



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 o seu provedor mais seguro

Gilberto Zorello | gzorello@nic.br

IX Fórum Regional - Fortaleza
Fortaleza, CE | 12/04/23

registro.br nic.br cgi.br

Nossa Agenda

Programa por uma Internet mais Segura

- Objetivo / Plano de Ação
- Interação com Provedores
- Desenvolvimento do Programa
- MANRS
- 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
- **Incentivar o crescimento de uma cultura de segurança entre os operadores da rede**



Programa por uma Internet mais Segura

Plano de Ação

Ações executadas pelo NIC.br com os operadores dos ASes:

- Transversal no NIC.br: CERT.br, CEPTRO.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 da rede 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



- Reuniões bilaterais periódicas com as grandes operadoras
- Reuniões *on-line* com os responsáveis pelos ASes com maior quantidade de endereços IP notificados
- Envio de relatório gerencial mensal 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	2022-11	2022-12	2023-01	2023-02	MT4145	MT5678
ASN1	20	87	42	0	31	0	8	0	0	1	2	0	0	8	0	0	3	199	206	209	202	0	0
ASN2	44	29	5	0	10	0	6	0	0	2	3	0	0	0	0	0	3	98	91	98	102	0	1
Total	-43%	16%	36%	-100%	-1%		1%	-100%	-100%	71%	2%	-100%	-100%	1%		-100%	-10%	297	297	307	304	-100%	71%

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
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	87
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	29
Total														88	101	109	108	110	87	77	84	93	113	114	117		16%

Programa por uma Internet mais Segura

Interação com Provedores



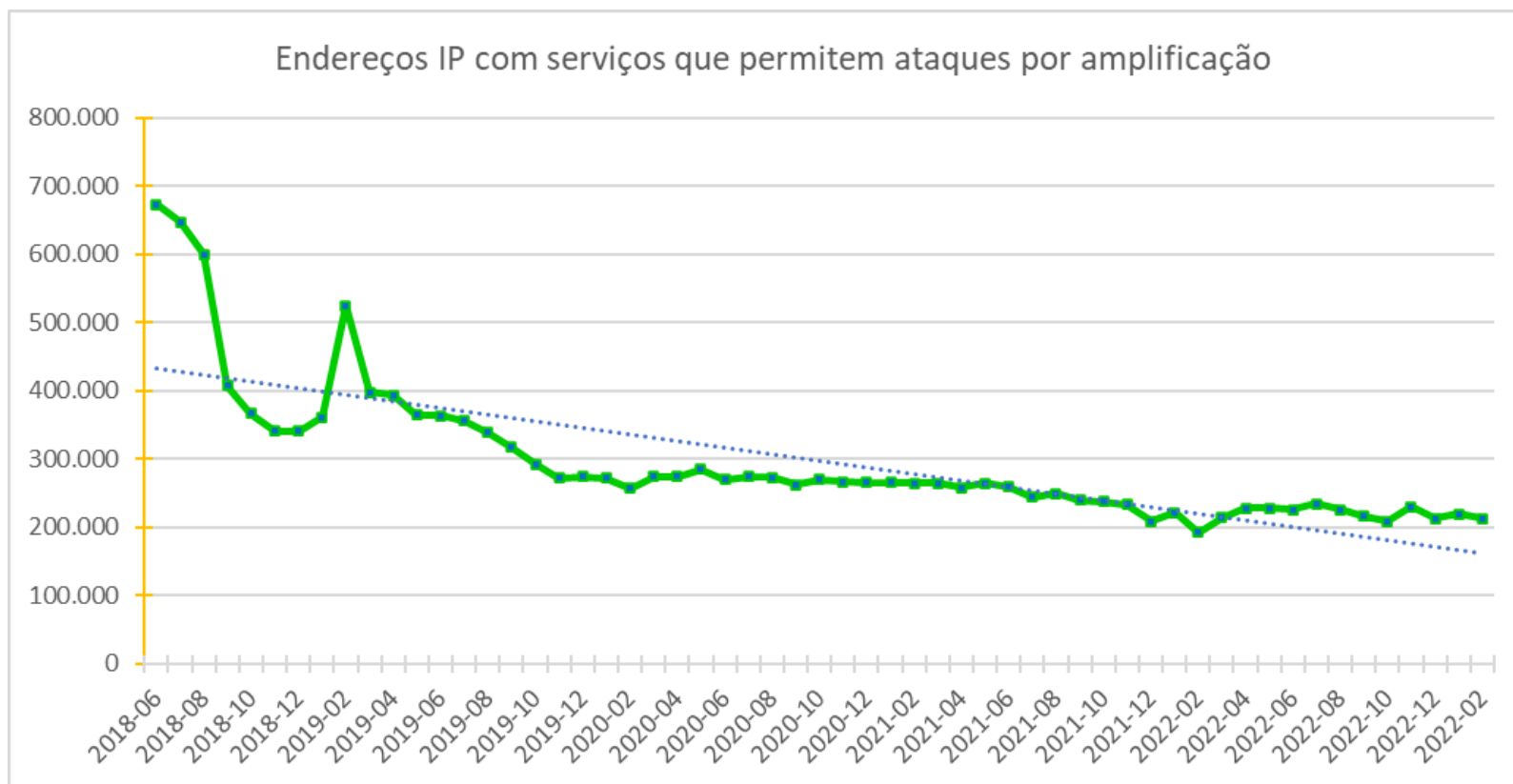
- Reuniões bilaterais periódicas com as grandes operadoras
- **Reuniões *on-line* com os responsáveis pelos ASes com maior quantidade de endereços IP notificados**
- Envio de relatório gerencial mensal para o acompanhamento da resolução dos problemas notificados pelo CERT.br
- Temas tratados nas reuniões bilaterais:
 - ***Acompanhamento da 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)*
 - **TOP – Teste os Padrões**

Programa por uma Internet mais Segura

Desenvolvimento do Programa - Amplificadores



- Quantidade de endereços IP notificados com serviços mal configurados



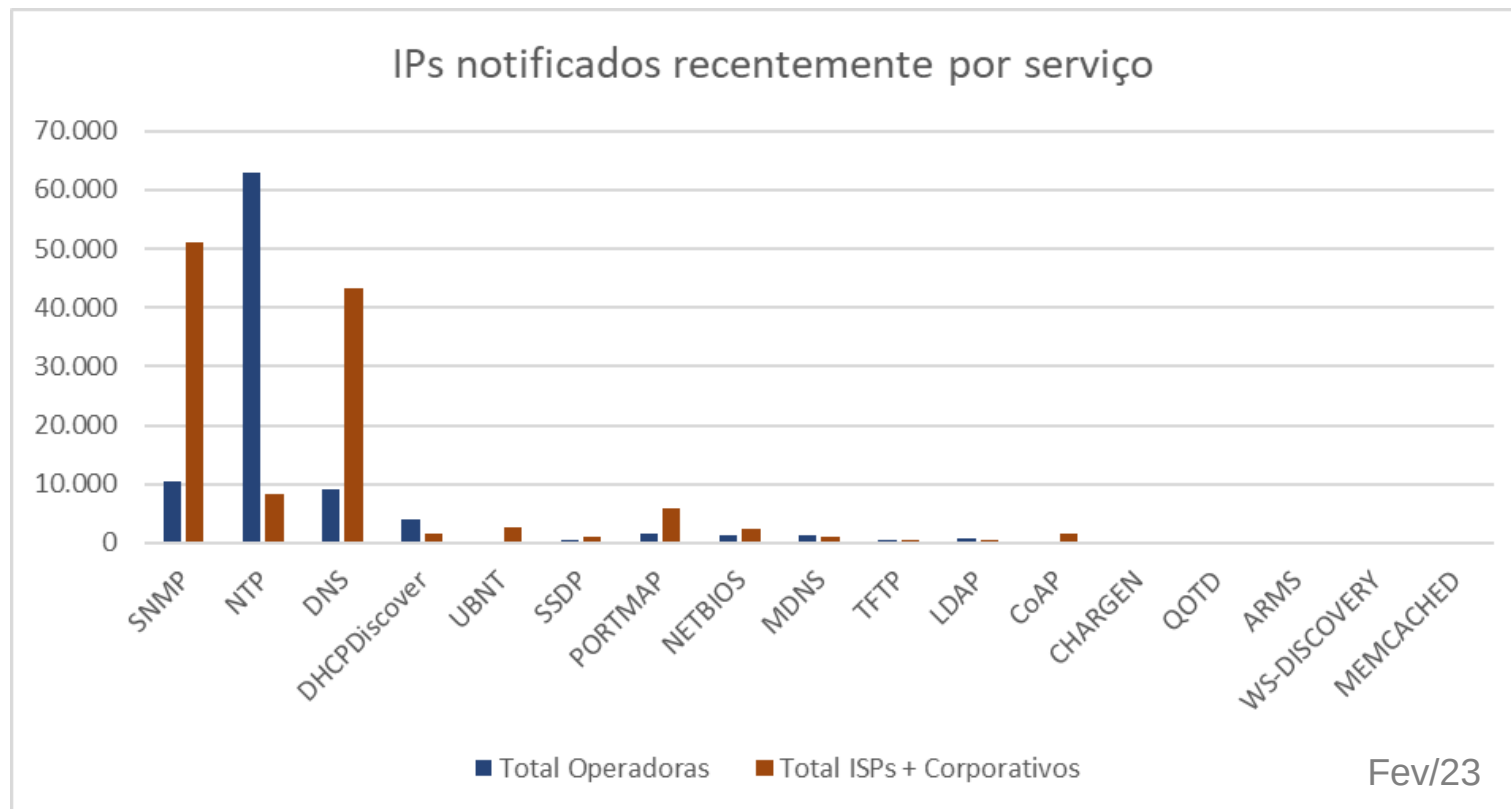
Redução de 71% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura

Desenvolvimento do Programa - Amplificadores



- Quantidade de endereços IP notificados por tipo de serviço



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



MANRS

Mutually Agreed Norms for Routing Security

<http://manrs.org>

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

Programa por uma Internet mais Segura

MANRS Observatory Readiness para um provedor

MONTH (PARTIAL)

March 2023

Q ASN

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	1
Total	1



Route misoriginations
Route leaks
Bogon announcements

Culprits ⁱ

Culprits	1
----------	---



Culprits

Routing completeness (IRR) ⁱ

Unregistered	0	0.0%
Registered	131	100.0%



Unregistered
Registered

Routing completeness (RPKI) ⁱ

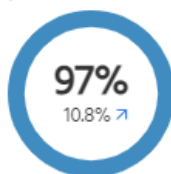
Valid	128	97.7%
Unknown	3	2.3%
Invalid	0	0.0%



Valid
Unknown
Invalid

MANRS Readiness ⁱ

Filtering ⁱ



Anti-spoofing ⁱ



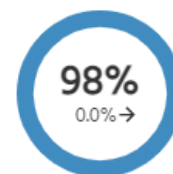
Coordination ⁱ



Global Validation IRR ⁱ



Global Validation RPKI ⁱ



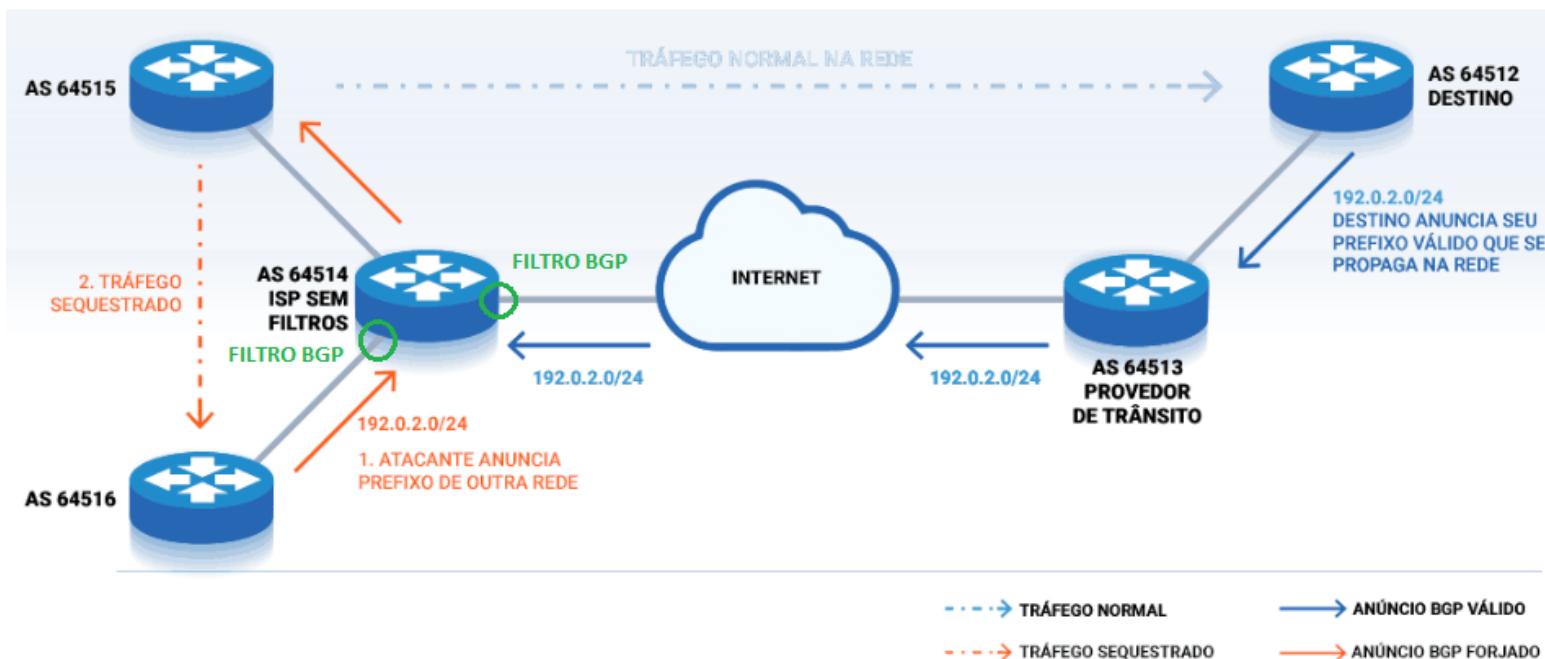
Ready Aspiring Lagging No Data Available

Programa por uma Internet mais Segura

Implementação de Filtros de Anúncios BGP – Ação 1

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

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

MANRS Observatory analisa 8 métricas:

- Hijacking
- Leak
- Bogon - prefixos
- Bogon - ASNs

Gerado pelo AS
ou
por cliente Direto

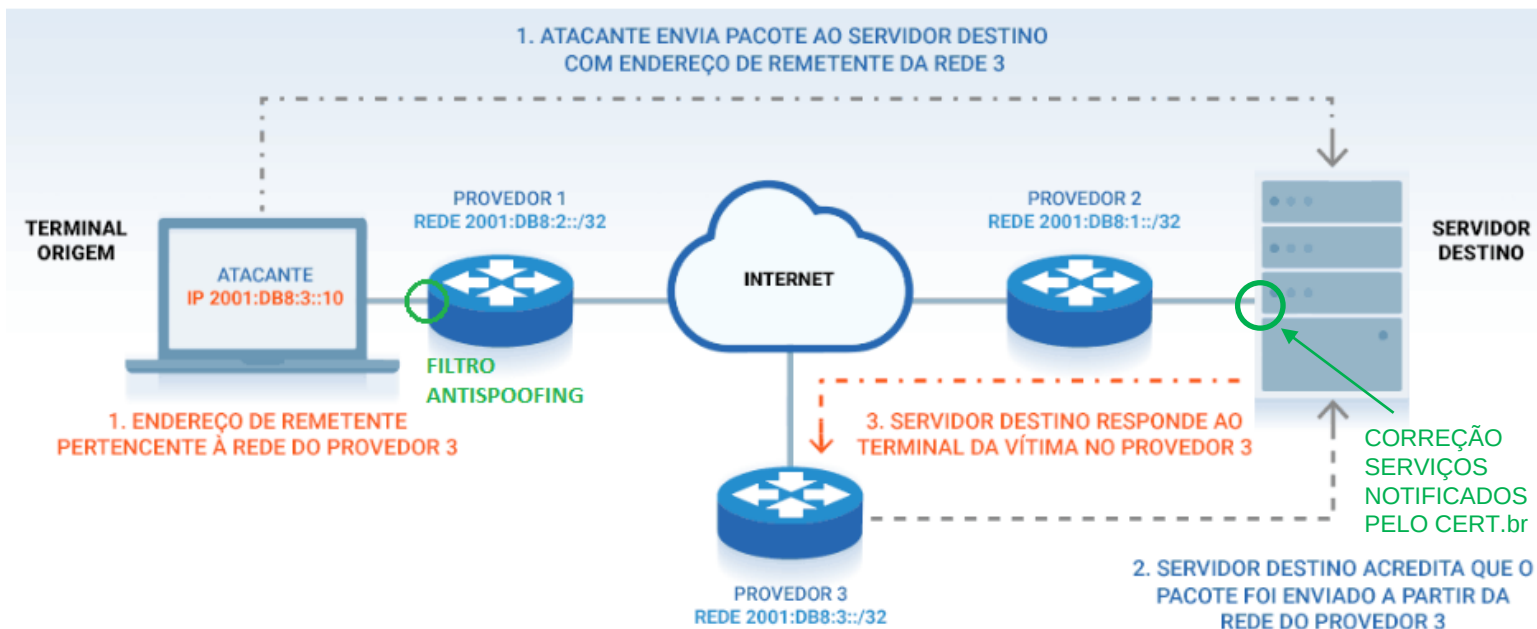
<https://observatory.manrs.org/#/about> 12

Programa por uma Internet mais Segura

Implementação de Filtros Antispoofing – Ação 2

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

Programa por uma Internet mais Segura

Coordenação entre Operadores – Ação 3

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 e do RIPEStat

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

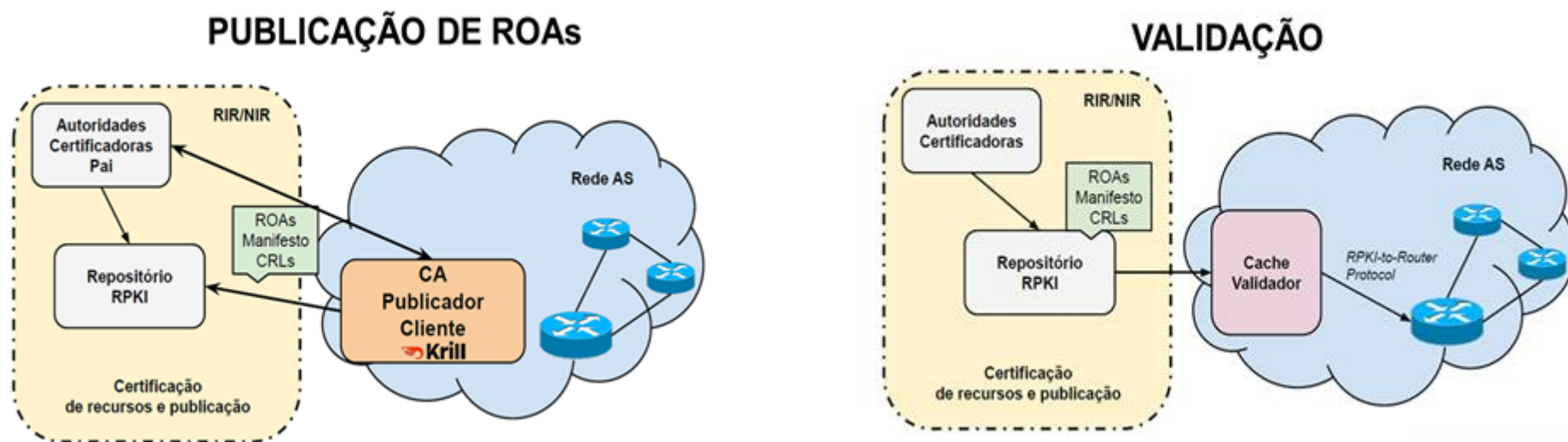
Programa por uma Internet mais Segura

Cadastro da Política de Roteamento – Ação 4

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



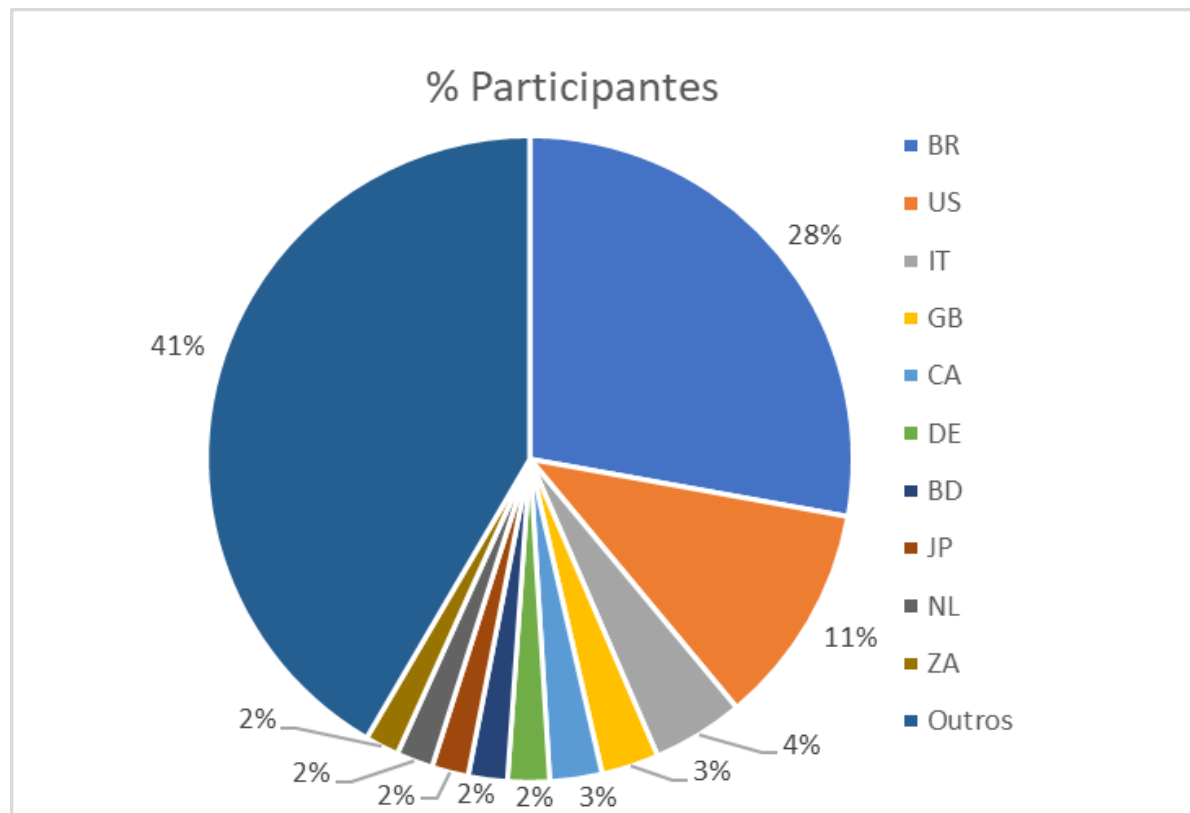
- MANRS Observatory analisa os ROAS Inválidos e não registrados por um Validador RPKI próprio

Programa por uma Internet mais Segura

Desenvolvimento do Programa - MANRS



- Distribuição por país dos Provedores participantes da iniciativa MANRS



Total de participantes: 765

Participantes do Brasil: 213

140 (2020)

174 (2021)

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



<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 – *Site*
- Teste TOP – *E-mail*
- Teste TOP - IPv6 e DNSSEC da rede do usuário

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

TOP – Teste os Padrões – Desenvolvimento

Teste TOP - IPv6 e DNSSEC da rede do usuário

89.488

Medições - IPv6 DNSSEC Finalizadas

54.630

Recurso c/ DNSSEC Validado

61%

% Recursivo c/ DNSSEC Validado

4876

AS Únicos Testados

55.737

IPv6 100% (Cenário VIII)

62%

% IPv6 100%



8/3/23

19

TOP – Teste os Padrões – Desenvolvimento

12.131

Domínios Únicos Site

29.095

Medições - Site

Teste TOP - *Site*

322

Quem é TOP Site

2.864

IPv6 100% Site

2.452

DNSSEC 100% Site

845

TLS 100% Site

3%

% Quem é TOP Site

24%

% IPv6 Site

20%

% DNSSEC Site

7%

% TLS Site



8/3/23

20

TOP – Teste os Padrões – Desenvolvimento

Teste TOP - *E-mail*

3.278

Domínios Únicos c/ MX

9.660

Medições - E-mail

55

Quem é TOP E-mail

744

IPv6 100% E-mail

376

DNSSEC 100% E-mail

689

Marcas Aut. 100% E-mail

70

STARTTLS 100% E-mail

1%

% Quem é TOP E-mail

23%

% IPv6 E-mail

11%

% DNSSEC E-mail

21%

% Marcas Aut. E-mail

2%

% STARTTLS E-mail



8/3/23

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)

Obrigado

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

@ gzorello@nic.br

12 de abril de 2023

nic.br **cgi.br**

www.nic.br | www.cgi.br