



Núcleo de Informação
e Coordenação do
Ponto 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

IX Fórum Regional - Edição Sudeste

Rio de Janeiro, RJ | 24/10/25



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





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+seq>



PROGRAMA
INTERNET
+SEGURA

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

PRINCIPAIS PROBLEMAS DE SEGURANÇA NA INFRAESTRUTURA DA INTERNET

- Ataques DDoS
- Sistemas mal configurados que permitem amplificação
- Sequestro de prefixos
- Vazamento de rotas
- Ataques de força bruta

PROGRAMA POR UMA INTERNET MAIS SEGURA
bcp.nic.br/i+seg

CORREÇÃO DOS PROBLEMAS

- Interação com Operadoras, ISPs e outros AS

MATERIAL EDUCACIONAL E MELHORES PRÁTICAS

CRIAR CULTURA DE SEGURANÇA

FILTROS NO IX.BR

INDICADORES DE SEGURANÇA

PALESTRAS E CURSOS

PRINCIPAIS AÇÕES A SEREM ADOTADAS POR TODOS

- MANRS
- Hardening
- Atender notificações do CERT.br

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/>

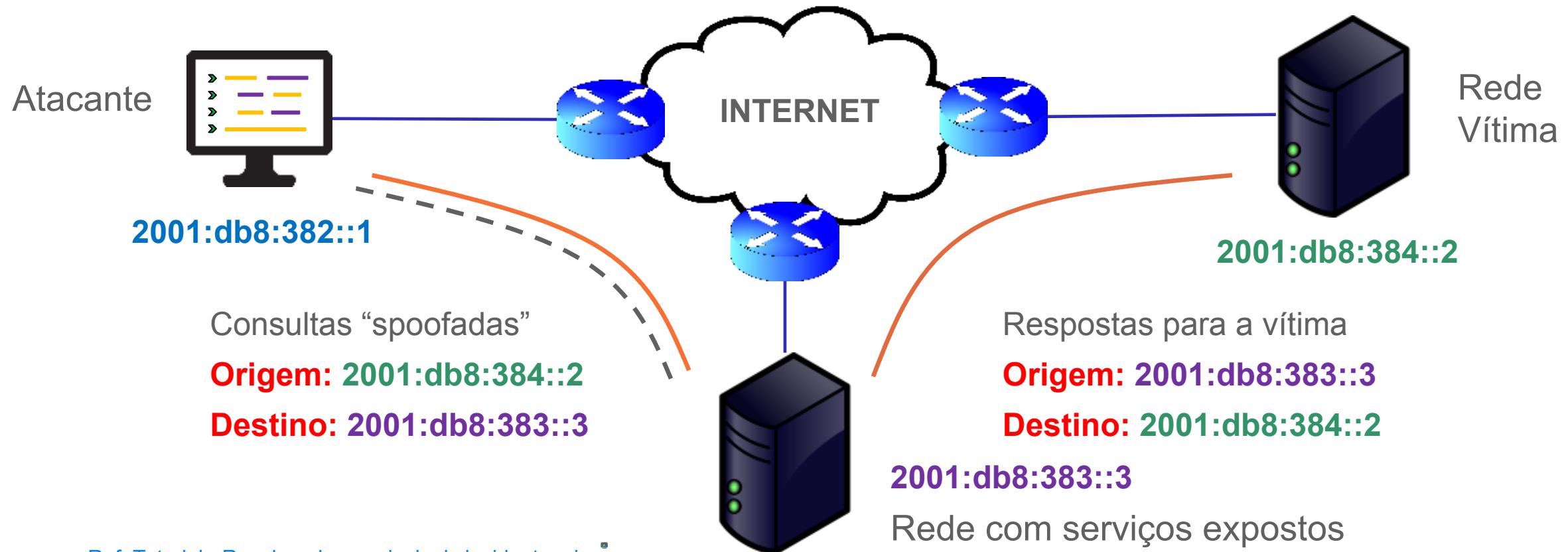


Programa por uma Internet mais Segura



Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque



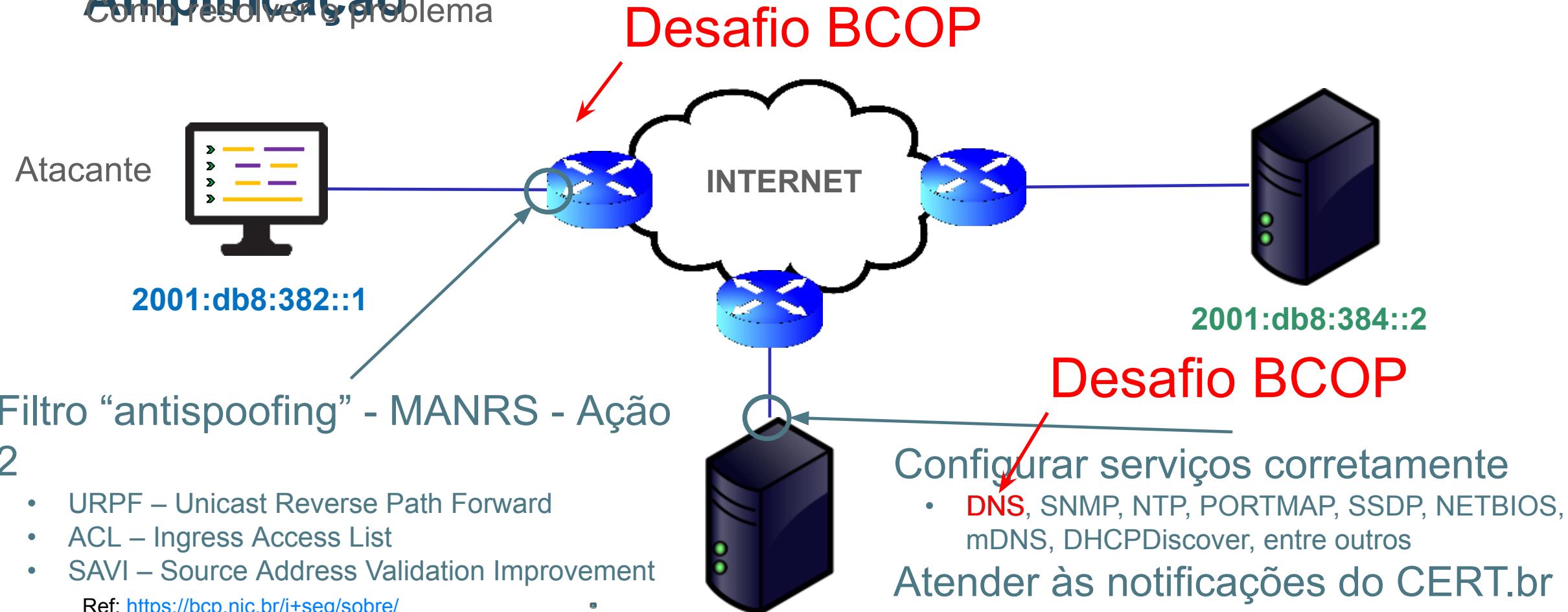
[Ref. Tutorial - Resolvendo os principais incidentes de segurança](#)

Programa por uma Internet mais Segura



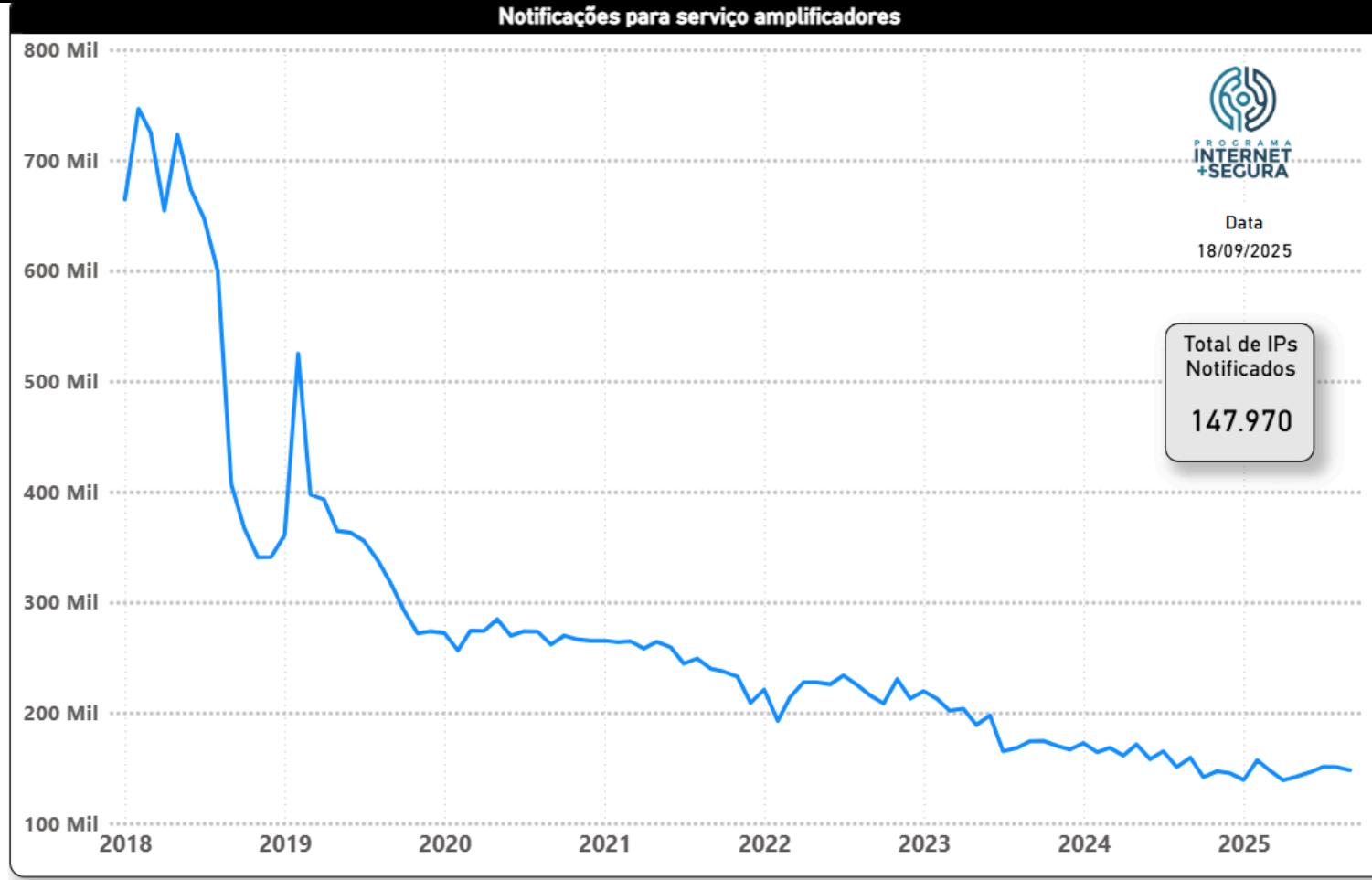
Negação de Serviço Reflexivo com Amplificação

Como resolver o problema



Programa por uma Internet mais Segura

Notificação de amplificadores - evolução

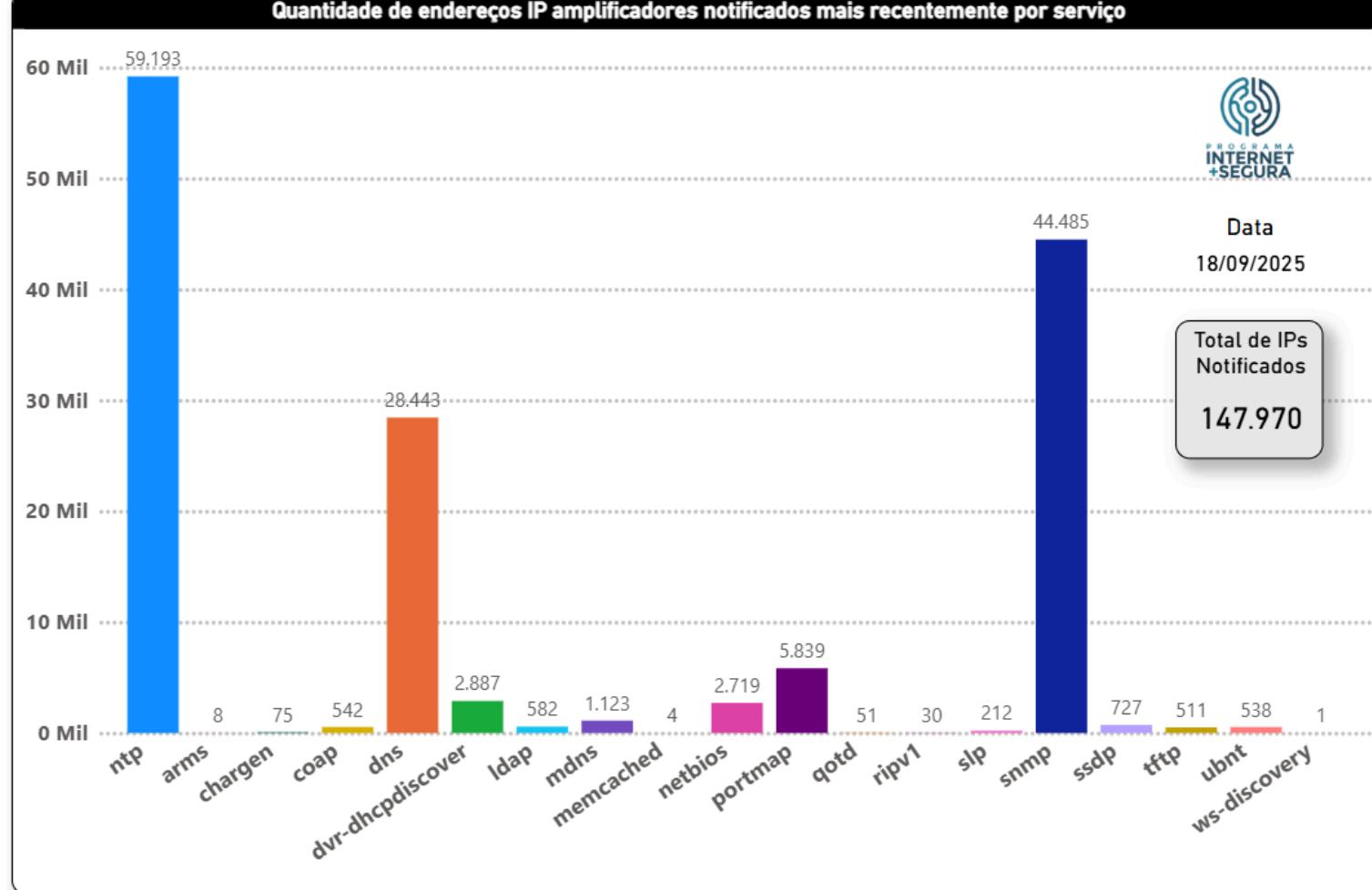


Brasil

- Início (fev/2018)
 - Endereços IP: 746.508
 - Serviços: 5
- Atual:
 - Endereços IP: 147.970
 - Serviços: 19
 - **Redução de 80%**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



Brasil

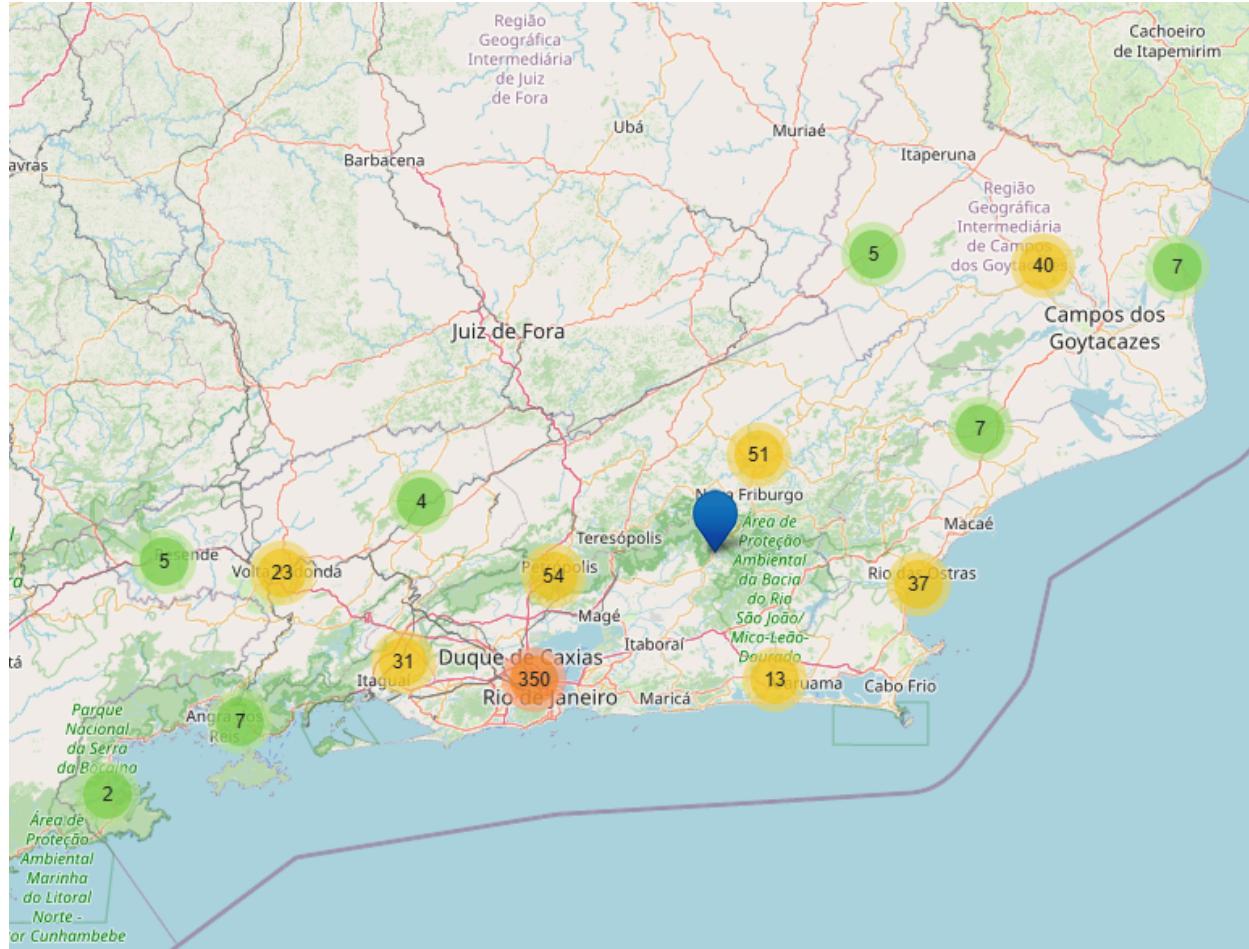
- 9.053 AS
- 5.138 AS notificados
- 147.970 endereços IP mal configurados
 - NTP 59.193
 - SNMP 44.485
 - DNS 28.443

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



PROGRAMA
INTERNET
+SEGURA



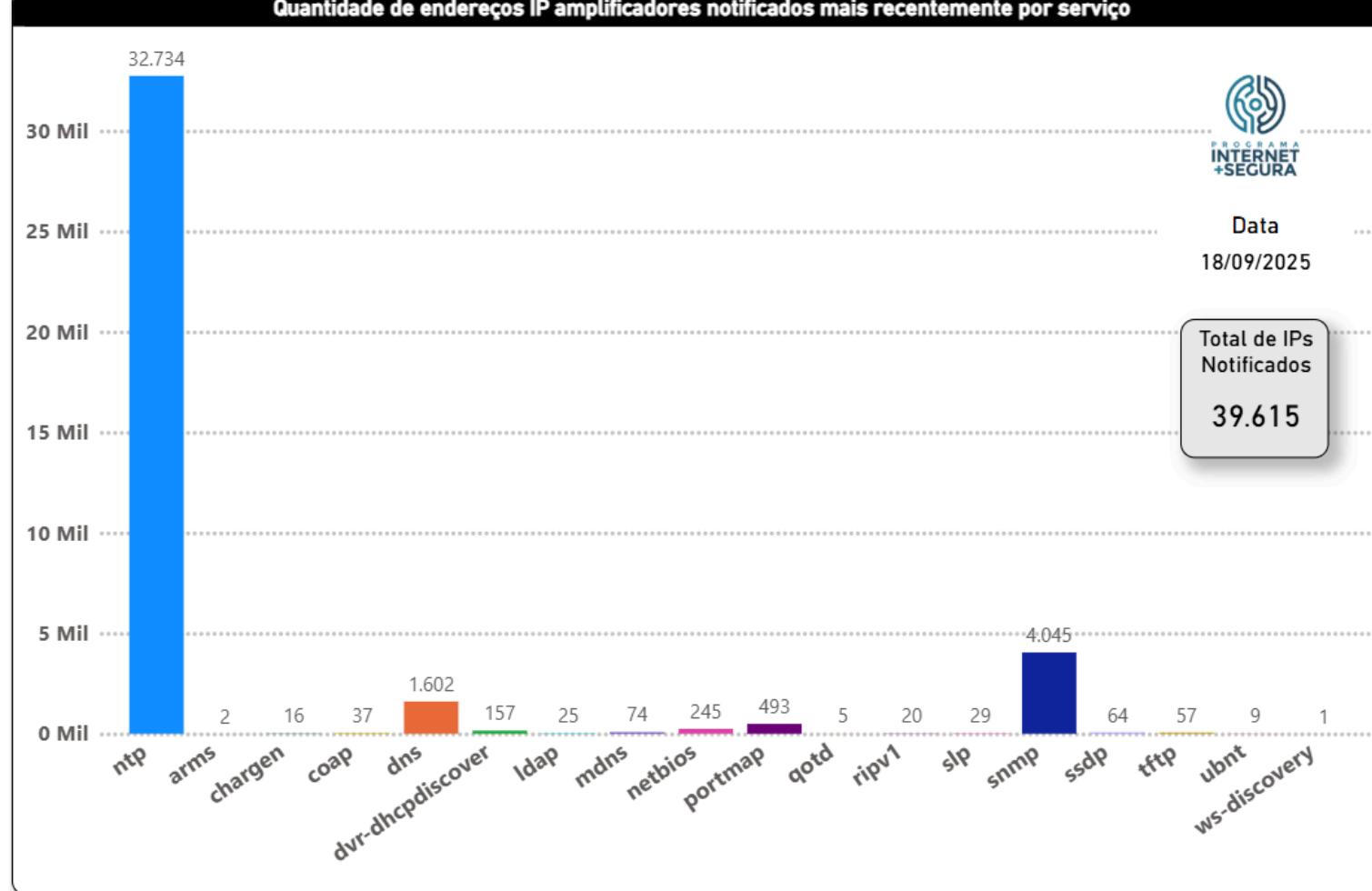
Rio de Janeiro (620 AS)

- | | |
|-------------------------|--------|
| • Rio de Janeiro | (231) |
| • Duque de Caxias | (30) |
| • Nova Iguaçu | (28) |
| • São Gonçalo | (26) |
| • Campos dos Goytacazes | (23) |
| • Niterói | (21) |
| • Magé | (14) |
| • Barra Mansa | (10) |
| • Macaé | (10) |
| • Cabo Frio | (9) |
| • Itaboraí | (9) |
| • Belford Roxo | (8) |
| • Maricá | (8) |
| • Petrópolis | (8) |
| • São João de Meriti | (8) |
| • Teresópolis | (8) |
| • Volta Redonda | (8) |

Ref. <https://mapadeas.ceptr.br>

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



Rio de Janeiro

- 618 AS
- 354 AS notificados
- 3 AS com mais de 250 IP notificados
- 39.615 endereços IP mal configurados
 - DNS 1.602
 - SNMP 4.045
 - NTP 32.734



MANRS

Mutually Agreed Norms for Routing Security

<http://manrs.org>

<https://bcn.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



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



Programa por uma Internet mais Segura

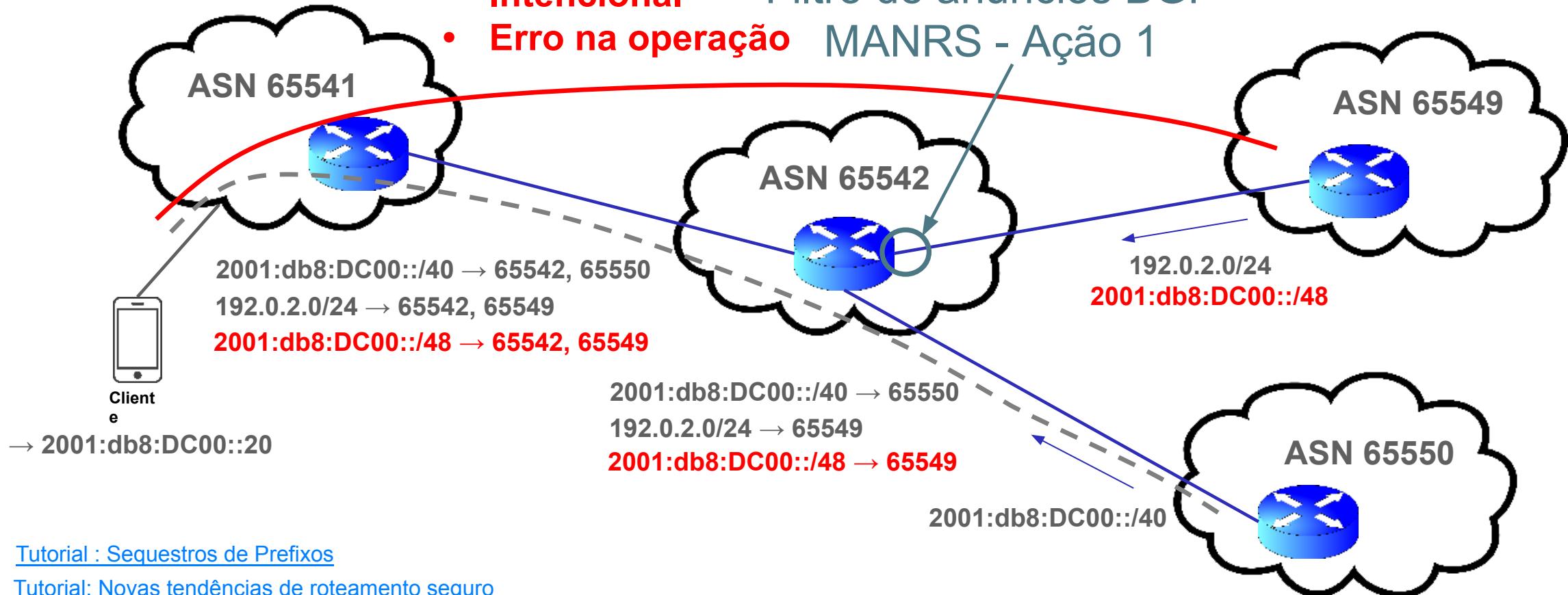


Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

- Intencional
- Erro na operação

Filtro de anúncios BGP
MANRS - Ação 1



[Tutorial : Sequestros de Prefixos](#)

[Tutorial: Novas tendências de roteamento seguro](#)

Programa por uma Internet mais Segura

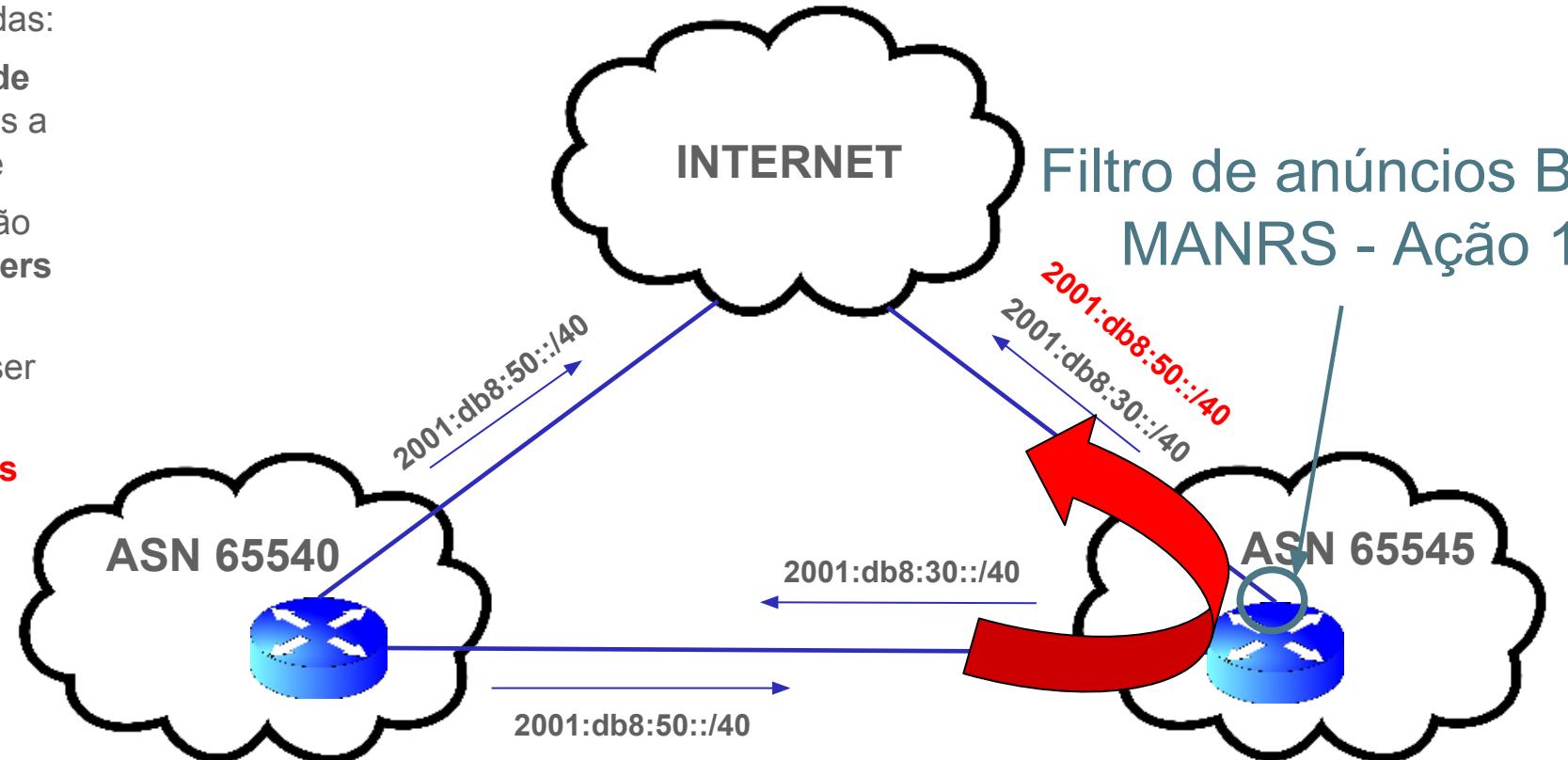


Vazamento de rotas (Route Leak)

- 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

Filtro de anúncios BGP MANRS - Ação 1



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

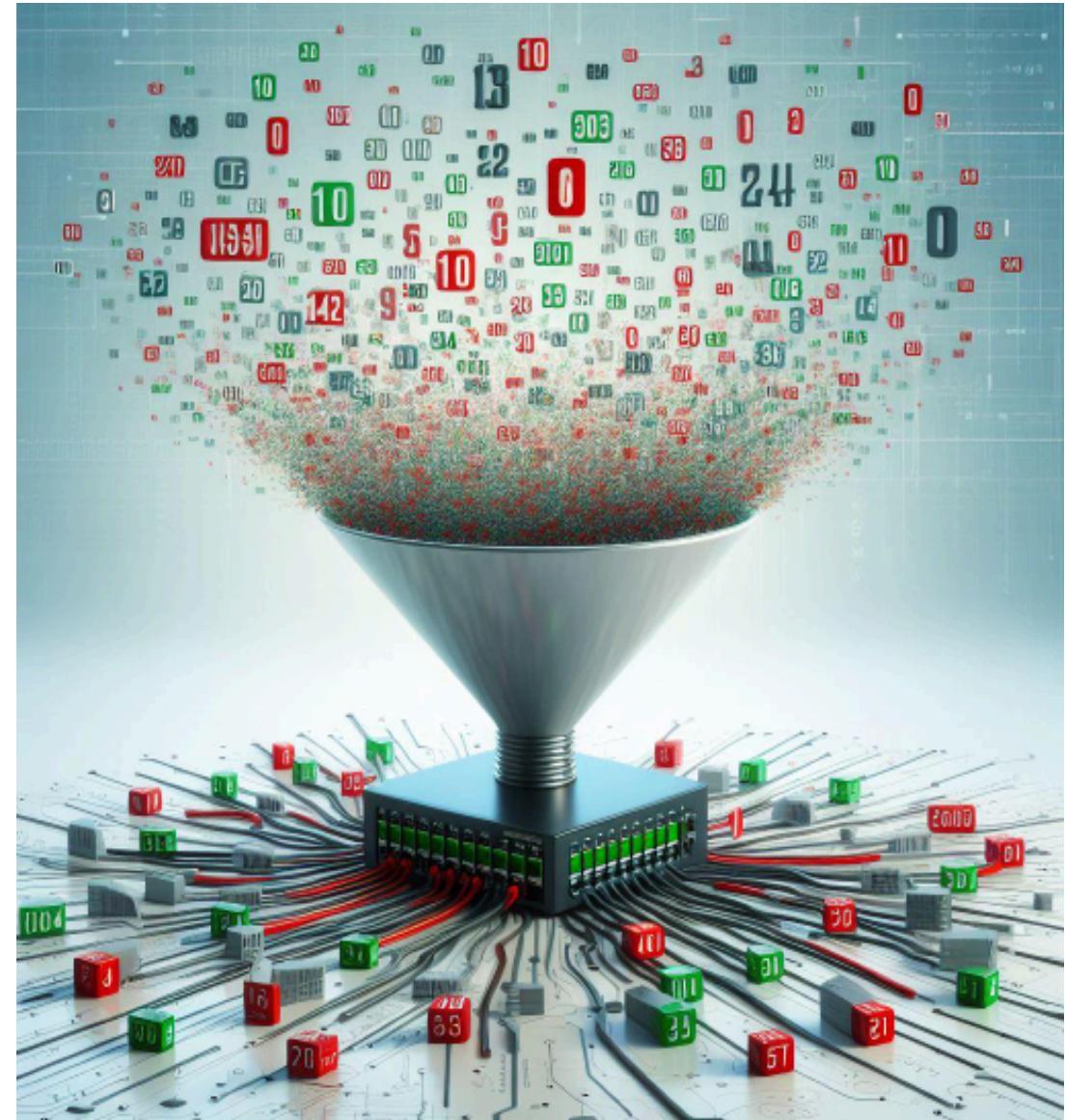
Programa por uma Internet mais Segura



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

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

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

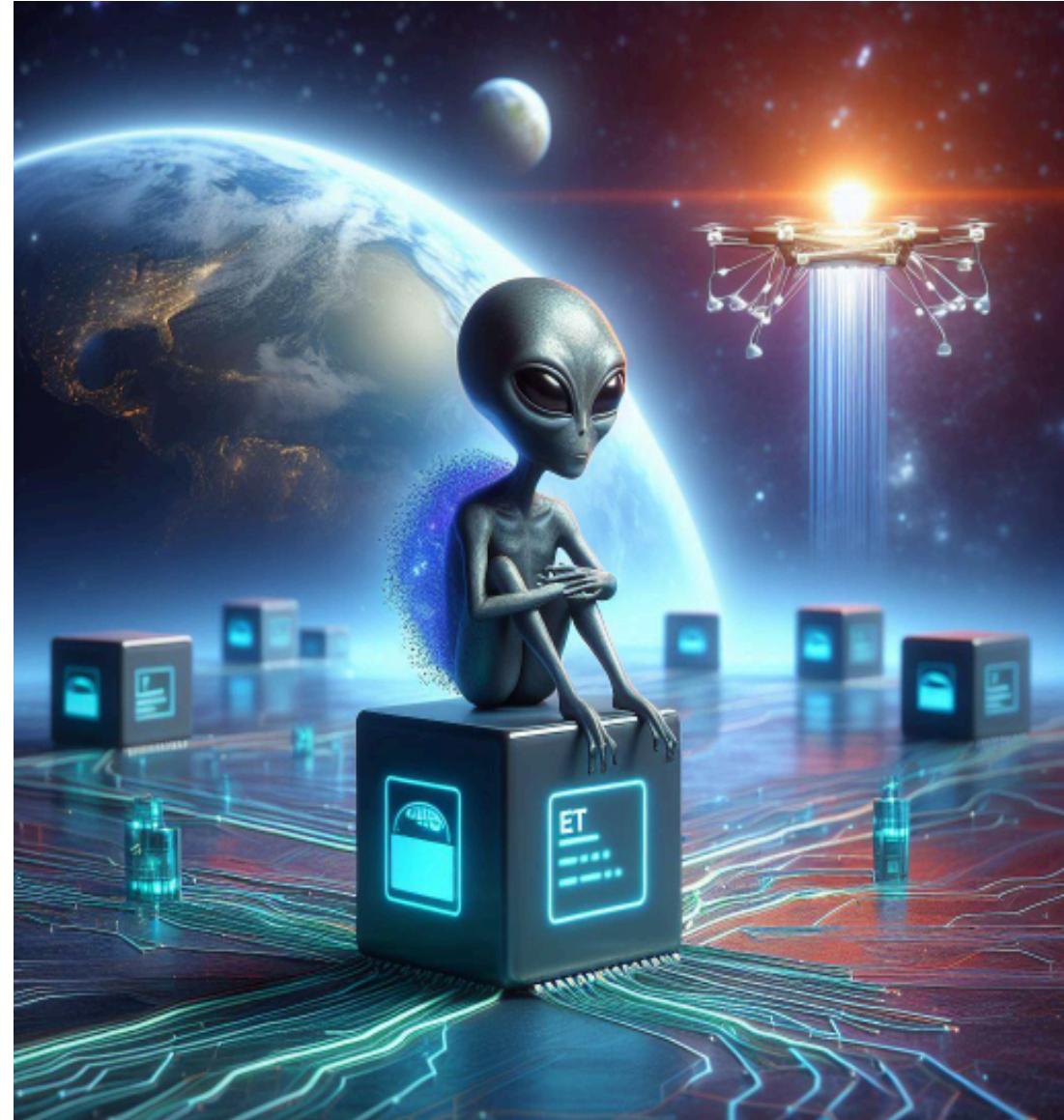


Programa por uma Internet mais Segura



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)!



<https://bcp.nic.br/antspoofing/>

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**



<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

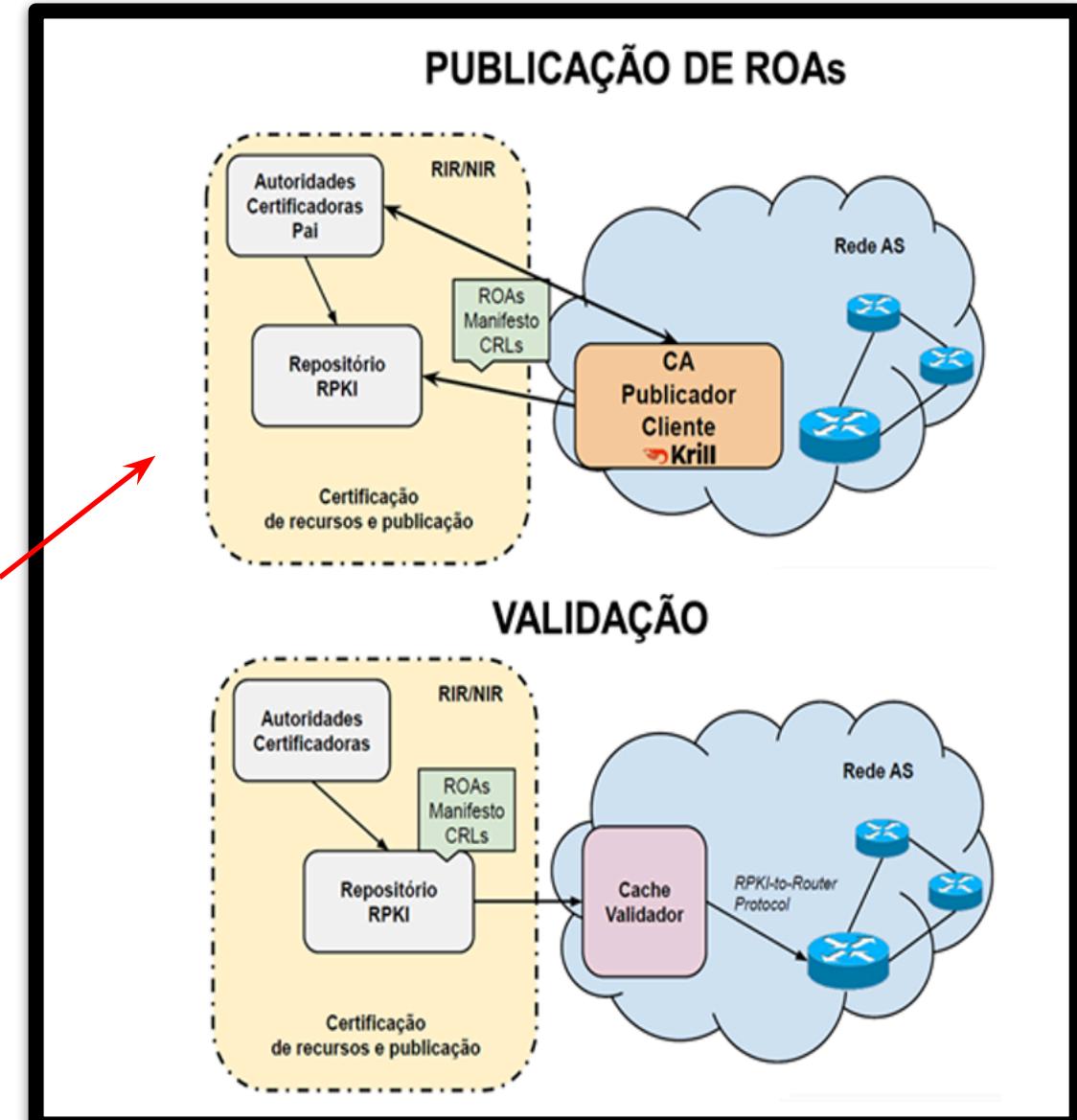
<https://bcp.nic.br/i+seg/acoes/>

Tutorial: [IRR na prática](#)

Tutorial: [Segurança no roteamento com RPKI](#)



Desafio BCOP



Programa por uma Internet mais Segura



Programa por uma Internet mais Segura

MANRS Observatory - 201 AS – ES



PROGRAMA
INTERNET
+SEGURA

| ASN | Holder | Country | UN Regions | UN Sub-Regions | RIR Regions | Filtering | Anti-spoofing | Coordination | Routing Information (IRR) | Routing Information (RPKI) | Participante MANRS | Status abuse | Status Notificações CERT.br |
|---------|--------|---------|------------|---------------------------------|-------------|-----------|---------------|--------------|---------------------------|----------------------------|--------------------|--------------|-----------------------------|
| ASN 9 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | | PEND | |
| ASN 11 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 12 | --- | US | Americas | Northern America | ARIN | 100% | 0% | 100% | 72% | 49% | | PEND | |
| ASN 18 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | | PEND | |
| ASN 20 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 23 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 27 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 32 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 34 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 76% | 100% | | PEND | |
| ASN 37 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 97% | 0% | | PEND | |
| ASN 46 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | NOK |
| ASN 58 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 59 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 15% | | PEND | NOK |
| ASN 61 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 63 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 100% | | PEND | |
| ASN 66 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | | PEND | |
| ASN 77 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | | PEND | |
| ASN 78 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | | PEND | |
| ASN 116 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | | PEND | |
| ASN 119 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 122 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | | PEND | |
| ASN 134 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 155 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 166 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | | PEND | |
| ASN 167 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 173 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | | PEND | |
| ASN 176 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | PEND | |
| ASN 178 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | | PEND | |
| ASN 191 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 98% | 0% | 0% | 100% | 100% | | PEND | |
| ASN 198 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | | PEND | |

Programa por uma Internet mais Segura

MANRS Observatory - 201 AS – ES



| ASN | Holder | Country | UN Regions | UN Sub-Regions | RIR Regions | Filtering | Anti-spoofing | Coordination | Routing Information (IRR) | Routing Information (RPKI) | Participante MANRS | Status abuse | Status Notificações CERT.br |
|---------|--------|---------|------------|---------------------------------|-------------|-----------|---------------|--------------|---------------------------|----------------------------|--------------------|--------------|-----------------------------|
| ASN 21 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | 28128 | BLOCK | |
| ASN 45 | --- | US | Americas | Northern America | ARIN | 100% | 0% | 100% | 82% | 36% | | BLOCK | |
| ASN 70 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | | BLOCK | |
| ASN 104 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | | BLOCK | |
| ASN 110 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | | BLOCK | |
| ASN 189 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | | BLOCK | |
| ASN 192 | --- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 0% | 100% | 0% | | BLOCK | |

Programa por uma Internet mais Segura

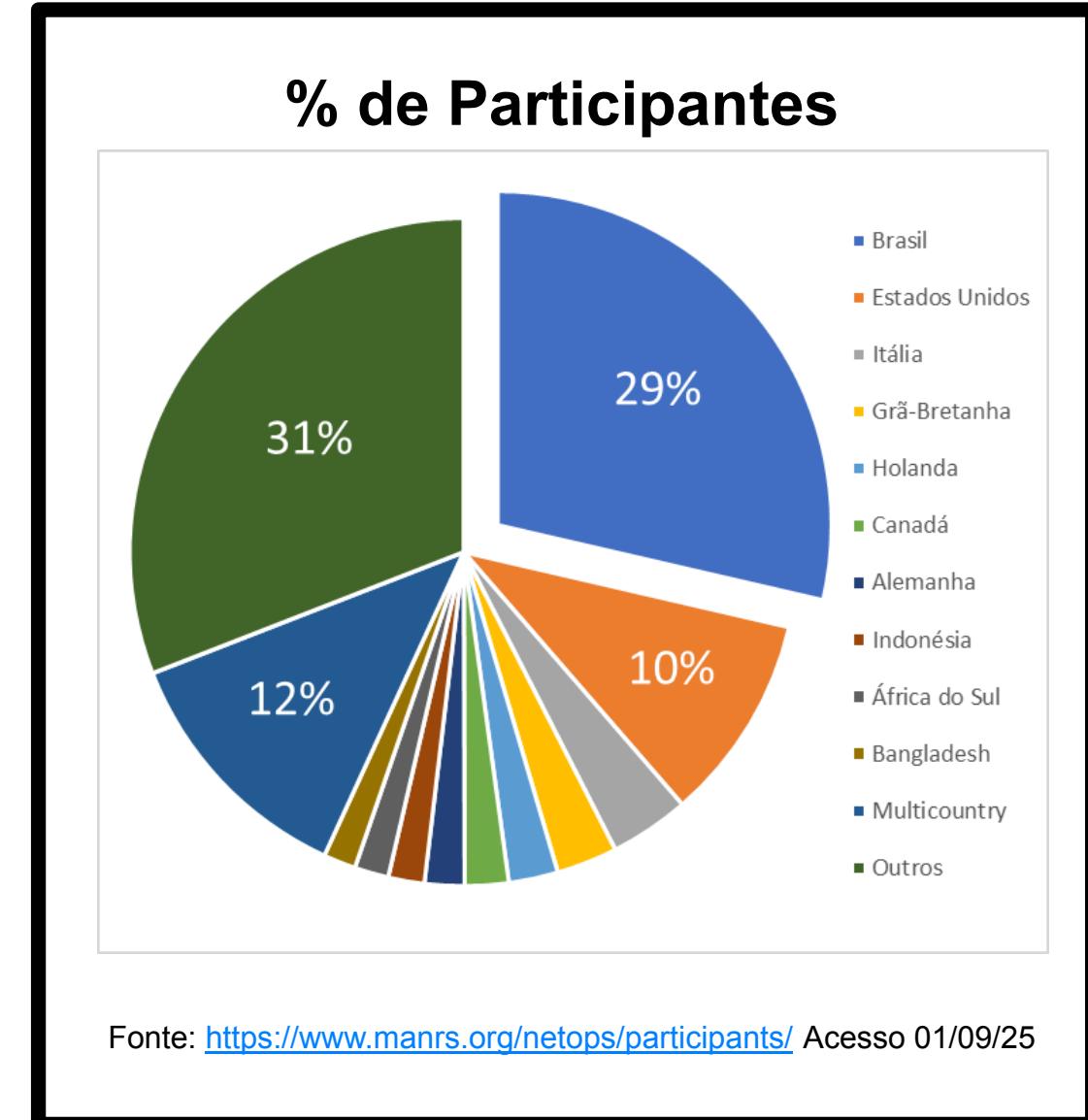


Participantes por país

- Total: 1.087
- Participantes no Brasil → 311



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



Programa por uma Internet mais Segura

MANRS Observatory - 201 AS – ES



| ASN | Holder | Country | UN Regions | UN Sub-Regions | RIR Regions | Filtering | Anti-spoofing | Coordination | Routing Information (IRR) | Routing Information (RPKI) | Participante MANRS | Status abuse-c |
|---------|--------|---------|------------|---------------------------------|-------------|-----------|---------------|--------------|---------------------------|----------------------------|--------------------|----------------|
| ASN 1 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 99% | 98% | 1916 | OK |
| ASN 21 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | 28128 | BLOCK |
| ASN 24 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 100% | 100% | 100% | 100% | 28171 | OK |
| ASN 29 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 100% | 100% | 100% | 100% | 28260 | OK |
| ASN 35 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | 28366 | OK |
| ASN 42 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 100% | 100% | 100% | 100% | 28658 | OK |
| ASN 86 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 100% | 100% | 100% | 100% | 53181 | OK |
| ASN 123 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 36% | 100% | 100% | 100% | 262369 | OK |
| ASN 143 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | 262808 | OK |
| ASN 148 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | 262888 | OK |
| ASN 149 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | 262896 | OK |
| ASN 154 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | 262977 | OK |
| ASN 162 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 94% | 0% | 263047 | OK |
| ASN 163 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 100% | 263057 | OK |
| ASN 201 | -- | BR | Americas | Latin America and the Caribbean | LACNIC | 100% | 0% | 100% | 100% | 0% | 263982 | OK |



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

<https://kindns.org/>

An ICANN
Initiative



Programa por uma Internet mais Segura

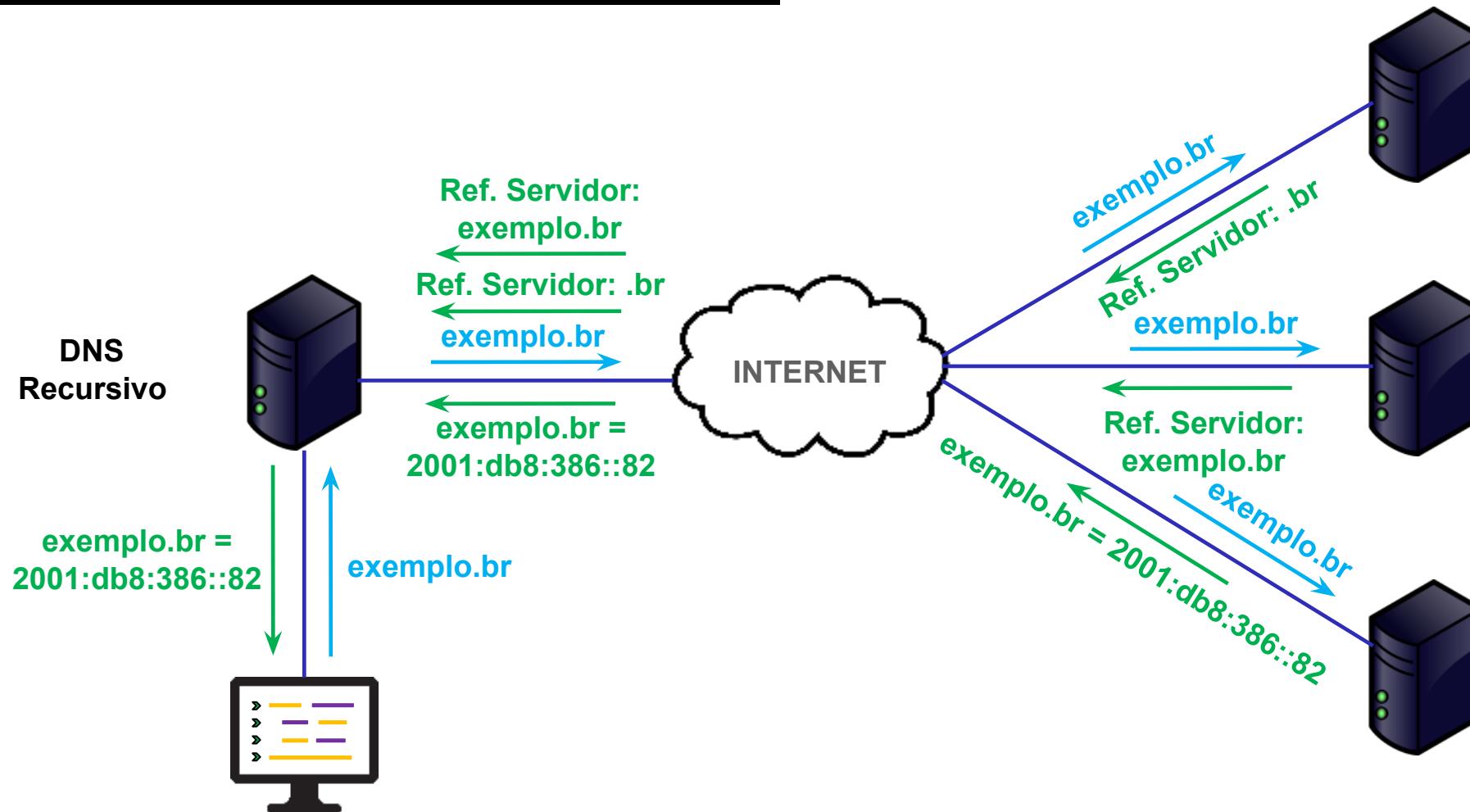
Processo de Recursão DNS



DNS
Autoritativo Raiz
“.”

DNS
Autoritativo
“.br”

DNS
Autoritativo
“exemplo.br”



Tutorial: [Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning](#)

Programa por uma Internet mais Segura

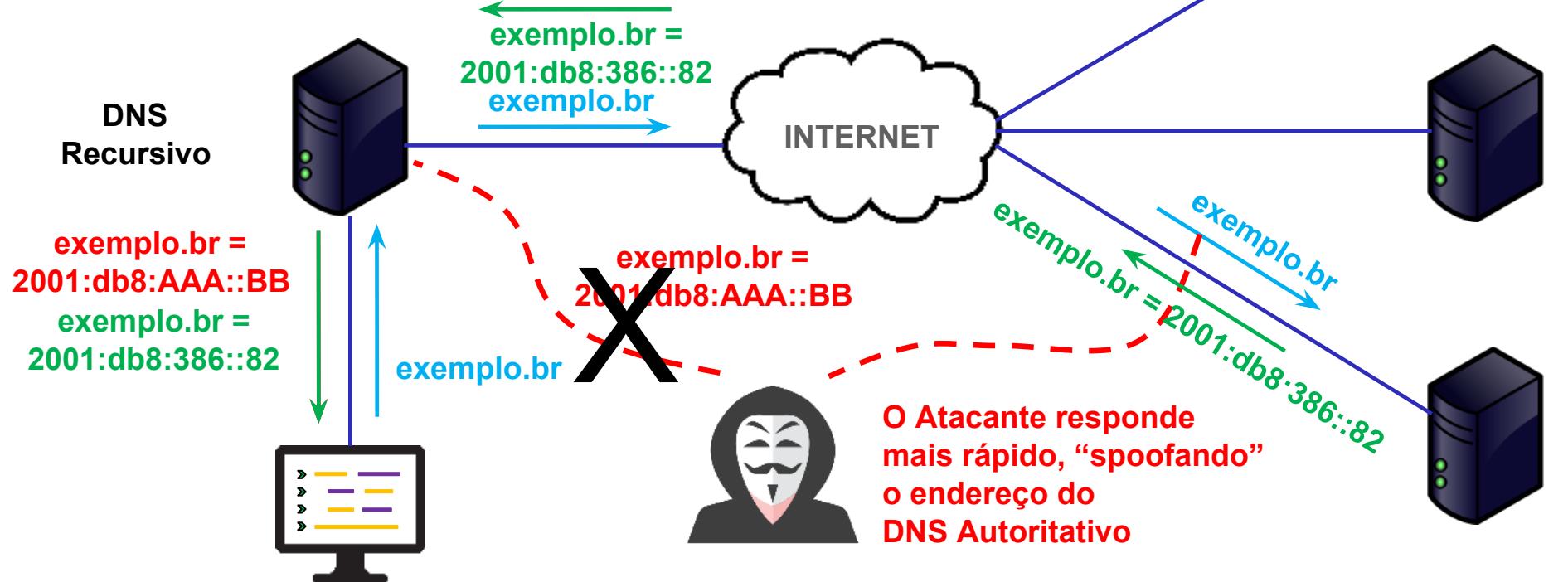


Ataque DNS - Poisoning

O servidor de nomes recursivo valida as assinaturas DNSSEC do nome de domínio (Ação 1 KINDNS - TOP)

DNSSEC - RFC 9364

- * Consultas DNS seguras
- * Garante autenticidade e integridade
- * Não garante confidencialidade
- * Não protege contra DDoS



Tutorial: [Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning](#)

DNS
Autoritativo Raiz
“.”

DNS
Autoritativo
“.br”

DNS
Autoritativo
“exemplo.br”



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/>

Tutorial: [Configurando o seu DNS de forma simples e segura](#)





TOP
TESTE OS PADRÕES

<https://top.nic.br>



The screenshot shows the homepage of the TOP Testes Padrões website. At the top, there's a navigation bar with links for 'Quem é TOP', 'Sobre', 'Referências', and 'Comunicações'. The main heading reads: '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 main sections:

- Teste TOP - Site**: Endereço IP moderno? Domínio assinado? Canivela segura? Opções de segurança?
Nome de domínio do seu site: Iniciar o teste
- Teste TOP - E-mail**: Endereço IP moderno? Domínio assinado? Proteção contra phishing? Conexão segura?
Nome de domínio do seu e-mail: Iniciar o teste
- Teste TOP - IPv6 e DNSSEC da sua rede**: Endereços modernos e seguros? Analise uma lista com links validados?
Iniciar o teste

<https://top.nic.br>

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!

Programa por uma Internet mais Segura

Testes realizados

- Teste TOP Site ← Desafio BCOP
 - 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
- ↑
Desafio BCOP

[Tutorial: Teste para padrões técnicos e modernos de Internet](#)

The screenshot shows the homepage of the TOP (TESTE OS PADRÕES) website. At the top right are links for 'Quem é TOP', 'Sobre', 'Participar', and 'Comunicados'. The main content area features a question: 'Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?'. Below this are three large cards: 'Teste TOP - Site' (green), 'Teste TOP - E-mail' (blue), and 'Teste TOP - IPv6 e DNSSEC da sua rede' (purple). Each card has a placeholder for a domain name and a 'Iniciar o teste' button.

<https://top.nic.br>

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://bcn.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>



Programa por uma Internet mais Segura

APOIO



A CONECTIVIDADE AO SEU ALCANCE



Obrigado

Gilberto Zorello
gzorello@nic.br
@@ br



24 de outubro de 2025

nic.br cgi.br
www.nic.br | www.cgi.br