



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

Programa por uma Internet mais segura

Como tornar a o seu provedor mais seguro

Gilberto Zorello | gzorello@nic.br

IX Fórum Regional Nordeste

Feira de Santana, BA | 16/06/23

registro.br nic.br cgi.br

Nossa Agenda

Programa por uma Internet mais Segura

- Objetivo / Plano de Ação
- Interação com Provedores e Operadoras
- Ações do Programa
 - MANRS
 - Notificação de Amplificadores
 - TOP – Teste os Padrões



Programa por uma Internet mais Segura

Objetivo

Atuar em apoio à comunidade técnica da Internet

- Redução dos ataques de Negação de Serviço
- **Melhora da Segurança de Roteamento na rede**
- Redução das vulnerabilidades e falhas de configuração
- **Divulgar melhores práticas que devem ser utilizadas nas redes: Notificação de Amplificadores, MANRS, IPv6, DNSSEC, TLS, DMARC**
- **Incentivar o crescimento de uma cultura de segurança entre os operadores das redes**



Programa por uma Internet mais Segura

Plano de Ação

Ações executadas pelo NIC.br

- Transversal no NIC.br: CERT.br, CEPTR0.br, IX.br, Registro.br, Sistemas, Comunicação
- **Conscientização por meio de palestras, cursos e treinamentos**
- Criação de materiais didáticos e boas práticas
- Interação com operadores das redes para disseminação da **cultura de segurança, adoção de melhores práticas e mitigação dos problemas existentes**
- Implementação de filtros de rotas no IX.br, que contribui para melhorar o cenário geral
- **Estabelecimento de métricas e acompanhamento da efetividade das ações**





Programa por uma Internet mais Segura

Interação com Provedores e Operadoras



- Reuniões bilaterais periódicas com as grandes operadoras
- Reuniões *on-line* com os responsáveis pelos ASes com maior quantidade de endereços IP notificados
- Ações do Programa tratados nas reuniões bilaterais:
 - Correção dos serviços mal configurados notificados pelo CERT.br, que podem ser abusados para fazer parte de ataques DDoS
 - Adoção de Boas Práticas de roteamento (**MANRS**)
 - Verificação da adoção de melhores práticas de configuração de servidores de DNS recursivos, IPv6, Site e E-mail com o TOP – Teste os Padrões
 - Apresentação de medições, por AS, sobre o status da adoção das boas práticas recomendadas

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores



- Estatísticas das notificações encaminhadas pelo CERT.br referentes aos endereços IP que podem ser abusados em ataques por amplificação

| ASN | DNS | SNMP | NTP | SSDP | PORTMAP | MEMCACHED | NETBIOS | QOTD | CHARGEN | LDAP | MDNS | UBNT | WS-DISCOVERY | TFTP | CoAP | ARMS | DHCPDiscover | 2023-02 | 2023-03 | 2023-04 | 2023-05 | MT4145 | MT5678 |
|-------|------|------|-----|------|---------|-----------|---------|-------|---------|------|------|------|--------------|------|------|------|--------------|---------|---------|---------|---------|--------|--------|
| ASN1 | 20 | 109 | 42 | 1 | 12 | 0 | 6 | 0 | 0 | 1 | 2 | 0 | 0 | 8 | 0 | 1 | 2 | 202 | 194 | 205 | 204 | 0 | 0 |
| ASN2 | 41 | 28 | 4 | 0 | 7 | 0 | 5 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 102 | 99 | 98 | 89 | 0 | 0 |
| Total | -33% | 32% | 17% | -54% | -53% | | -15% | -100% | -100% | 29% | -13% | | -100% | -9% | | 20% | -64% | 304 | 293 | 303 | 293 | | -100% |

| ASN | SNMP | | | | | | | | | | | | | | | | | | | | | | | | | | SNMP | | | |
|-------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|------|---------|---------|---------|
| | 2021-01 | 2021-02 | 2021-03 | 2021-04 | 2021-05 | 2021-06 | 2021-07 | 2021-08 | 2021-09 | 2021-10 | 2021-11 | 2021-12 | 2022-01 | 2022-02 | 2022-03 | 2022-04 | 2022-05 | 2022-06 | 2022-07 | 2022-08 | 2022-09 | 2022-10 | 2022-11 | 2022-12 | 2023-01 | 2023-02 | | 2023-03 | 2023-04 | 2023-05 |
| | # | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ASN1 | 54 | 49 | 46 | 50 | 48 | 47 | 45 | 73 | 71 | 74 | 77 | 80 | 80 | 67 | 73 | 83 | 82 | 84 | 64 | 55 | 57 | 66 | 83 | 84 | 87 | 87 | 81 | 85 | 109 | 109 |
| ASN2 | 25 | 26 | 30 | 31 | 24 | 24 | 28 | 26 | 18 | 23 | 22 | 21 | 26 | 21 | 28 | 26 | 26 | 26 | 23 | 22 | 27 | 27 | 30 | 30 | 30 | 29 | 30 | 30 | 28 | 28 |
| Total | | | | | | | | | | | | | | | | | 108 | 110 | 87 | 77 | 84 | 93 | 113 | 114 | 117 | 116 | 111 | 115 | | 32% |

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores



- Estatísticas das notificações encaminhadas pelo CERT.br referentes aos endereços IP que podem ser abusados em ataques por amplificação
- **Mensalmente é encaminhado relatório gerencial para o acompanhamento da resolução dos problemas notificados pelo CERT.br**

| ASN | DNS | SNMP | NTP | SSDP | PORTMAP | MEMCACHED | NETBIOS | QOTD | CHARGEN | LDAP | MDNS | UBNT | WS-DISCOVERY | TFTP | CoAP | ARMS | DHCPDiscover | 2023-02 | 2023-03 | 2023-04 | 2023-05 | MT4145 | MT5678 |
|-------|------|------|-----|------|---------|-----------|---------|-------|---------|------|------|------|--------------|------|------|------|--------------|---------|---------|---------|---------|--------|--------|
| ASN1 | 20 | 109 | 42 | 1 | 12 | 0 | 6 | 0 | 0 | 1 | 2 | 0 | 0 | 8 | 0 | 1 | 2 | 202 | 194 | 205 | 204 | 0 | 0 |
| ASN2 | 41 | 28 | 4 | 0 | 7 | 0 | 5 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 102 | 99 | 98 | 89 | 0 | 0 |
| Total | -33% | 32% | 17% | -54% | -53% | | -15% | -100% | -100% | 29% | -13% | | -100% | -9% | | 20% | -64% | 304 | 293 | 303 | 293 | | -100% |

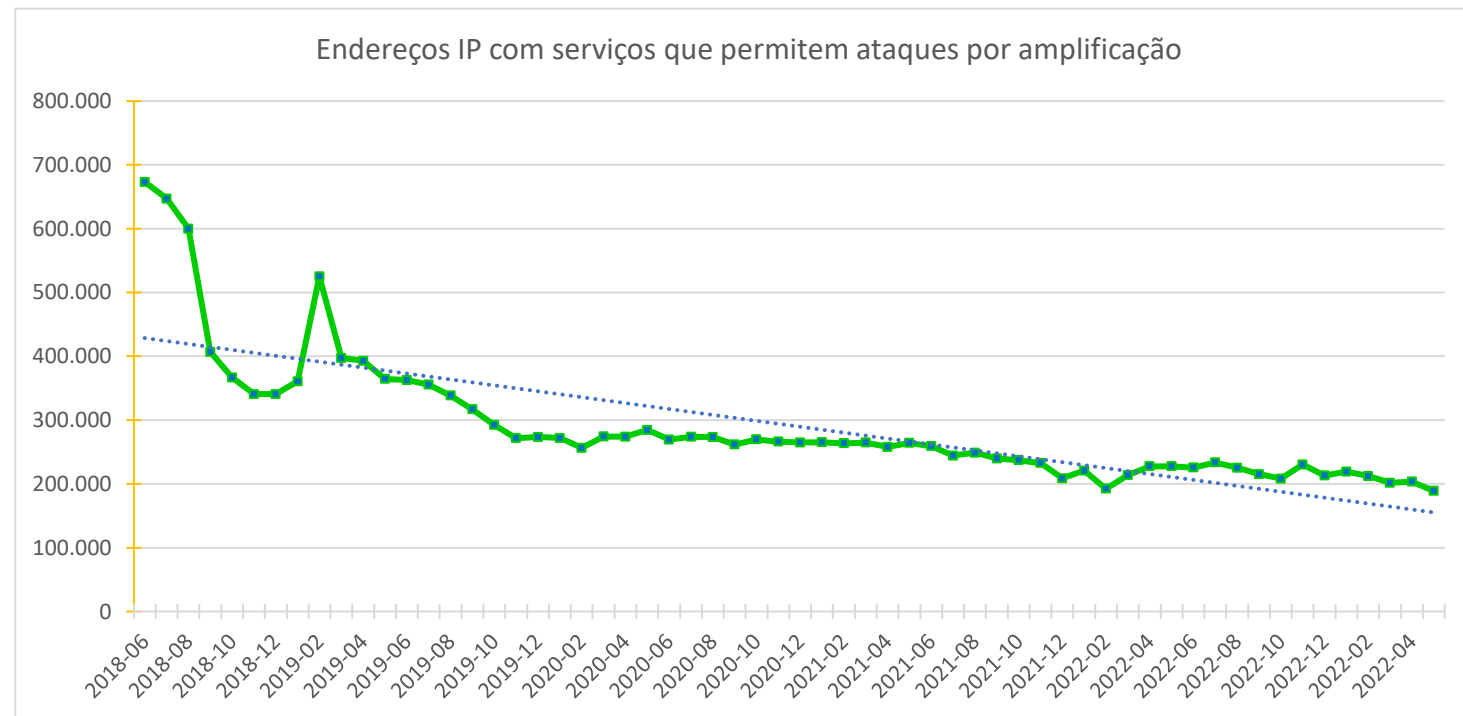
| ASN | SNMP | | | | | | | | | | | | | | | | | | | | | | | | | | SNMP | | | |
|-------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|------|---------|---------|---------|
| | 2021-01 | 2021-02 | 2021-03 | 2021-04 | 2021-05 | 2021-06 | 2021-07 | 2021-08 | 2021-09 | 2021-10 | 2021-11 | 2021-12 | 2022-01 | 2022-02 | 2022-03 | 2022-04 | 2022-05 | 2022-06 | 2022-07 | 2022-08 | 2022-09 | 2022-10 | 2022-11 | 2022-12 | 2023-01 | 2023-02 | | 2023-03 | 2023-04 | 2023-05 |
| | # | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ASN1 | 54 | 49 | 46 | 50 | 48 | 47 | 45 | 73 | 71 | 74 | 77 | 80 | 80 | 67 | 73 | 83 | 82 | 84 | 64 | 55 | 57 | 66 | 83 | 84 | 87 | 87 | 81 | 85 | 109 | 109 |
| ASN2 | 25 | 26 | 30 | 31 | 24 | 24 | 28 | 26 | 18 | 23 | 22 | 21 | 26 | 21 | 28 | 26 | 26 | 26 | 23 | 22 | 27 | 27 | 30 | 30 | 30 | 29 | 30 | 30 | 28 | 28 |
| Total | | | | | | | | | | | | | | | | | 108 | 110 | 87 | 77 | 84 | 93 | 113 | 114 | 117 | 116 | 111 | 115 | | 32% |

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores



- Quantidade de endereços IP notificados com serviços mal configurados



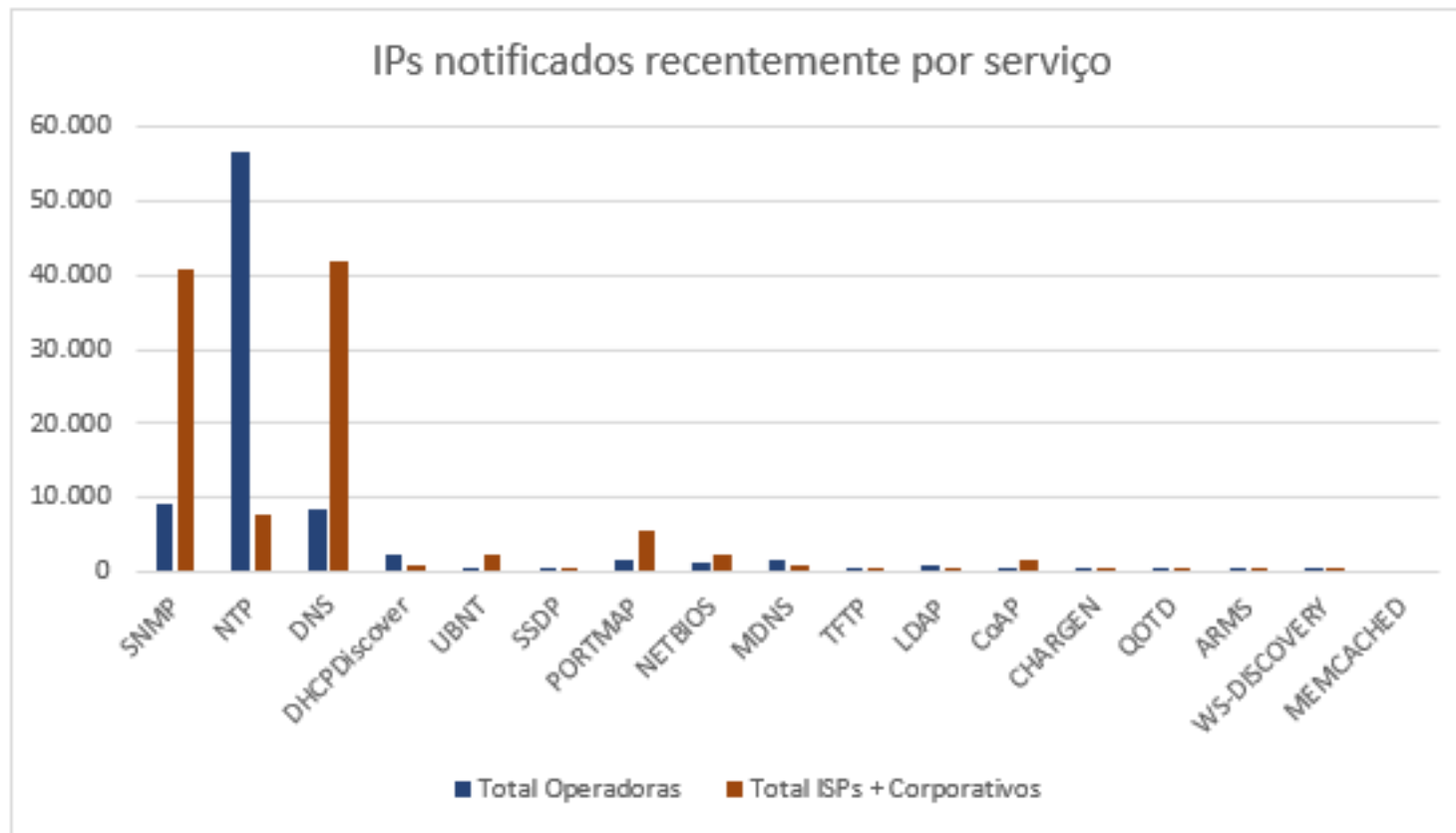
Redução de 74% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores



- Quantidade de endereços IP notificados por tipo de serviço



Mai/23

Principais ofensores: **ISPs e ASes corporativos** → **SNMP habilitado e DNS recursivo aberto**
Grandes operadoras → **NTP mal configurado**

Programa por uma Internet mais Segura

Ações do Programa – MANRS



MANRS

Mutually Agreed Norms for Routing Security

<http://manrs.org>

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

<https://www.manrs.org/netops/participants/>

Programa por uma Internet mais Segura

MANRS Observatory Readiness - Brasil

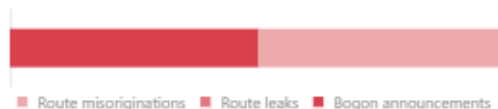
MONTH (PARTIAL) June 2023 COUNTRY Brazil

Overview

State of Routing Security

Incidents

| | |
|-----------------------|-----------|
| Route misoriginations | 41 |
| Route leaks | 0 |
| Bogon announcements | 42 |
| Total | 83 |



Culprits

| | |
|----------|----|
| Culprits | 52 |
|----------|----|



Routing Information (IRR)

| | | |
|--------------|--------|-------|
| Unregistered | 2,245 | 2.6% |
| Registered | 85,133 | 97.4% |



Routing Information (RPKI)

| | | |
|---------|--------|-------|
| Valid | 27,821 | 32.0% |
| Unknown | 58,941 | 67.7% |
| Invalid | 307 | 0.3% |



Route Origin Validation

| | |
|------------------------------|------|
| ROV-based Filtering Rate (%) | 4.8% |
|------------------------------|------|

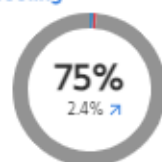


MANRS Readiness

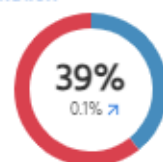
Filtering



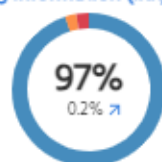
Anti-spoofing



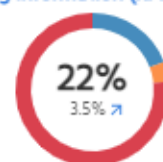
Coordination



Routing Information (IRR)



Routing Information (RPKI)



● Ready ● Aspiring ● Lagging ● No Data Available

Este Dash Board, com informações por AS, é acessível aos participantes do MANRS

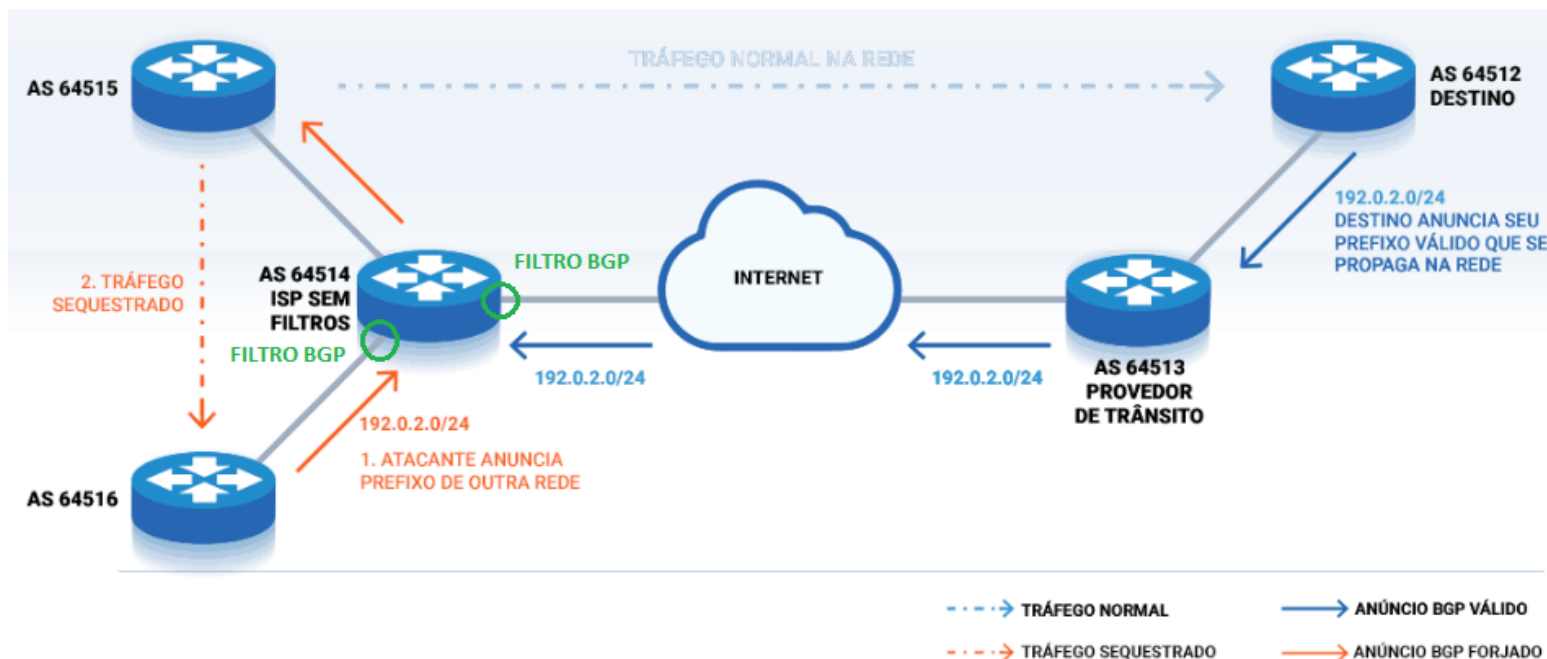
Fonte: <https://observatory.manrs.org/#/overview>

Programa por uma Internet mais Segura

Ação 1 - Implementação de Filtros de Anúncios BGP

Ataque por Sequestro de Prefixos (Hijacking)

Topologia de rede sem filtros de anúncios



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

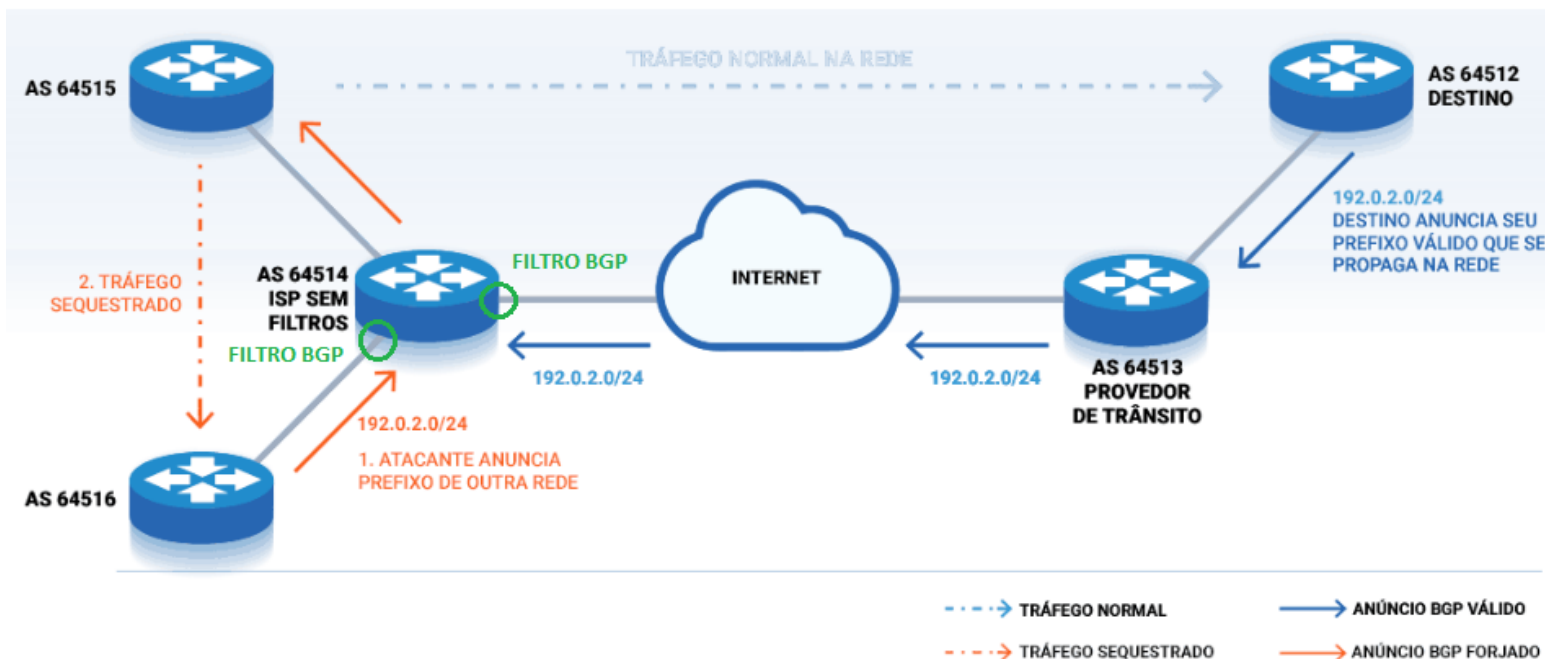
Programa por uma Internet mais Segura

Ação 1 - Implementação de Filtros de Anúncios BGP

Ataque por Sequestro de Prefixos (Hijacking)

Topologia de rede sem filtros de anúncios

O provedor deve garantir a correção dos próprios anúncios e de seus clientes



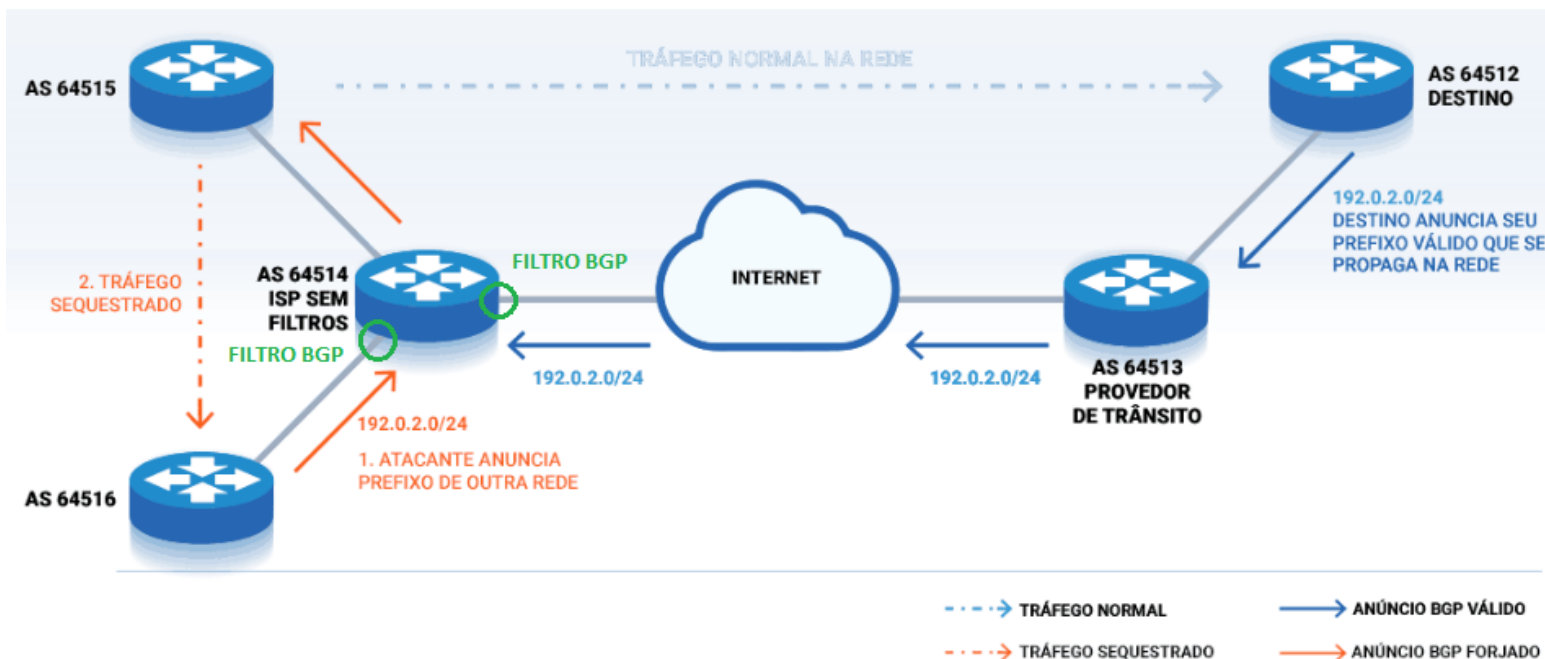
Fonte: <https://bcp.nic.br/i+seg/sobre/>

Programa por uma Internet mais Segura

Ação 1 - Implementação de Filtros de Anúncios BGP

Ataque por Sequestro de Prefixos (Hijacking)

Topologia de rede sem filtros de anúncios



O provedor deve garantir a correção dos próprios anúncios e de seus clientes

BGP Stream recebe alertas de:

- Hijacking (sequestro de prefixos)
- Leak (vazamento de rotas)
- Outages
- Últimos 180 dias de eventos
- Monitoramento se seus anúncios BGP

<https://bgpstream.crosswork.cisco.com/>

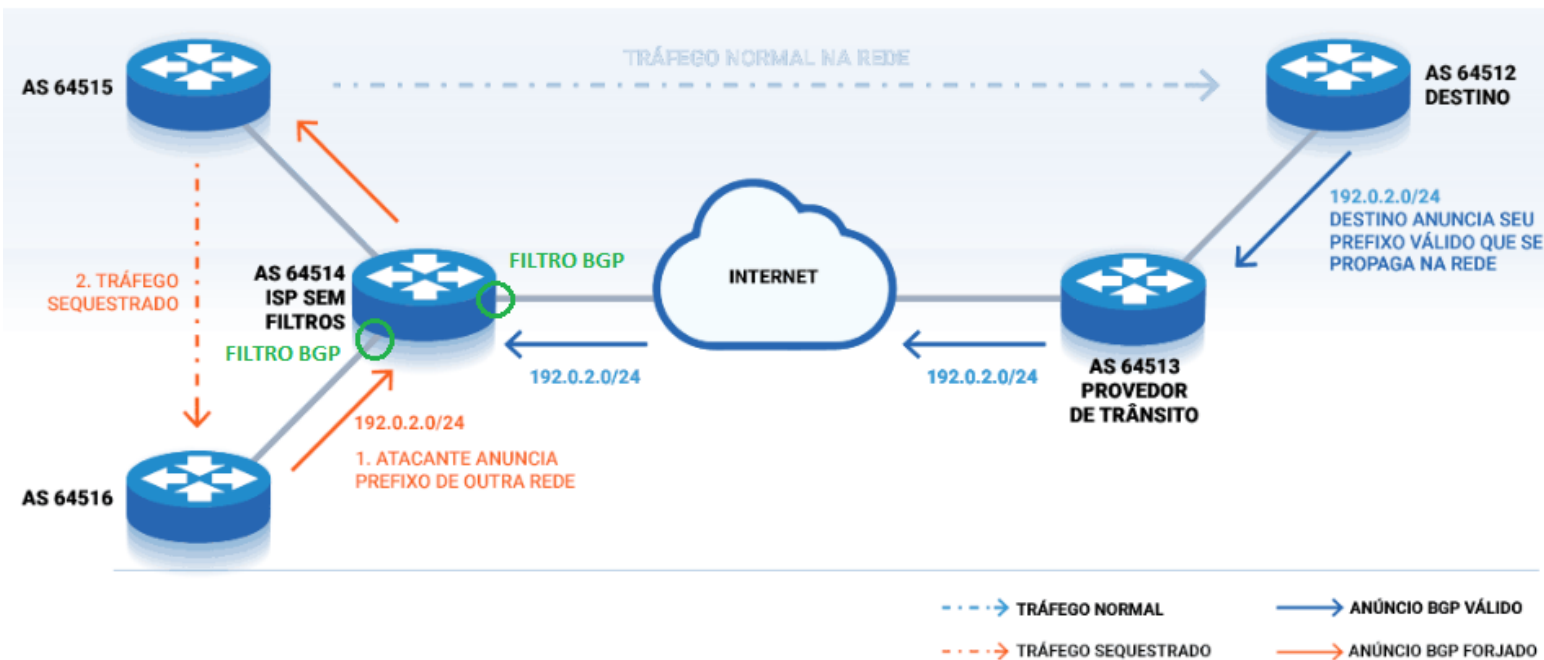
Fonte: <https://bcp.nic.br/i+seg/sobre/>

Programa por uma Internet mais Segura

Ação 1 - Implementação de Filtros de Anúncios BGP

Ataque por Sequestro de Prefixos (Hijacking)

Topologia de rede sem filtros de anúncios



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

O provedor deve garantir a correção dos próprios anúncios e de seus clientes

BGP Stream recebe alertas de:

- Hijacking (sequestro de prefixos)
- Leak (vazamento de rotas)
- Outages
- Últimos 180 dias de eventos
- Monitoramento se seus anúncios BGP

<https://bgpstream.crosswork.cisco.com/>

MANRS Observatory analisa 8 métricas:

- Hijacking
 - Leak
 - Bogon - prefixos
 - Bogon - ASNs
- Gerado pelo AS
ou por
seu cliente Direto

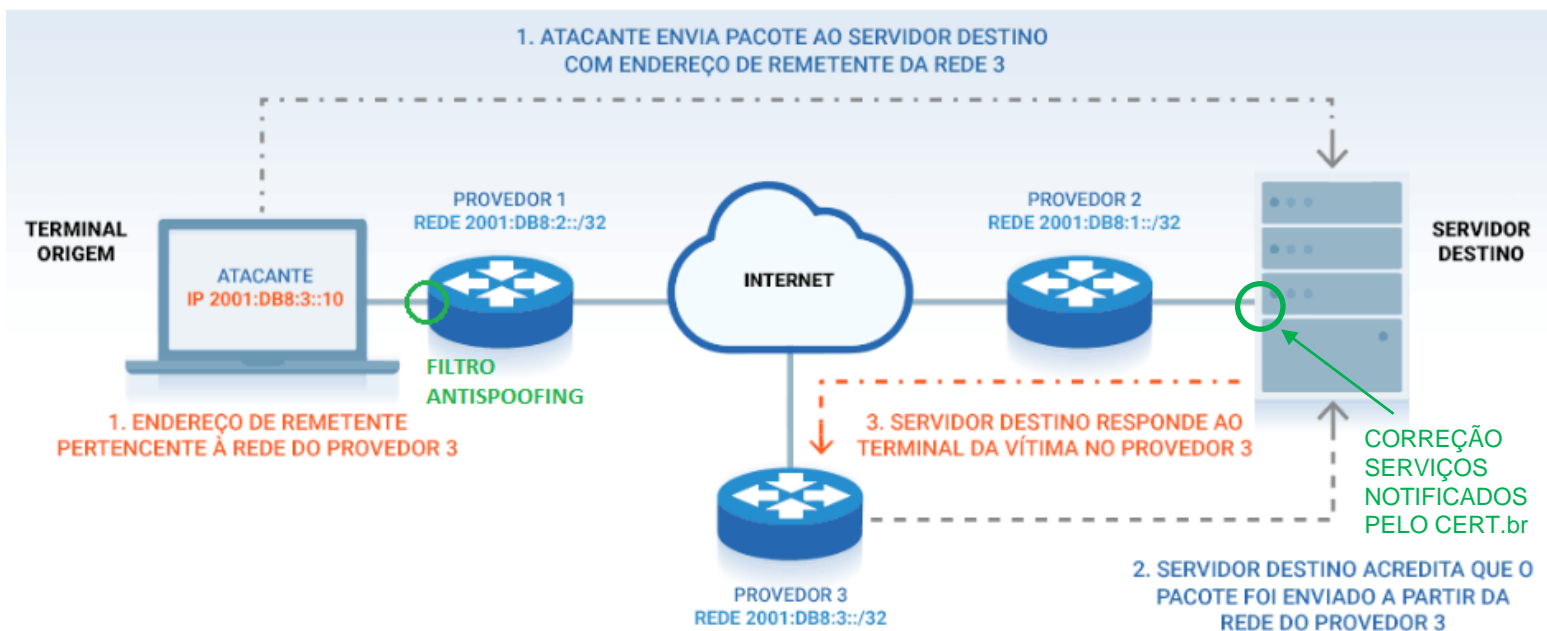
<https://observatory.manrs.org/#/about> 13

Programa por uma Internet mais Segura

Ação 2 - Implementação de Filtros Antispoofing

Ataque DoS por reflexão

Ataque DoS utilizando endereço de remetente forjado (Spoofing)



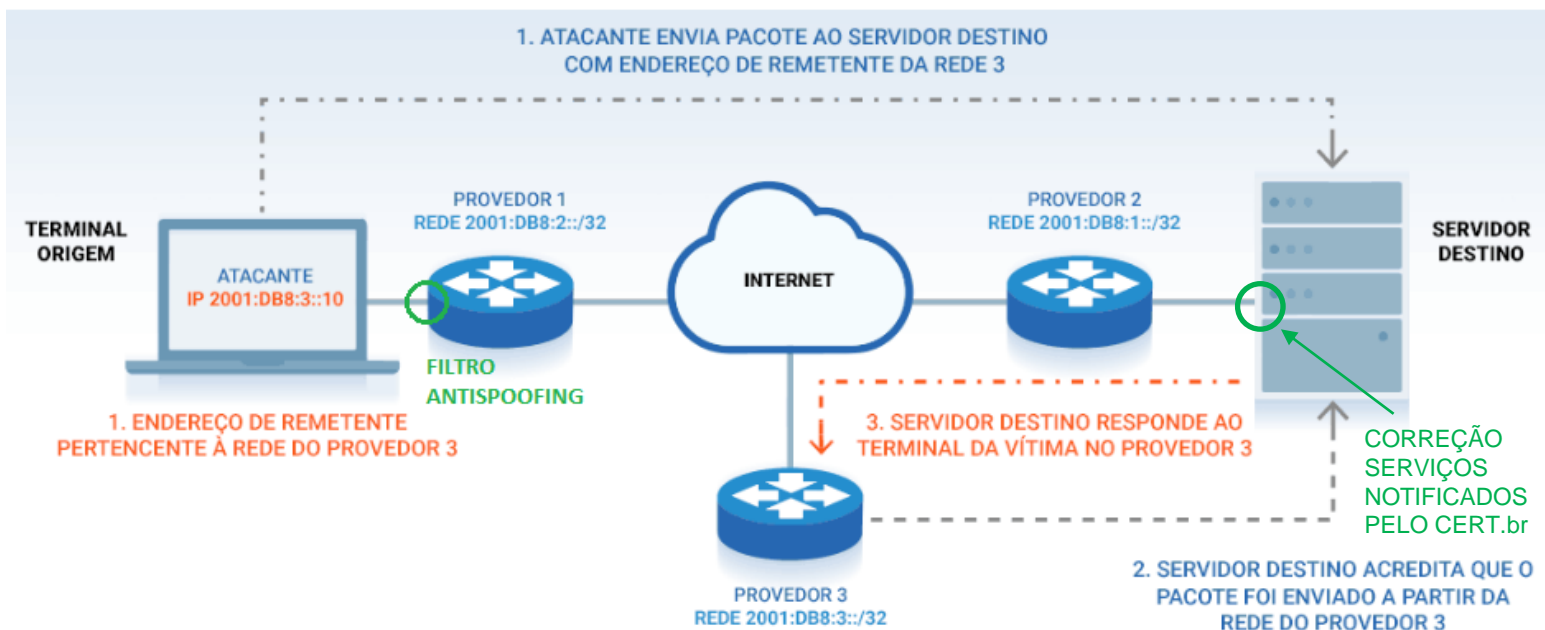
Fonte: <https://bcp.nic.br/i+seg/sobre/>

Programa por uma Internet mais Segura

Ação 2 - Implementação de Filtros Antispoofing

Ataque DoS por reflexão

Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Implementação de filtro antispoofing o mais próximo do cliente

uRPF (Unicast Reverse Path Forwarding)

- Strict Mode
- Loose Mode
- VRF Mode

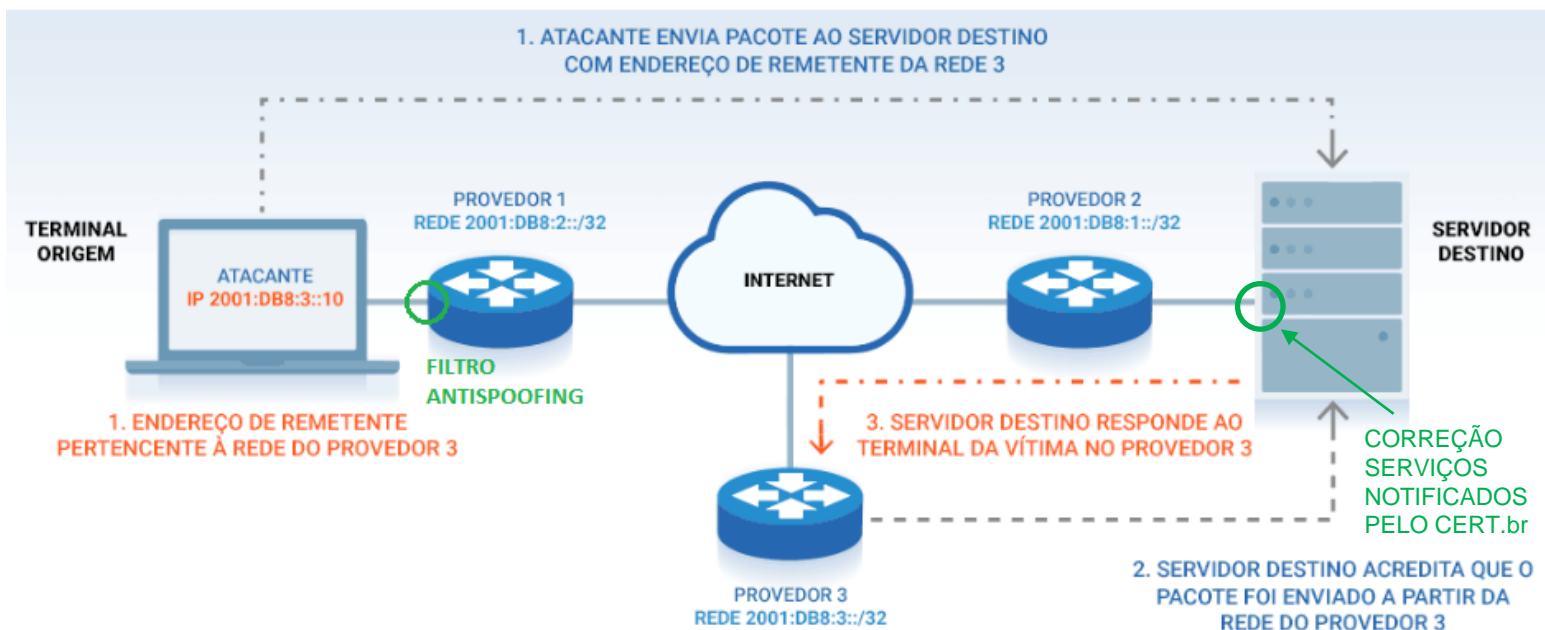
Fonte: <https://bcp.nic.br/i+seg/sobre/>

Programa por uma Internet mais Segura

Ação 2 - Implementação de Filtros Antispoofing

Ataque DoS por reflexão

Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Implementação de filtro antispoofing o mais próximo do cliente

uRPF (Unicast Reverse Path Forwarding)

- Strict Mode
- Loose Mode
- VRF Mode

Testes contra o CAIDA Spoofer

<https://www.caida.org/projects/spoofer/>

MANRS Observatory analisa a base de dados do CAIDA Spoofer

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

Programa por uma Internet mais Segura

Ação 3 - Coordenação entre Operadores

Facilitar a comunicação operacional global e a coordenação entre os operadores de rede

Endereços de *e-mail* indicados no Whois:



<https://registro.br/tecnologia/ferramentas/whois/>

Titular

Roteamento

Abuse

Endereços de *e-mail* indicados no PeeringDB:



<https://www.peeringdb.com/>

NOC

Abuse

Outros

Programa por uma Internet mais Segura

Ação 3 - Coordenação entre Operadores

Facilitar a comunicação operacional global e a coordenação entre os operadores de rede

Endereços de *e-mail* indicados no Whois:



<https://registro.br/tecnologia/ferramentas/whois/>

Titular

Roteamento

Abuse

- As notificações de segurança do CERT.br são encaminhadas para o *e-mail* do campo Abuse

Endereços de *e-mail* indicados no PeeringDB:



<https://www.peeringdb.com/>

NOC

Abuse

Outros

Programa por uma Internet mais Segura

Ação 3 - Coordenação entre Operadores

Facilitar a comunicação operacional global e a coordenação entre os operadores de rede

Endereços de *e-mail* indicados no Whois:



<https://registro.br/tecnologia/ferramentas/whois/>

Titular

Roteamento

Abuse

- As notificações de segurança do CERT.br são encaminhadas para o *e-mail* do campo Abuse
- Utilize grupos de *e-mails* ao invés de *e-mails* pessoais
- Manter compatibilidade dos pontos de contatos em relação a cadastros em outras bases (Whois, PeeringDB, IRR)

Endereços de *e-mail* indicados no PeeringDB:



<https://www.peeringdb.com/>

NOC

Abuse

Outros

Programa por uma Internet mais Segura

Ação 3 - Coordenação entre Operadores

Facilitar a comunicação operacional global e a coordenação entre os operadores de rede

Endereços de e-mail indicados no Whois:



<https://registro.br/tecnologia/ferramentas/whois/>

Titular

Roteamento

Abuse

Endereços de e-mail indicados no PeeringDB:



<https://www.peeringdb.com/>

NOC

Abuse

Outros

- As notificações de segurança do CERT.br são encaminhadas para o e-mail do campo Abuse
- Utilize grupos de e-mails ao invés de e-mails pessoais
- Manter compatibilidade dos pontos de contatos em relação a cadastros em outras bases (Whois, PeeringDB, IRR)
- Manter pontos de contatos atualizados após mudanças internas e incorporação de outros ASes
- O MANRS Observatory analisa os pontos de contato técnicos do PeeringDB

Programa por uma Internet mais Segura

Ação 3 - Coordenação entre Operadores

Facilitar a comunicação operacional global e a coordenação entre os operadores de rede

Endereços de *e-mail* indicados no Whois:



<https://registro.br/tecnologia/ferramentas/whois/>

Titular

Roteamento

Abuse

- As notificações de segurança do CERT.br são encaminhadas para o *e-mail* do campo Abuse
- Utilize grupos de *e-mails* ao invés de *e-mails* pessoais
- Manter compatibilidade dos pontos de contatos em relação a cadastros em outras bases (Whois, PeeringDB, IRR)
- Manter pontos de contatos atualizados após mudanças internas e incorporação de outros ASes
- O MANRS Observatory analisa os pontos de contato técnicos do PeeringDB

Endereços de *e-mail* indicados no PeeringDB:



<https://www.peeringdb.com/>

NOC

Abuse

Outros

Verificar se estão recebendo notificações do CERT.br: há endereços de *e-mail* que não recebem mensagens de cert@cert.br: SPAM, caixa cheia, host/domínio not found, inválido (~40 tipos de erros)

O Registro.br faz validação dos pontos de contato de Abuse: se não foi validado, é enviado um aviso e se não responde em seis meses a administração dos recursos é bloqueada no sistema

Programa por uma Internet mais Segura

Ação 4 - Cadastro da Política de Roteamento

IRR - Internet Routing Registry

- Cadastro da política da política de Roteamento no IRR ([RADB](#)) ou no [TC](#)
- MANRS Observatory analisa a base de dados do RIPEStat (<https://stat.ripe.net/ui2013/>)

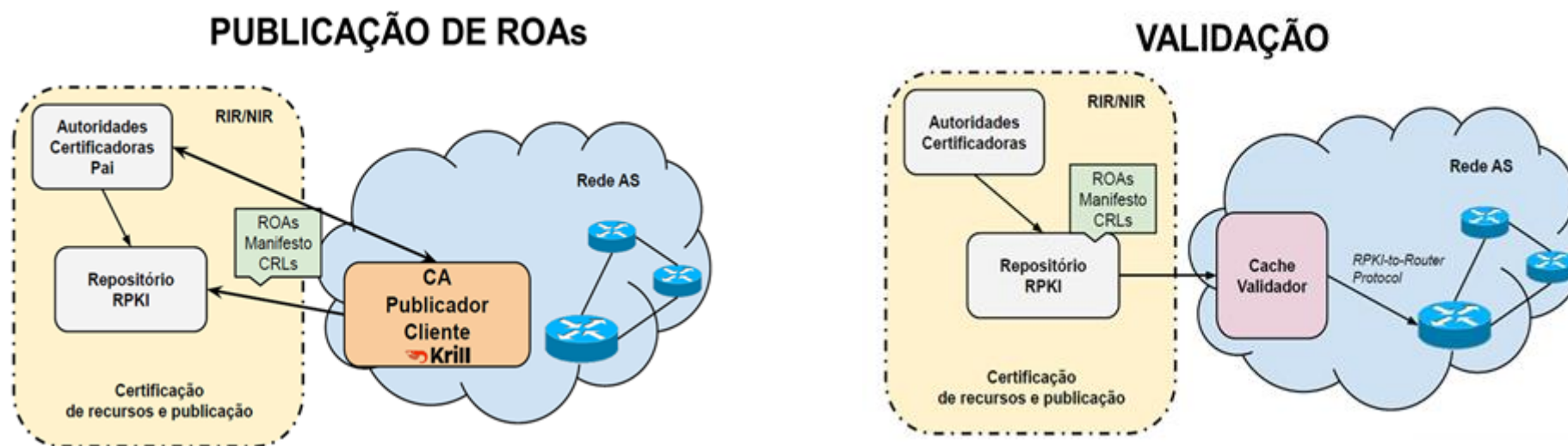
Programa por uma Internet mais Segura

Ação 4 - Cadastro da Política de Roteamento

IRR - Internet Routing Registry

- Cadastro da política da política de Roteamento no IRR ([RADB](#)) ou no [TC](#)
- MANRS Observatory analisa a base de dados do RIPEStat (<https://stat.ripe.net/ui2013/>)

RPKI - Resource Public Key Infrastructure



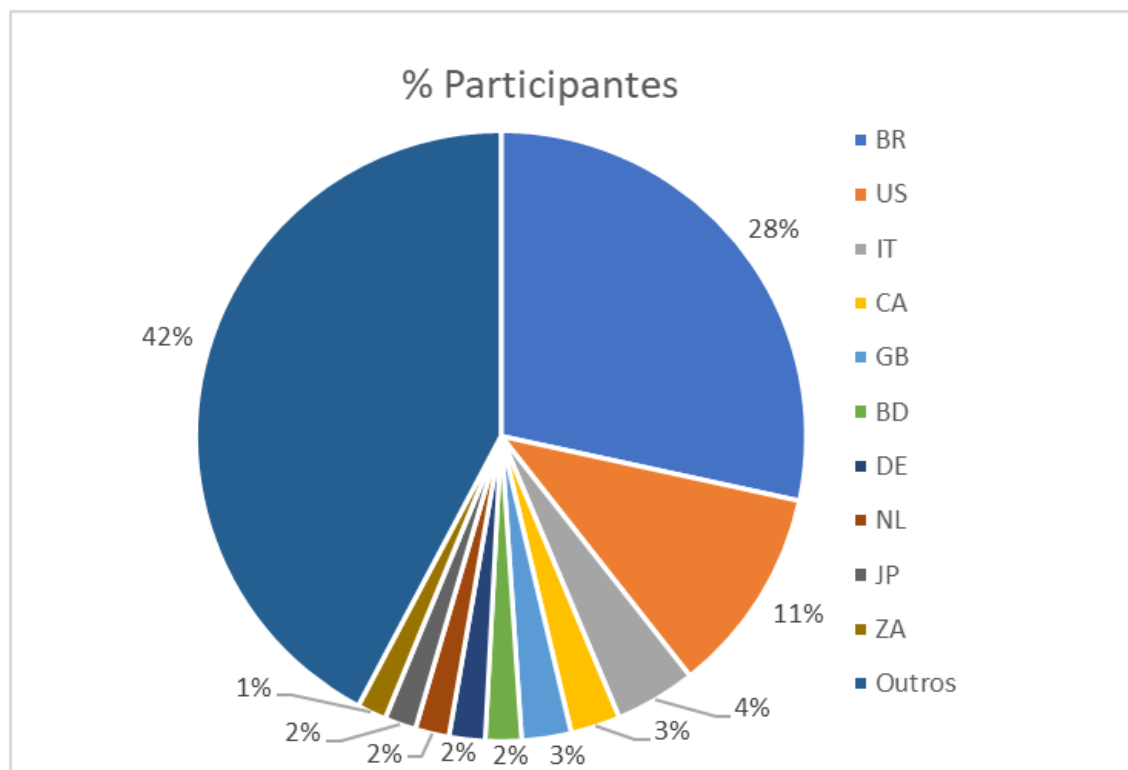
- MANRS Observatory analisa os ROAS publicados com um Validador RPKI próprio

Programa por uma Internet mais Segura

Participantes do MANRS



- Distribuição por país dos Provedores participantes da iniciativa MANRS



Total de participantes: 838

Participantes do Brasil: 238 (Mai/23)

206 (2022)

174 (2021)

140 (2020)

Fonte: <https://www.manrs.org/netops/participants/> Acesso mai/23

Programa por uma Internet mais Segura

Ações do Programa – TOP – Teste os Padrões



<https://top.nic.br>

TOP – Teste os Padrões – O que é?



Ajuda a verificar se a Internet que utiliza está seguindo os padrões abertos mais recentes de Internet

- **Teste TOP - IPv6 e DNSSEC (Conexão do usuário)**
- Teste TOP – *Site* (IPv6, DNSSEC, TLS, Opções de Segurança)
- **Teste TOP – *E-mail* (IPv6, DNSSEC, STARTTLS, DMARC)**

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

TOP – Teste os Padrões – O que é?



Teste TOP - IPv6 e DNSSEC

- **IPv6**
 - Verifica se o servidor recursivo é capaz de acessar servidores de nomes via IPv6
 - **Verifica se o usuário é capaz de acessar computadores via IPv6 (DNS e diretamente)**
 - Verifica se as Extensões de Privacidade IPv6 para SLAAC estão habilitadas
- **DNSSEC**
 - Verifica se os servidores de nomes recursivos utilizados validam as assinaturas DNSSEC

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

TOP – Teste os Padrões – O que é?



Teste TOP - Site

- **IPv6**
 - Verifica se os servidores de **nomes** e **web** são acessíveis por IPv6
- **DNSSEC**
 - Verifica se a assinatura **DNSSEC** do domínio é válida
- **HTTPS**
 - Verifica se o servidor **web** oferece **HTTPS**, está atualizado e configurado corretamente
- **Opções de segurança**
 - Verifica se as opções de segurança recomendadas estão aplicadas: *X-Frame-Options*, *X-Content-Type-Options*, *Content-Security-Policy* (CSP), *Referrer-Policy*

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

TOP – Teste os Padrões – O que é?



Teste TOP – *E-mail*

- **IPv6**
 - Verifica se os servidores de **nomes** e de **e-mail** são acessíveis por IPv6
- **DNSSEC**
 - Verifica se as assinaturas **DNSSEC** do domínio e do servidor de *e-mail* são válidas
- **DMARC, DKIM e SPF**
 - Verifica se o domínio possui as marcas de autenticidade contra **phishing** de *e-mails*
- **STARTTLS e DANE**
 - Verifica se o servidor de recebimento de **e-mail** do domínio está atualizado e configurado corretamente para estabelecer uma conexão segura com os servidores de envio de *e-mail*

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

TOP – Teste os Padrões – Desenvolvimento

Teste TOP - IPv6 e DNSSEC da rede do usuário

113.779

Med. - IPv6 DNSSEC Final.

71.054

Recurso c/ DNSSEC Validado

62%

% Recursivo c/ DNSSEC Validado

5.314

AS Únicos Testados

71.152

Usuários com IPv6

63%

% Usuários IPv6 100%

Medições totais IPv6 100%



14/6/23

TOP – Teste os Padrões – Desenvolvimento

14.393

Domínios Únicos Site

34.185

Medições - Site

Teste TOP - *Site*

357

Quem é TOP Site

3.315

IPv6 100% Site

3.314

DNSSEC 100% Site

1.012

TLS 100% Site

2%

% Quem é TOP Site

23%

% IPv6 Site

23%

% DNSSEC Site

7%

% TLS Site



13/6/23

24

TOP – Teste os Padrões – Desenvolvimento

3.626
Domínios Únicos c/ MX

10.887
Medições - E-mail

Teste TOP - *E-mail*

64
Quem é TOP E-mail

813
IPv6 100% E-mail

413
DNSSEC 100% E-mail

782
Marcas Aut. 100% E-mail

82
STARTTLS 100% E-mail

1%
% Quem é TOP E-mail

22%
% IPv6 E-mail

11%
% DNSSEC E-mail

22%
% Marcas Aut. E-mail

2%
% STARTTLS E-mail



13/6/23

25

TOP – Teste os Padrões - Apoio



<https://top.nic.br>



A CONECTIVIDADE AO SEU ALCANCE



Dúvidas

?

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

<https://top.nic.br> (TOP)

gzorello@nic.br

Obrigado

@ gzorello@nic.br

16 de junho de 2023

nic.br **cgi.br**

www.nic.br | www.cgi.br