

Segurança de Redes

Programa por uma Internet mais segura

Gilberto Zorello | gzorello@nic.br

IX Fórum Edição Norte

Manaus, AM | 23/08/24

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





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>



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

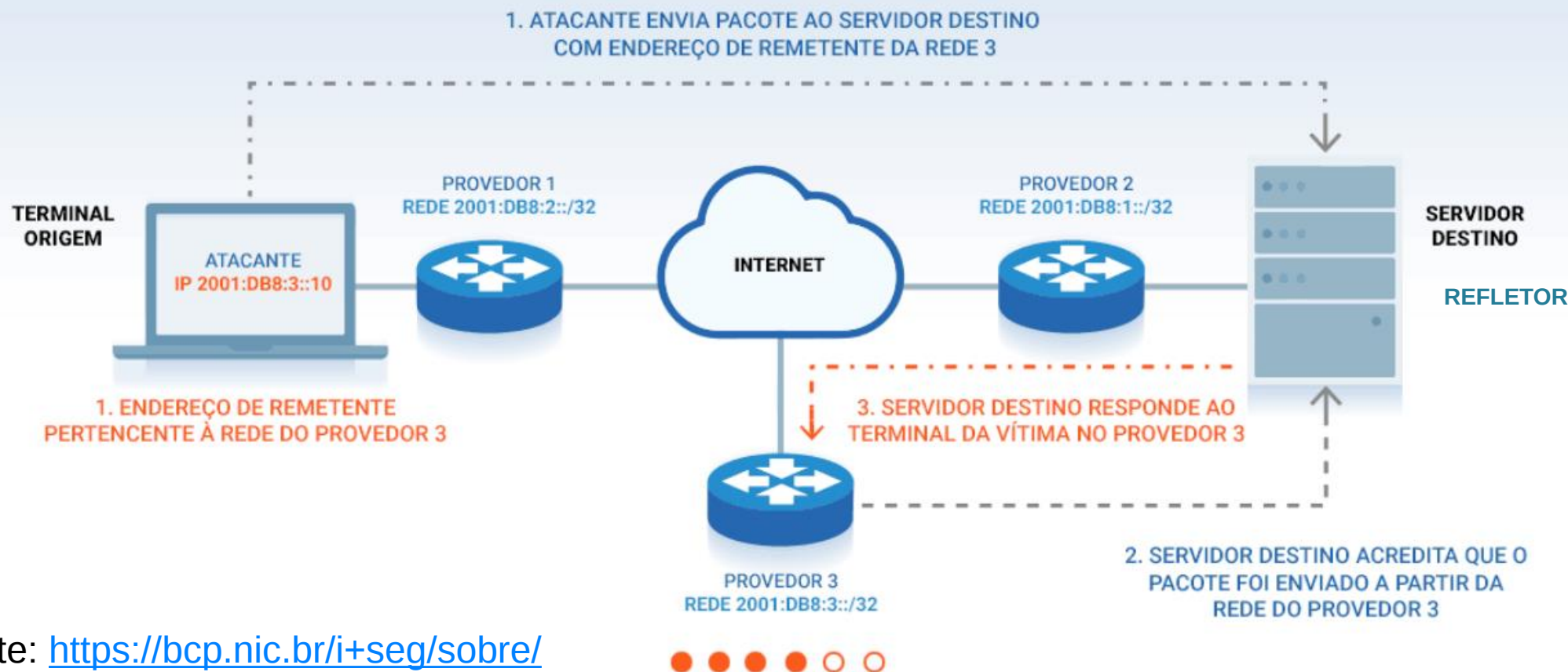
<https://bcp.nic.br/i+seg/acoes/amplificacao/>



Programa por uma Internet mais Segura

Ataque DoS por reflexão

Ataque DoS utilizando endereço de remetente forjado (Spoofing)

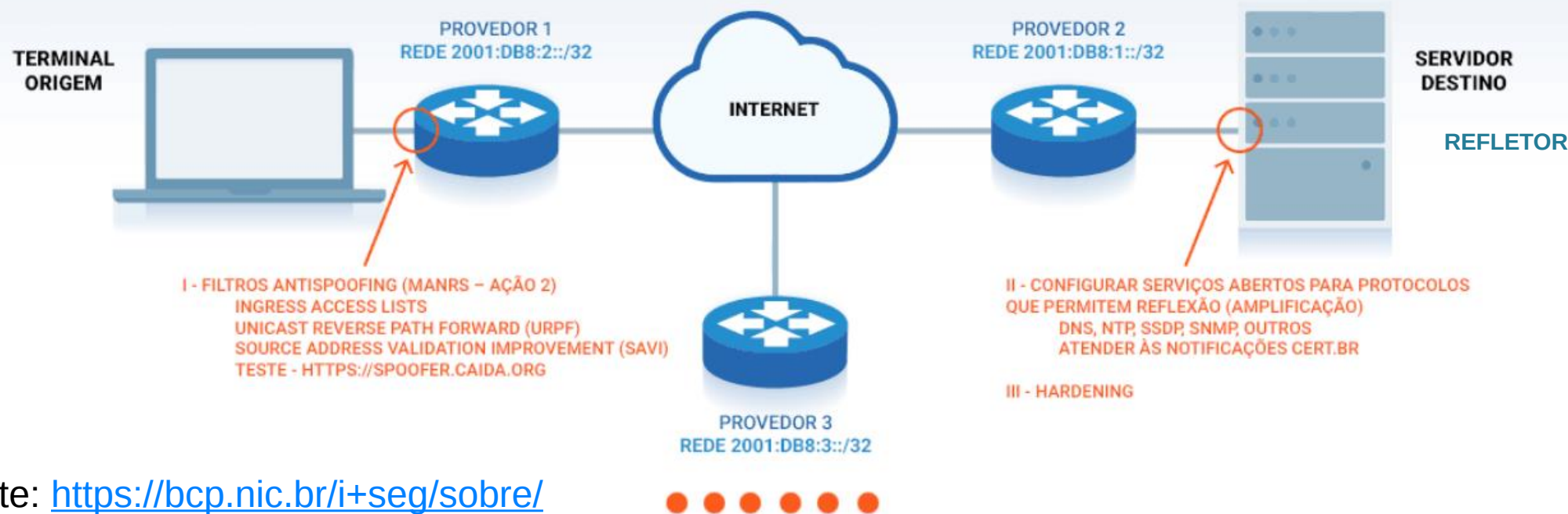


Fonte: <https://bcp.nic.br/i+seg/sobre/>

Programa por uma Internet mais Segura

Ataque DoS por reflexão

Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening



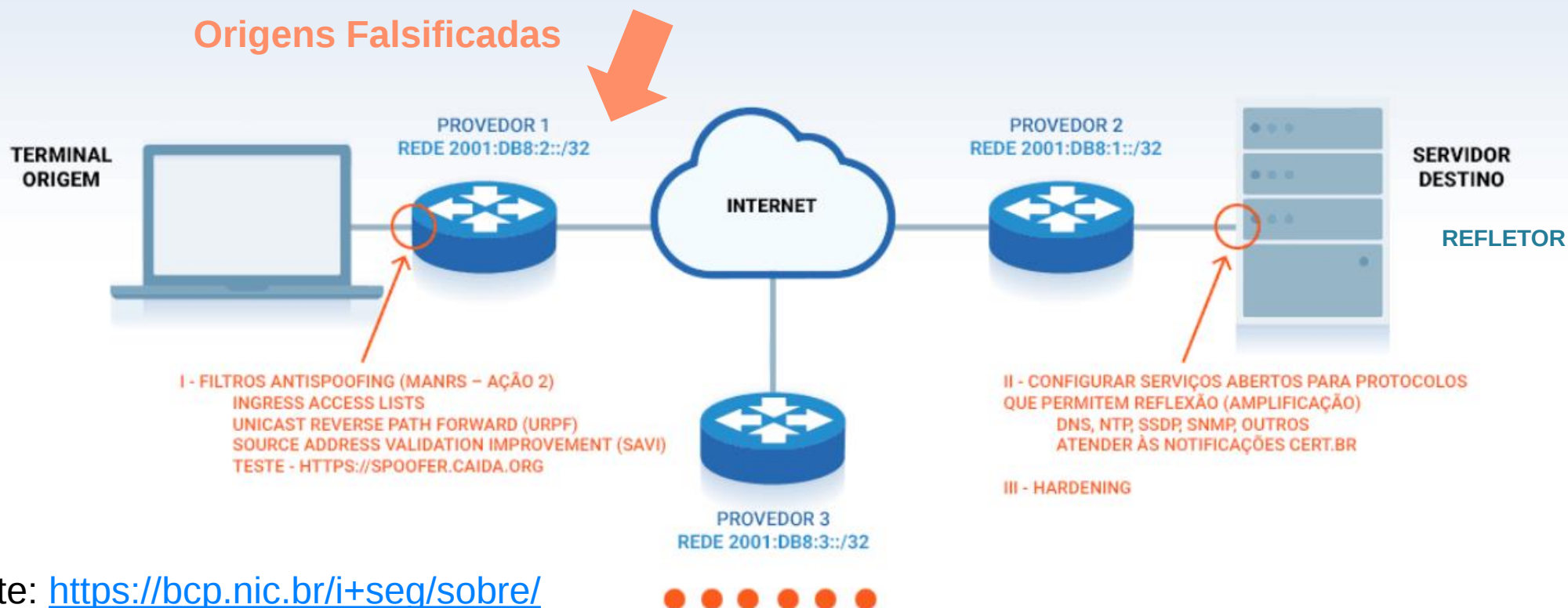
Fonte: <https://bcp.nic.br/i+seg/sobre/>

Programa por uma Internet mais Segura

Ataque DoS por reflexão

Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening

Desafio BCOP 2024

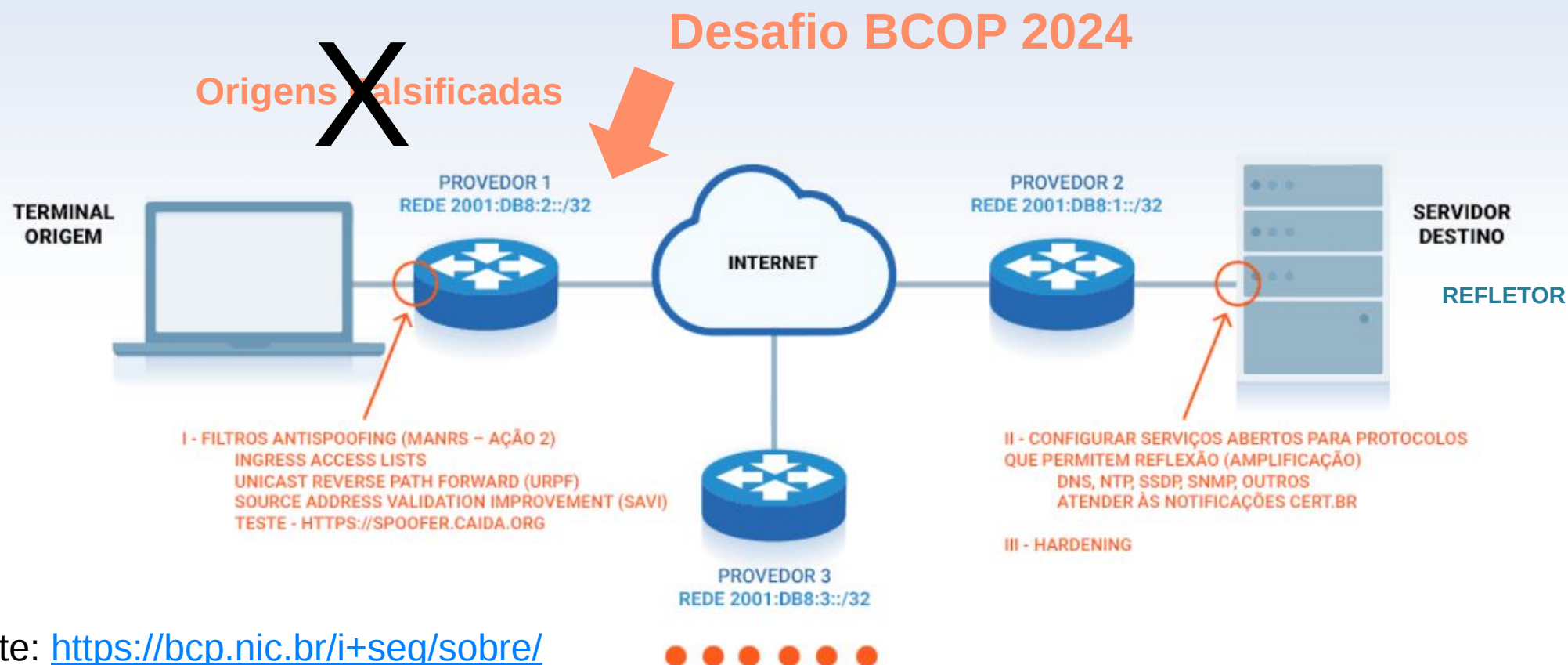


Fonte: <https://bcp.nic.br/i+seg/sobre/>

Programa por uma Internet mais Segura

Ataque DoS por reflexão

Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening



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

Programa por uma Internet mais Segura

Ataque DoS por reflexão

Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening



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

Programa por uma Internet mais Segura

Ataque DoS por reflexão

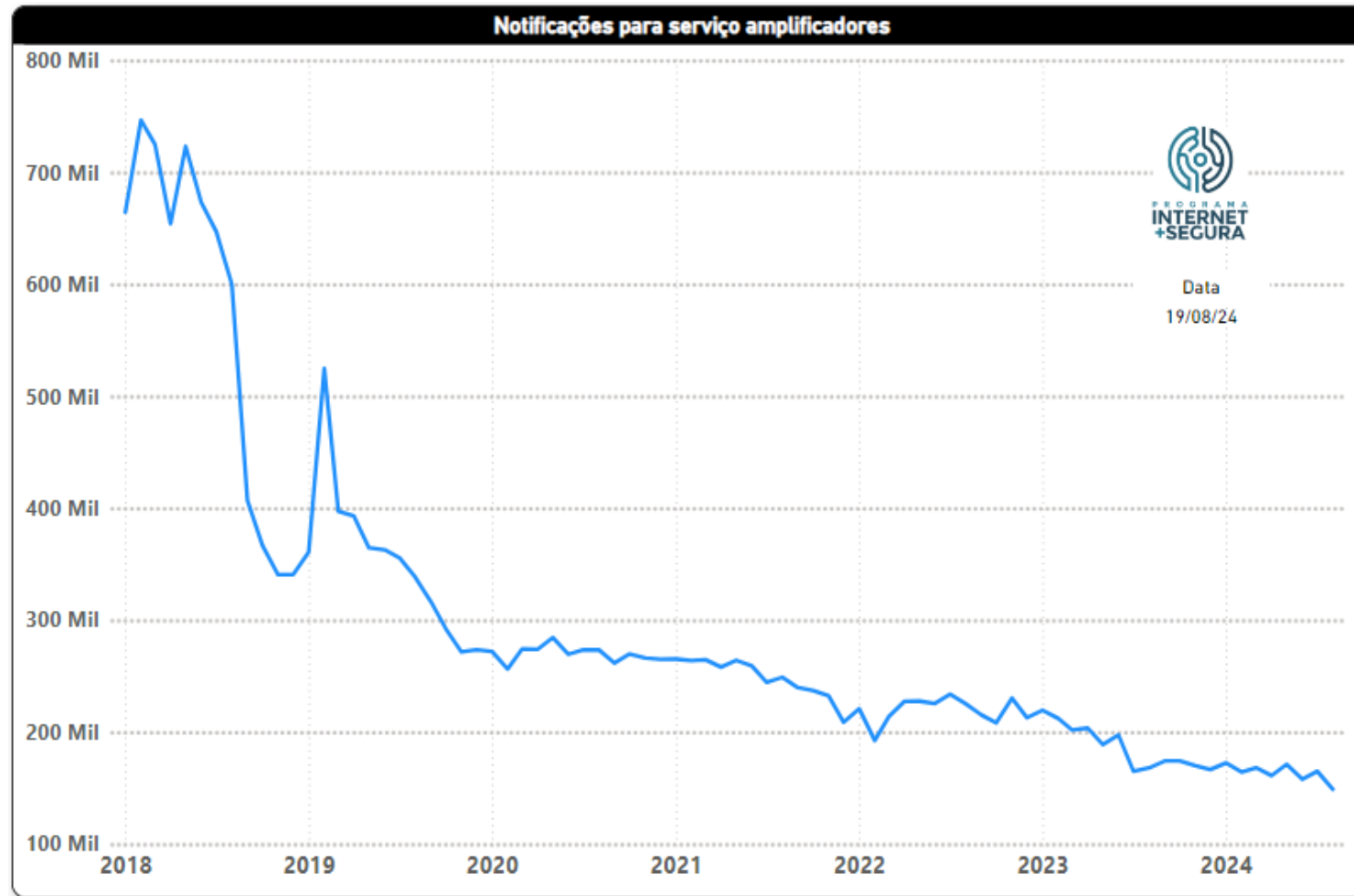
Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening



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

Programa por uma Internet mais Segura

Notificação de amplificadores - evolução

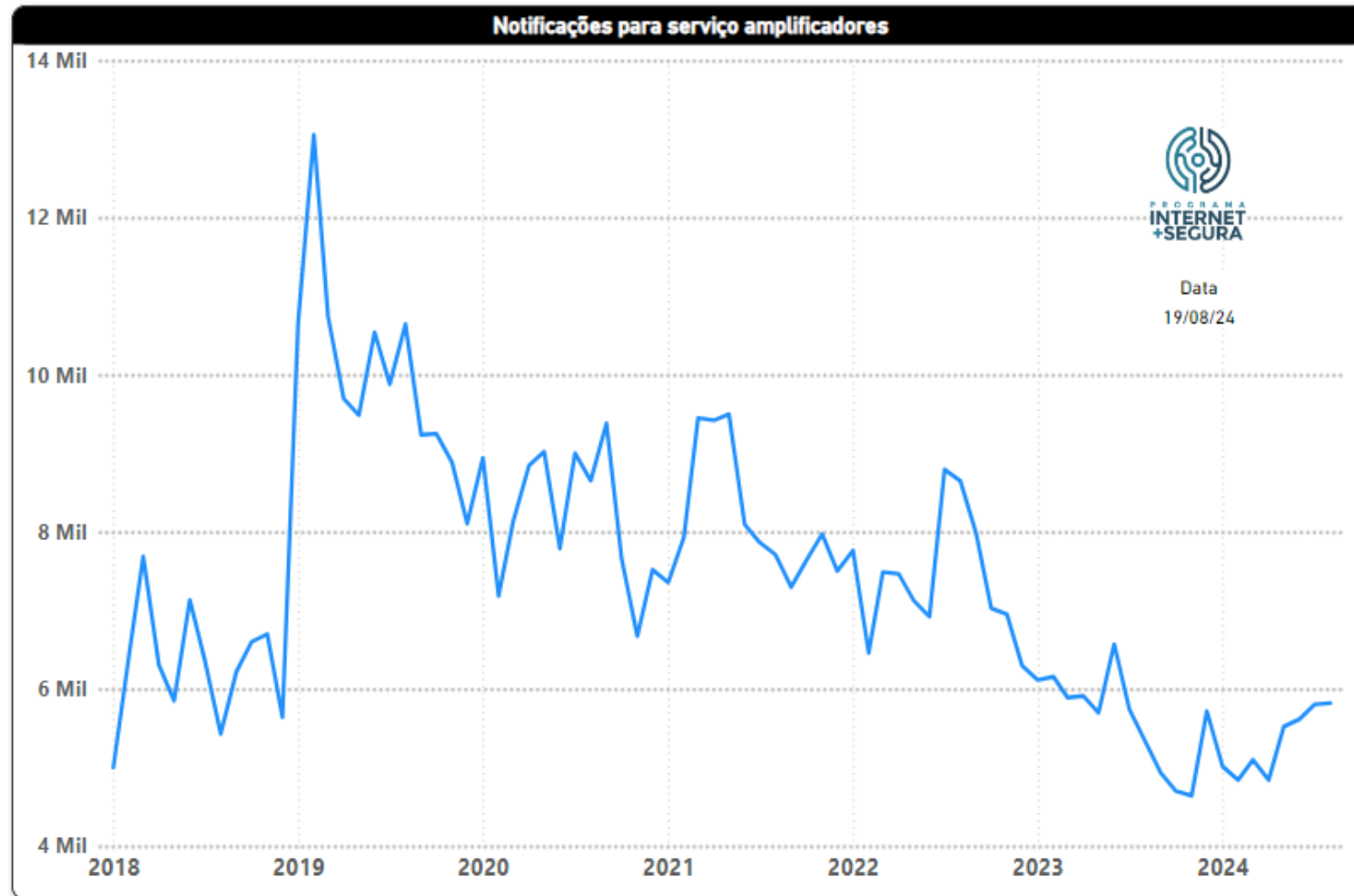


Brasil

- Início (fev/2018)
 - Endereços IP: 746.508
 - Serviços: 5
- Atual:
 - Endereços IP: 150.670
 - Serviços: 19
 - **Redução de 80%**

Programa por uma Internet mais Segura

Notificação de amplificadores - evolução

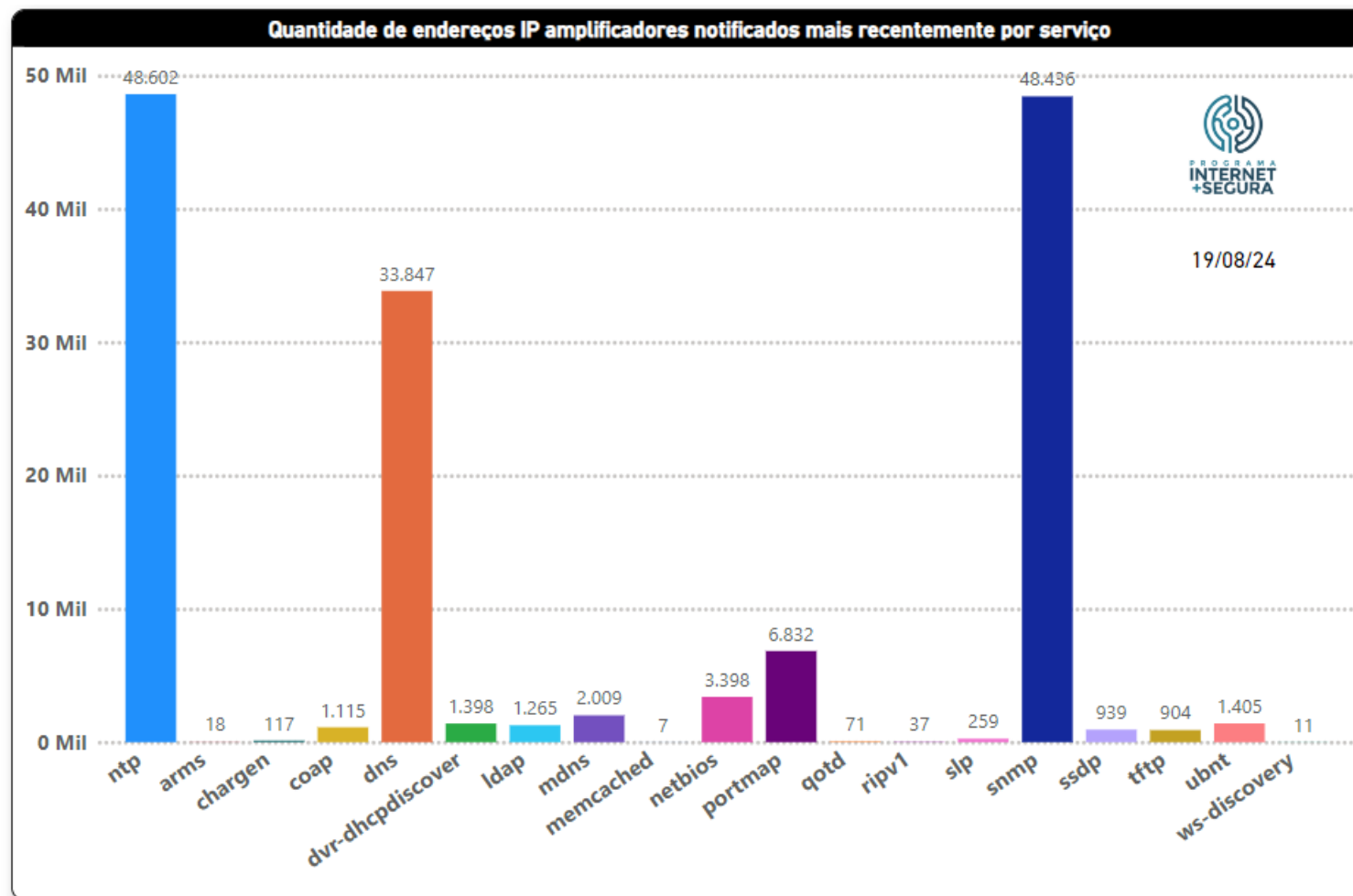


Região Norte

- Pico (fev/2019)
 - Endereços IP: 13.053
 - Serviços: 12
- Atual:
 - Endereços IP: 5.842
 - Serviços: 16

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

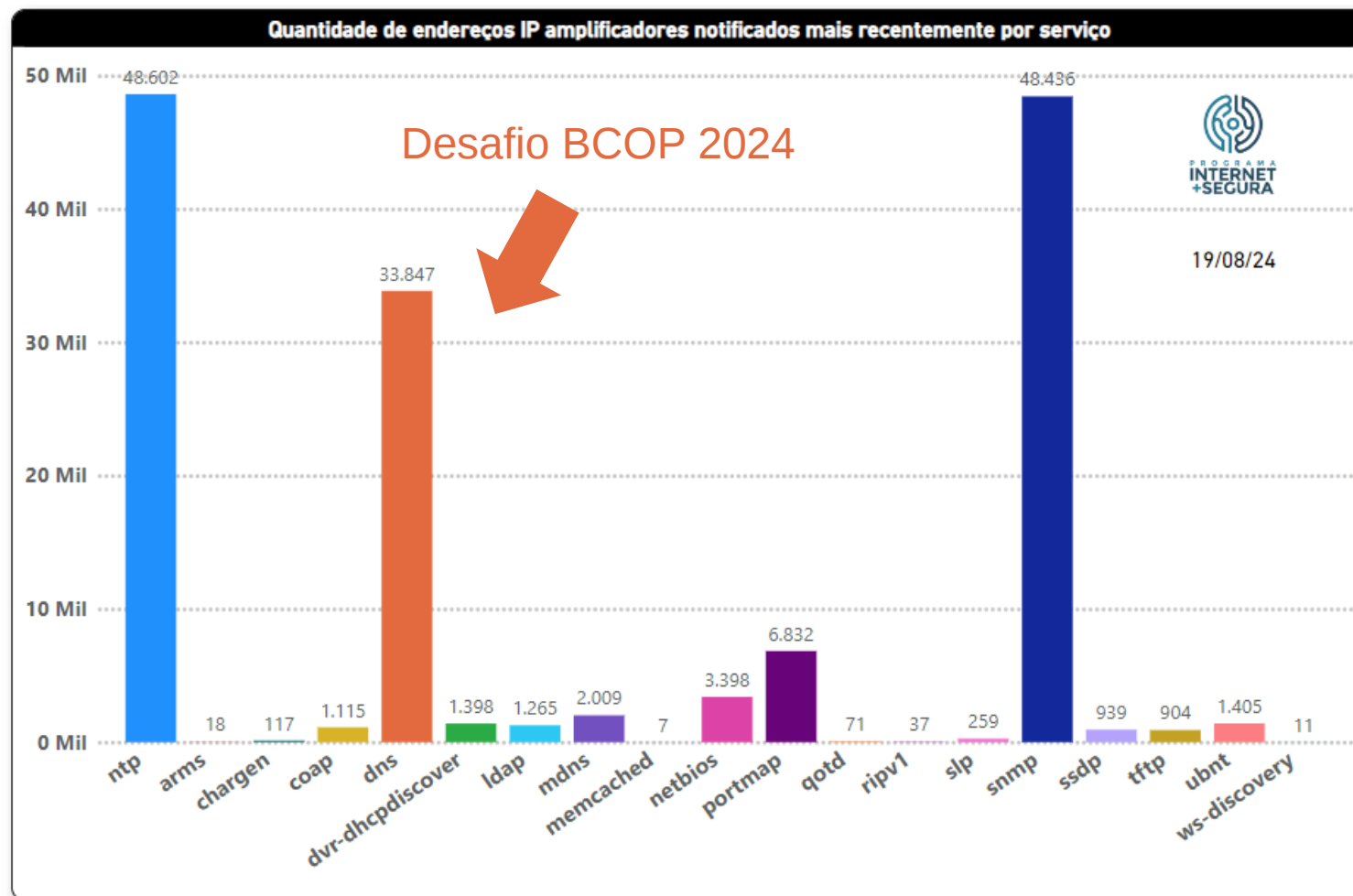


Brasil

- 5241 AS notificados
- 150670 endereços IP mal configurados
- **SNMP 48436**
- **DNS 33847**
- **NTP 48602**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

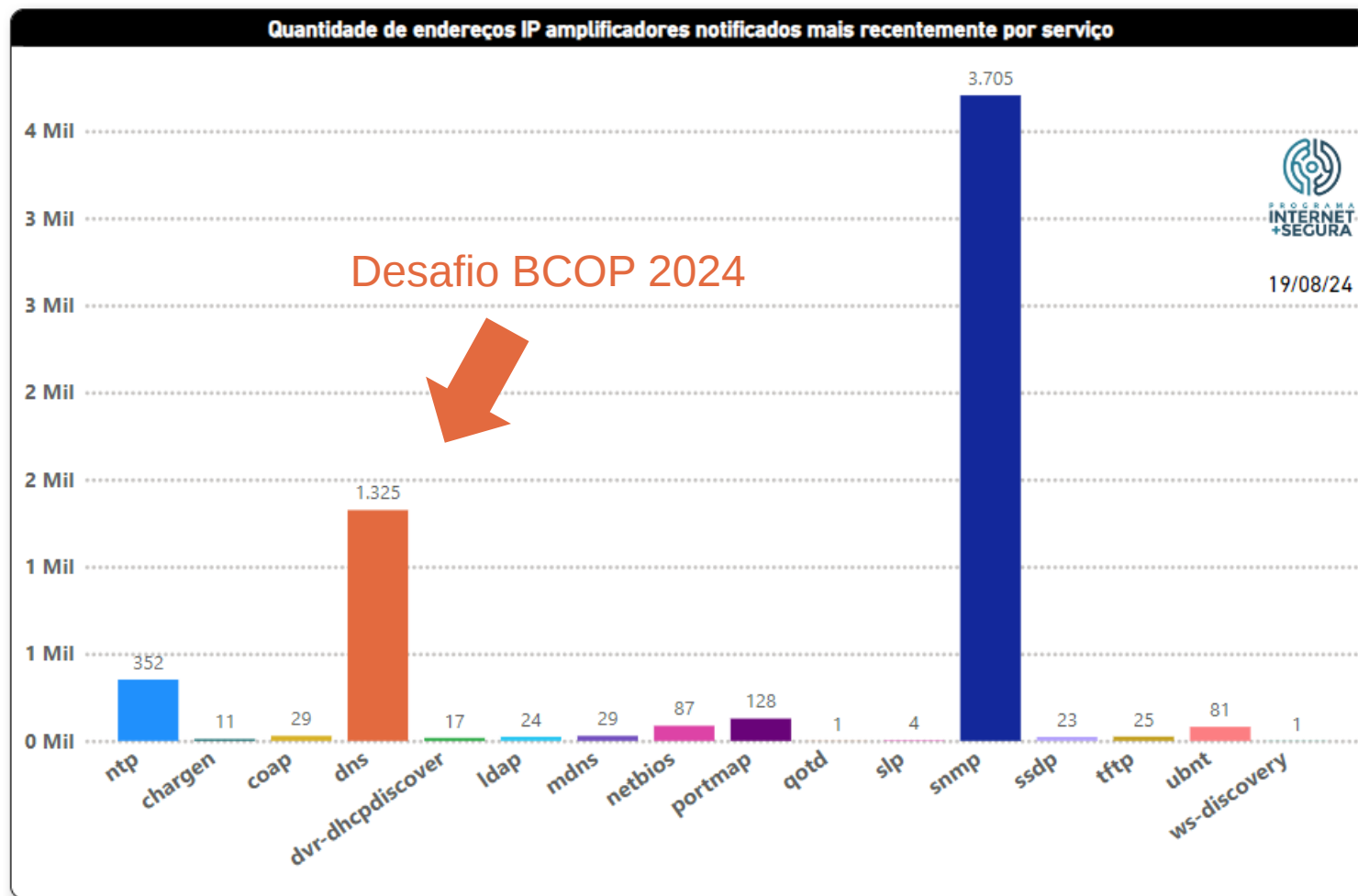


Brasil

- 5241 AS notificados
- 150670 endereços IP mal configurados
- **SNMP 48436**
- **DNS 33847**
- **NTP 48602**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



Região Norte

- 342 AS notificados
- 5842 endereços IP mal configurados
- **SNMP 3705**
- **DNS 1325**
- **NTP 352**



MANRS

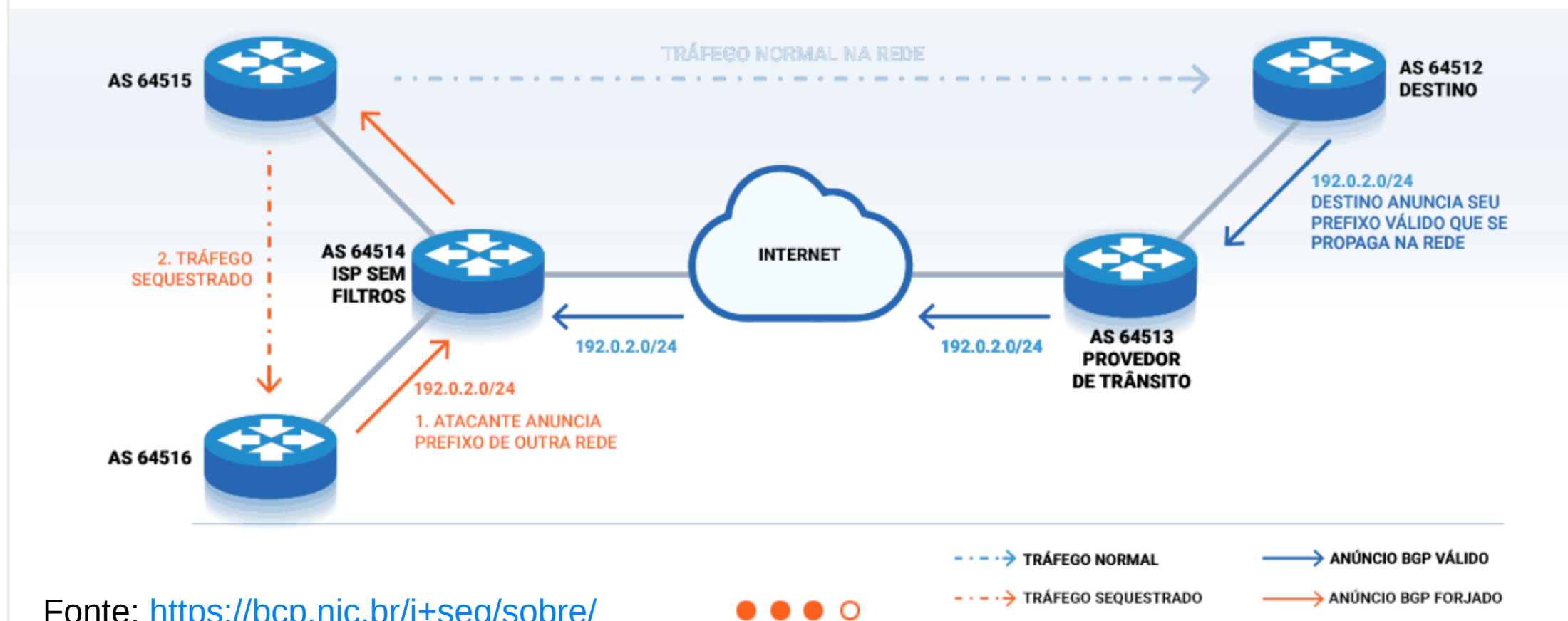
Mutually Agreed Norms for Routing Security

<http://manrs.org>

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

Programa por uma Internet mais Segura

Ataque por Sequestro de Prefixos (Hijacking) Topologia de rede sem filtros de anúncios

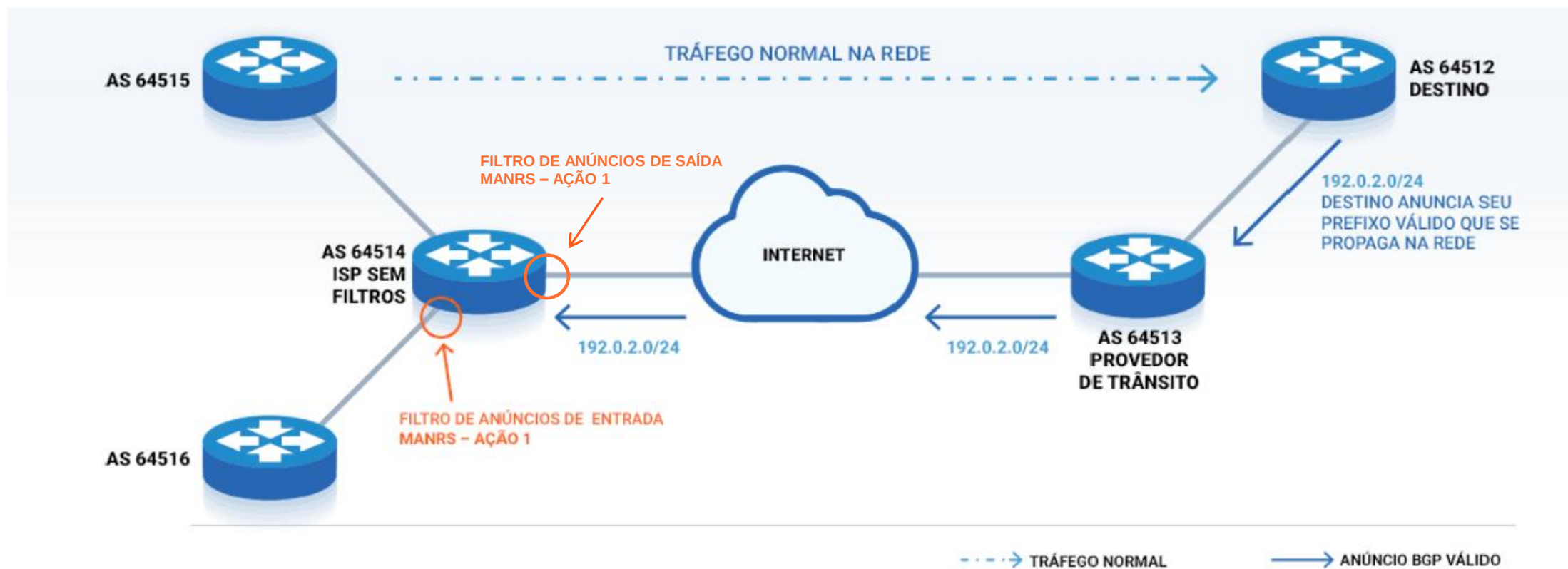


Fonte: <https://bcp.nic.br/i+seg/sobre/>

Programa por uma Internet mais Segura

Ataque por Sequestro de Prefixos (Hijacking)

Solução: Filtro de anúncios de entrada (clientes) – MANRS - Ação 1



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



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/>



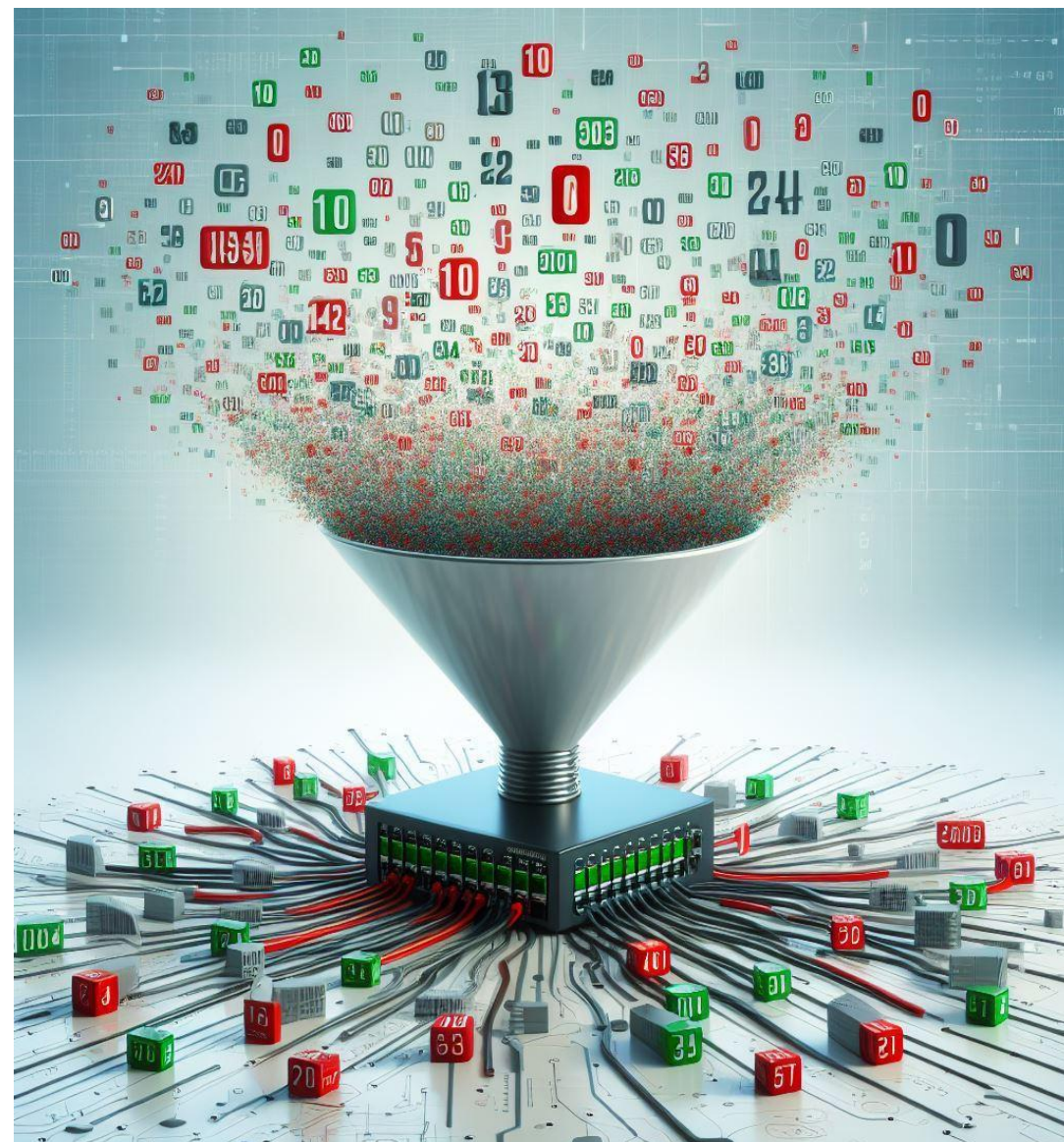
Programa por uma Internet mais Segura



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>

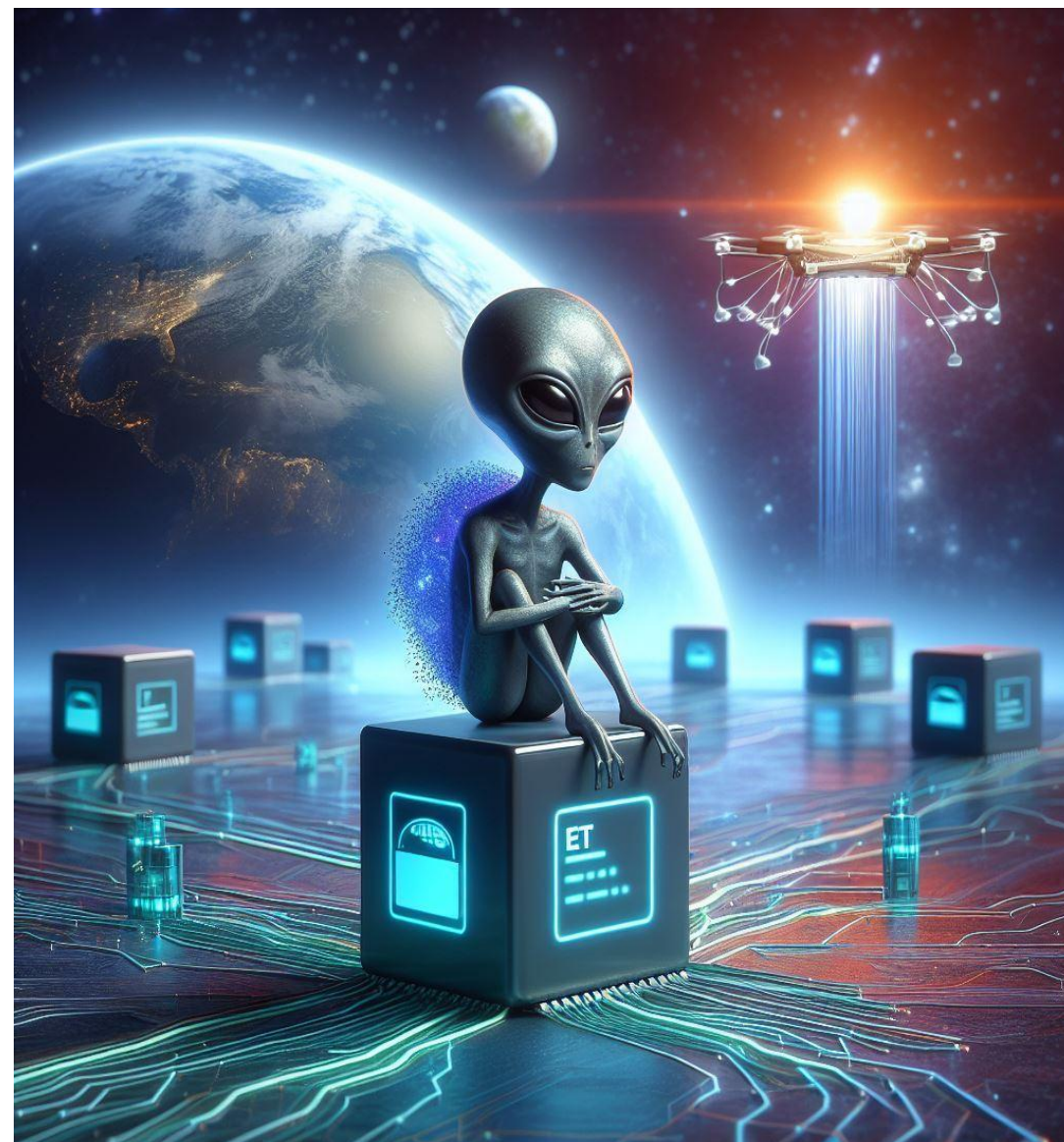


Programa por uma Internet mais Segura



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**



Programa por uma Internet mais Segura

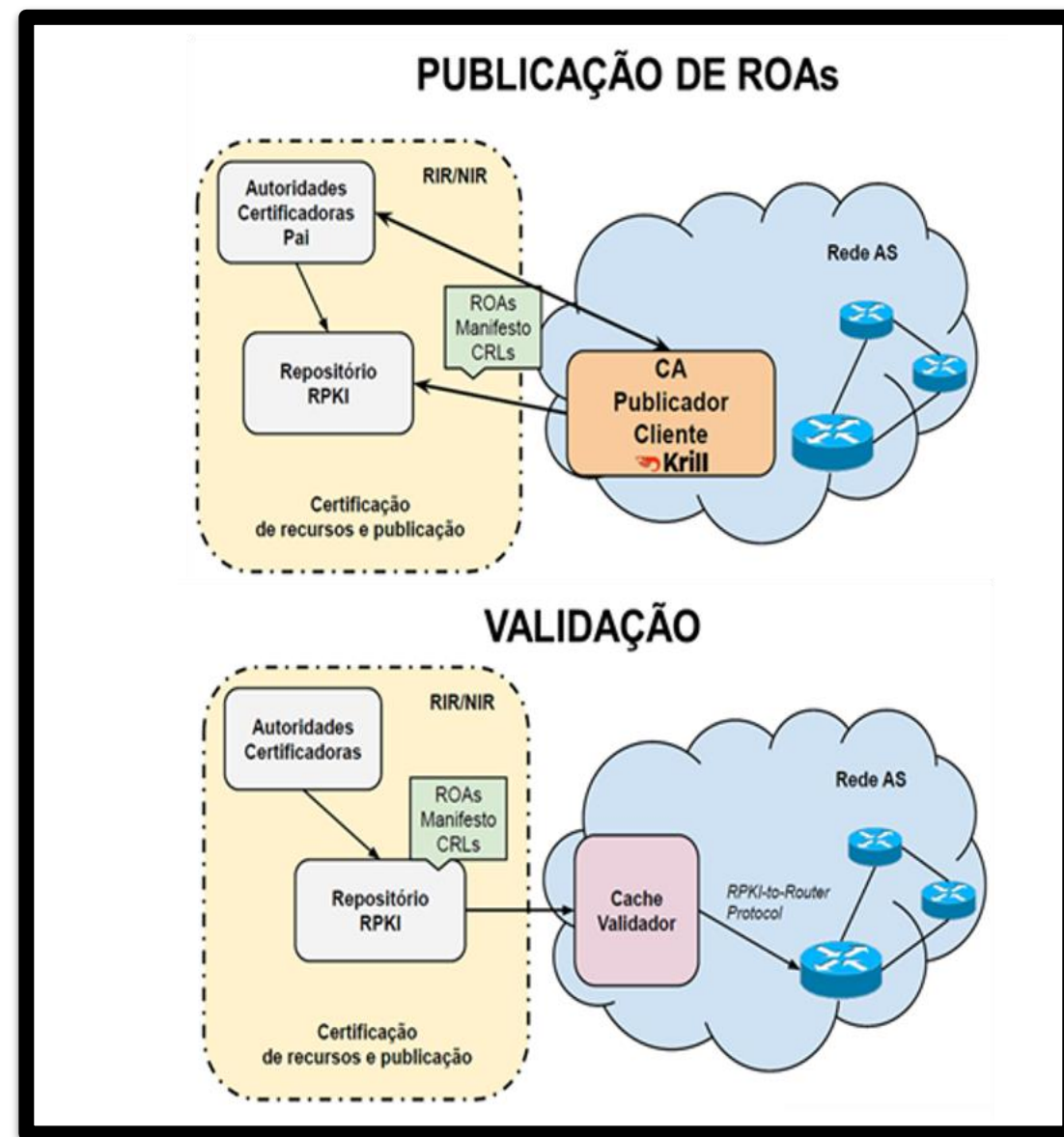


MANRS - Ação 4 - Cadastro da Política de Roteamento

- **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 - 545 AS - NO

MONTH

July 2024



MANRS

Incidents

Route misoriginations
Route leaks
Bogon announcements

Total

Culprits

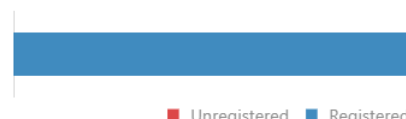
5
0
3
8

Routing Information (IRR)

6
Unregistered
Registered

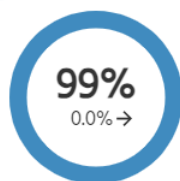
Routing Information (RPKI)

1.1%	Valid	1,482	35.4%
98.9%	Unknown	2,674	64.0%
	Invalid	24	0.6%

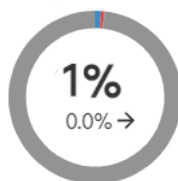


MANRS Readiness

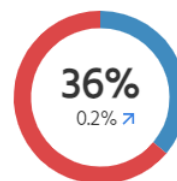
Filtering



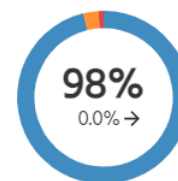
Anti-spoofing



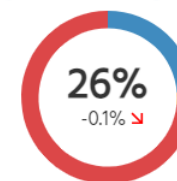
Coordination



Routing Information (IRR)



Routing Information (RPKI)



● Ready ● Aspiring ● Lagging ● No Data Available

Programa por uma Internet mais Segura

MANRS Observatory - 545 AS - NO

MONTH

July 2024



MANRS

Incidents

Route misoriginations
Route leaks
Bogon announcements

Total

Culprits

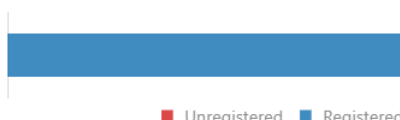
5
0
3
8

Routing Information (IRR)

6
Unregistered
Registered

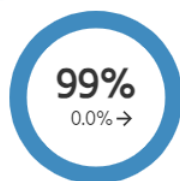
Routing Information (RPKI)

1.1% Valid
98.9% Unknown
Invalid
1,482
2,674
24
35.4%
64.0%
0.6%

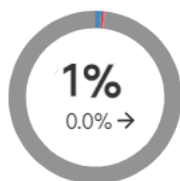


MANRS Readiness

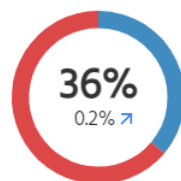
Filtering



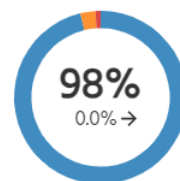
Anti-spoofing



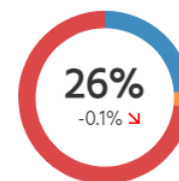
Coordination



Routing Information (IRR)



Routing Information (RPKI)



Ready Aspiring Lagging No Data Available

Desafio BCOP 2024

Programa por uma Internet mais Segura

MANRS Observatory - 23 AS – Part. IX NO



MANRS

MONTH

July 2024

Incidents

Route misoriginations
Route leaks
Bogon announcements
Total

0
0
1
1

Culprits

Culprits

Routing Information (IRR)

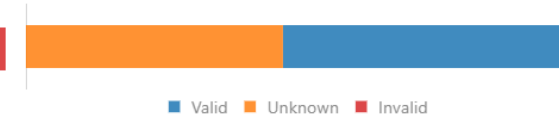
1 Unregistered
Registered

45
223

Routing Information (RPKI)

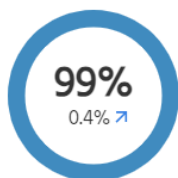
16.8% Valid
83.2% Unknown
Invalid

142 53.0%
126 47.0%
0 0.0%

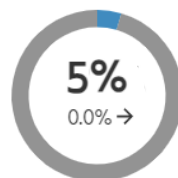


MANRS Readiness

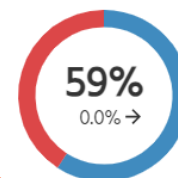
Filtering



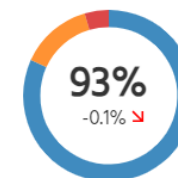
Anti-spoofing



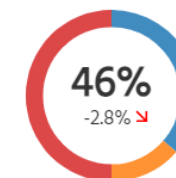
Coordination



Routing Information (IRR)



Routing Information (RPKI)



● Ready ● Aspiring ● Lagging ● No Data Available

Desafio BCOP 2024

Programa por uma Internet mais Segura



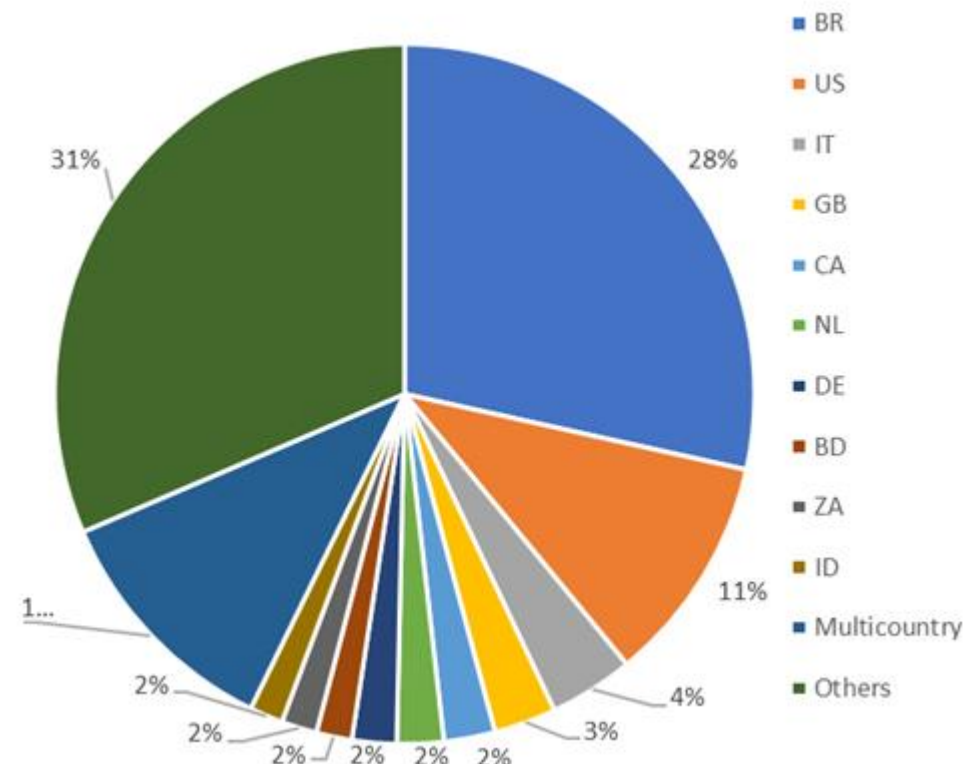
Participantes por país

- Total: 973
- Participantes no Brasil → 277 (ago/24)



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

% de Participantes



Fonte: <https://www.manrs.org/netops/participants/> Acesso ago/24



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

<https://kindns.org/>

Programa por uma Internet mais Segura

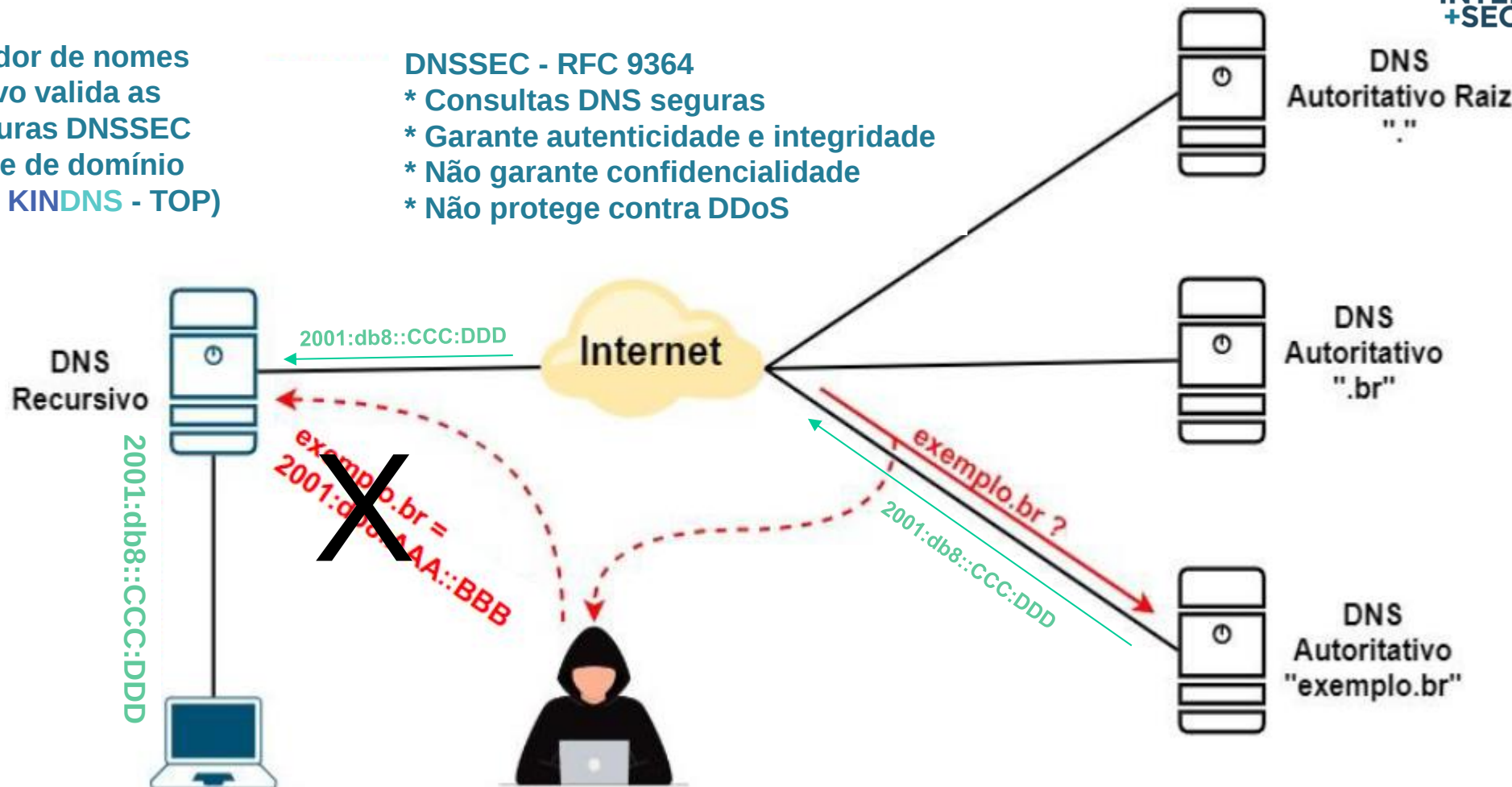
Ataque DNS - Poisoning



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



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

Programa por uma Internet mais Segura

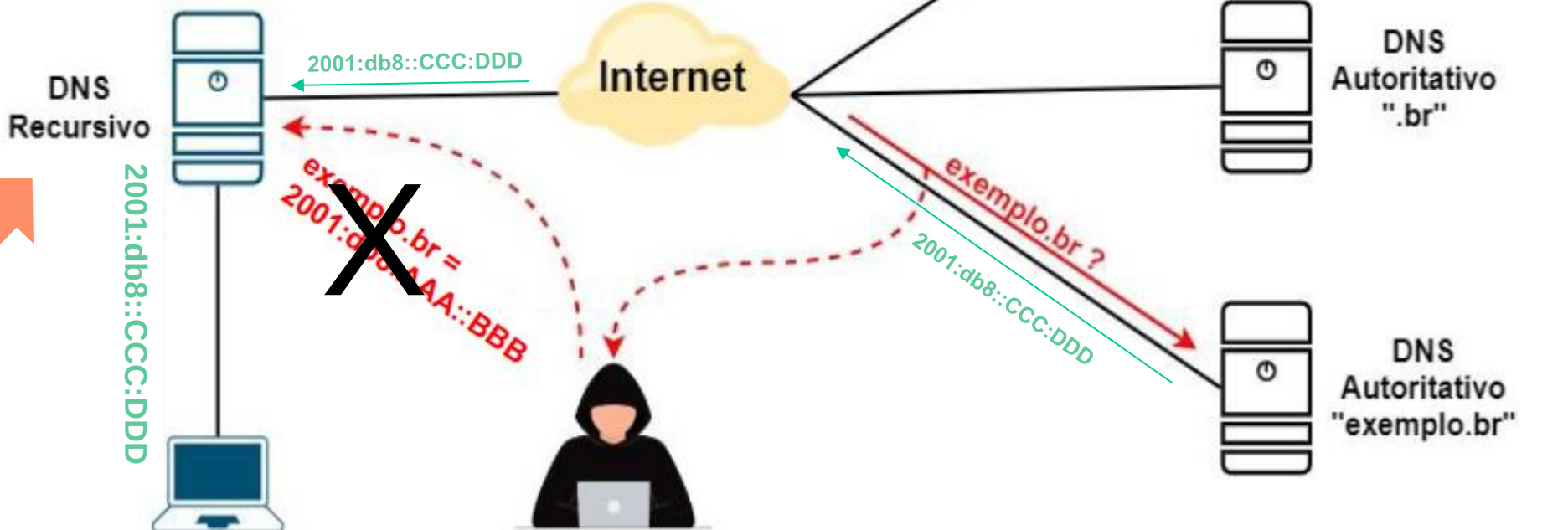
Ataque DNS - Poisoning



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



Desafio
BCOP 2024

DNS Recursivo
próprio

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/>





<https://top.nic.br>



Quem é TOPSobreReferênciasComunicados

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!

<https://top.nic.br>

Programa por uma Internet mais Segura

Implemente as melhores práticas



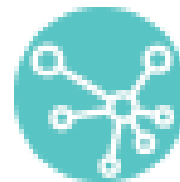
MANRS



BCP

Portal de boas práticas
para a Internet no Brasil

Desafio BCOP 2024



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>



Programa por uma Internet mais Segura

APOIO



A CONECTIVIDADE AO SEU ALCANCE



gzorello@nic.br

