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

Programa por uma Internet mais segura

Como tornar a o seu provedor mais seguro

Gilberto Zorello | gzorello@nic.br

IX Fórum Regional Centro Oeste

Cuiabá, MT | 18/08/23

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: Notificação de Amplificadores, MANRS, IPv6, DNSSEC, TLS, DMARC**
- **Incentivar o crescimento de uma cultura de segurança entre os operadores das redes**

PROGRAMA INTERNET +SEGURA

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
- **Conscientização por meio de palestras, cursos e treinamentos**
- Criação de materiais didáticos e boas práticas
- Interação com operadores das redes para incentivar o crescimento de uma **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 INTERNET +SEGURA

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

Programa por uma Internet mais Segura
Interação com Provedores e Operadoras

- Reuniões bilaterais on-line com as grandes operadoras e **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-DICOVERY	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

- 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**

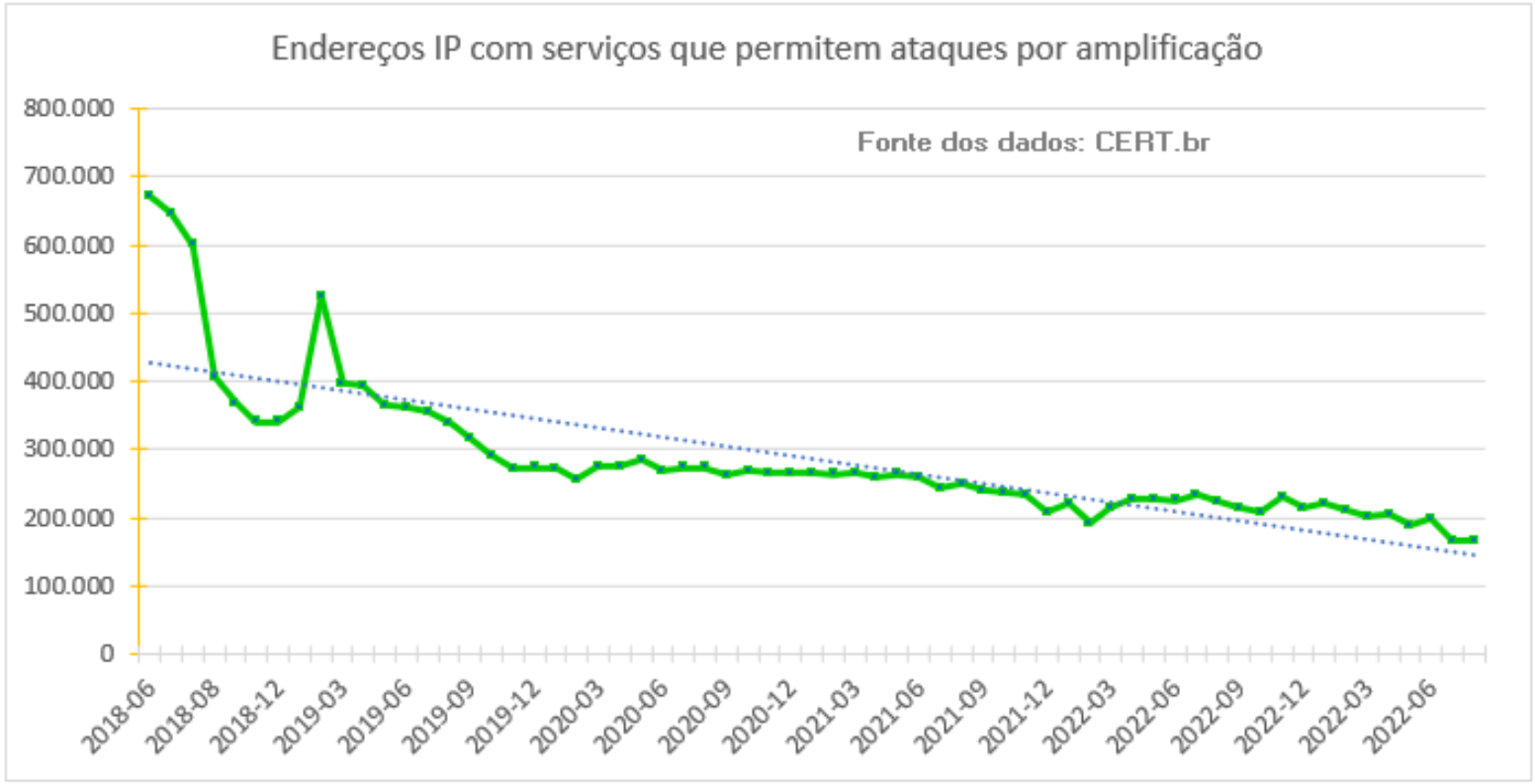
ASN	DNS	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DICOVERY	TFTP	CoAP	ARMS	DHCPDiscover	2023-04	2023-05	2023-06	2023-07	MT4145	MT5678
ASN1	14	115	40	1	28	0	5	0	0	1	2	0	0	4	0	1	0	205	204	215	211	0	0
ASN2	44	28	0	1	7	0	7	0	0	1	2	0	0	0	0	0	0	98	89	93	90	0	1
Total	-11%	32%	-4%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

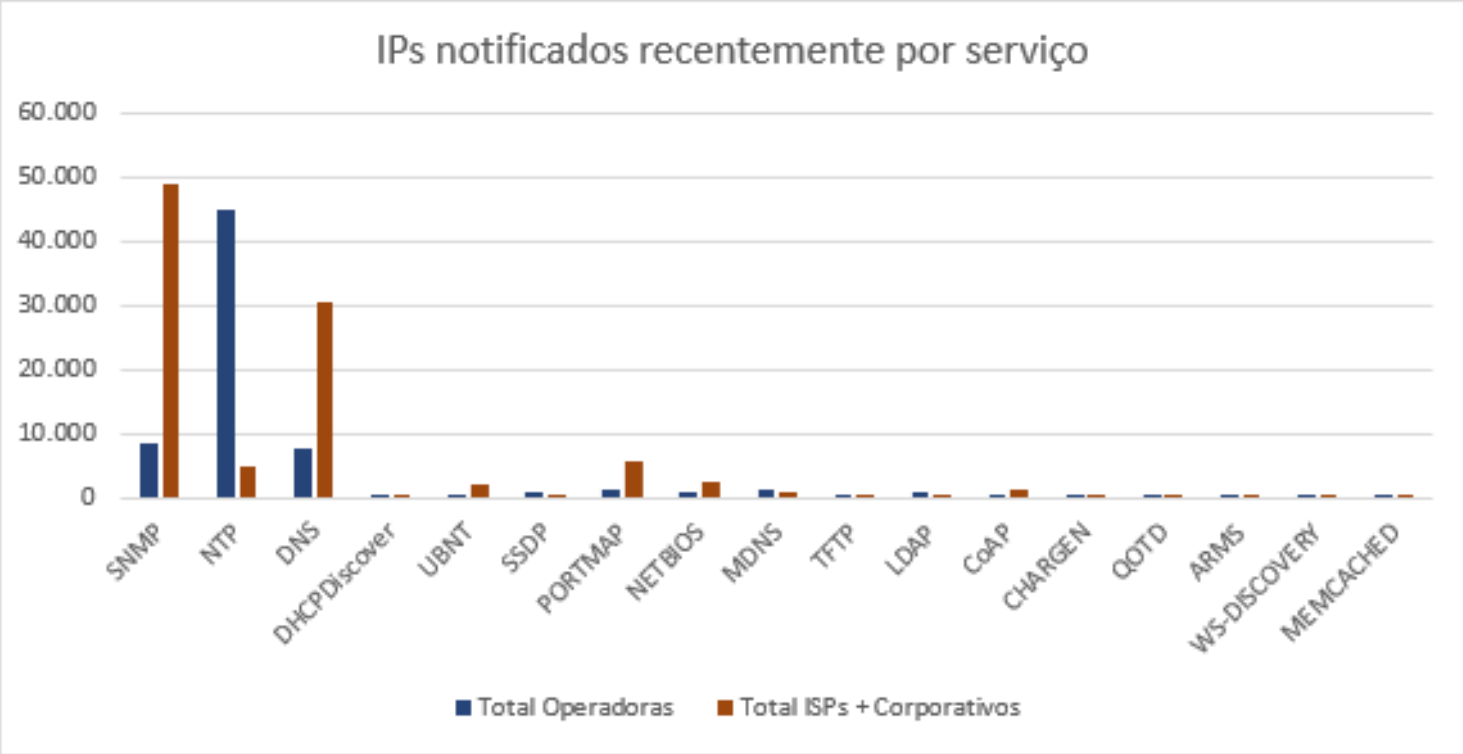


Redução de 77% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores

- Quantidade de endereços IP notificados por tipo de serviço



Agoi/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

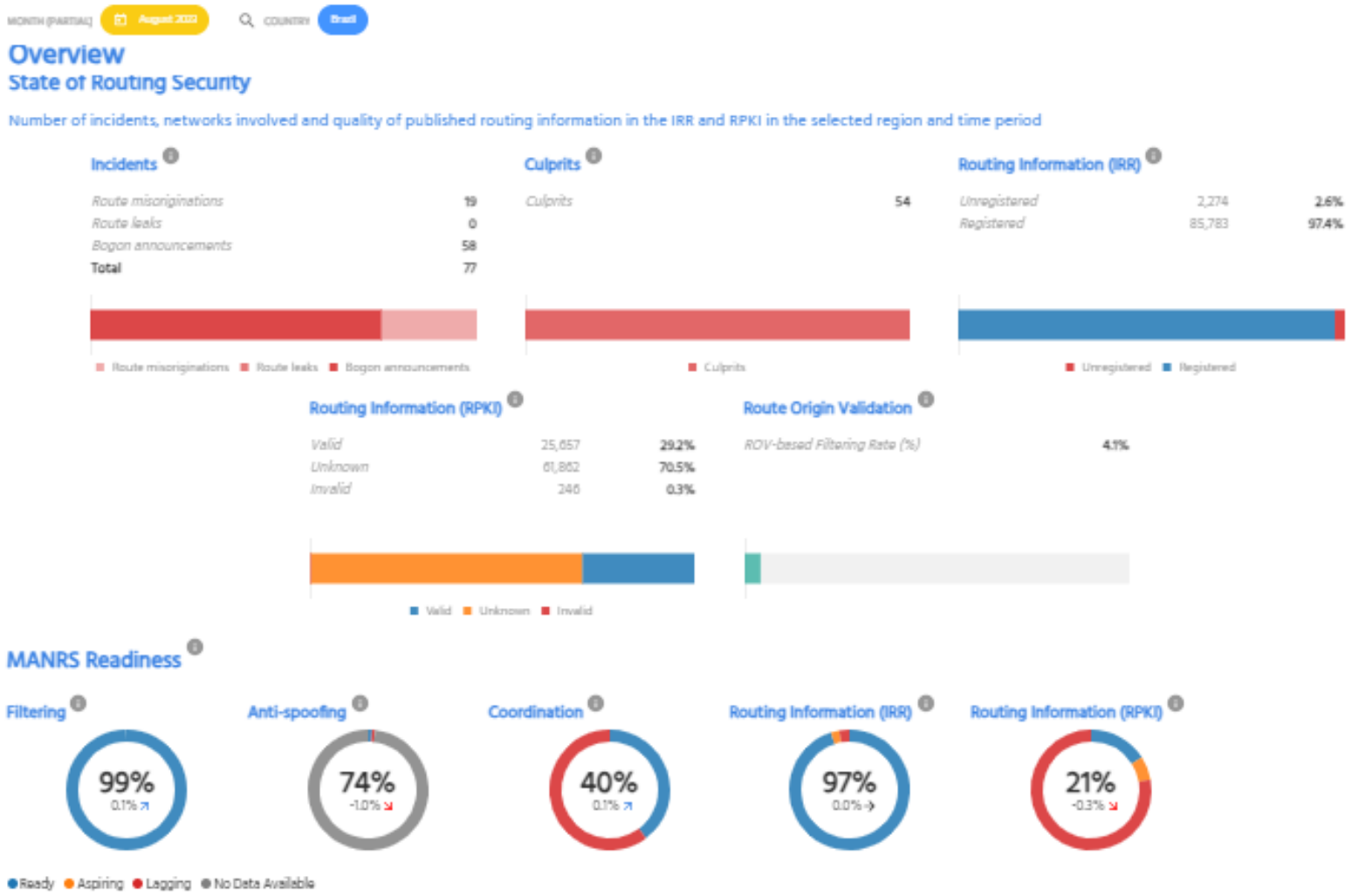
http://manrs.org

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

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

Programa por uma Internet mais Segura

MANRS Observatory Readiness - Brasil

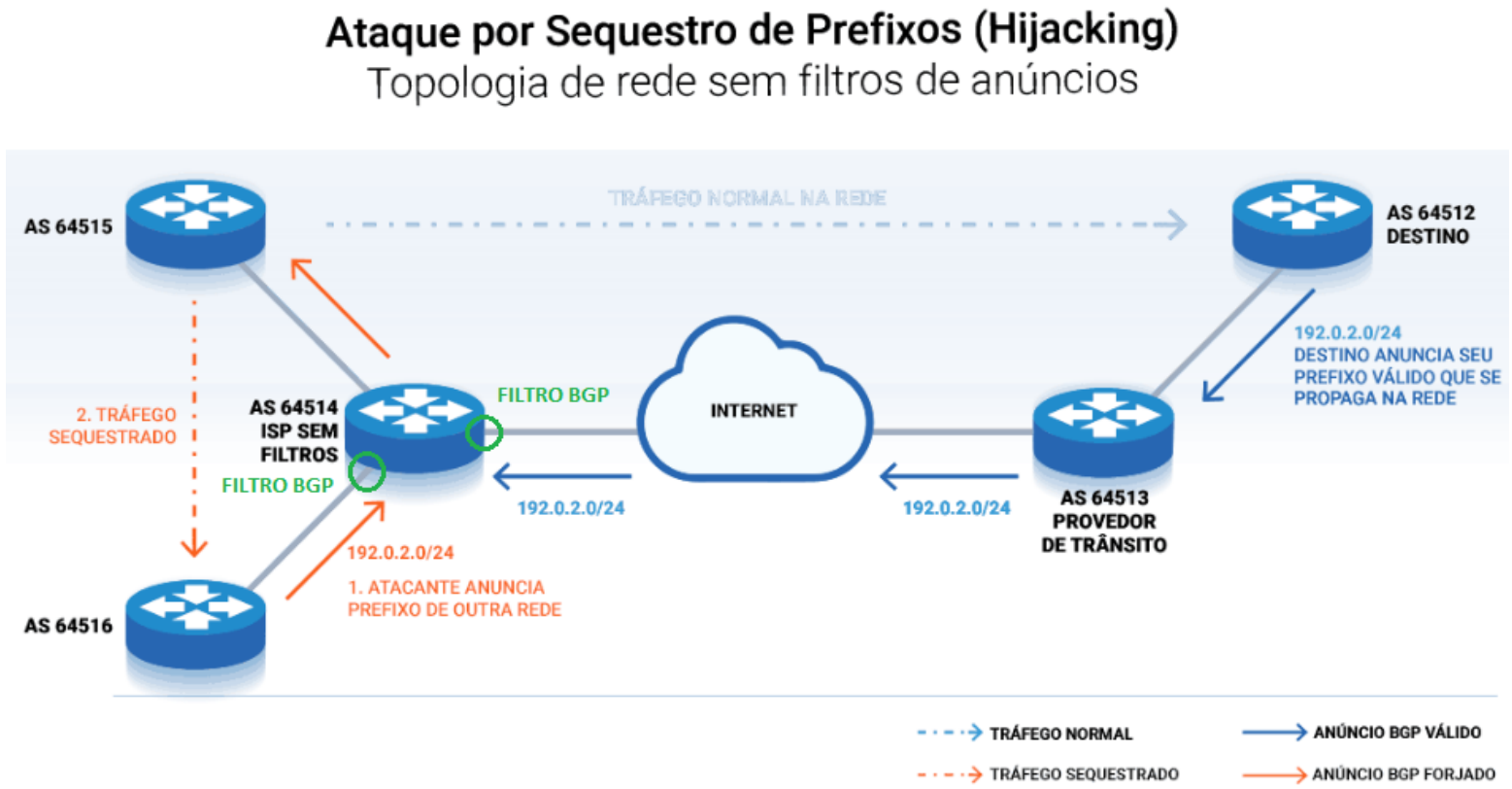


Este Dash Board, com informações por AS, é acessível aos participantes do MANRS

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

Programa por uma Internet mais Segura

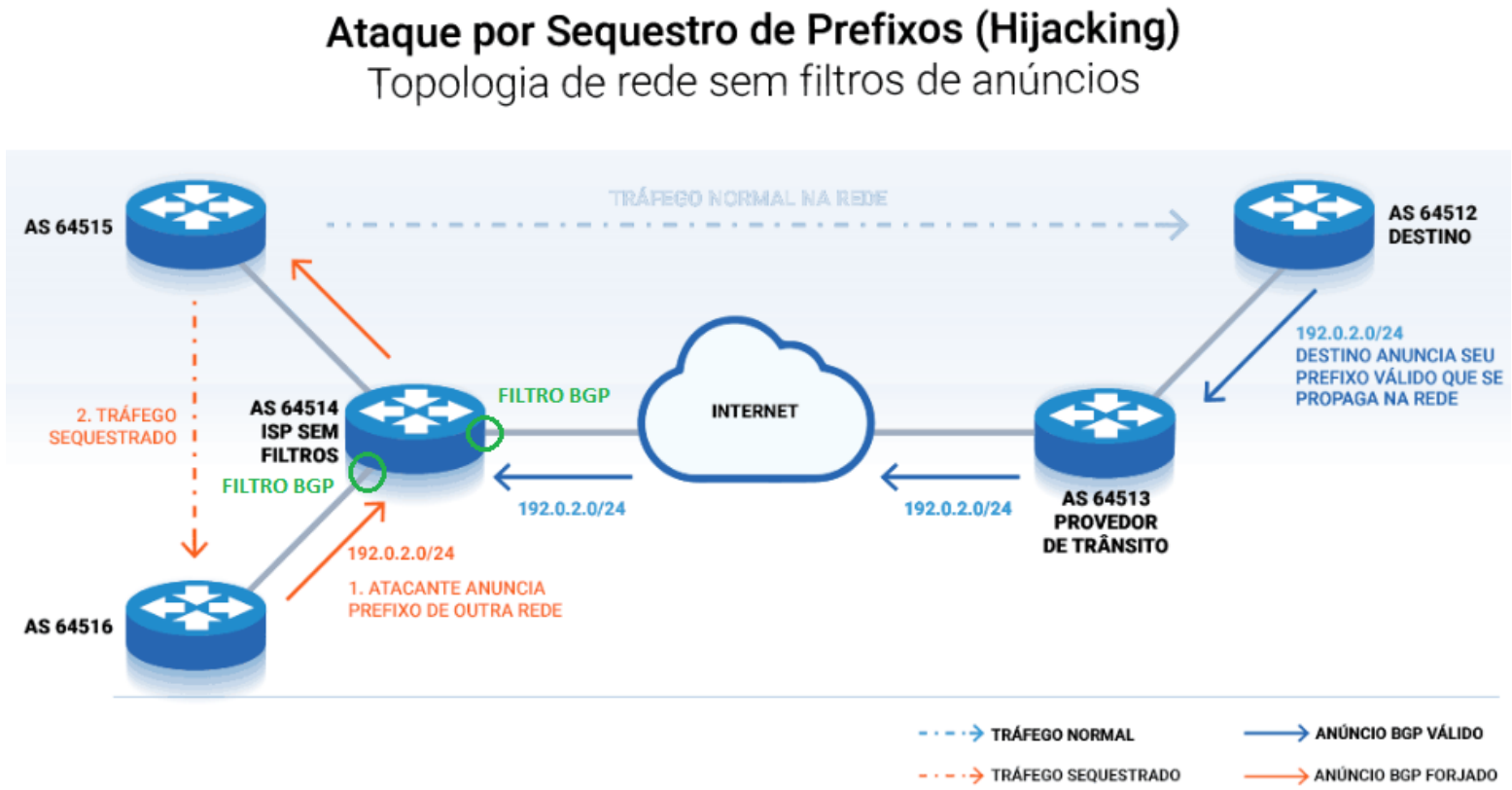
Ação 1 - Implementação de Filtros de Anúncios BGP



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

Programa por uma Internet mais Segura

Ação 1 - Implementação de Filtros de Anúncios BGP

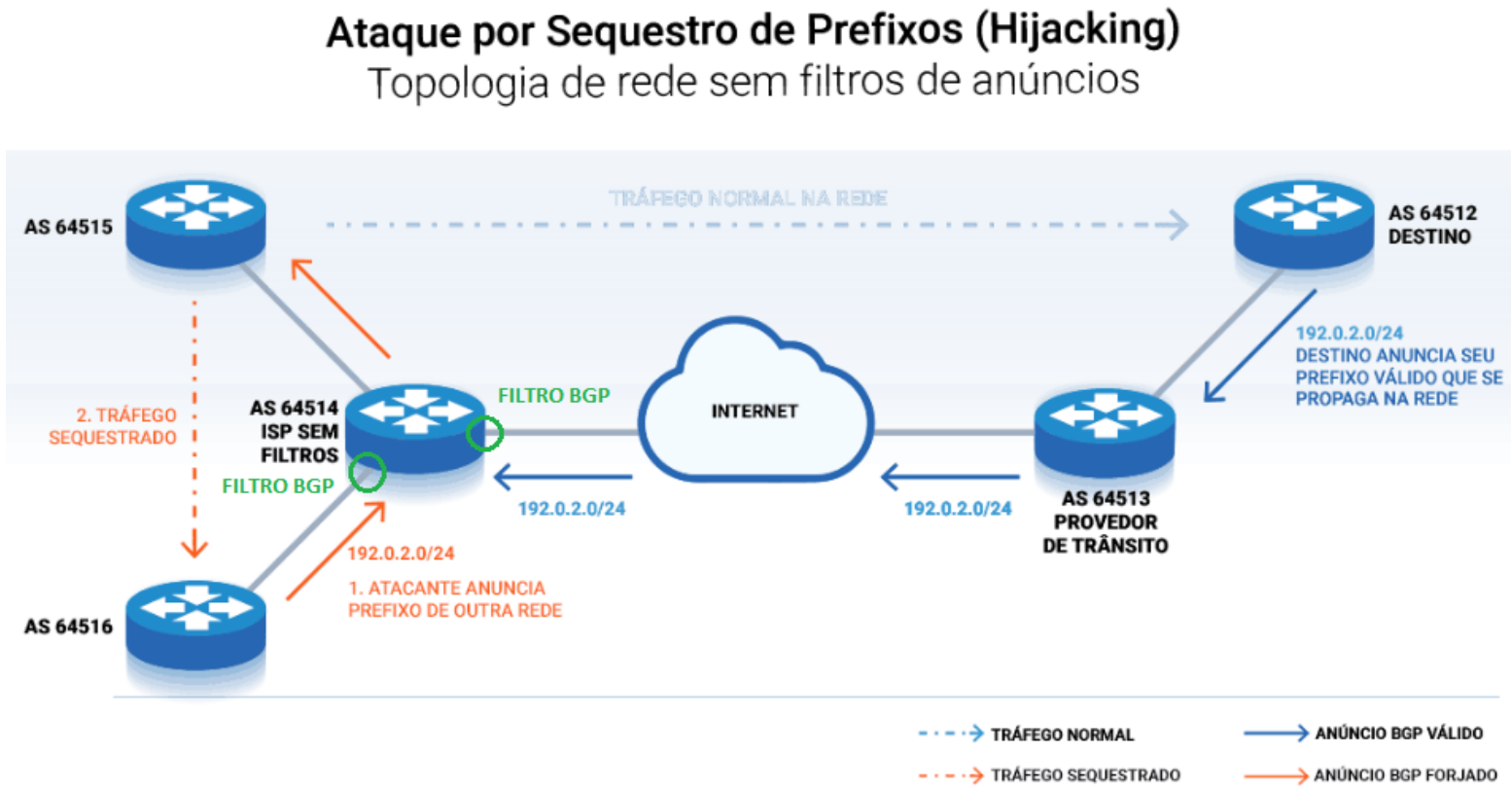


O provedor deve garantir a correção dos próprios anúncios e de seus clientes

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

Programa por uma Internet mais Segura

Ação 1 - Implementação de Filtros de Anúncios BGP



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

BGP Stream recebe alertas de:

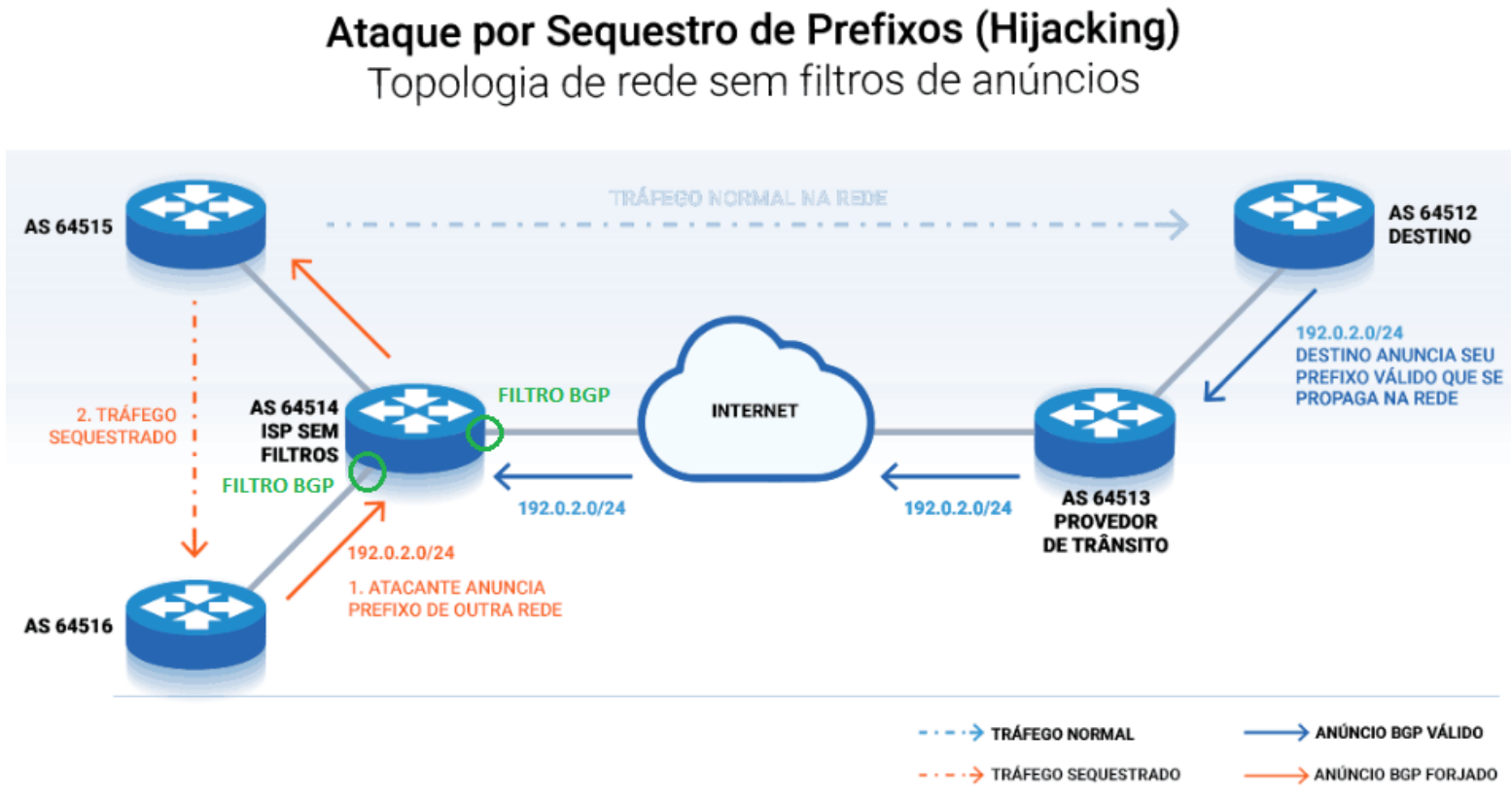
- Hijacking (sequestro de prefixos)
- Leak (vazamento de rotas)
- Outages
- Últimos 180 dias de eventos
- Monitoramento de seus anúncios BGP

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



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:

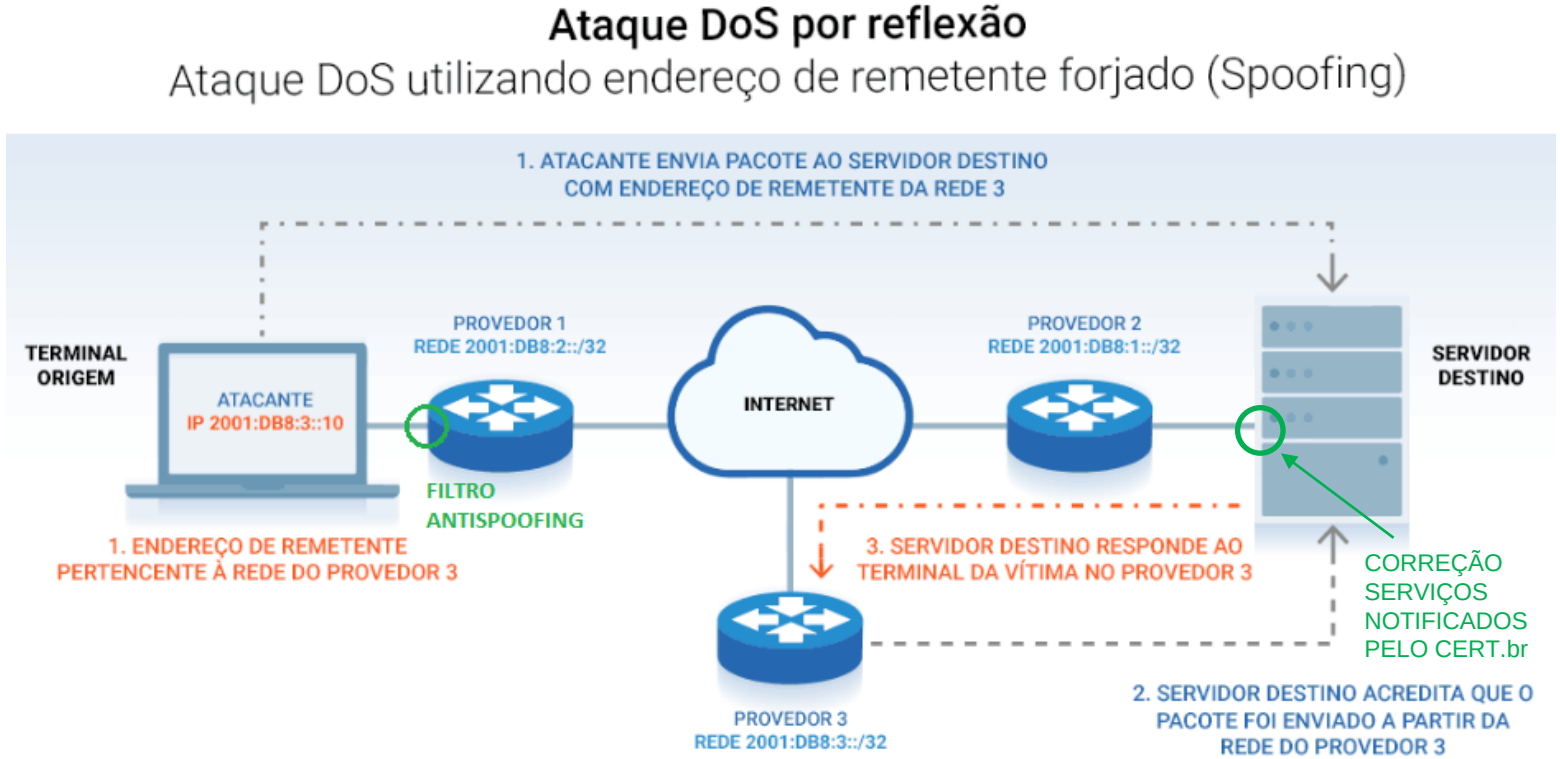
- Hijacking
- Leak
- Bogon - prefixos
- Bogon - ASNs

} Gerado pelo AS ou por seu cliente Direto

https://observatory.manrs.org/#/about

Programa por uma Internet mais Segura

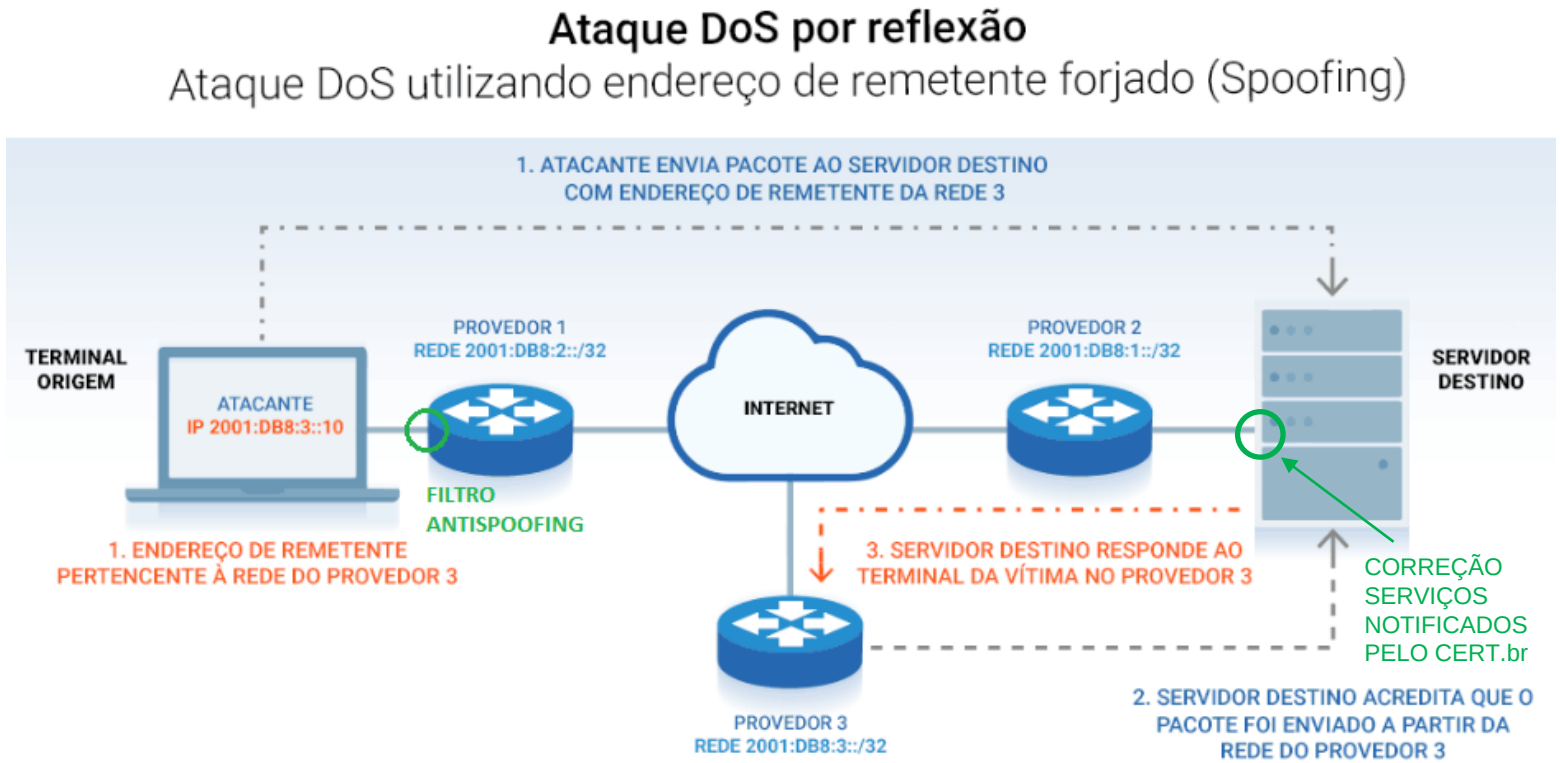
Ação 2 - Implementação de Filtros Antispoofing



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

Programa por uma Internet mais Segura

Ação 2 - Implementação de Filtros Antispoofing



Implementação de filtro antispoofing o mais próximo do cliente

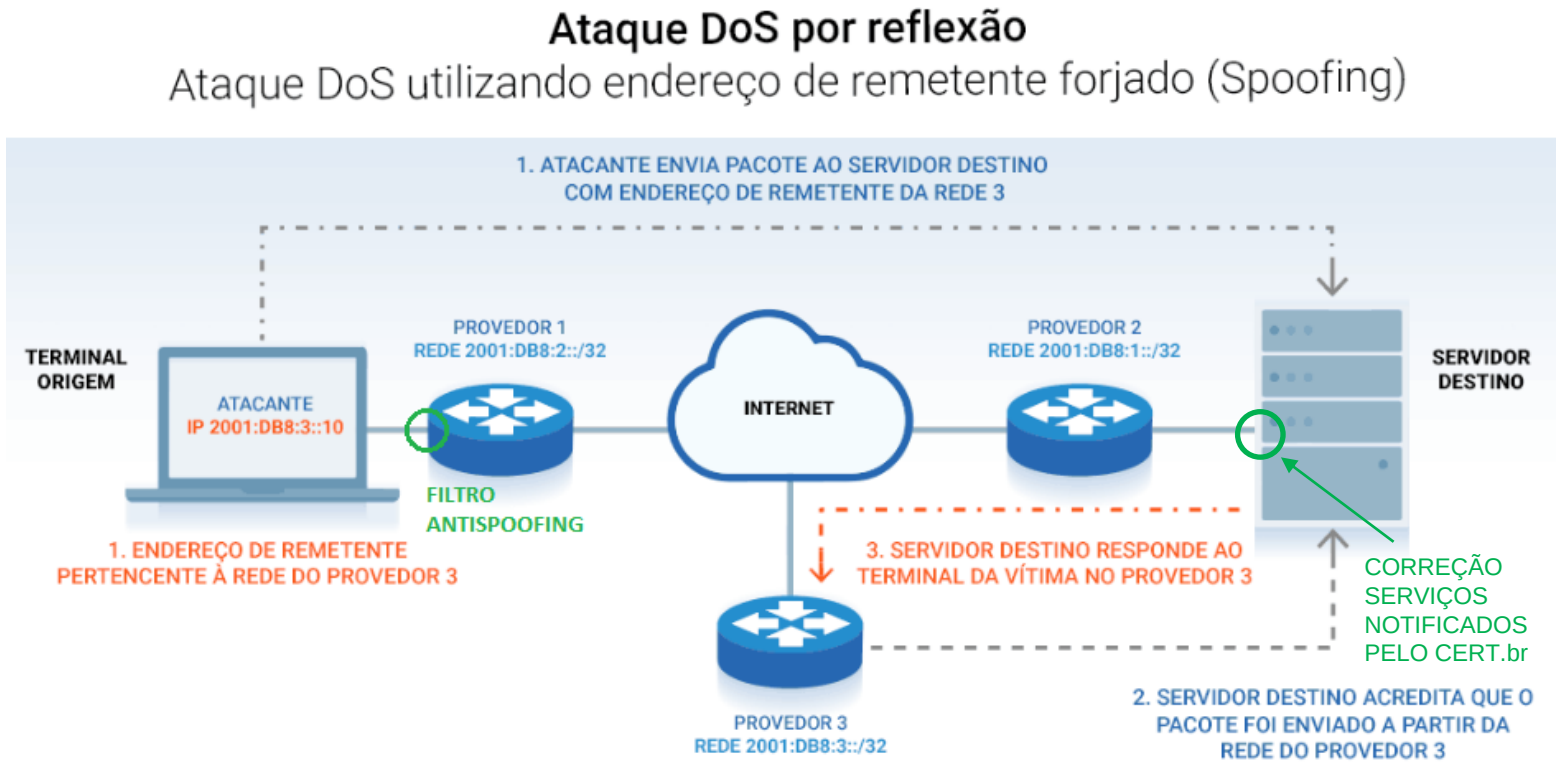
uRPF (Unicast Reverse Path Forwarding)

- 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



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

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

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:

nic.br | registro.br

Titular

Roteamento

Abuse

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

Endereços de *e-mail* indicados no PeeringDB:

PeeringDB

NOC

Abuse

Outros

https://www.peeringdb.com/

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:

Titular

Roteamento

Abuse

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

Endereços de *e-mail* indicados no PeeringDB:

NOC

Abuse

Outros

https://www.peeringdb.com/

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

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:

Titular

Roteamento

Abuse

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

Endereços de *e-mail* indicados no PeeringDB:

NOC

Abuse

Outros

https://www.peeringdb.com/

- 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)

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:

Titular

Roteamento

Abuse

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

Endereços de *e-mail* indicados no PeeringDB:

NOC

Abuse

Outros

https://www.peeringdb.com/

- 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:

nic.br | registro.br

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

Titular

Roteamento

Abuse

Endereços de *e-mail* indicados no PeeringDB:

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

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

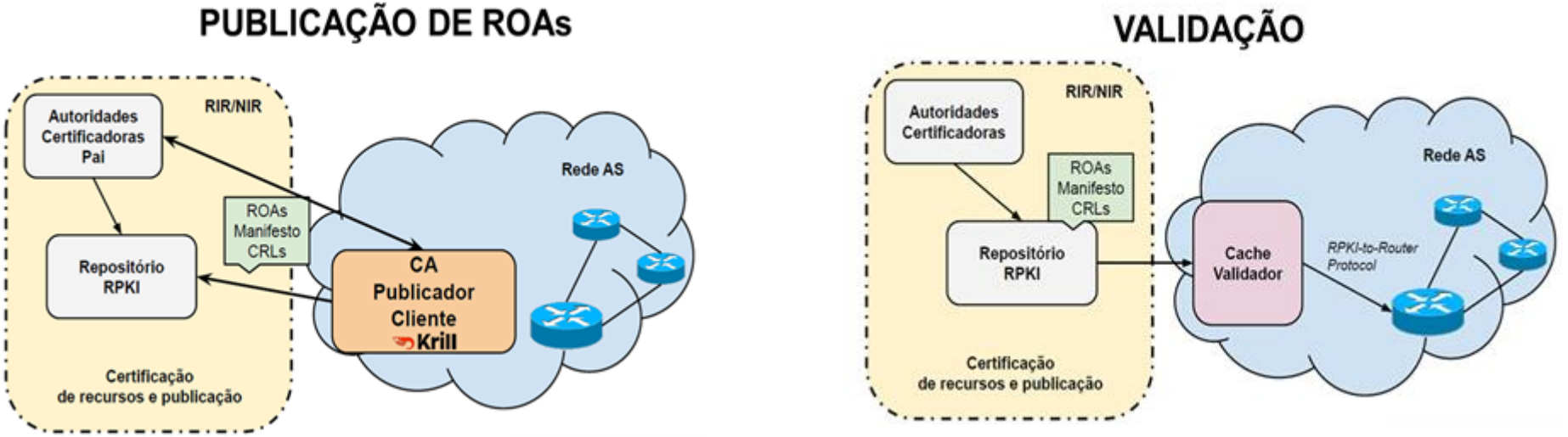
- Cadastro da política da política de Roteamento no IRR (RADB) ou no TC
- MANRS Observatory analisa a base de dados do RIPEStat (https://stat.ripe.net/ui2013/)

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/)

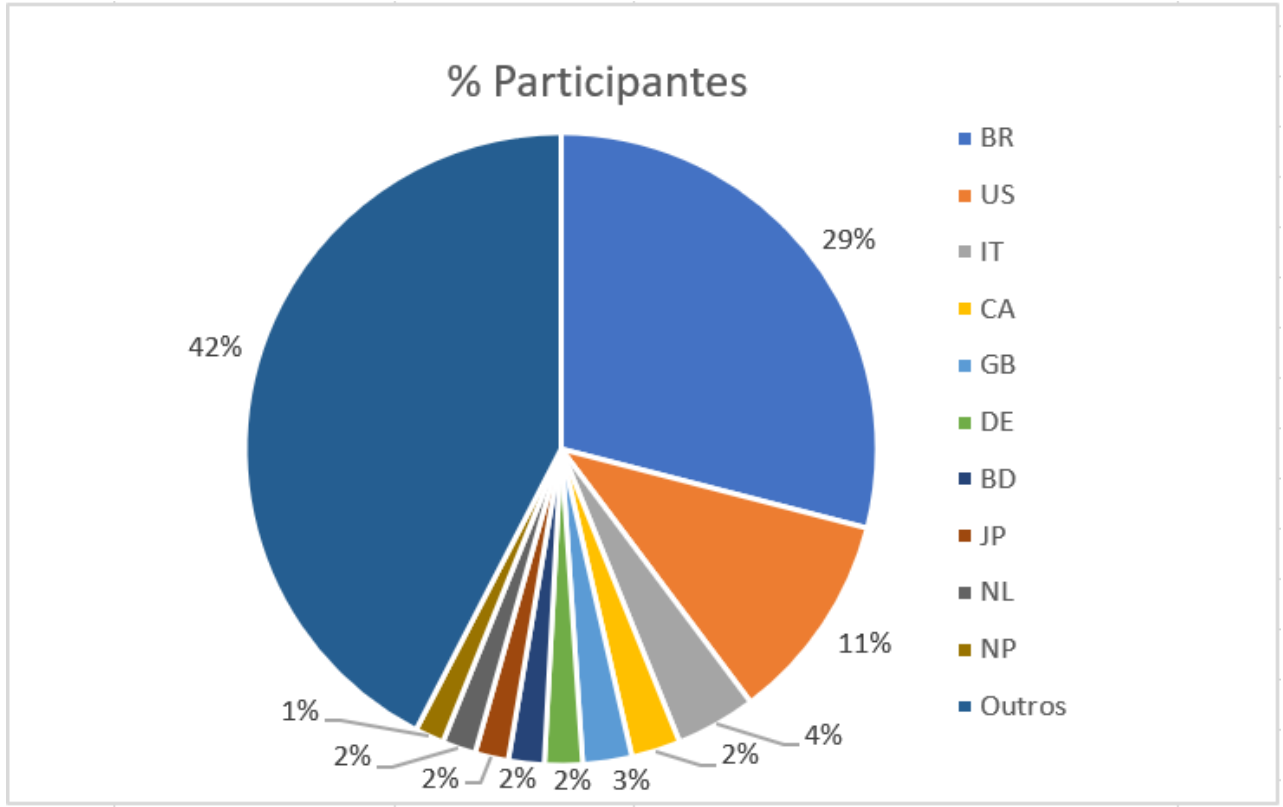
RPKI - Resource Public Key Infrastructure



- 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: 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 – 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

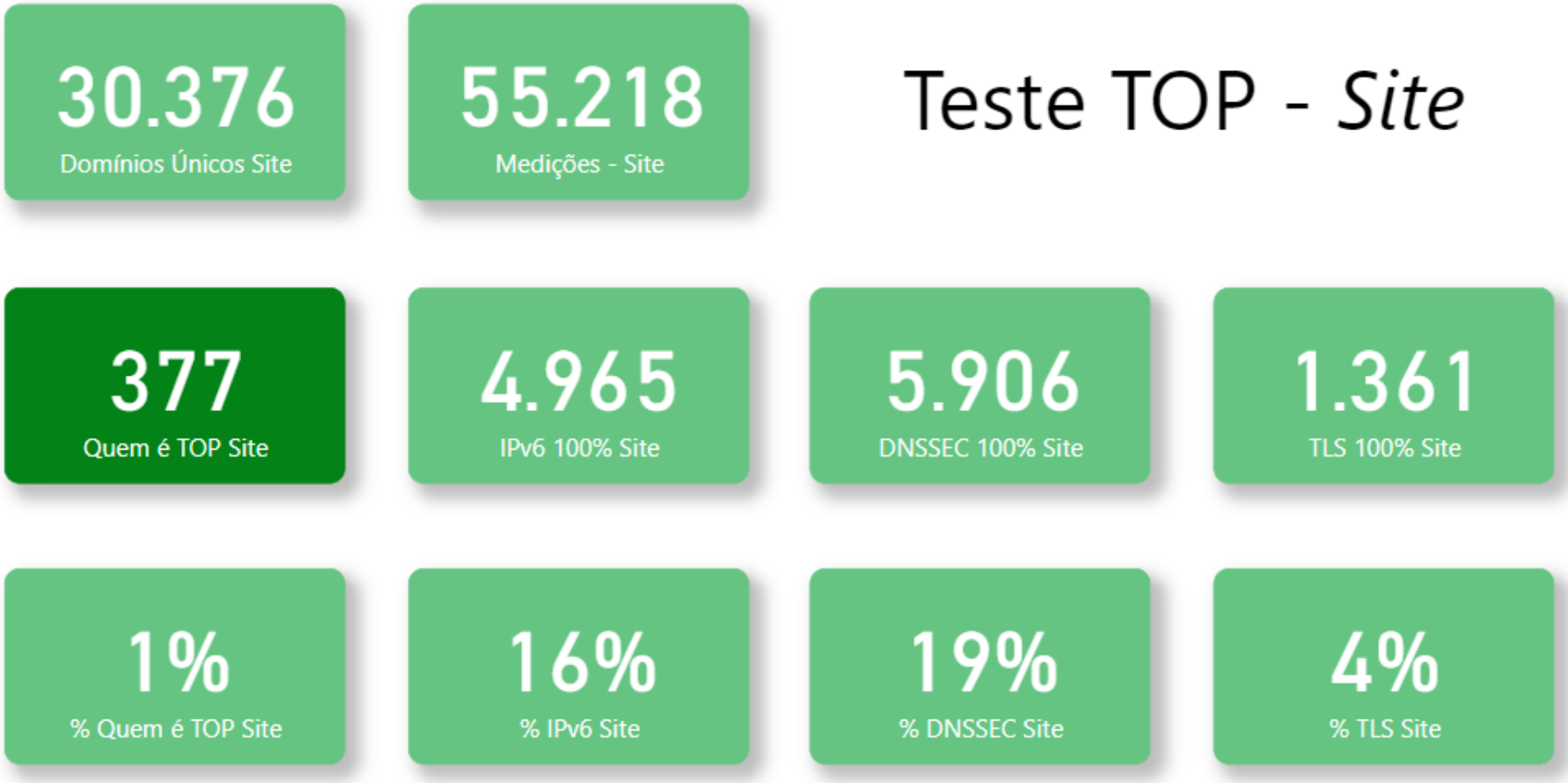
Teste TOP - IPv6 e DNSSEC da rede do usuário

Medições totais IPv6 100%

TESTE OS PADRÕES

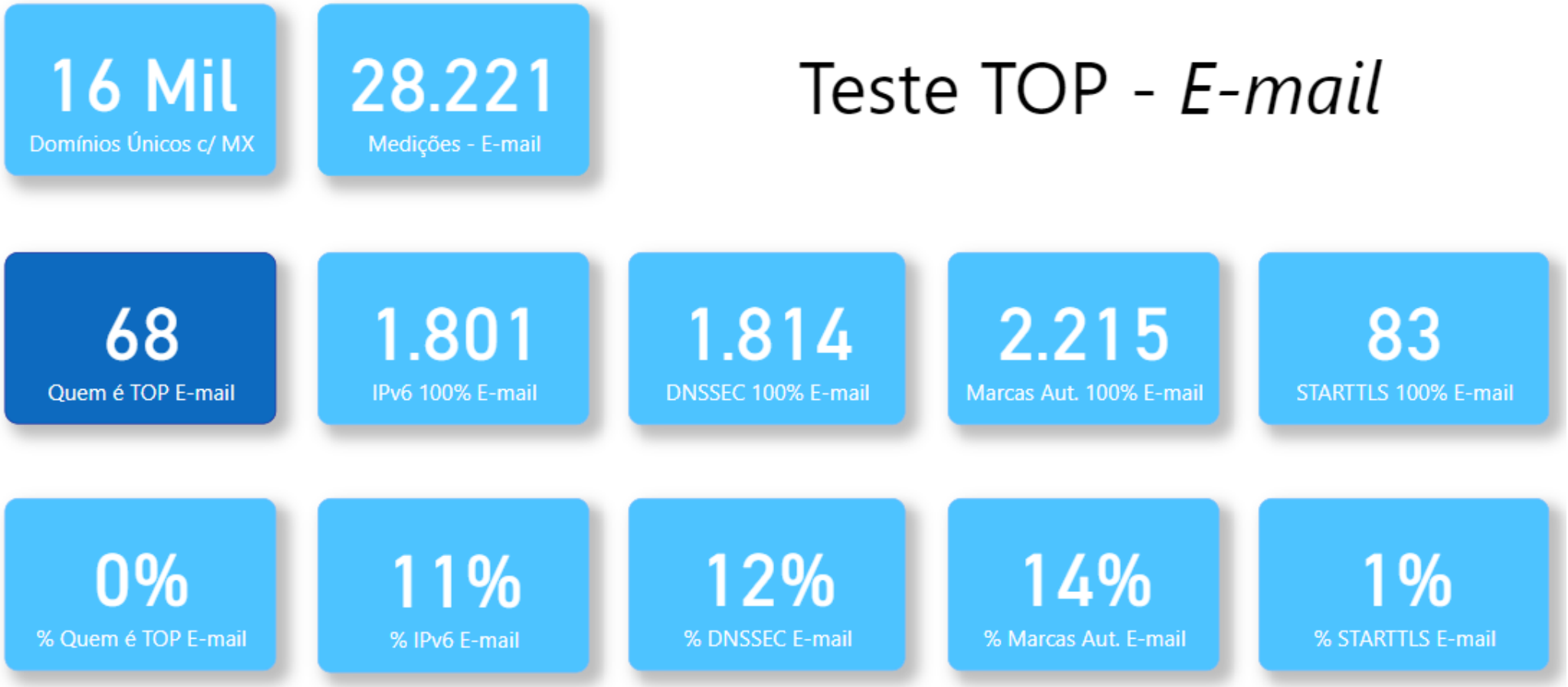
15/8/23

TOP – Teste os Padrões – Desenvolvimento



TESTE OS PADRÕES

TOP – Teste os Padrões – Desenvolvimento



TOP – Teste os Padrões - Apoio

TESTE OS PADRÕES

https://top.nic.br

conexis brasil.digital
A CONECTIVIDADE AO SEU ALCANCE

abranet
Associação Brasileira de Internet

AbraHosting
ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE INFRAESTRUTURA DE HOSPEDAGEM NA INTERNET

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

Dúvidas

?

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

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

gzorello@nic.br

Obrigado

gzorello@nic.br

18 de agosto de 2023

nic.br cgi.br

www.nic.br | www.cgi.br