



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

Link ISP 2023 - InternetSul

Gramado, RS | 25/08/23

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**
- **Incentivo ao 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, CEPTRO.br, IX.br, Registro.br, Sistemas, Comunicação
- **Criação de materiais didáticos e boas práticas**
- Conscientização por meio de palestras, cursos e treinamentos
- **Interação com operadores das redes**
- Implementação de filtros de rotas no IX.br
- **Estabelecimento de métricas e acompanhamento da efetividade das ações**





Programa por uma Internet mais Segura

Interação com Provedores e Operadoras



- Reuniões bilaterais 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**
 - **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
- Relatório gerencial encaminhado mensalmente

ASN	DNS	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DISCOVERY	TFTP	CoAP	ARMS	DHCPDiscover	2023-04	2023-05	2023-06	2023-07	MT4145	MT5678
ASN1	14	115	40	1	28	0	5	0	0	1	2	0	0	4	0	1	0	205	204	215	211	0	0
ASN2	44	28	0	1	7	0	7	0	0	1	2	0	0	0	0	0	0	98	89	93	90	0	1
Total	-11%	32%	-4%	-4%	-7%		0%	-100%	-100%	-25%	-11%		-100%	-52%		20%	-100%	303	293	308	301		33%

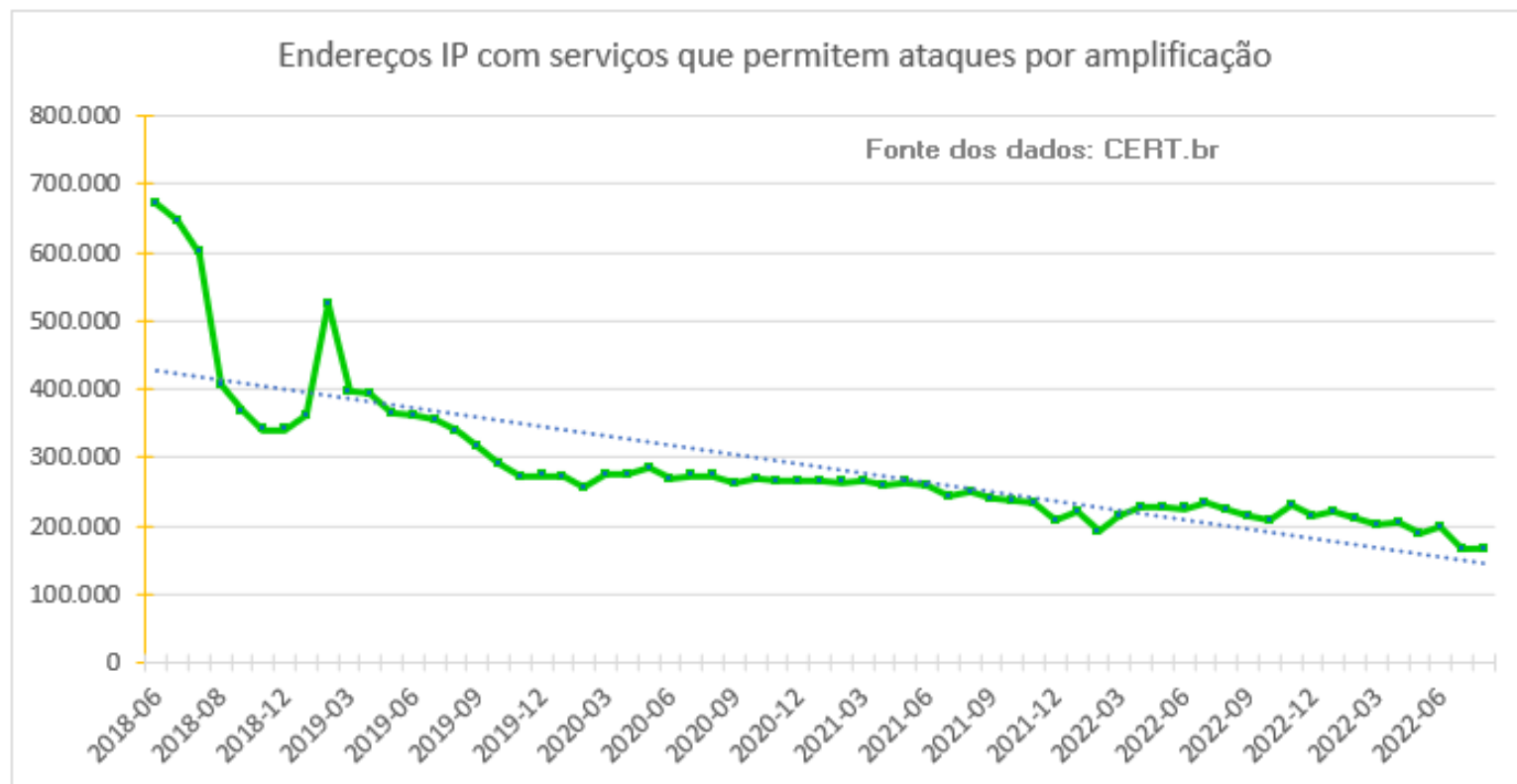
ASN	SNMP																												
	2021-03	2021-04	2021-05	2021-06	2021-07	2021-08	2021-09	2021-10	2021-11	2021-12	2022-01	2022-02	2022-03	2022-04	2022-05	2022-06	2022-07	2022-08	2022-09	2022-10	2022-11	2022-12	2023-01	2023-02	2023-03	2023-04	2023-05	2023-06	2023-07
	#																												
ASN1	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	110	115
ASN2	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	30	28
Total																	87	77	84	93	113	114	117	116	111	115	137	140	

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores



- Quantidade de endereços IP notificados com serviços mal configurados



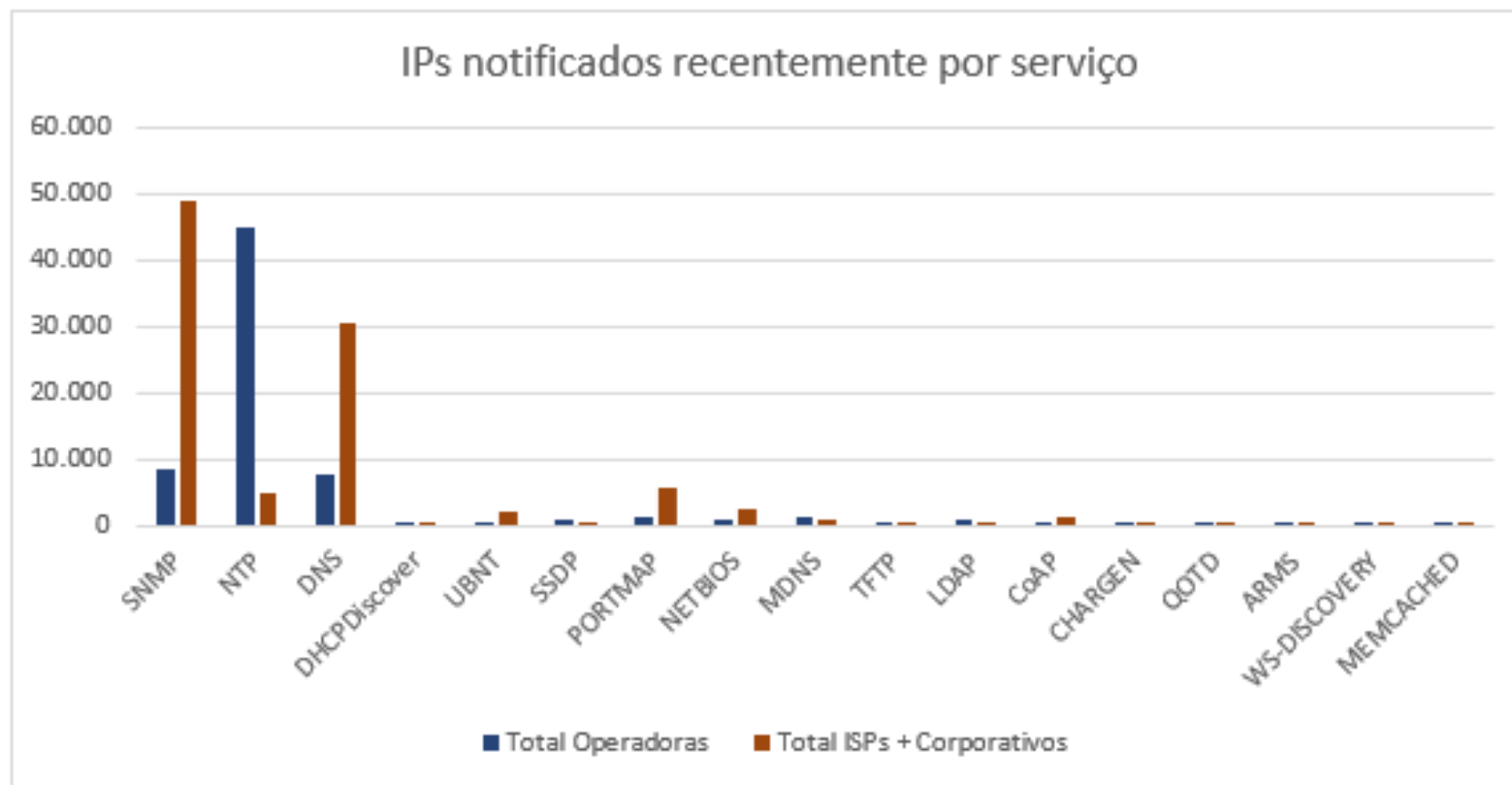
Redução de 77% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores



- Quantidade de endereços IP notificados por tipo de serviço



Ago/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) August 2023 COUNTRY Brazil

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

Route misoriginations	27
Route leaks	0
Bogon announcements	72
Total	99



Route misoriginations Route leaks Bogon announcements

Culprits

Culprits	64
----------	----



Culprits

Routing Information (IRR)

Unregistered	2,374	2.7%
Registered	84,773	97.3%



Unregistered Registered

Routing Information (RPKI)

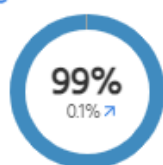
Valid	26,480	30.2%
Unknown	61,017	69.6%
Invalid	189	0.2%



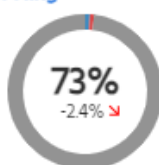
Valid Unknown Invalid

MANRS Readiness

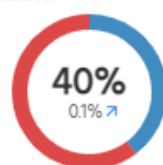
Filtering



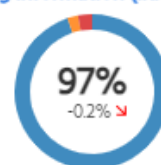
Anti-spoofing



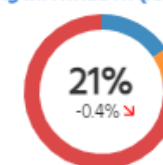
Coordination



Routing Information (IRR)



Routing Information (RPKI)



Ready Aspiring Lagging No Data Available

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

Ação 1 - Implementação de Filtros de Anúncios BGP

Topologia de rede sem filtros de anúncios



BGP Stream recebe alertas de:

- <https://bqpsstream.crosswork.cisco.com/>

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

Gerado pelo AS
ou por
seu cliente Direto

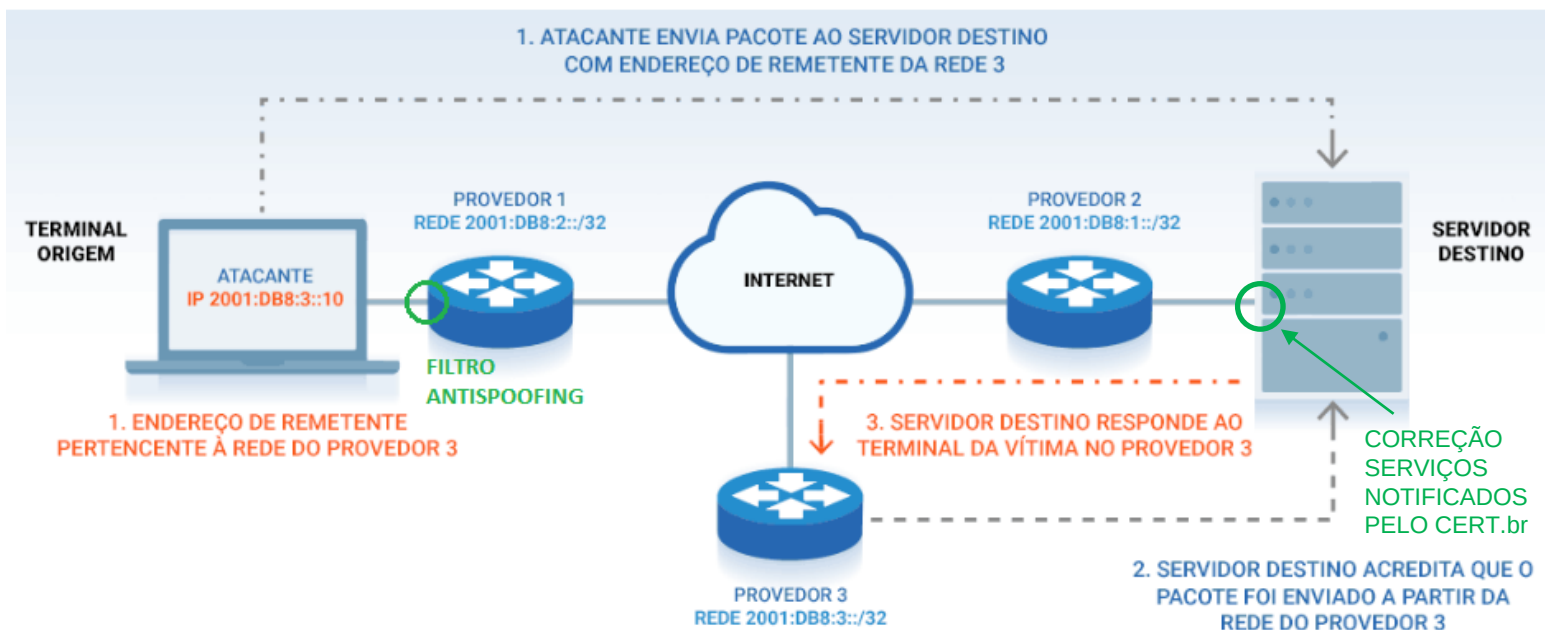
<https://observatory.manrs.org/#/about> 13

Programa por uma Internet mais Segura

Ação 2 - Implementação de Filtros Antispoofing

Ataque DoS por reflexão

Ataque DoS utilizando endereço de remetente forjado (Spoofing)



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

- 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

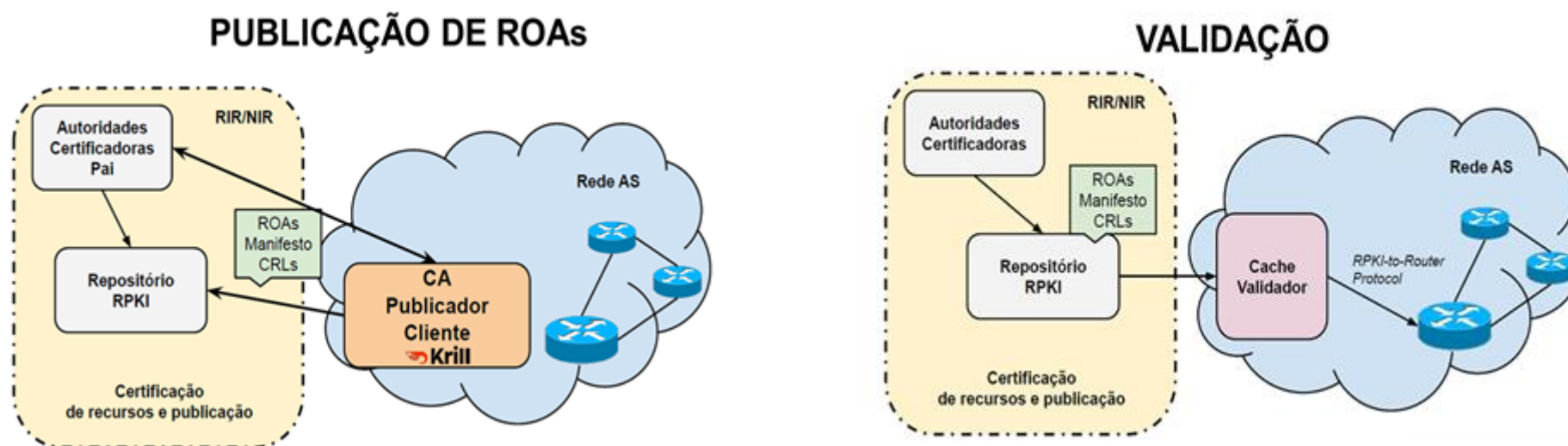
Programa por uma Internet mais Segura

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/>)

RPKI - Resource Public Key Infrastructure



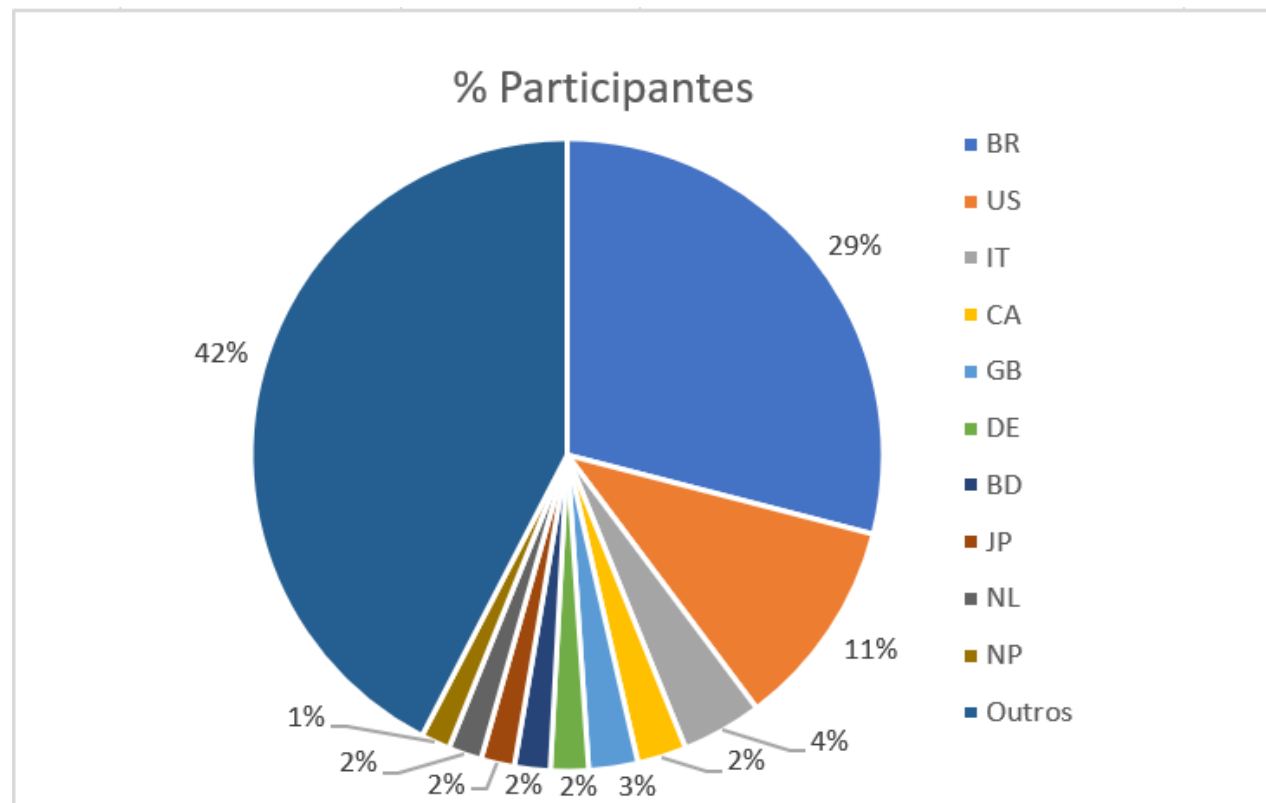
- MANRS Observatory analisa os ROAS publicados com um Validador RPKI próprio

Programa por uma Internet mais Segura

Participantes do MANRS



- Distribuição por país dos Provedores participantes da iniciativa MANRS



Total de participantes: 875

Participantes do Brasil: 254 (Ago/23)

206 (2022)

174 (2021)

140 (2020)

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

Teste TOP - IPv6 e DNSSEC da rede do usuário

134.805

Med. - IPv6 DNSSEC Final.

85.834

Recurso c/ DNSSEC Validado

64%

% Recursivo c/ DNSSEC Validado

5.632

AS Únicos Testados

84.684

Usuários com IPv6

63%

% Usuários IPv6 100%

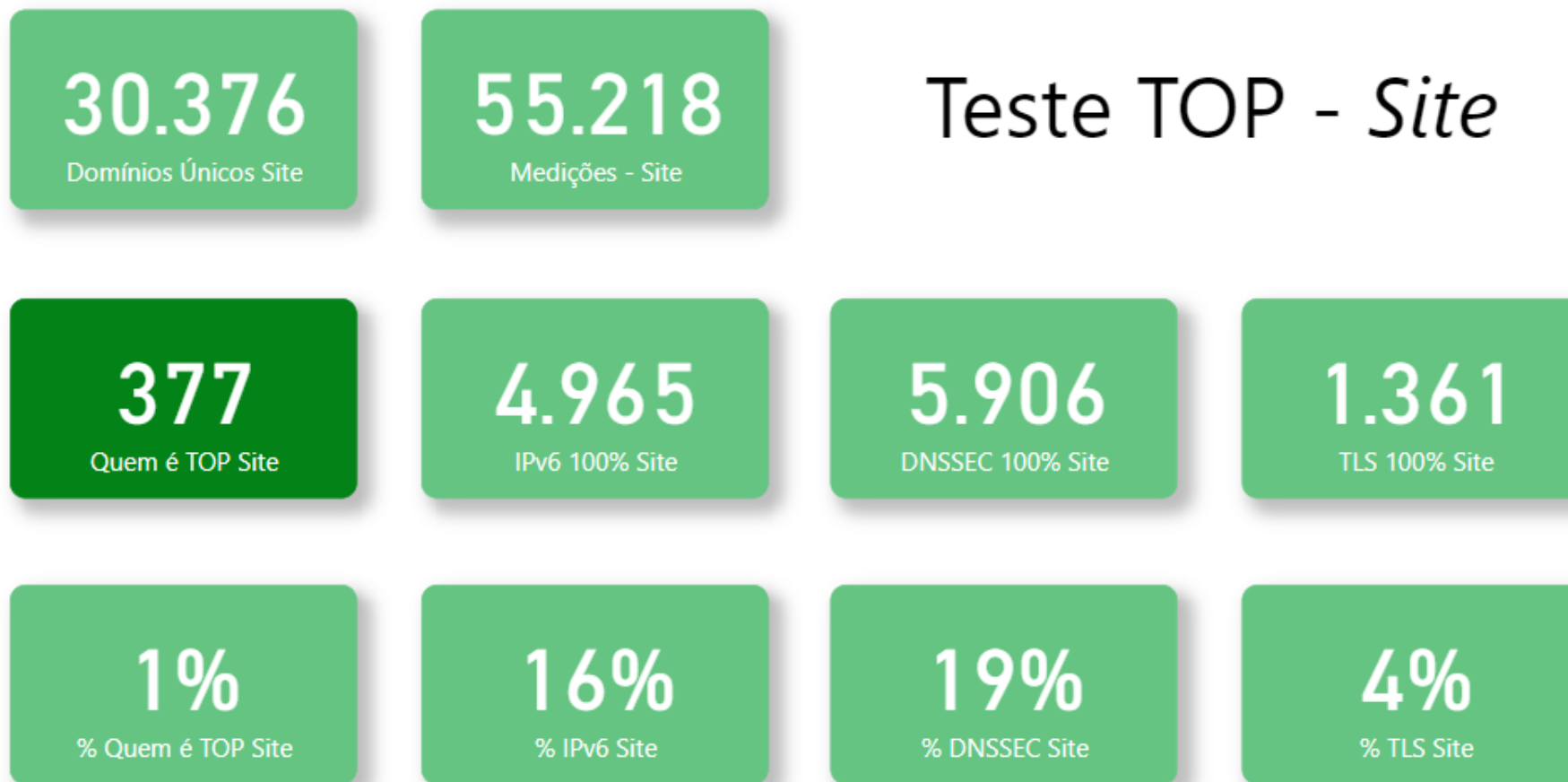
Medições totais IPv6 100%



15/8/23

20

TOP – Teste os Padrões – Desenvolvimento



15/8/23

21

TOP – Teste os Padrões – Desenvolvimento

16 Mil

Domínios Únicos c/ MX

28.221

Medições - E-mail

Teste TOP - *E-mail*

68

Quem é TOP E-mail

1.801

IPv6 100% E-mail

1.814

DNSSEC 100% E-mail

2.215

Marcas Aut. 100% E-mail

83

STARTTLS 100% E-mail

0%

% Quem é TOP E-mail

11%

% IPv6 E-mail

12%

% DNSSEC E-mail

14%

% Marcas Aut. E-mail

1%

% STARTTLS E-mail



15/8/23

22

TOP – Teste os Padrões - Apoio



<https://top.nic.br>



A CONECTIVIDADE AO SEU ALCANCE



Obrigado

Gilberto Zorello

@ gzorello@nic.br

25 de agosto de 2023

nic.br **cgi.br**

www.nic.br | www.cgi.br

