nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.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

2º CONECTA NET

Montes Claros, MG | 01/12/23

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

- Redução dos ataques de Negação de Serviço
- **Melhora da Segurança de Roteamento na rede**
- Redução das vulnerabilidades e falhas de configuração
- **Divulgar boas 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 das ações**

PROGRAMA INTERNET +SEGURA

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

Programa por uma Internet mais Segura
Interação com Provedores e Operadoras

- Reuniões bilaterais on-line com **os responsáveis pelos ASes mais notificados**
- Ações tratadas nas reuniões bilaterais:
  - **Correção dos serviços mal configurados notificados pelo CERT.br, que podem ser abusados em ataques DDoS**
  - Adoção de Boas Práticas de roteamento (**MANRS**)
  - **Adoção das práticas recomendadas e testadas pelo TOP**
  - Apresentação de medições, por AS

Programa por uma Internet mais Segura
Notificação de Amplificadores

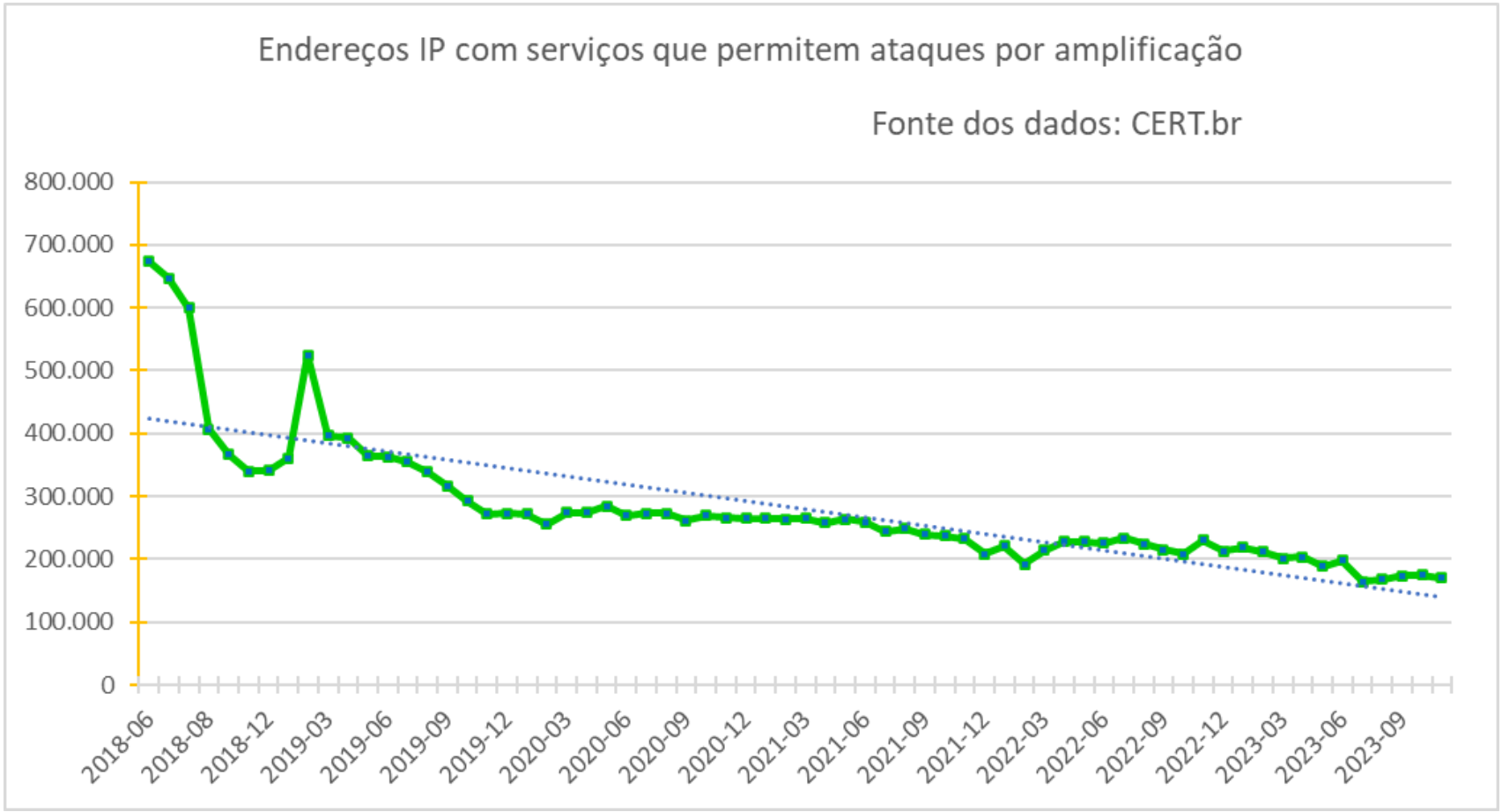
- Estatísticas das notificações encaminhadas pelo CERT.br
- **Relatório gerencial encaminhado mensalmente**

ASN	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DICOVERY	TFTP	CoAP	ARMS	SLP	DHCPDiscover	2023-08	2023-09	2023-10	Mais Recente	MT4145	MT5678
ASN1	103	42	0	23	0	3	0	0	1	2	0	0	3	0	1	3	0	205	204	209	199	0	0
ASN2	40	5	2	10	0	7	0	0	3	2	0	0	0	0	0	0	0	136	142	114	125	0	1
Total	11%	6%	26%	-5%		-20%			37%	-6%			-54%		9%		-100%	**341**	**346**	**323**	**321**		9%

ASN	SNMP																	SNMP
	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	2023-08	2023-09	2023-10	2023-11	
ASN1	64	55	57	66	83	84	87	87	81	85	109	110	115	116	104	111	103	103
ASN2	23	22	27	27	30	30	30	29	30	30	28	30	28	34	38	31	40	40
Total					113	114	117	116	111	115	137	140	143	150	142	142		11%

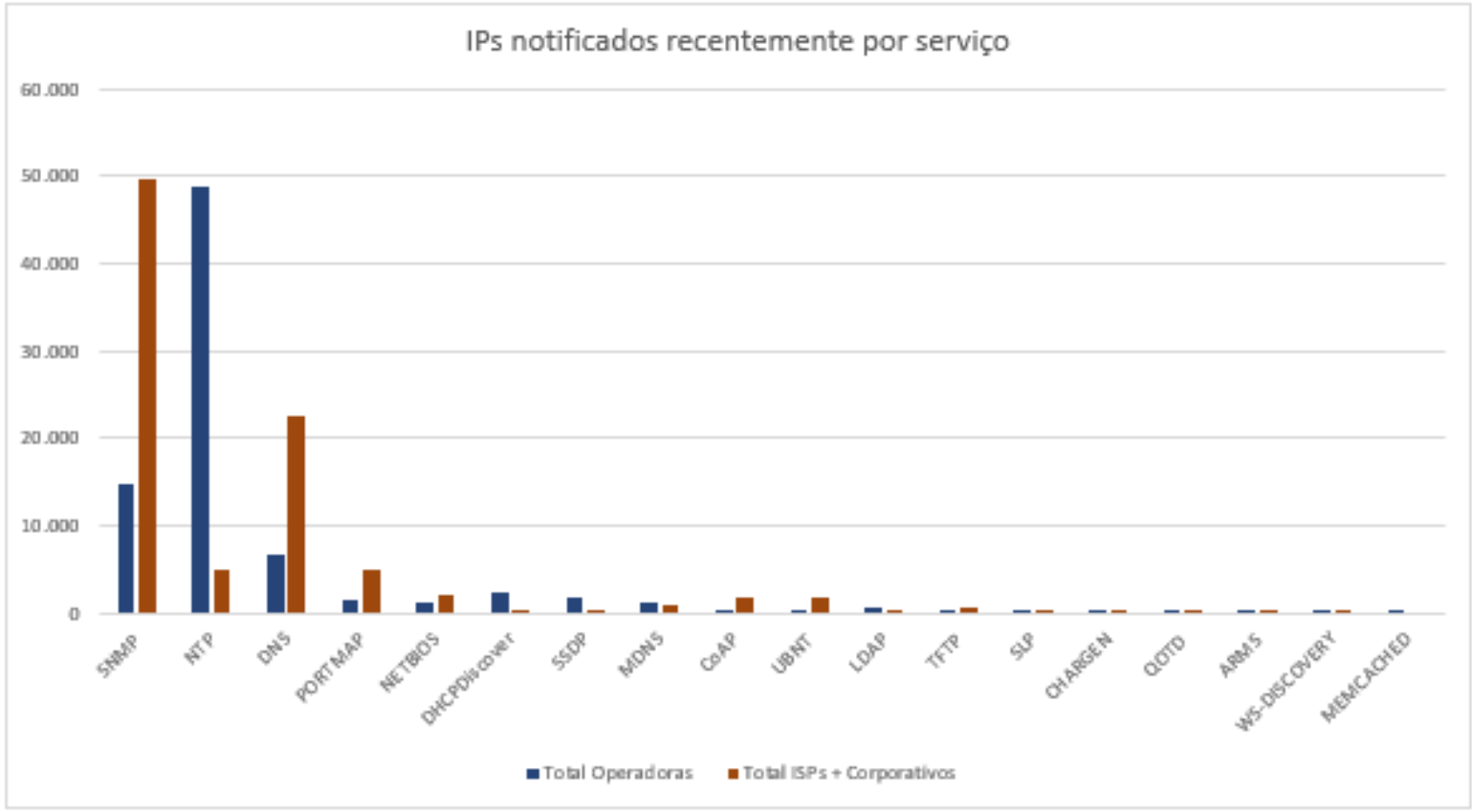
O serviço SLP (Service Location Protocol passou a ser notificado em nov/23 pelo CERT.br

Programa por uma Internet mais Segura
Notificação de Amplificadores



Redução de 76% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura
Notificação de Amplificadores



Nov/23

Principais ofensores: ISPs e ASes corporativos → SNMP habilitado e DNS recursivo aberto

Grandes operadoras → NTP mal configurado

Programa por uma Internet mais Segura
MANRS

MANRS

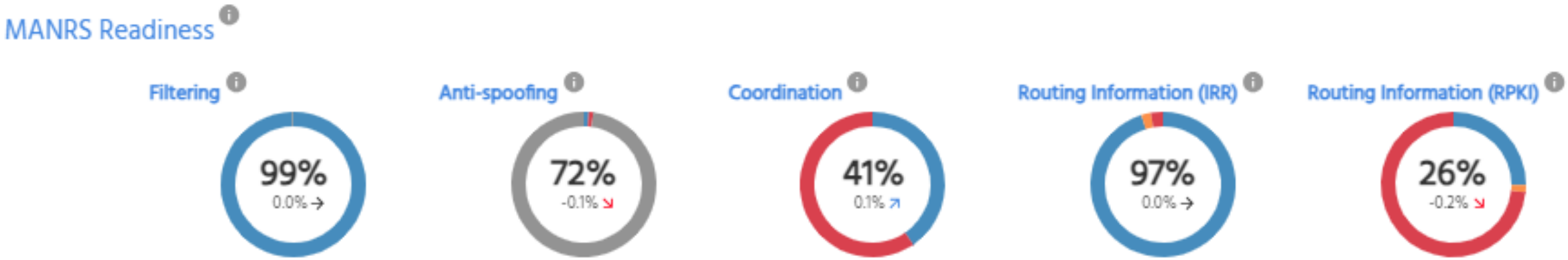
Mutually Agreed Norms for Routing Security

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



Nov/23

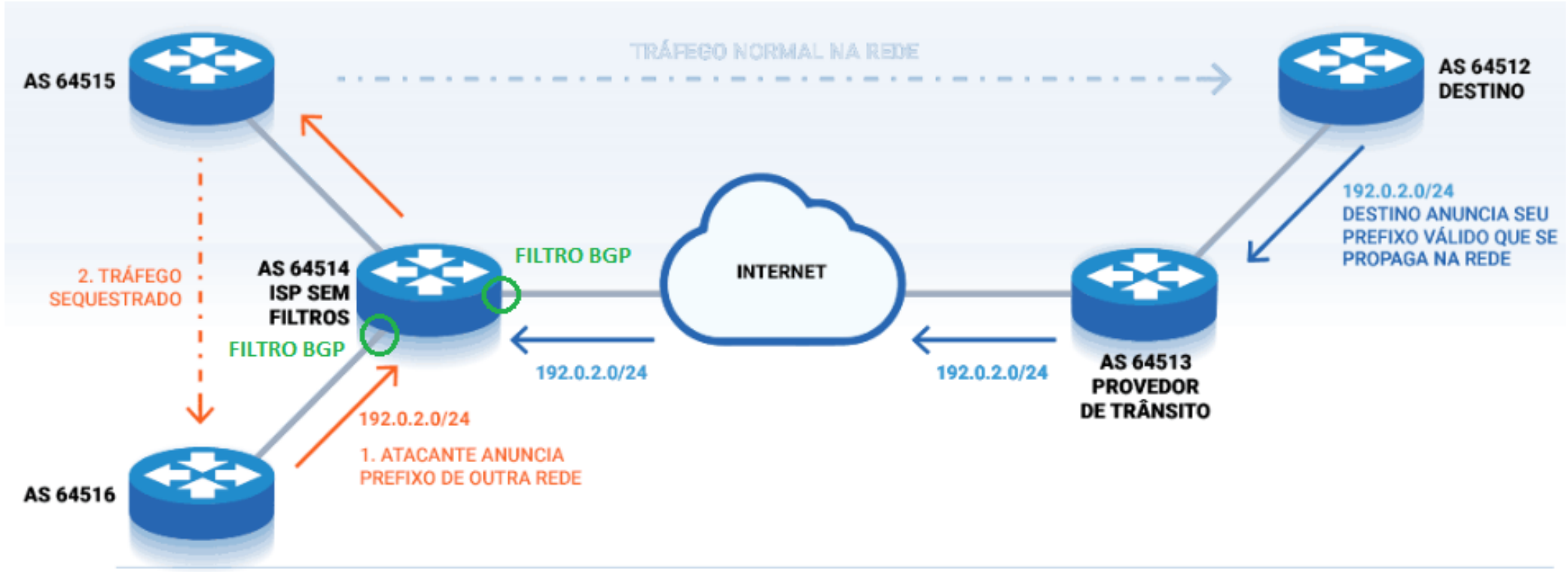
Fonte: https://observatory.manrs.org/#/overview

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



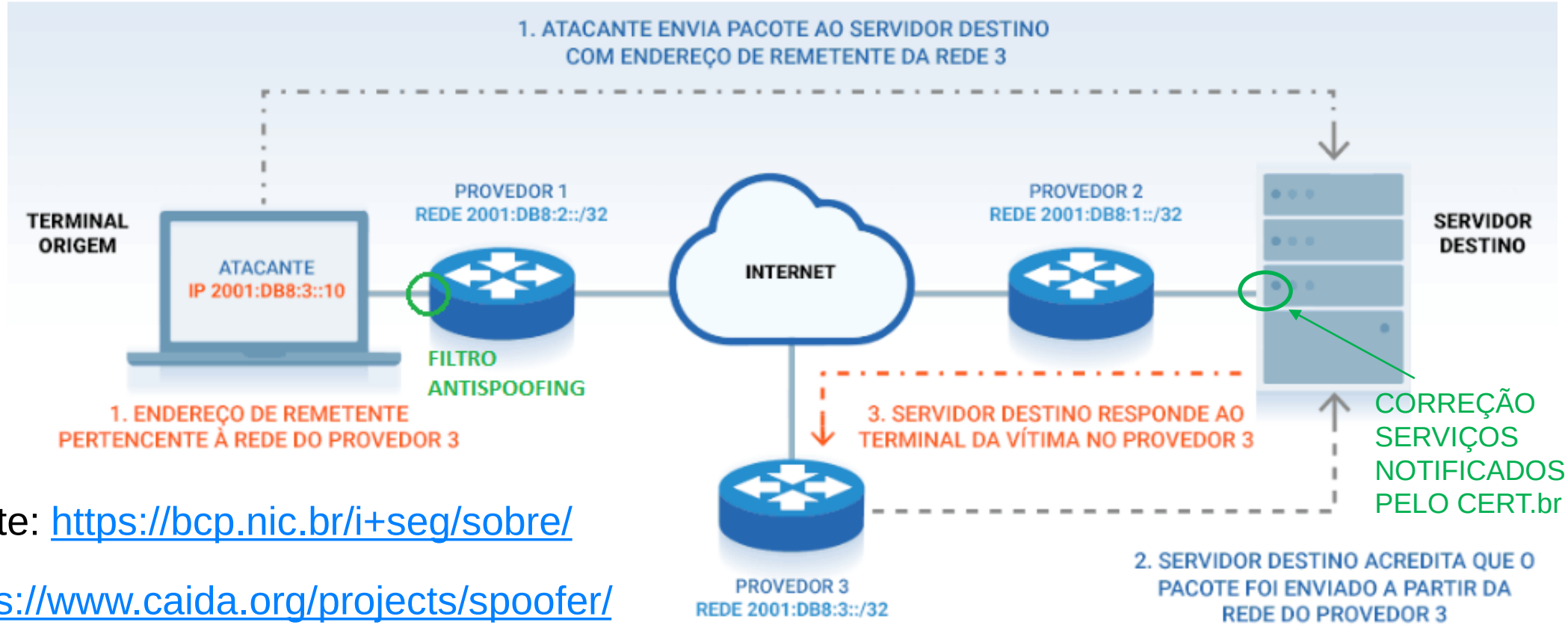
Fonte: https://bcp.nic.br/i+seg/sobre/

Programa por uma Internet mais Segura

Ação 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/

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

Programa por uma Internet mais Segura

Ação 3 - Coordenação entre Operadores

Facilitar a comunicação operacional global e a coordenação entre os operadores

Endereços de *e-mail* indicados no Whois:

nic.br | registro.br

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

Titular

Roteamento

Abuse

Endereços de *e-mail* indicados no

PeeringDB

https://www.peeringdb.com/

NOC

Abuse

Outros

- **CERT.br → *e-mail* do campo Abuse do Whois**
- Grupos de *e-mails* ao invés de *e-mails* pessoais
- **Compatibilidade dos pontos de contatos de outras bases (Whois, PeeringDB, IRR)**

Programa por uma Internet mais Segura

Ação 3 - Coordenação entre Operadores

Facilitar a comunicação operacional global e a coordenação entre os operadores

Endereços de *e-mail* indicados no Whois:

nic.br | registro.br

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

Titular

Roteamento

Abuse

Endereços de *e-mail* indicados no

PeeringDB

https://www.peeringdb.com/

NOC

Abuse

Outros

- **CERT.br → *e-mail* do campo Abuse do Whois**
- Grupos de *e-mails* ao invés de *e-mails* pessoais
- **Compatibilidade dos pontos de contatos de outras bases (Whois, PeeringDB, IRR)**
- Manter pontos de contatos atualizados: mudanças internas e incorporação de outros ASes
- **MANRS Observatory: 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

Endereços de *e-mail* indicados no Whois:

nic.br | registro.br

Titular

Roteamento

Abuse

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

Endereços de *e-mail* indicados no

PeeringDB

NOC

Abuse

Outros

https://www.peeringdb.com/

- **CERT.br → *e-mail* do campo Abuse do Whois**
- Grupos de *e-mails* ao invés de *e-mails* pessoais
- **Compatibilidade dos pontos de contatos de outras bases (Whois, PeeringDB, IRR)**
- Manter pontos de contatos atualizados: mudanças internas e incorporação de outros ASes
- **MANRS Observatory: pontos de contato técnicos do PeeringDB**

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

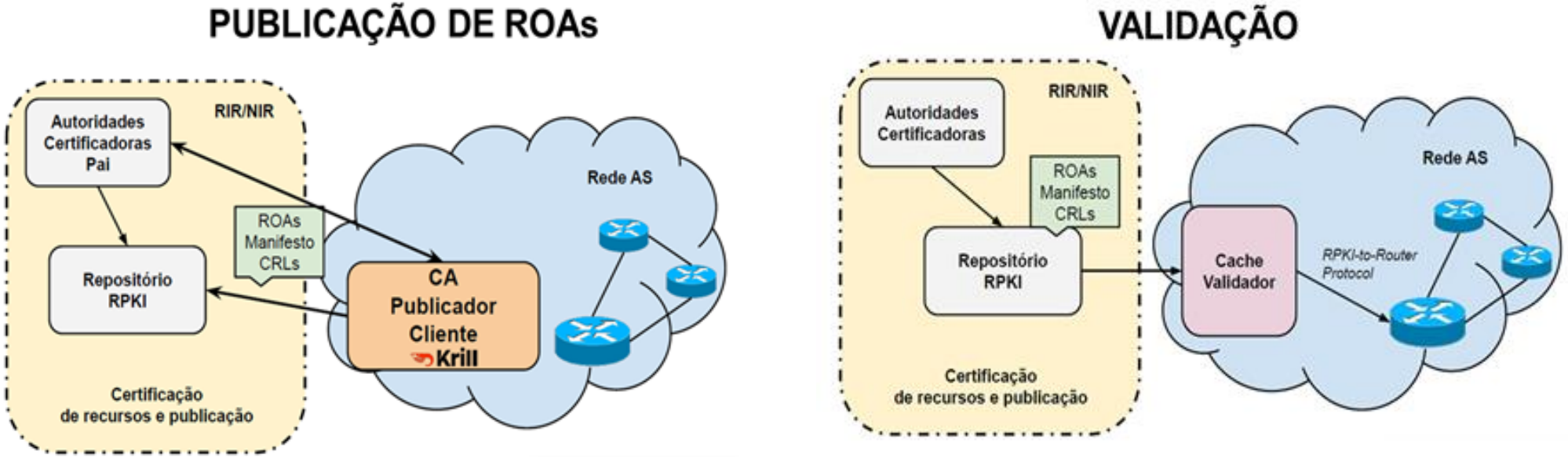
Programa por uma Internet mais Segura

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/)

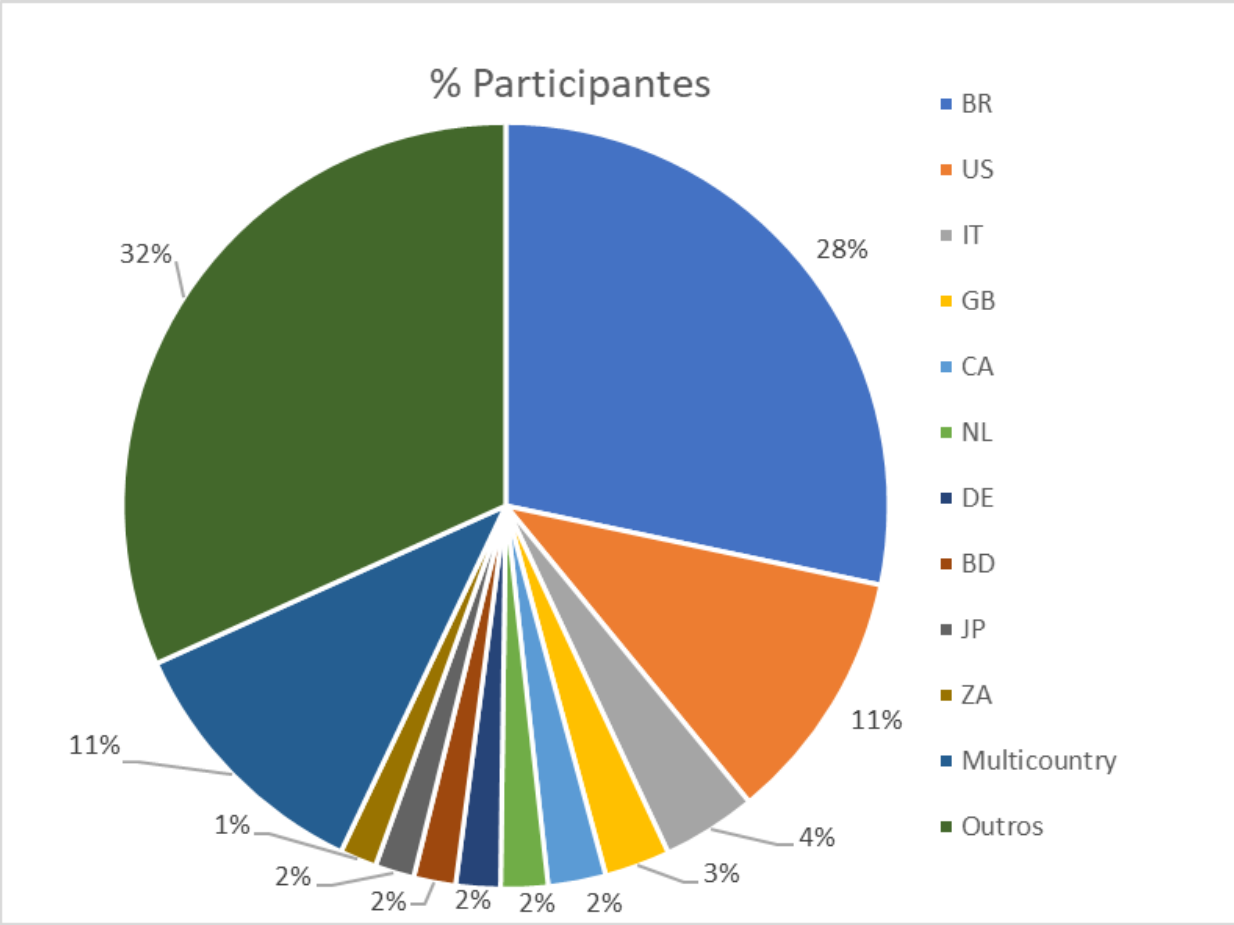
RPKI - Resource Public Key Infrastructure



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

Programa por uma Internet mais Segura

Participantes do MANRS



Total de participantes:

904

Participantes do Brasil:

256 (Nov/23)

206 (2022)

174 (2021)

140 (2020)

Fonte:
https://www.manrs.org/netops/participants/
Acesso nov/23

Programa por uma Internet mais Segura

TOP – TESTE OS PADRÕES

https://top.nic.br

Programa por uma Internet mais Segura

TOP – TESTE OS PADRÕES

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)**

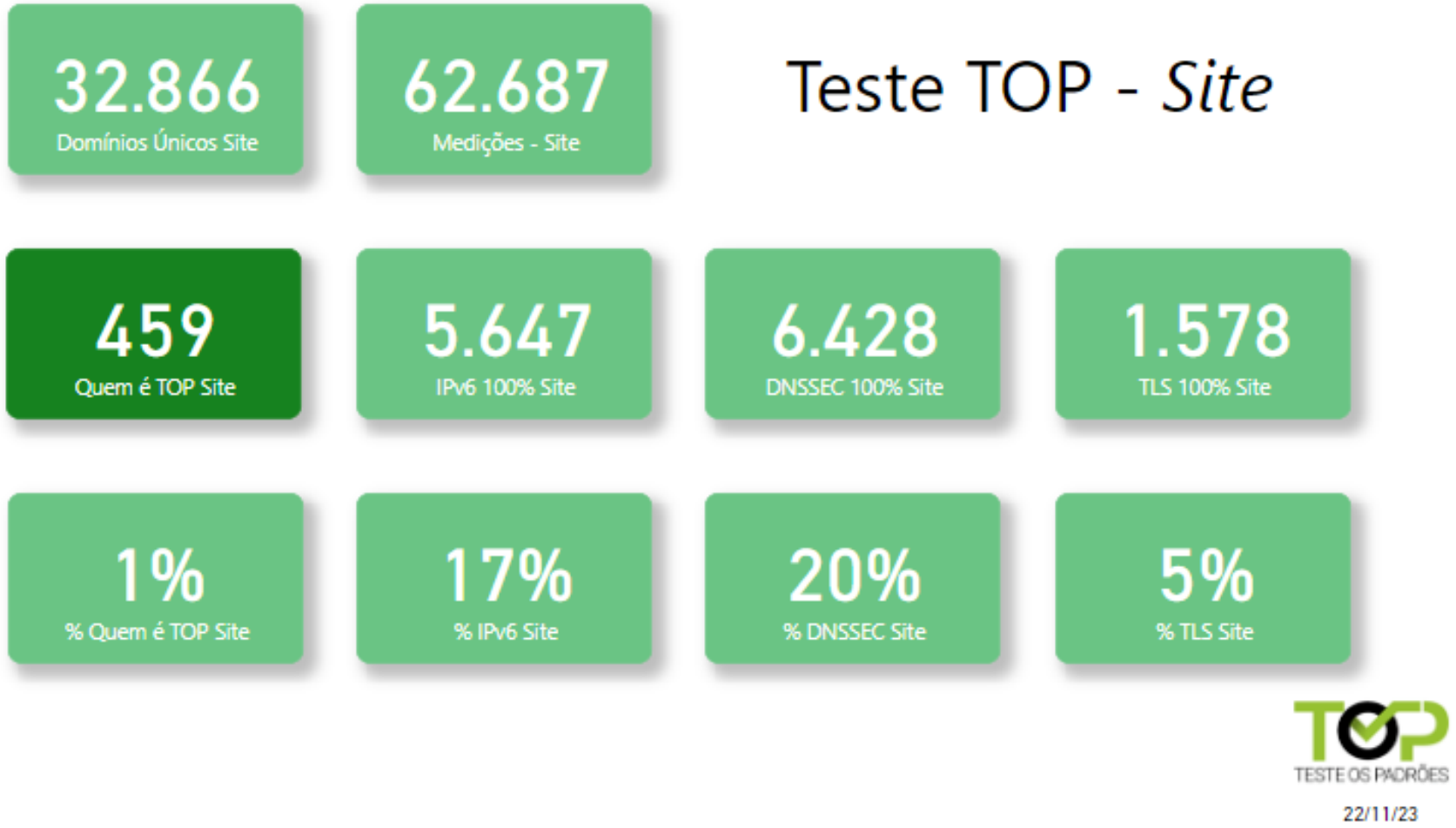
Acesso: https://top.nic.br

Programa por uma Internet mais Segura

TOP – TESTE OS PADRÕES

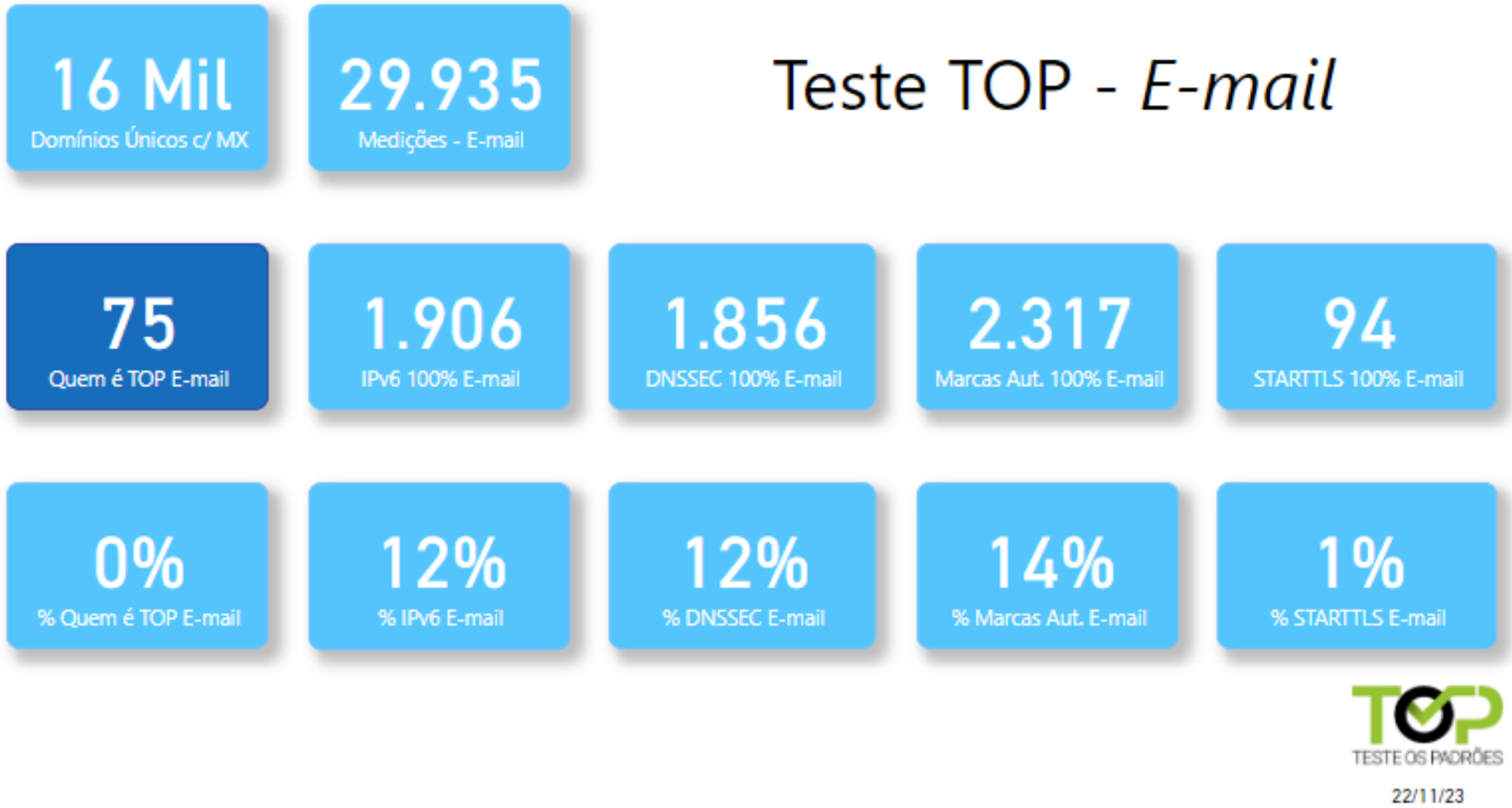
Programa por uma Internet mais Segura

TOP – TESTE OS PADRÕES



Programa por uma Internet mais Segura

TOP – TESTE OS PADRÕES



Programa por uma Internet mais Segura

Apoio

conexis brasil.digital
A CONECTIVIDADE AO SEU ALCANCE

abranet
Associação Brasileira de Internet

AbraHosting
ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE INFRAESTRUTURA DE HOSPEDAGEM NA INTERNET

TOP
TESTE OS PADRÕES

REDETELESUL

abrint

TelComp
Competição para o Futuro Digital

abramulti
Associação brasileira dos operadores de telecomunicações e provedores de internet.

APRONET
Associação Catarinense dos Provedores de Internet

RNP
REDE NACIONAL DE ENSINO E PESQUISA

InternetSul

Obrigado

Gilberto Zorello

gzorello@nic.br

1 de dezembro de 2023

nic.br cgi.br

www.nic.br | www.cgi.br