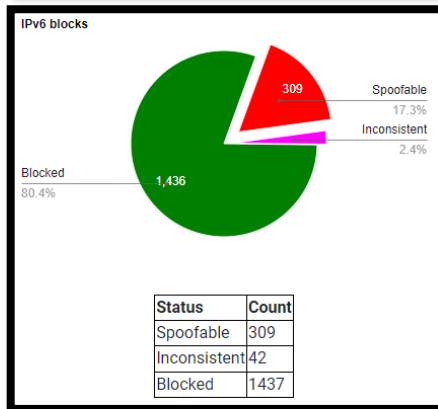
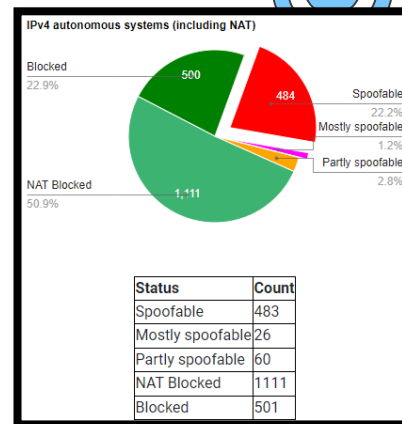
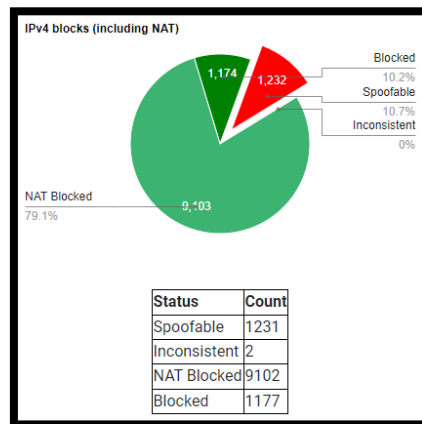
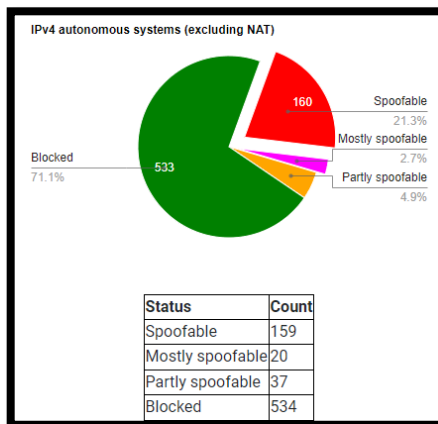
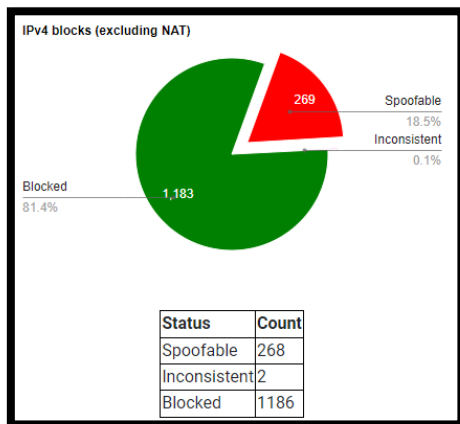
- Diferentes classes de endereços IPv4 e IPv6 falsificados, incluindo privados e encaminháveis.
- Capacidade de fazer Spoofing a endereços vizinhos e adjacentes
- Capacidade de fazer Spoofing de pacotes de entrada (em direção ao cliente) e de saída (do cliente)
- Onde ao longo do caminho é observada filtragem
- Presença de um dispositivo NAT ao longo do caminho



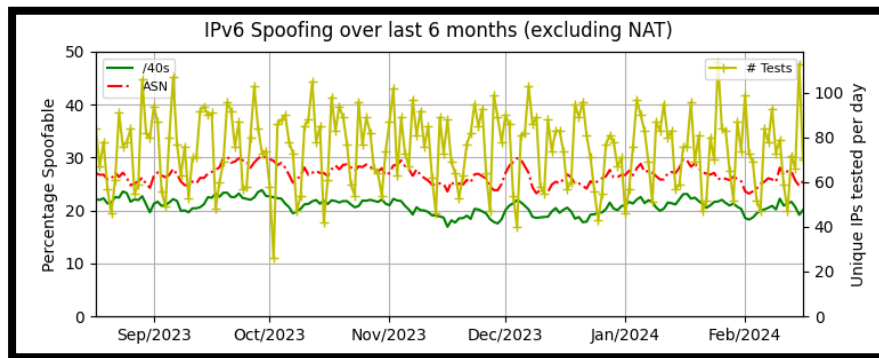
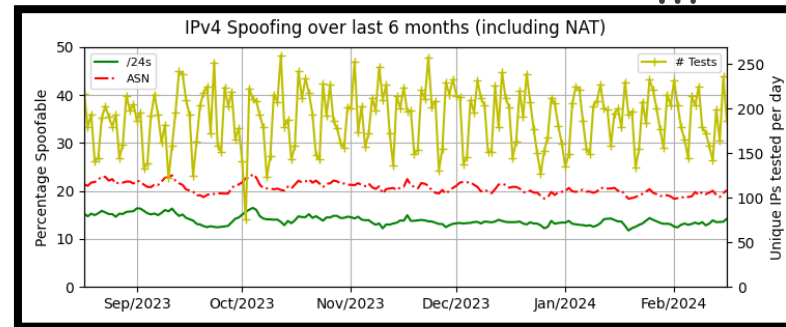
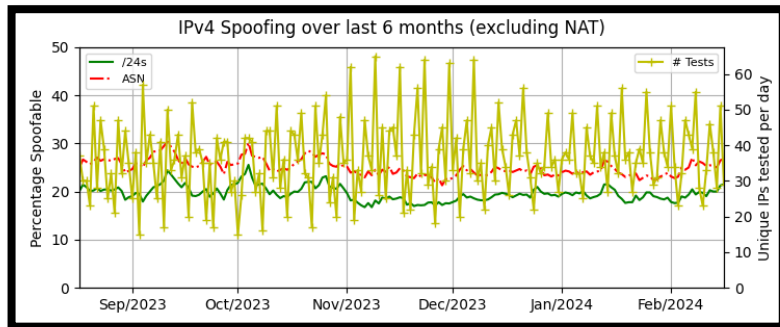


04 Resultados

Resumo do último ano



Resumo de spoofing observado nos últimos 6 meses

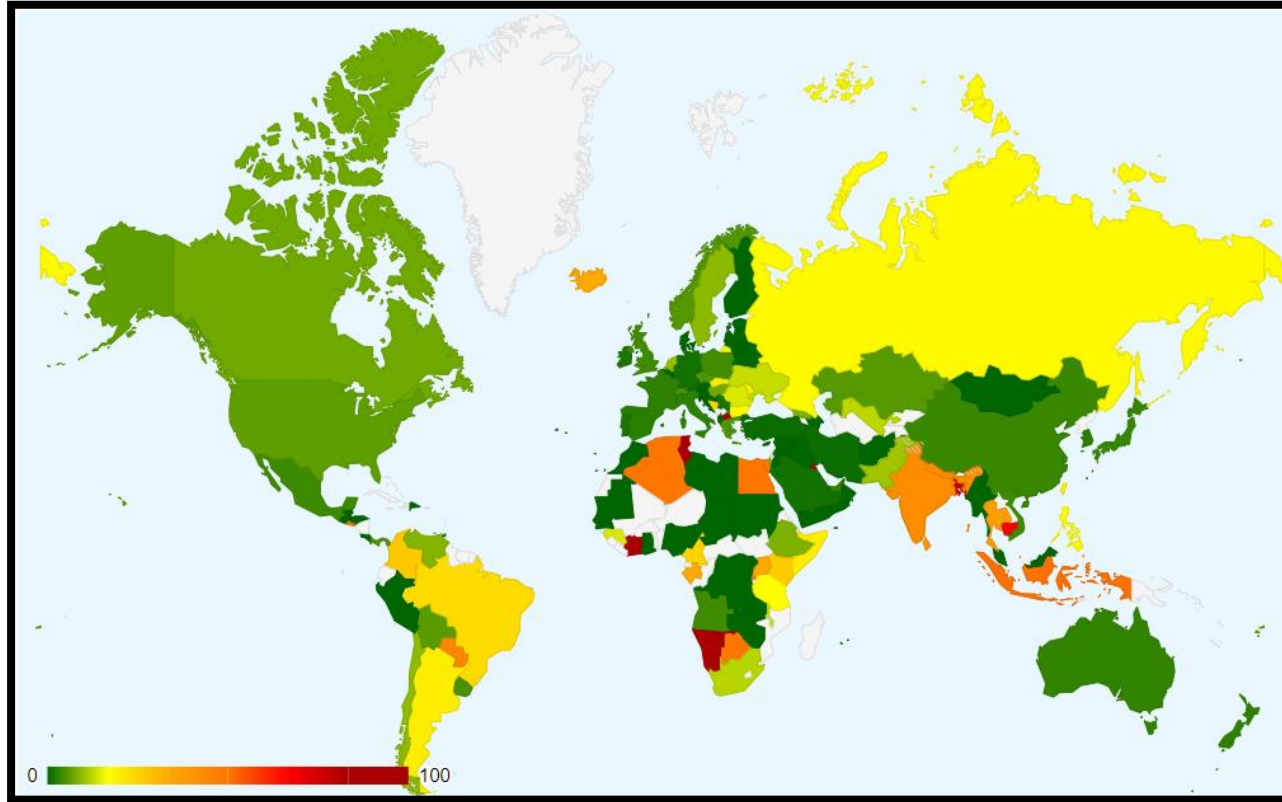


Os dez principais resultados do teste Spoofer (do ano passado)

by ASN	Client IP blocks	Spoofing IP blocks
24560 (AIRTELBROADBAND-AS-AP)	212	203 (95.8%)
8452 (TE-AS)	49	36 (73.5%)
7418	190	27 (14.2%)
23969 (TOT-NET)	27	27 (100.0%)
7303	53	26 (49.1%)
209 (CENTURYLINK-US-LEGACY-QWEST)	75	20 (26.7%)
3462 (HINET)	44	15 (34.1%)
262675	14	13 (92.9%)
7713 (telkomnet-as-ap)	15	13 (86.7%)
28668	13	12 (92.3%)

by Country	Client IP blocks	Spoofing IP blocks
bra (Brazil)	1918	424 (22.1%)
ind (India)	525	223 (42.5%)
usa (United States)	2020	122 (6.0%)
tha (Thailand)	102	38 (37.3%)
arg (Argentina)	180	36 (20.0%)
egy (Egypt)	72	36 (50.0%)
nld (Netherlands)	361	36 (10.0%)
chl (Chile)	352	33 (9.4%)
idn (Indonesia)	59	30 (50.8%)
zaf (South Africa)	190	23 (12.1%)

Distribuição Geográfica



Testes recentes em Portugal

AS numbers or (partial) names:

Country codes: prt

☐ Only show non-remediated spoofing

[Change filters](#)

Spoof status key

received Spoofed packet was received.

rewritten Spoofed packet was received, but the source address was changed en route.

blocked Spoofed packet was not received, but unspoofed packet was.

unknown Neither spoofed nor unspoofed packet was received.



Pattern of tests from this IP block indicates a switch from allowing spoofing to blocking it.

Session ▾	Timestamp (UTC) ▾	Client IP Block ▾	ASN ▾	Country ▾	NAT ▾	Outbound Private Status ▾	Outbound Routable Status ▾	Adj Spoof Prefix Len ▾	Results
1719230	2024-02-16 10:23:02	82.155.173.x/24	3243 (MEO-RESIDENCIAL)	prt (Portugal)	yes	blocked	blocked	none	Report
1719230	2024-02-16 10:23:02	2001:8a0:ffx::/40	3243 (MEO-RESIDENCIAL)	prt (Portugal)	no	blocked	blocked	/64	Report
1717053	2024-02-11 20:27:44	85.138.128.x/24	2860 (NOS_COMUNICACOES)	prt (Portugal)	yes	blocked	blocked	none	Report
1716608	2024-02-10 18:25:01	176.79.168.x/24	3243 (MEO-RESIDENCIAL)	prt (Portugal)	yes	rewritten	rewritten	none	Report
1716608	2024-02-10 18:25:01	2001:8a0:dex::/40	3243 (MEO-RESIDENCIAL)	prt (Portugal)	no	blocked	blocked	/64	Report
1716270	2024-02-09 22:08:01	82.155.154.x/24	3243 (MEO-RESIDENCIAL)	prt (Portugal)	yes	rewritten	rewritten	none	Report
1716270	2024-02-09 22:08:01	2001:8a0:e5xx::/40	3243 (MEO-RESIDENCIAL)	prt (Portugal)	no	blocked	blocked	/64	Report
1712680	2024-02-02 21:01:12	82.155.154.x/24	3243 (MEO-RESIDENCIAL)	prt (Portugal)	yes	rewritten	rewritten	none	Report
1712680	2024-02-02 21:01:12	2001:8a0:e5xx::/40	3243 (MEO-RESIDENCIAL)	prt (Portugal)	no	blocked	blocked	/64	Report
1712463	2024-02-02 14:48:28	85.138.128.x/24	2860 (NOS_COMUNICACOES)	prt (Portugal)	yes	blocked	blocked	none	Report
1711571	2024-01-31 23:10:01	85.138.128.x/24	2860 (NOS_COMUNICACOES)	prt (Portugal)	yes	blocked	blocked	none	Report
1709448	2024-01-27 17:36:54	194.210.224.x/24	1930 (RCCN)	prt (Portugal)	no	blocked	blocked	/20	Report
1709448	2024-01-27 17:36:54	2001:690:21xx::/40	1930 (RCCN)	prt (Portugal)	no	blocked	✓ blocked	/32	Report
1708982	2024-01-26 19:46:40	82.155.154.x/24	3243 (MEO-RESIDENCIAL)	prt (Portugal)	yes	rewritten	rewritten	none	Report
1708175	2024-01-25 11:01:48	193.136.167.x/24	1930 (RCCN)	prt (Portugal)	no	blocked	blocked	/21	Report
1708175	2024-01-25 11:01:48	2001:690:21xx::/40	1930 (RCCN)	prt (Portugal)	no	blocked	blocked	/32	Report
1707714	2024-01-24 14:18:45	85.138.128.x/24	2860 (NOS_COMUNICACOES)	prt (Portugal)	yes	blocked	blocked	none	Report
1706626	2024-01-22 13:23:51	85.138.128.x/24	2860 (NOS_COMUNICACOES)	prt (Portugal)	yes	blocked	blocked	none	Report



05

Conclusão

