

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

egi.br

Comitê Gestor da
Internet no Brasil

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

Segurança de Redes

Programa por uma Internet mais segura

Gilberto Zorello | gzorello@nic.br

CONNECTA NET CHAPECÓ

Chapecó, SC | 21/02/25

nic.br

Programa por uma Internet mais Segura

Nossa agenda



Objetivo / Plano de Ação

Interação com Provedores e Operadoras

Ações do Programa

Notificação de Amplificadores

MANRS

KINDNS

TOP – Teste os Padrões



MANRS



PROGRAMA
INTERNET
+SEGURA



TESTE OS PADRÕES



KINDNS



Objetivos do Programa

- Reduzir ataques DDoS
- Melhorar a segurança de roteamento
- Reduzir vulnerabilidades e falhas de configuração
- Divulgar melhores práticas de segurança
- **Aumentar a cultura de segurança**

<https://bcp.nic.br/i+seg>



PROGRAMA
**INTERNET
+SEGURA**

<https://bcp.nic.br/i+seg>



Configuração de serviços expostos na Internet

- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

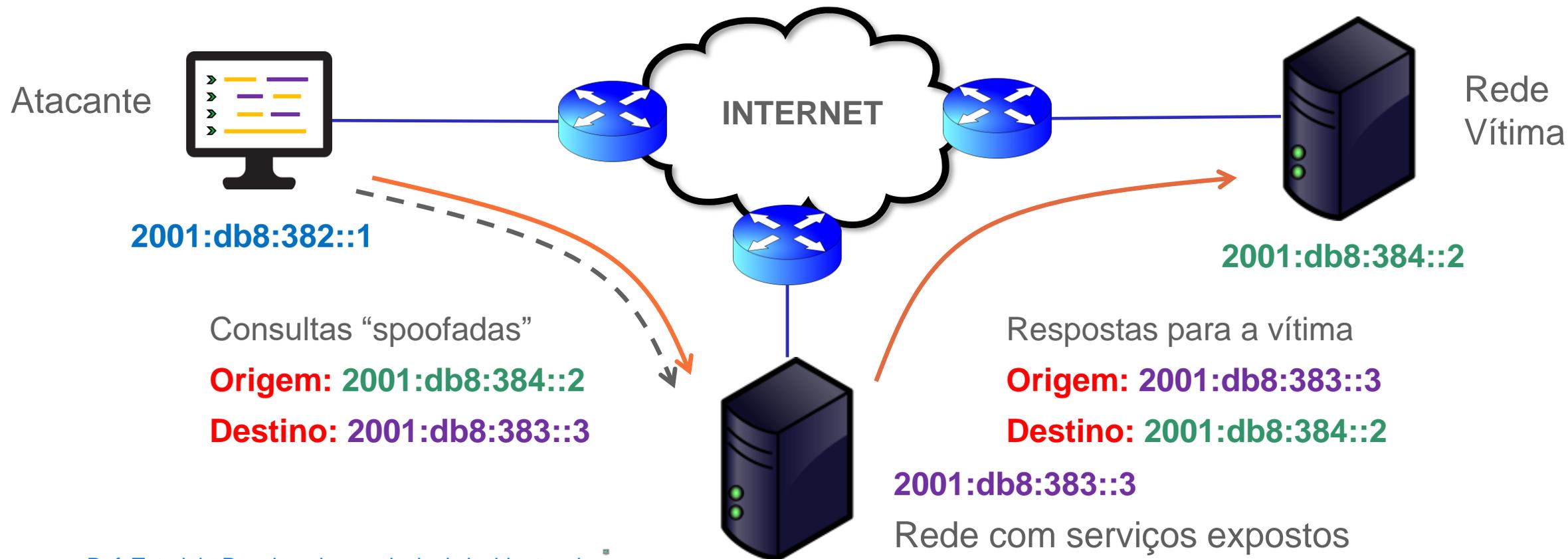
<https://bcp.nic.br/i+seg/acoes/amplificacao/>



Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque

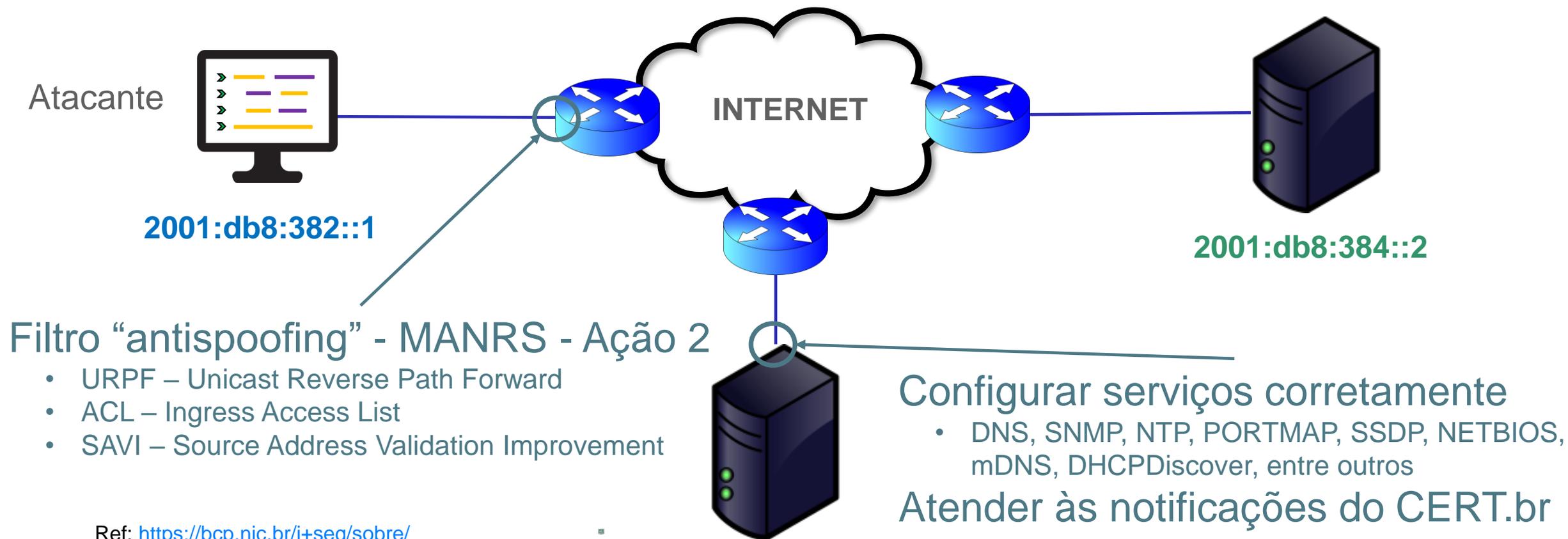


[Ref. Tutorial - Resolvendo os principais incidentes de segurança](#)

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

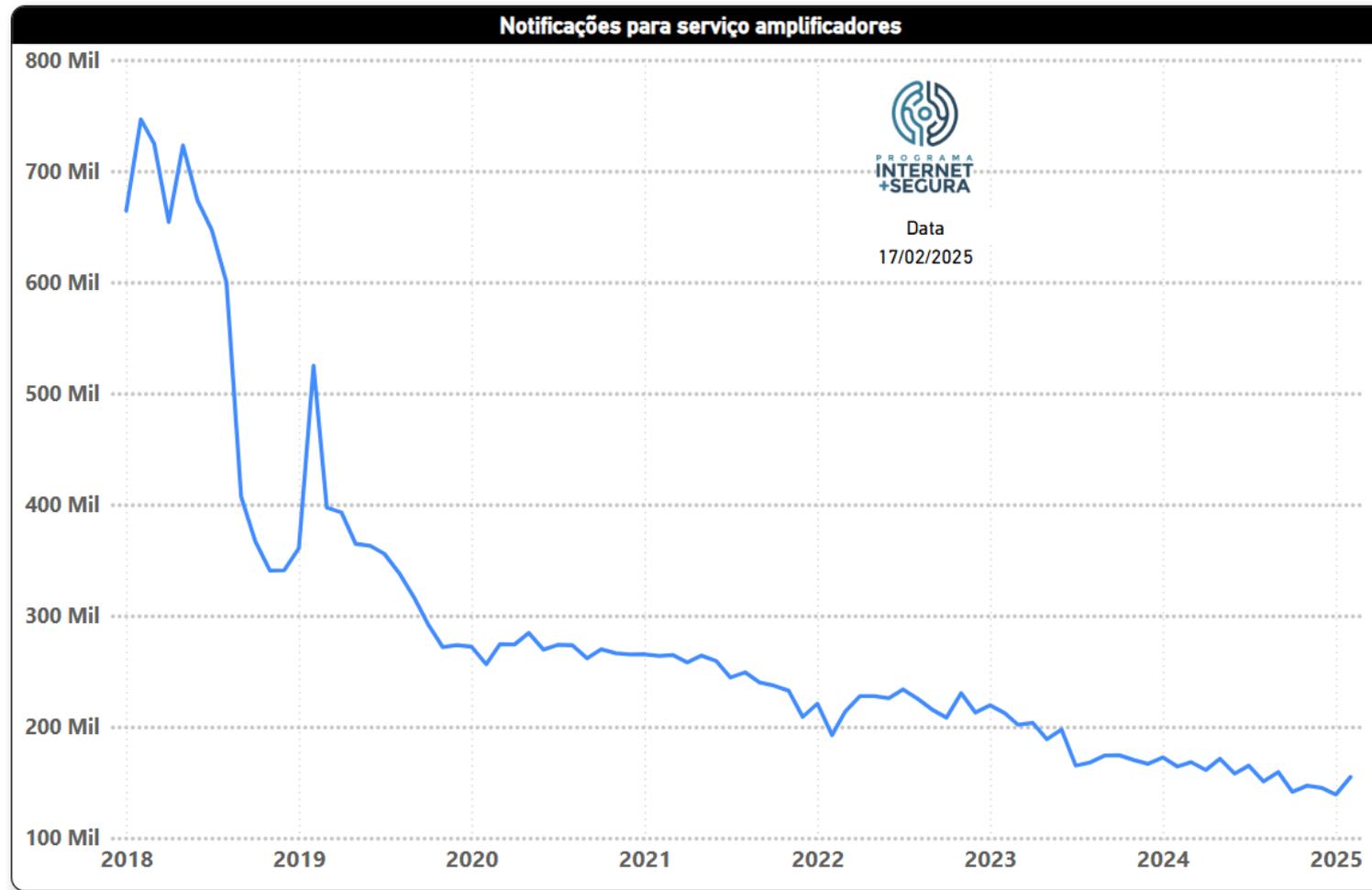
Como resolver o problema



Ref: <https://bcp.nic.br/i+seg/sobre/>

Programa por uma Internet mais Segura

Notificação de amplificadores - evolução



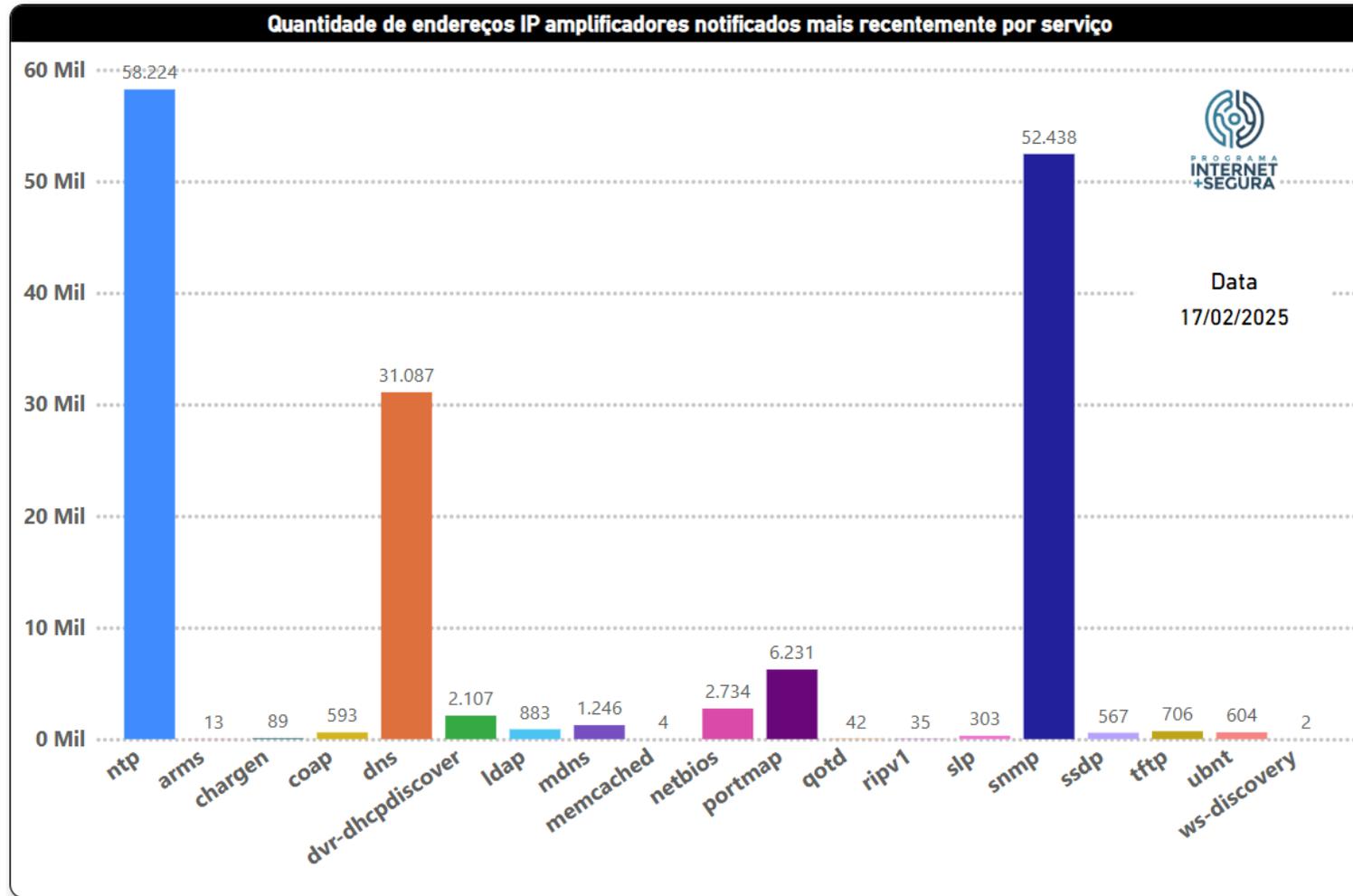
Brasil

- Início (fev/2018)
 - Endereços IP: 746.508
 - Serviços: 5
- Atual:
 - Endereços IP: 157.908
 - Serviços: 19
 - **Redução de 79%**

Fev/25

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

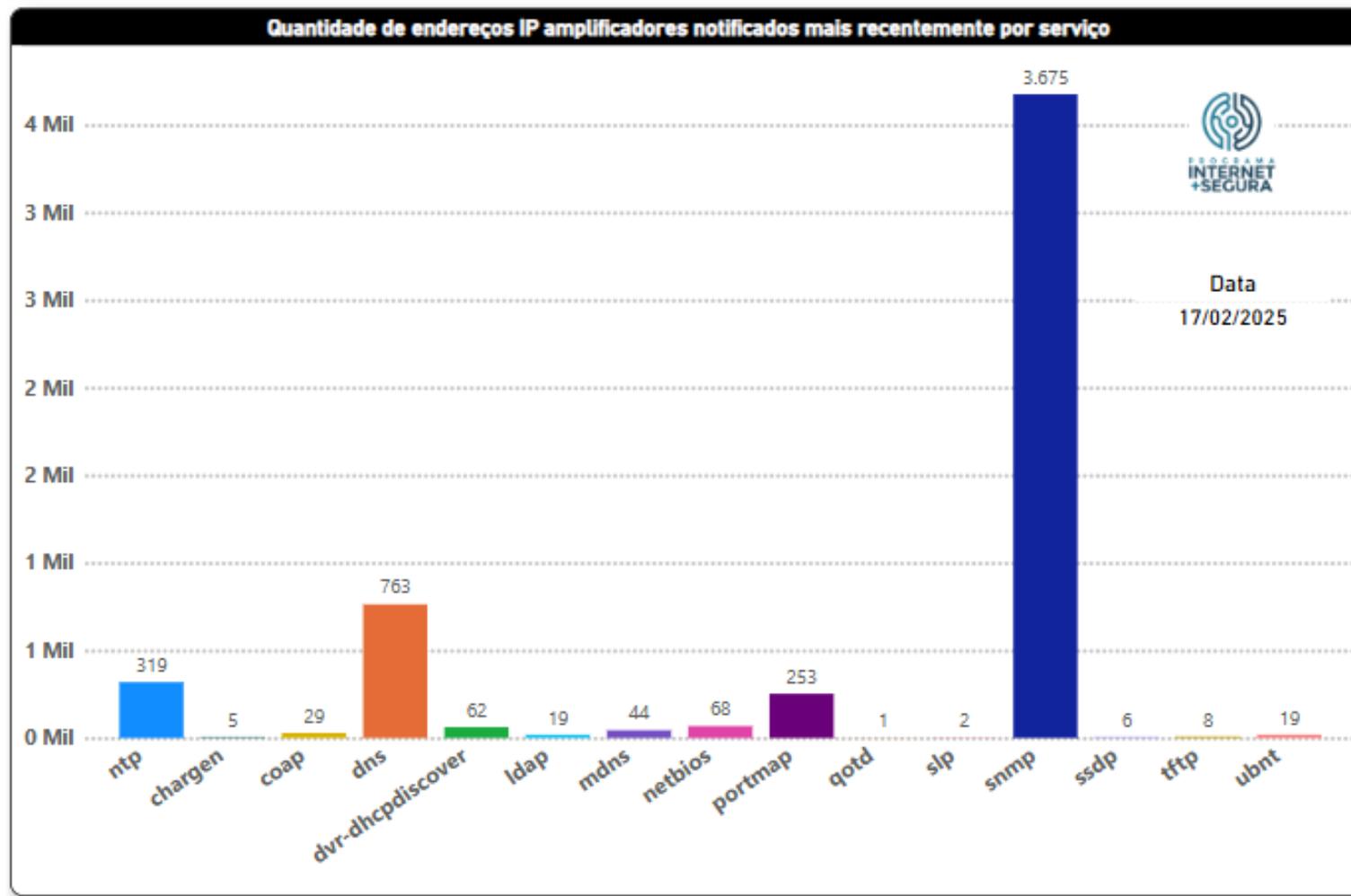


Brasil

- 9.038 AS
- 5.179 AS notificados
- 157.908 endereços IP mal configurados
- **NTP 58.224**
- **SNMP 52.438**
- **DNS 31.087**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

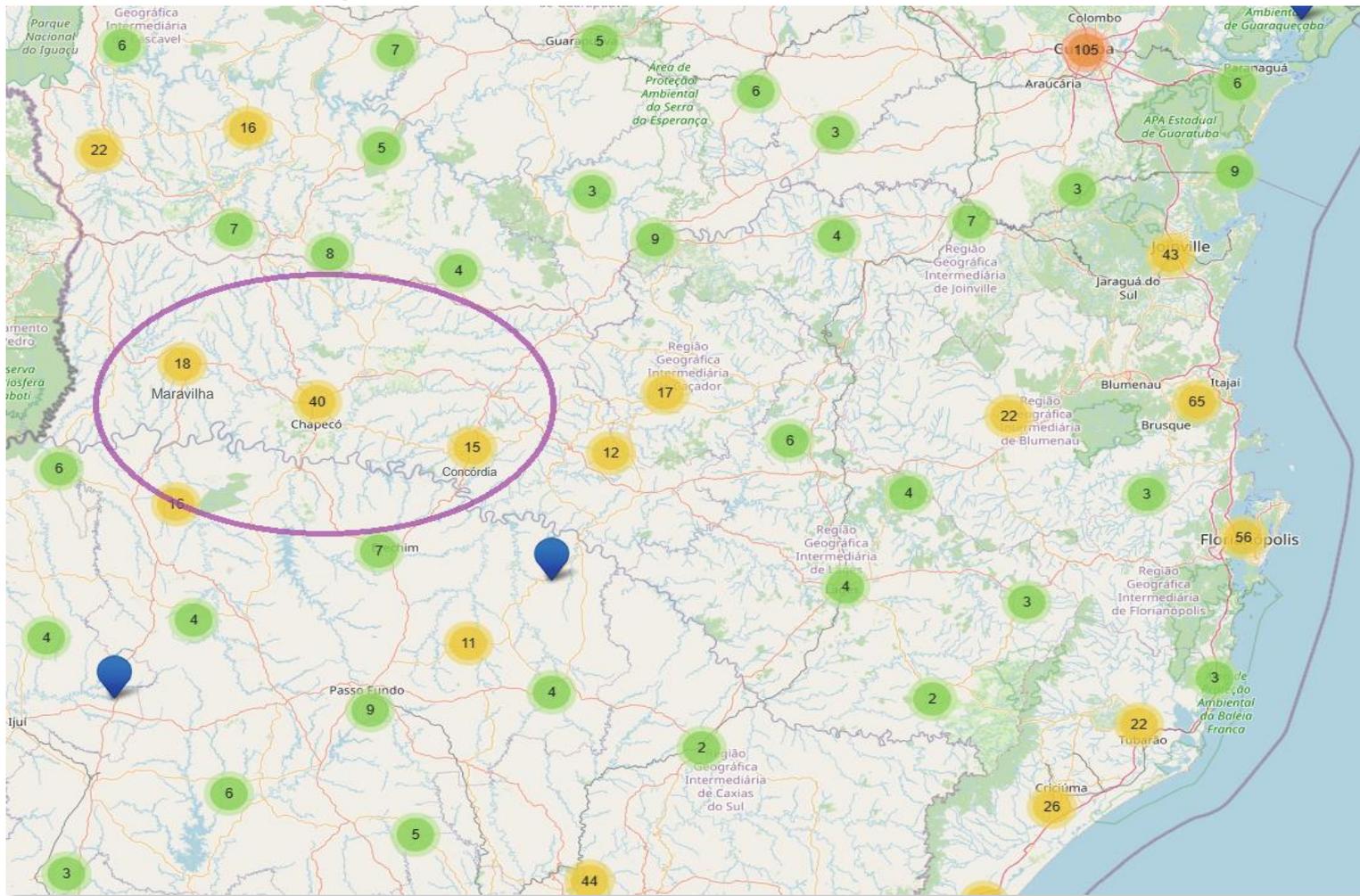


Santa Catarina

- 389 AS
- 211 AS notificados
- 5.283 endereços IP mal configurados
 - **SNMP 3.675**
 - **DNS 763**
 - **NTP 319**
 - **PORTMAP 253**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

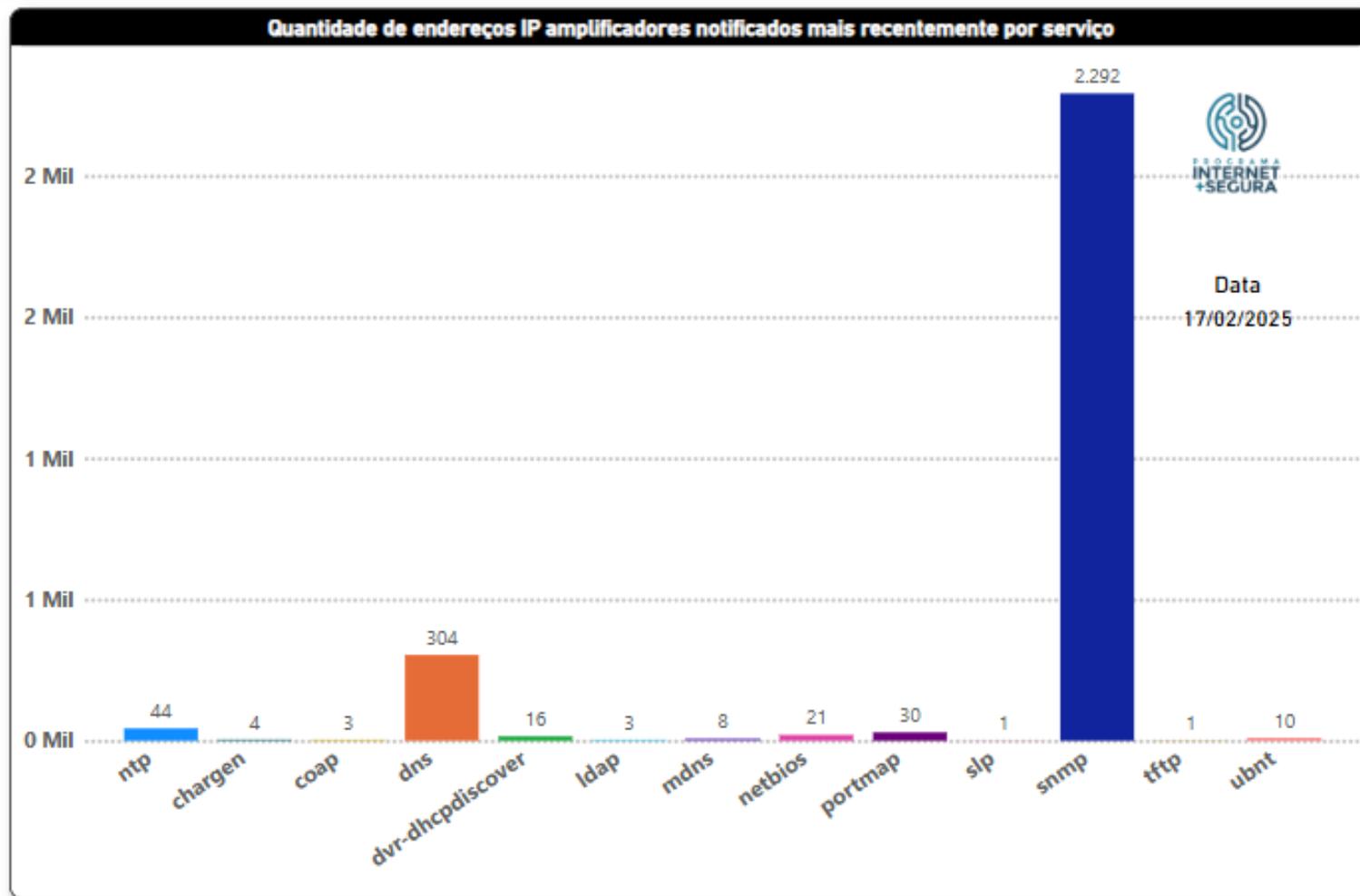


Região Oeste de SC

- Chapecó (40)
- Maravilha (18)
- Concórdia (15)
- 73 AS
- 44 AS notificados
- 2.737 endereços IP mal configurados

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



Região Oeste de SC

- 44 AS notificados
- 2.737 endereços IP mal configurados
- **SNMP 2.292**
- **DNS 304**
- **NTP 44**



MANRS

Mutually Agreed Norms for Routing Security

<http://manrs.org>

<https://bcp.nic.br/i+seg/acoes/manrs/>

Programa por uma Internet mais Segura



Boas práticas de roteamento global

- MANRS - Internet Society (trocadilho em inglês)
- BGP é inseguro!
- Filtros BGP
- Filtro Anti Spoofing (endereço de origem)
- Pontos de contato de segurança no Peering DB, whois, IRR
- Cadastro da política de roteamento no IRR e RPKI



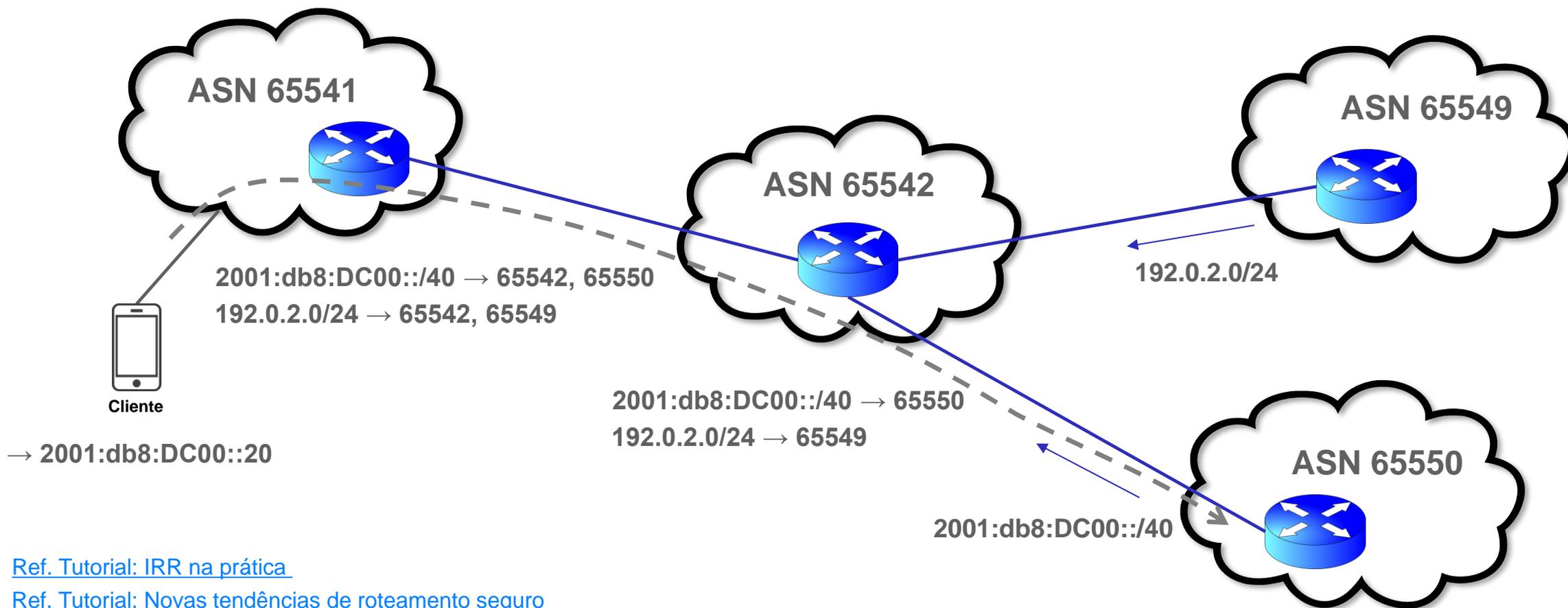
MANRS

<https://bcp.nic.br/i+seg/acoes/manrs/>



Programa por uma Internet mais Segura

Sequestro de prefixos (Hijacking)

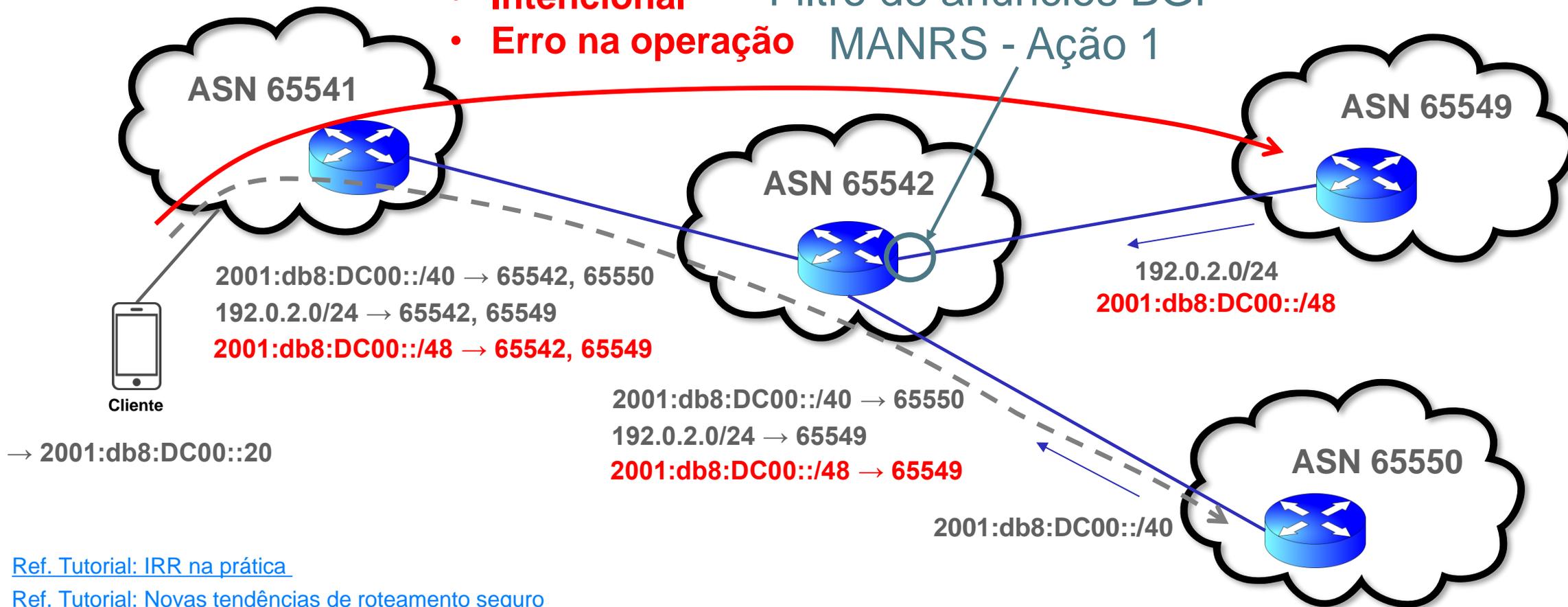


Programa por uma Internet mais Segura

Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

- **Intencional** Filtro de anúncios BGP
- **Erro na operação** MANRS - Ação 1

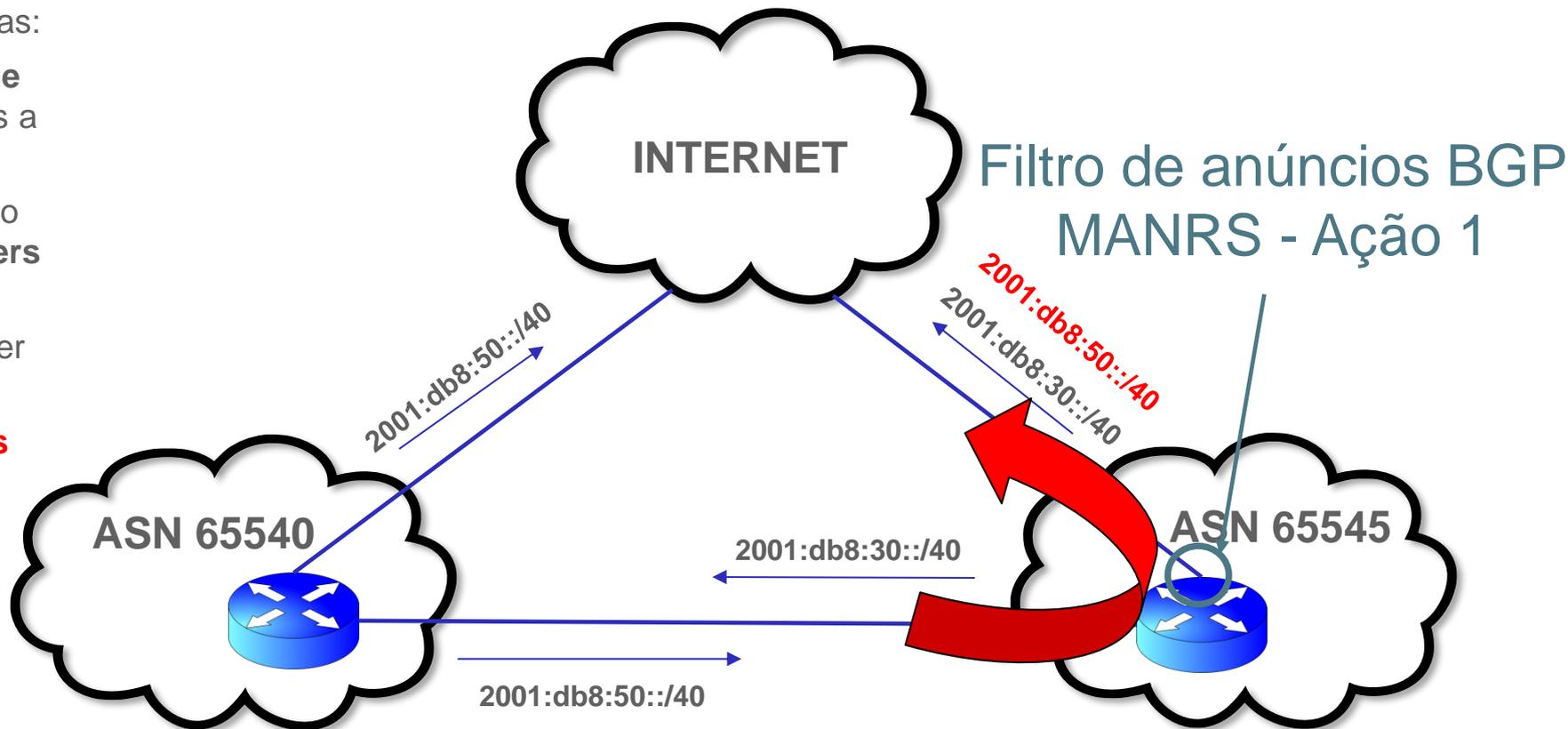


Programa por uma Internet mais Segura

Vazamento de rotas (Route Leak)

- Algumas **regras** devem ser cumpridas:
- Prefixos aprendidos do **provedor de trânsito** não devem ser anunciados a **outro provedor** ou a **peer** da rede
- Prefixos aprendidos de um **peer** não devem ser anunciados a outros **peers** nem ao **provedor de trânsito**
- Estes prefixos somente deveriam ser **anunciados a clientes**
- **Se as regras não forem cumpridas pode ocorrer vazamento de rotas**

Leak!
Normalmente são erros operacionais



[Ref. Tutorial: IRR na prática](#)

[Ref. Tutorial: novas tendências de roteamento seguro](#)

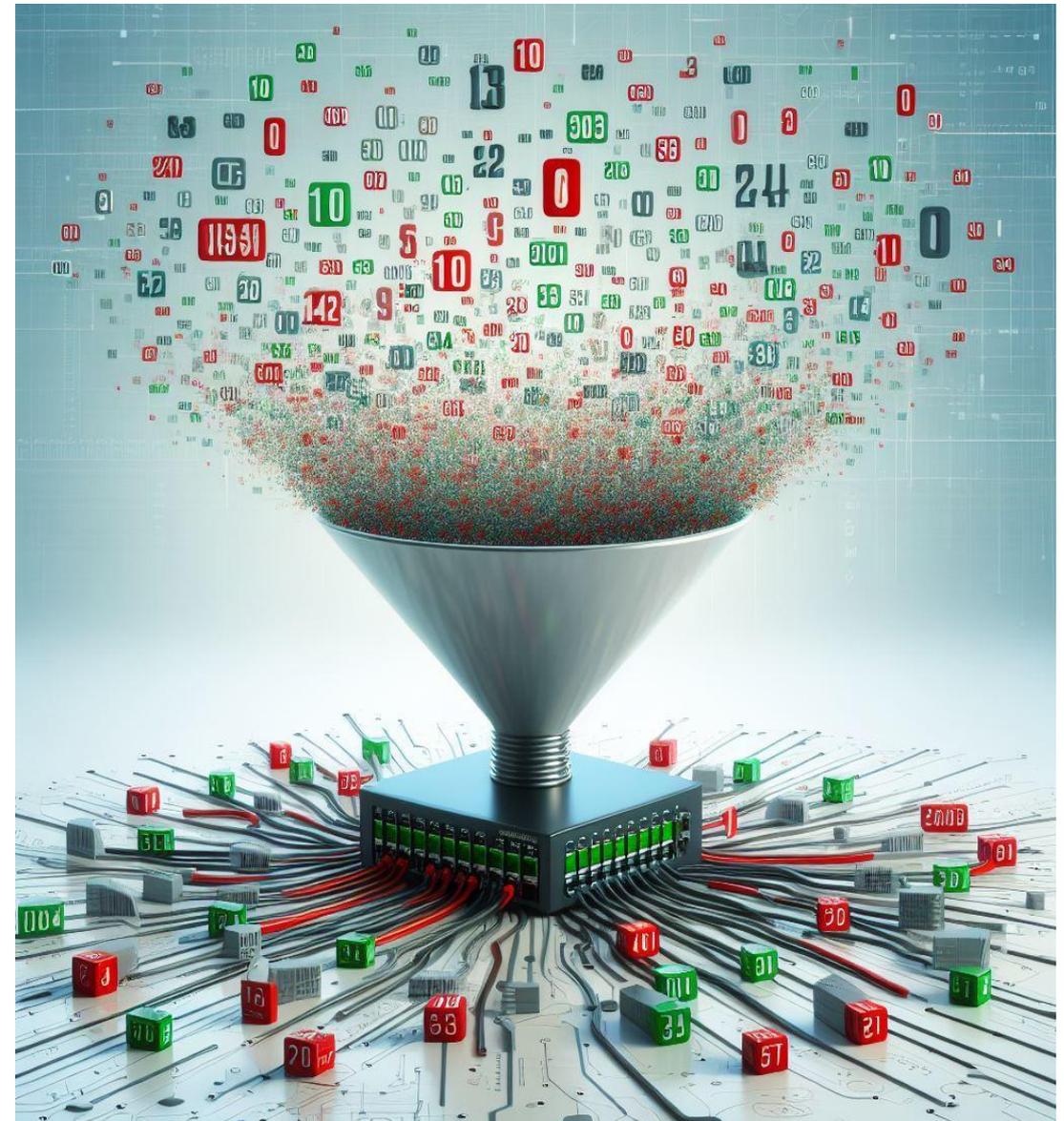
Programa por uma Internet mais Segura



MANRS - Ação 1 - Impedir a propagação de informações incorretas no BGP

- Implemente filtros no BGP para os seus prefixos e dos seus clientes

<https://bcp.nic.br/i+seg/acoes/manrs/#filtragem-de-rotas>

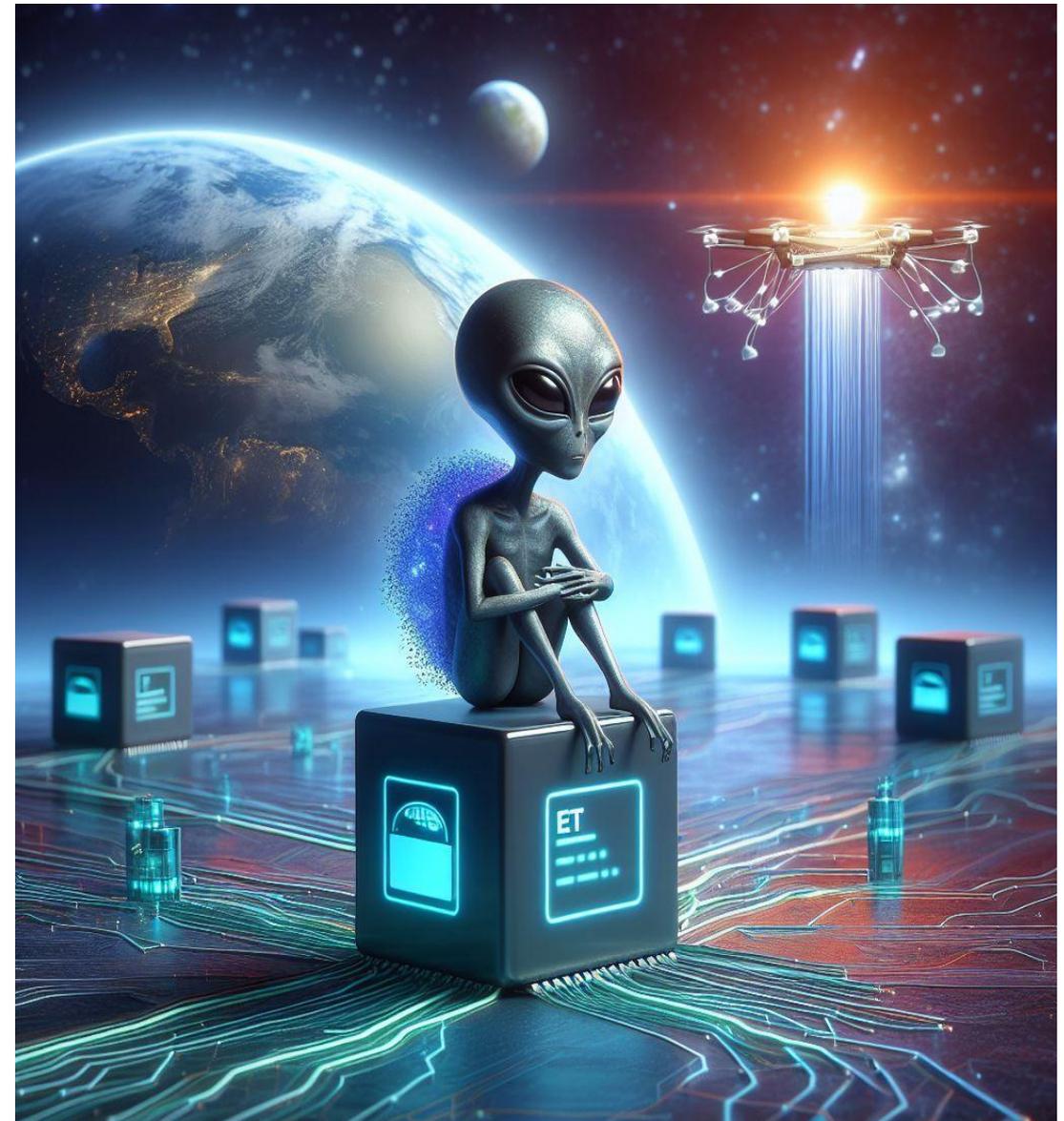


Programa por uma Internet mais Segura



MANRS - Ação 2 - Filtro Anti Spoofing

- Bloqueie pacotes com **origem** em IPs diferentes daqueles do seu bloco, eles **não podem sair de sua rede** (não podem ser originados na sua rede)!

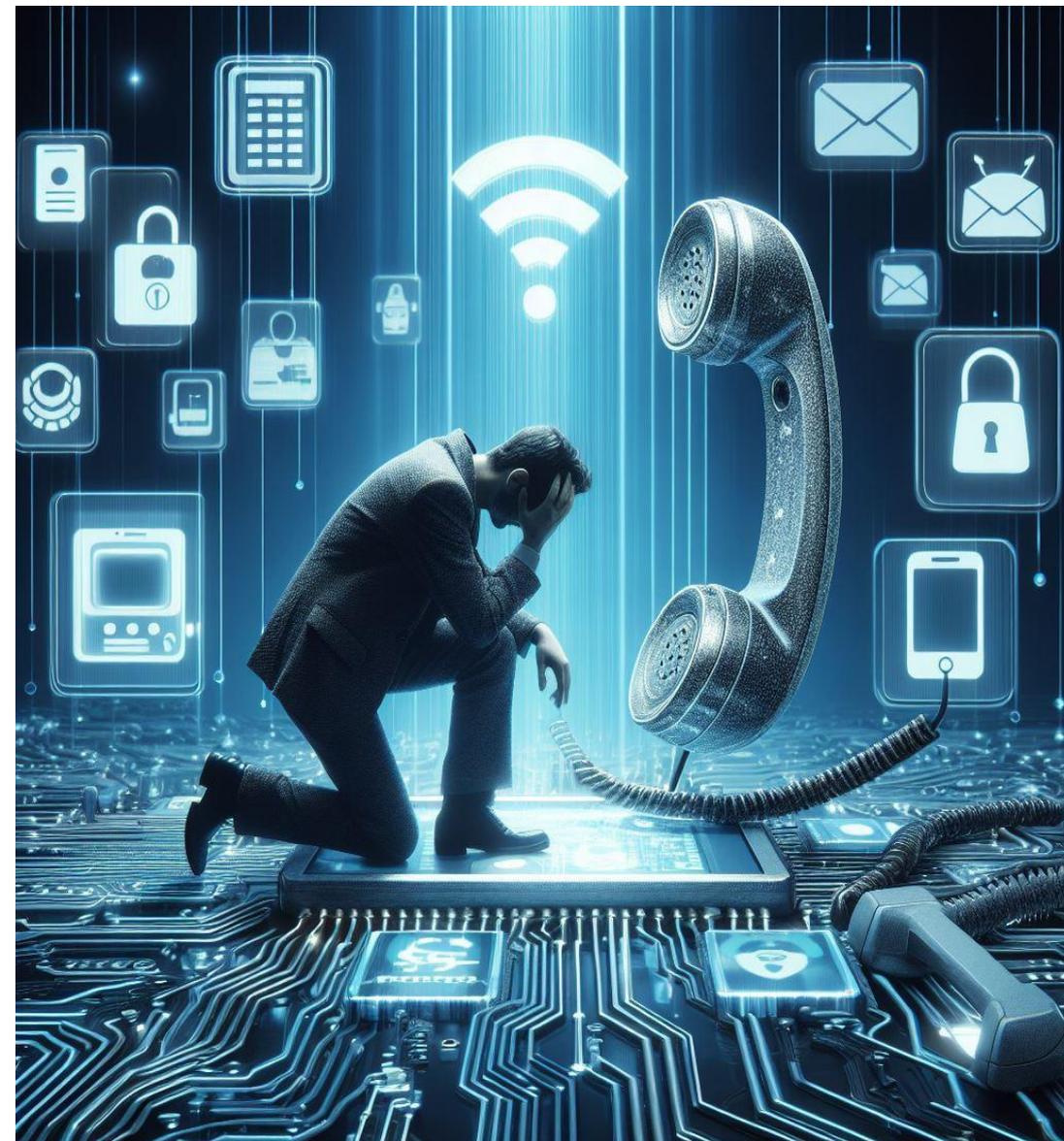


Programa por uma Internet mais Segura



MANRS - Ação 3 - Pontos de Contato

- Contatos de roteamento e abuse no Registro.br devem estar atualizados e serem de grupos de pessoas. Ex.: noc@seuprovedor.com.br
- Registro.br está validando os e-mails de abuse e a não resposta pode causar a **recuperação** (perda) dos endereços IP *
- Mensagens do CERT.br estão indo para o SPAM em alguns casos!
- Atualizar contatos no **PeeringDB** e **IRR**



MANRS

<https://bcp.nic.br/i+seg/acoes/manrs/#coordenacao>

Programa por uma Internet mais Segura

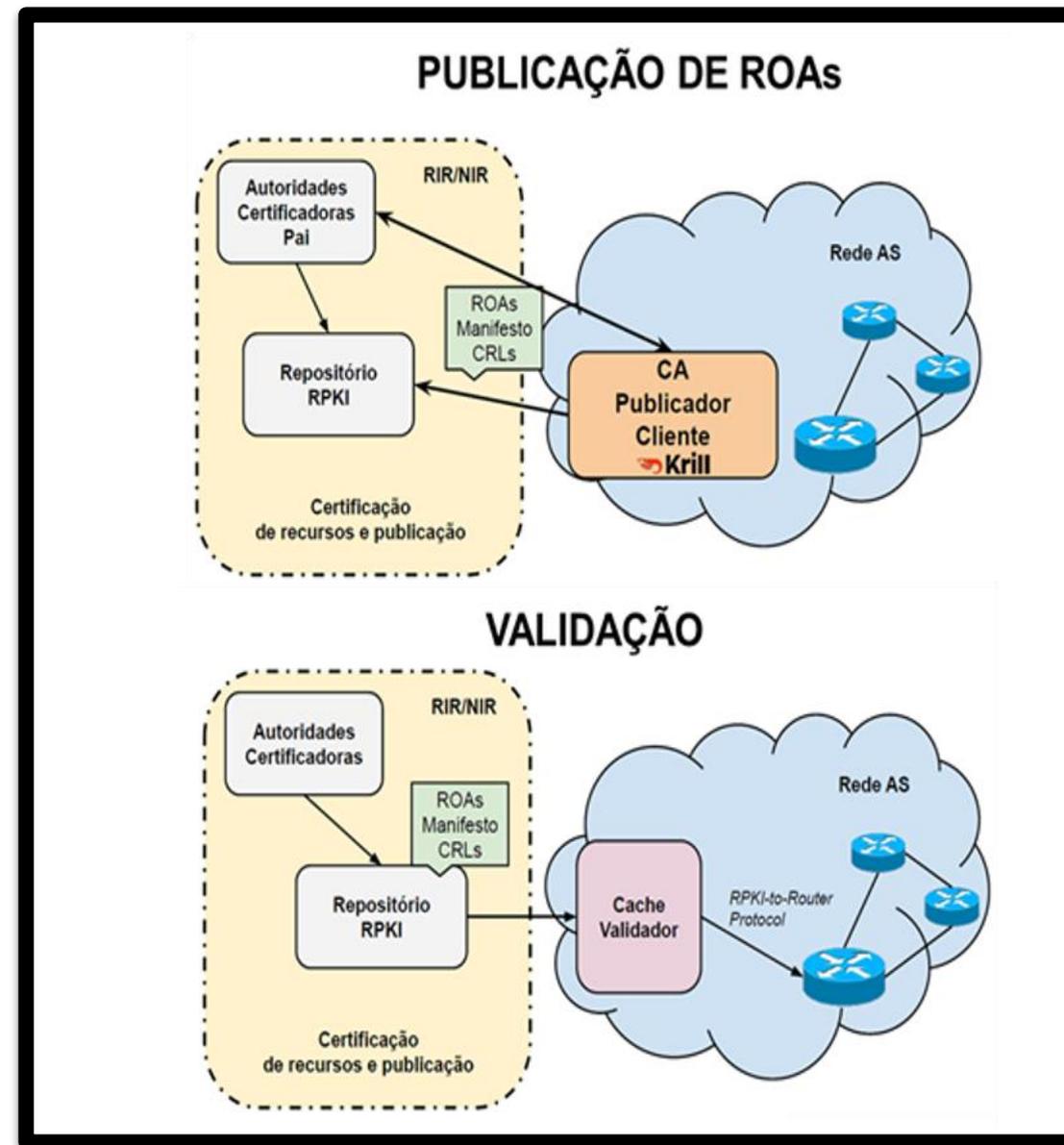


MANRS - Ação 4 - Cadastro da Política de Roteamento

- IRR - Internet Routing Registry
 - RADB
 - TC (gratuito)
- RPKI - Resource Public Key Infrastructure



<https://bcp.nic.br/i+seg/acoes/>



Programa por uma Internet mais Segura

MANRS Observatory - 388 AS – SC

MANRS DASHBOARD

OVERVIEW HISTORY DETAILS COMPARISON ROA STATS ABOUT

Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents ⁱ

Route misoriginations	0
Route leaks	0
Bogon announcements	0
Total	0

■ Route misoriginations ■ Route leaks ■ Bogon announcements

Culprits ⁱ

Culprits	0
----------	---

■ Culprits

Routing Information (IRR) ⁱ

Unregistered	120	29%
Registered	3,994	97.1%

■ Unregistered ■ Registered

Routing Information (RPKI) ⁱ

Valid	2,163	52.6%
Unknown	1,940	47.1%
Invalid	11	0.3%

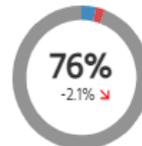
■ Valid ■ Unknown ■ Invalid

MANRS Readiness ⁱ

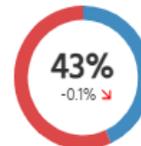
Filtering ⁱ



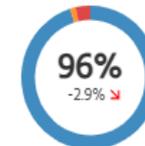
Anti-spoofing ⁱ



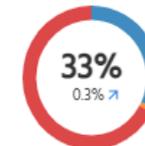
Coordination ⁱ



Routing Information (IRR) ⁱ



Routing Information (RPKI) ⁱ



● Ready ● Aspiring ● Lagging ● No Data Available

Programa por uma Internet mais Segura

MANRS Observatory - 73 AS – Oeste de SC



MANRS DASHBOARD

OVERVIEW HISTORY DETAILS COMPARISON ROA STATS ABOUT

Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents ⁱ

Route misoriginations	0
Route leaks	0
Bogon announcements	0
Total	0

Route misoriginations Route leaks Bogon announcements

Culprits ⁱ

Culprits	0
----------	---

Culprits

Routing Information (IRR) ⁱ

Unregistered	20	2.1%
Registered	916	97.9%

Unregistered Registered

Routing Information (RPKI) ⁱ

Valid	523	55.9%
Unknown	412	44.0%
Invalid	1	0.1%

Valid Unknown Invalid

Route Origin Validation ⁱ

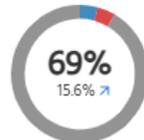
ROV-based Filtering Rate (%) 0.6%

MANRS Readiness ⁱ

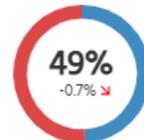
Filtering ⁱ



Anti-spoofing ⁱ



Coordination ⁱ



Routing Information (IRR) ⁱ



Routing Information (RPKI) ⁱ



Ready Aspiring Lagging No Data Available

Programa por uma Internet mais Segura



Participantes por país

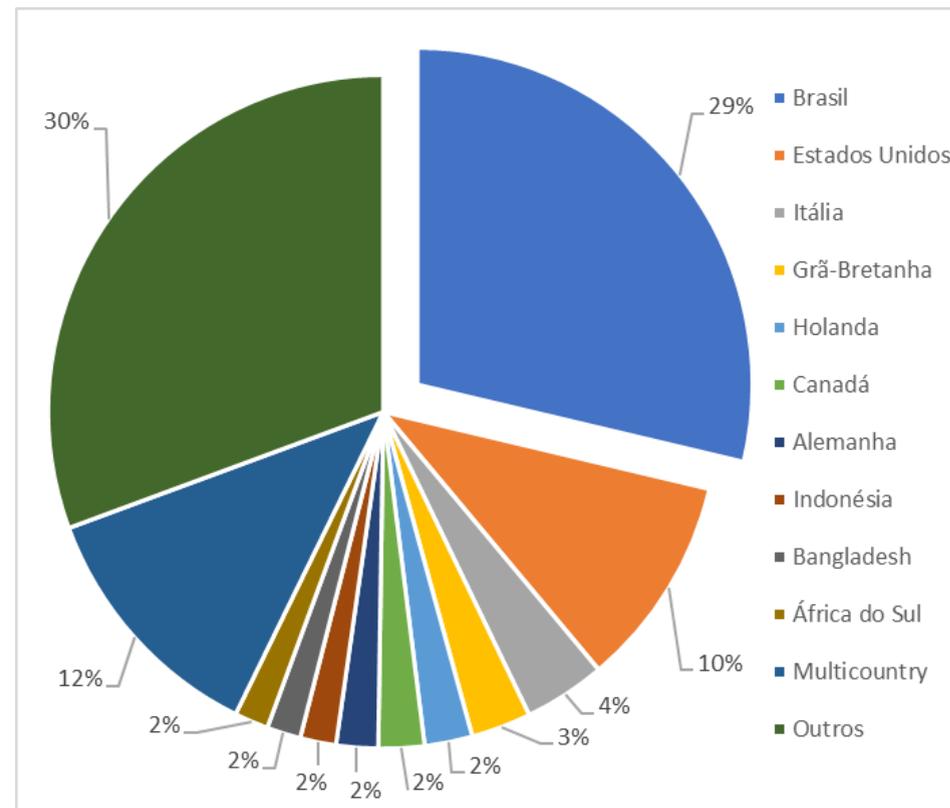
- Total: 1.039
- Participantes no Brasil → 298 (fev/25)



MANRS

2024 → 292
2023 → 258
2022 → 206
2021 → 174
2020 → 140

% de Participantes



Fonte: <https://www.manrs.org/netops/participants/> Acesso fev/25



Stands for **K**nowledge-Sharing and
Instantiating **N**orms for **D**NS and **N**aming
Security

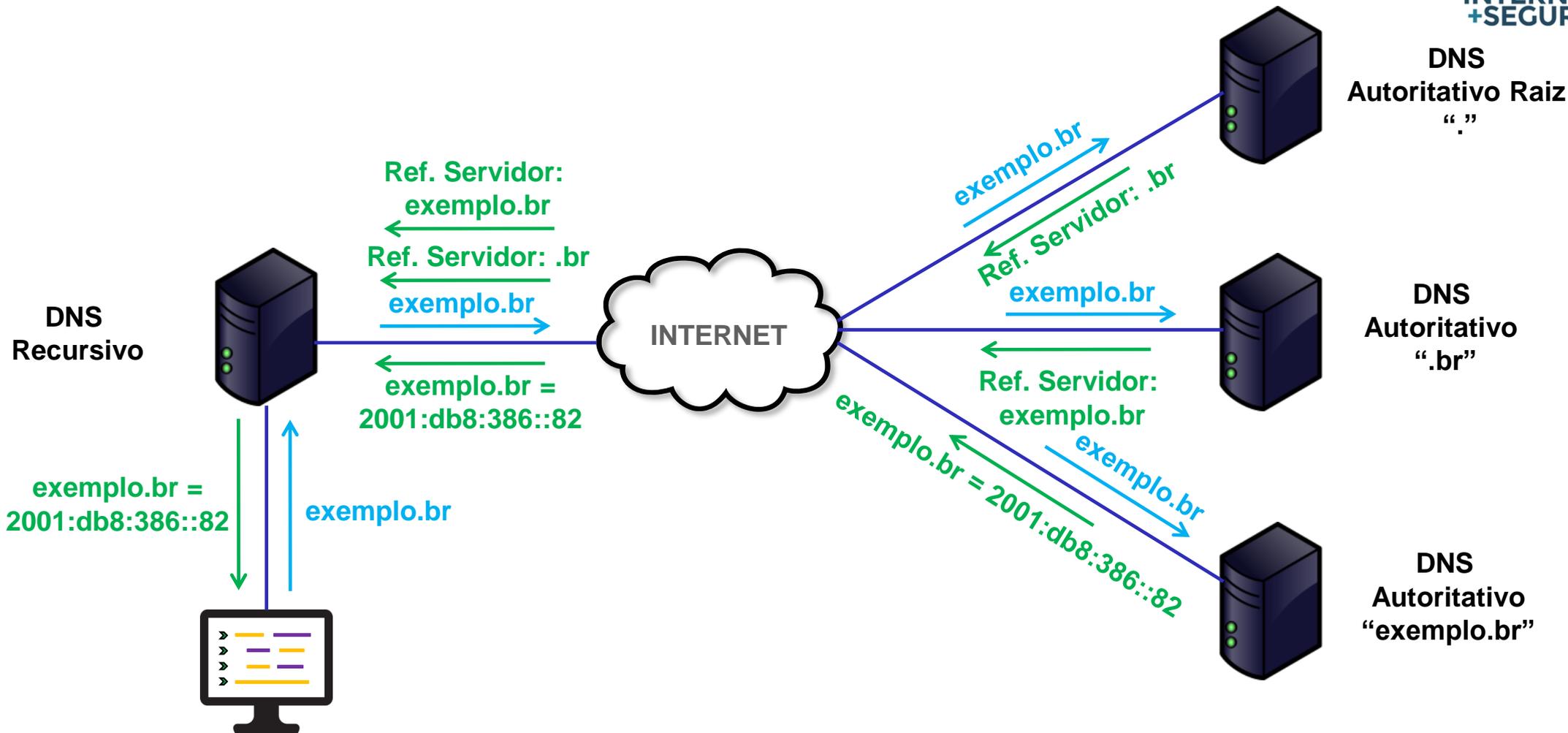
<https://kindns.org/>

Programa por uma Internet mais Segura

Processo de Recursão DNS



PROGRAMA
INTERNET
+SEGURA



Fonte: [\[#SemanaCap 7\] Curso - Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning](#)



Programa por uma Internet mais Segura



Boas práticas para DNS

- KinDNS da ICANN (trocadilho em inglês)
- Configuração correta do recursivo somente para seus usuários
- Validação do DNSSEC no recursivo
- Configuração do autoritativo do seu nome de domínio com DNSSEC

<https://kindns.org/>



TOP

TESTE OS PADRÕES

<https://top.nic.br>

TOP
TESTE OS PADRÕES

Quem é TOP Sobre Referências Comunicados

Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?

Teste TOP - Site
Endereço IP moderno?
Domínio assinado? Conexão segura? Opções de segurança?

Nome de domínio do seu *site*:
www.exemplo.com.br

Iniciar o teste

Teste TOP - E-mail
Endereço IP moderno?
Domínio assinado? Proteção contra *phishing*? Conexão segura?

Nome de domínio do seu e-mail:
@exemplo.com.br

Iniciar o teste

Teste TOP - IPv6 e DNSSEC da sua rede
Endereços modernos acessíveis? Assinaturas de domínio validadas?

Iniciar o teste

Programa por uma Internet mais Segura



Teste os padrões

- Teste do DNS recursivo na sua rede (DNSSEC)!
- Teste do IPv6 na sua rede!
- Teste do seu site!
- Teste do seu e-mail!
- Mostra o que está errado e links com informações para corrigir!

Acesso: <https://top.nic.br>

Programa por uma Internet mais Segura

Testes realizados

- Teste TOP Site
 - IPv6, DNSSEC, HTTPS, Opções de Segurança, RPKI*, Security.txt (RFC 9116)*
- Teste TOP E-mail
 - IPv6, DNSSEC, STARTTLS, DMARC, RPKI*
- Teste TOP IPv6 e DNSSEC do recursivo da sua rede

* Novos testes

Acesso: <https://top.nic.br>

The screenshot shows the TOP website interface. At the top left is the TOP logo with the tagline 'TESTE OS PADRÕES'. At the top right is the 'PROGRAMA INTERNET +SEGURA' logo. Below the navigation bar, there is a main heading: 'Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?'. Below this, there are three test cards:

- Teste TOP - Site**: Includes questions about modern IP addresses, signed domains, secure connections, and security options. The input field shows 'www.exemplo.com.br'.
- Teste TOP - E-mail**: Includes questions about modern IP addresses, signed domains, phishing protection, and secure connections. The input field shows '@exemplo.com.br'.
- Teste TOP - IPv6 e DNSSEC da sua rede**: Includes questions about modern addresses, accessibility, and validated domain signatures. The input field is empty.

Each card has a 'Iniciar o teste' button at the bottom.

Programa por uma Internet mais Segura

Implemente as melhores práticas - Selos



MANRS



KINDNS

Reuniões on-line com os responsáveis pelos AS (KPI)

- Serviços notificados mal configurados *
- Adoção do MANRS
- Adoção do KINDNS
- Testes do TOP: conexão, site e e-mail

<https://bcp.nic.br/i+seg>

<https://kindns.org/>

<https://top.nic.br>

* Relatório mensal



Camada 8 - NIC.br

- Podcast sobre a infraestrutura da Internet
- Edição Novembro/24

<https://www.nic.br/podcasts/camada8/episodio-57>



CAMADA 8
<nic.br>

**INTERNET
MAIS SEGURA**

COM GILBERTO ZORELLO,
COORDENADOR DE PROJETOS NO NIC.BR

Programa por uma Internet mais Segura

APOIO



A CONECTIVIDADE AO SEU ALCANCE



Obrigado

Gilberto Zorello

@ gzorello@nic.br

21 de fevereiro de 2025

nic.br **cgi.br**

www.nic.br | www.cgi.br

