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

nic.br cgi.br | registro.br

GTER 46 | GTS 32
São Paulo, SP | 14/12/18

ATULIZAÇÕES SOBRE O PROGRAMA POR UMA INTERNET MAIS SEGURA

Gilberto Zorello

gzorello@nic.br

registro.br nic.br cgi.br

Agenda

- Programa por uma Internet mais segura
- MANRS
- Desenvolvimento do Programa
- Outras ações importantes
- Ações no IX

Ações para resolver os problemas de segurança e estabilidade na infraestrutura da Internet

Programa por uma Internet mais Segura
Iniciativa

Lançado pelo CGI.br e NIC.br

Painel do IX Fórum 11 em dez/17 [1]

Apoio: Internet Society, ABRANET, SindiTelebrasil, ABRINT

Objetivo - atuar em apoio à comunidade técnica da Internet para:

- **Redução de ataques de Negação de Serviço originados nas redes brasileiras**
- Reduzir **Sequestro de Prefixos**, **Vazamento de Rotas** e **Falsificação de IP de Origem**
- **Redução das vulnerabilidades e falhas de configuração presentes nos elementos da rede**
- Aproximar as diferentes equipes responsáveis pela segurança e estabilidade da rede
- **Criar uma cultura de segurança**

Programa por uma Internet mais Segura
Plano de Ação

Para solucionar os problemas de segurança, as ações devem ser realizadas pelos operadores dos Sistemas Autônomos, com apoio no NIC.br

Ações coordenadas a serem executadas pelo NIC.br:

- Conscientização por meio de palestras, cursos e treinamentos
- **Criação de materiais didáticos e boas práticas**
- Interação com **Associações de Provedores** e seus afiliados para disseminação da **Cultura de Segurança**, adoção de **Melhores Práticas** e **mitigação** de problemas existentes:
  - **especificação, configuração e operação de CPEs em suas respectivas redes**
  - implantação das ações básicas para melhorar a Segurança de Roteamento, preconizadas pelo **MANRS** [2]
- **Implementação de filtros de rotas no IX.br, que contribui para a melhora do cenário geral**
- Estabelecimento de métricas e acompanhamento da efetividade das ações

MANRS

Mutually Agreed Norms for Routing Security

Apoiado pela Internet Society

Segurança e estabilidade da Internet
Problemas de segurança

- Todos tentam proteger sua própria rede. Olham apenas o que está entrando!
  - **Isso é caro! Requer equipamentos e configurações complexas! Não tem resolvido!**
- Poucos olham o que sai da sua rede!
  - **Isso é simples. Fácil. Barato.**

Programa por uma Internet mais Segura
MANRS

O MANRS endereça as principais ameaças de segurança por meio de ações técnicas e colaborativas por todos os operadores da Internet

Para aumentar a robustez do sistema de roteamento da rede é necessário que:

- Operadores de rede e os IX adotem as ações do MANRS
- **As empresas contratantes demandem que estas ações sejam aplicadas pelos seus provedores de serviços**

MANRS

Sequestro de Prefixos

Vazamento de Rotas

Falsificação de IP de Origem

MANRS

Mutually Agreed Norms for Routing Security

Saiba mais em:

http://manrs.org

http://bcp.nic.br

Programa por uma Internet mais Segura
Como Resolver os problemas

Todos devem implementar estas recomendações [9]:

1. **Garantir que seus anúncios BGP sejam de seus próprios blocos IP e de seus clientes, pela definição de políticas de roteamento e filtros, e assegurar que estas políticas sejam seguidas**
   - Dificulta sequestro de blocos IP e redirecionamento de tráfego
2. **Garantir que os IP de origem que saem da rede não sejam falsificados: antispoofing [3] [6]**
   - Impede que os computadores infectados de seus usuários iniciem ataques de amplificação
3. **Garantir que seus contatos estejam atualizados e acessíveis por terceiros de maneira global: Whois do Registro.br, PeeringDB e Site da Empresa**
   - Permite que equipes de segurança de outras redes te avisem sobre problemas que detectam na sua rede
4. **Publicar suas políticas de roteamento em bases de dados externas: IRR (RADb, TC, NTTCOM) e RPKI**
   - Facilita a validação de roteamento em escala global

Programa por uma Internet mais Segura
Benefícios

Os Provedores se beneficiam com a implantação do MANRS:

- Adiciona um **valor competitivo** em um mercado onde todos oferecem serviços semelhantes e direcionado ao **preço**
- **Mostra aos seus clientes competência e comprometimento na área de segurança**
- Ajuda a resolver problemas de rede
- **Empresas indicam que pagariam mais por serviços efetivamente seguros (Pesquisa 451 Research)**
- **Incentivamos os ISPs a participarem do programa MANRS**

Status do Desenvolvimento do Programa

Programa por uma Internet mais Segura
Desenvolvimento do Programa - Cursos

- **Curso de Boas Práticas Operacionais p/ Sistemas Autônomos – BCOP**
  - Funcionamento da Internet, papel dos ASs, uso do endereçamento IP, boas práticas de roteamento e **segurança**, engenharia de tráfego, **hardening de equipamentos** e **prática em laboratório**
  - Este curso foi reestruturado de acordo com as premissas do Programa e do MANRS
  - Oferecido na semana do IX Fórum: dez cidades ao ano em todo o Brasil
  - Cursos já oferecidos: São Paulo, Teresina, Belo Horizonte, Goiânia, Aracaju, Salvador, Florianópolis, Porto Alegre: **251** alunos certificados
- **Tutorial LACNIC 30 – Rosário / Argentina - 9/18**
- Tutorial GTER 45 Florianópolis - 5/18
- **Tutorial ABRINT na Estrada – Rio de Janeiro – 12/18**

Programa por uma Internet mais Segura
Desenvolvimento do Programa - Palestras

- **Palestras sobre o Programa e MANRS:**
  - GTER 45 Florianópolis – 5/18
  - **ABRINT 2018 - 5/18**
  - Encontro Nacional ABRINT 2018 - 6/18
  - **Congresso da Sociedade Brasileira de Computação - 7/18**
  - Congresso RTI - Ribeirão Preto - 8/18
  - **Eventos Regionais REDETELESUL 2018 – Londrina – 8/18**
  - ABRINT na Estrada – Cascavel – 9/18
  - **Futurecom 2018 – 10/18**
  - Evento com Associações de ISP – 10/18
  - **33rd Euro-IX Forum – 11/18**
  - VIII Fórum da Internet Brasil – 11/18
  - **Eventos Regionais REDETELESUL 2018 – Curitiba – 11/18**
  - ABRINT na Estrada – Rio de Janeiro – 6/12

Programa por uma Internet mais Segura
Desenvolvimento do Programa - Operadoras

Ações diretas do Programa por uma Internet mais Segura:

- **Reuniões técnicas com grandes operadoras (VIVO, CLARO, OI, TIM, ALGAR, SERCOMTEL):**
  - **Alinhamento com as Ações do MANRS**
    - Pontos de contato de abuse e roteamento
    - **Antispoofing**
    - Filtro de anúncios de entrada e saída
    - **Cadastro de políticas de Roteamento em bases externa**
  - **Fechamento de endereços IPs abertos para a Internet e abusáveis:**
    - **Em mar/18 – 725k IPs abertos // Hoje – 340k IPs abertos (- 53%)**
    - **Hoje: 206k grandes operadoras // 134k ISP e AS corporativos**
- **Melhora nos processos para atender às notificações do CERT.br e reduzir os Ips abertos e abusáveis…**

Panorama Atual
Endereços IP e ASN notificados pelo CERT.br

	DNS		SNMP		NTP		SSDP	
month	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
2018-01	2.412	61.875	2.130	479.247	823	97.075	888	25.982
2018-02	2.438	72.185	2.324	559.784	849	93.801	778	20.210
2018-03	2.476	63.811	2.278	515.345	844	84.483	544	11.431
2018-04	2.509	66.371	2.280	436.702	850	85.549	794	21.686
2018-05	2.343	65.270	2.390	502.861	870	88.788	846	23.174
2018-06	2.629	70.188	2.284	447.411	805	87.408	817	23.340
2018-07	2.721	68.415	2.436	431.907	881	89.484	787	17.255
2018-08	2.459	56.555	2.411	397.622	895	89.353	613	11.855
2018-09	2.767	62.942	2.366	193.432	772	87.378	836	21.836
2018-10	2.806	64.912	2.383	163.987	856	85.911	789	20.233
2018-11	2.604	60.937	2.376	137.331	851	87.155	814	20.124

O Brasil está em **terceiro** lugar entre os endereços IPs abertos para abuso utilizando o protocolo SNMP

Fonte: https://snmpscan.shadowserver.org/

Programa por uma Internet mais Segura
Desenvolvimento do Programa – ISPs e Indústria

Ações diretas do Programa por uma Internet mais Segura:

- **Ação com as maiores Associações de Provedores de Internet**
  - ABRANET, ABRINT, Telcomp, InternetSul, RedeTeleSul, AbraHosting, Abramulti
  - Ações de disseminação da **Cultura de Segurança,** adoção de **Melhores Práticas** e **mitigação** de problemas existentes
  - Desenvolvimento de site do Programa
  - Primeira reunião em 10/18.
- **Ação com a indústria**
  - Incorporação do SIMET com medições de qualidade e BCP 38 em produtos CPEs da indústria nacional e multinacional
  - Aderência dos produtos à recomendação de **Requisitos Mínimos para Aquisição de CPEs** – draft 4 em revisão final

Outras ações importantes divulgadas pelo Programa

Programa por uma Internet mais Segura
Recomendações Adicionais

Receber e tratar notificações que são enviadas [5]:

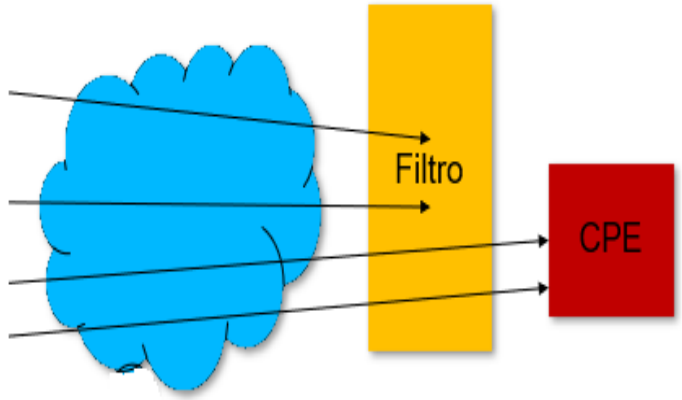
- Além de manter os e-mails de contato de **Abuso** e **Roteamento** do ASN no Whois atualizados
- Ajustar os procedimentos internos para tratamento das notificações de abuso e segurança e notificações de roteamento pelas respectivas equipes responsáveis
- **Ação 3 do MANRS.**

Reduzir ataques DDoS saindo de sua rede [4]:

- Análise proativa do tráfego que sai da rede utilizando netflows
- Configurar os CPEs para não ter serviços abertos que permitam amplificação e ter política de senhas seguras (hardening)

Programa por uma Internet mais Segura
Recomendações Adicionais

Filtrar tráfego de entrada tráfego de entrada ou bloquear comandos com destino a serviços que permitam amplificação:



- DNS (53/UDP), SNMP (161/UDP), NTP (123/UDP), SSDP (1900/UDP)

- **Para gerência de rede, permitir apenas blocos de redes de gerência da própria operadora**

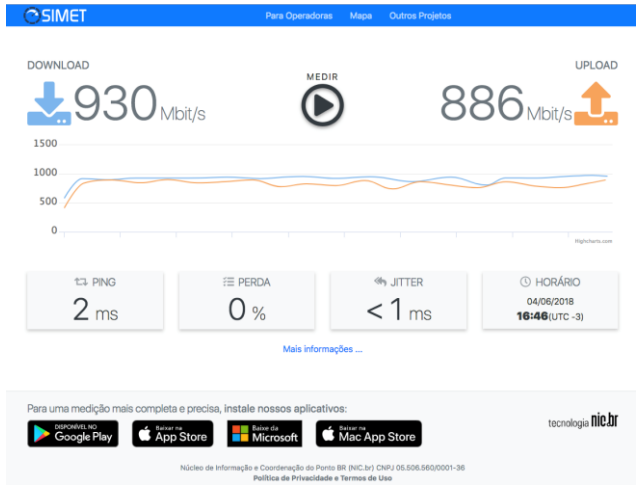
- Seguir as ações recomendadas pelo CERT.br nas notificações de ASNs e IPs com serviços abertos, passíveis de serem abusados para gerar ataques de amplificação

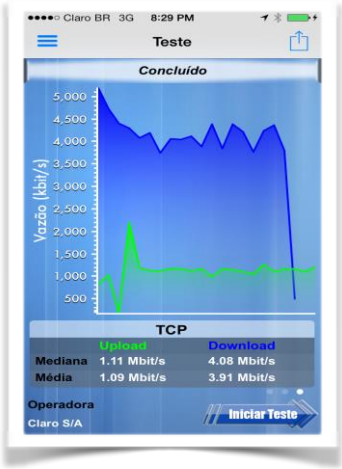
- **Cuidado com o NTP porque muitos clientes usam a porta 123 UDP também como porta de origem, recebendo respostas nessa porta**

Programa por uma Internet mais Segura

SIMET - Sistema de Medição de Qualidade da Internet

- **SIMET WEB**
  - Widget para ISP
  - Lista de Provedores
- **SIMET Mobile**
  - Android, IOS
- **SIMETBox**
  - Testes de Qualidade
  - Testes Porta 25
  - Teste BCP 38
    - Mesmo IP
    - Mesma rede
    - Outra rede
    - Endereço privado

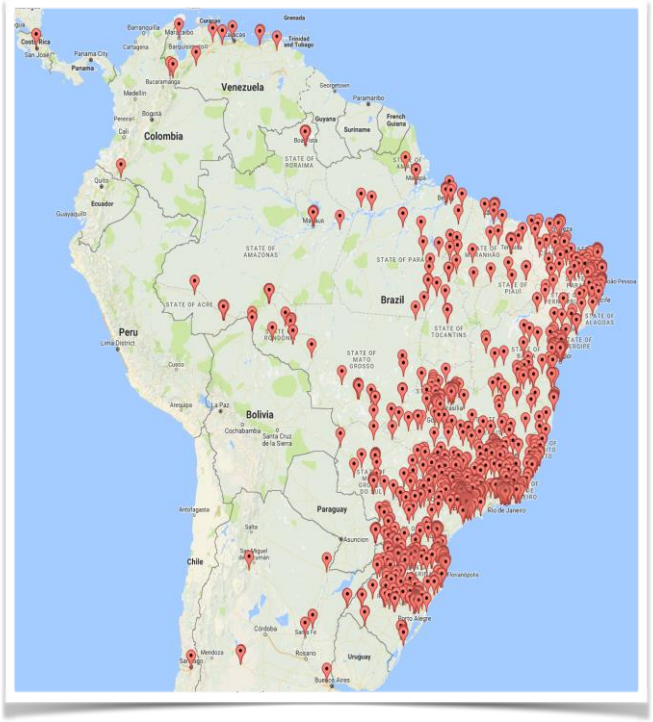




- **Medições com IPv4 e IPv6**
- **Testes realizados do usuário até um dos PTTs do IX.br, fora da rede medida**

Programa por uma Internet mais Segura

SIMET - Sistema de Medição de Qualidade da Internet



ISP pode adquirir roteadores para atender seus usuários (SOHO) com as seguintes características:

- Compatível com OpenWRT, destravado
- **64 MiB RAM e 8 MiB FLASH**
- Padrão de rede wi-fi IEEE 802.11 b/g/n para geolocalização

Exemplos:

- TP-Link Archer C60v2
- TP-Link Archer C7v4
- Mikrotik RBwAPG-5HacT2HnD (wAP AC)
- D-Link dwr-921 c3

Receba os dados das medições de todos os SIMET Box de sua rede

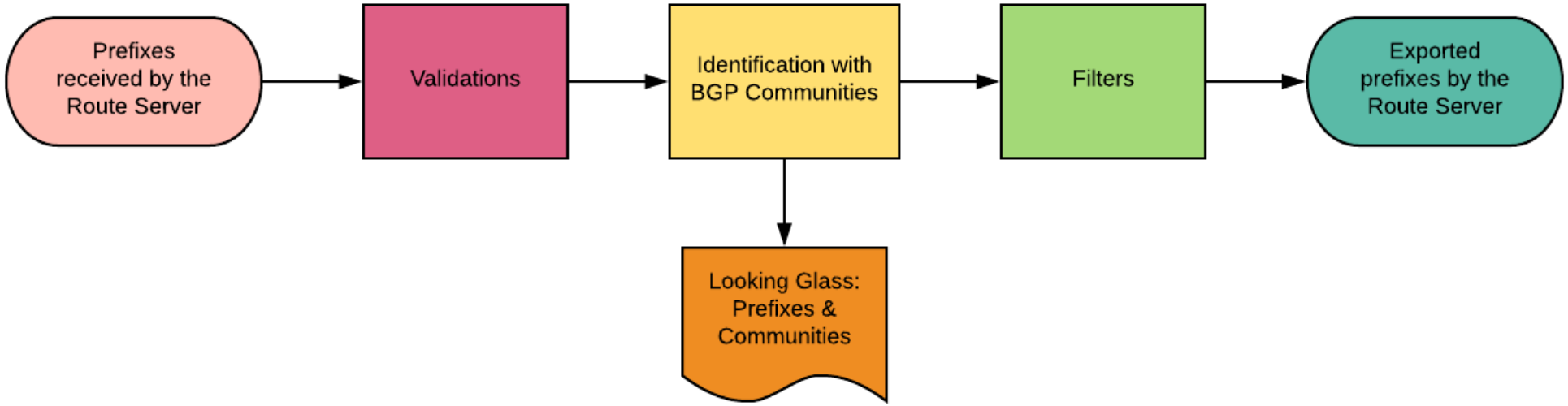
Ações no IX

Iniciativa Internet Segura no IX.br

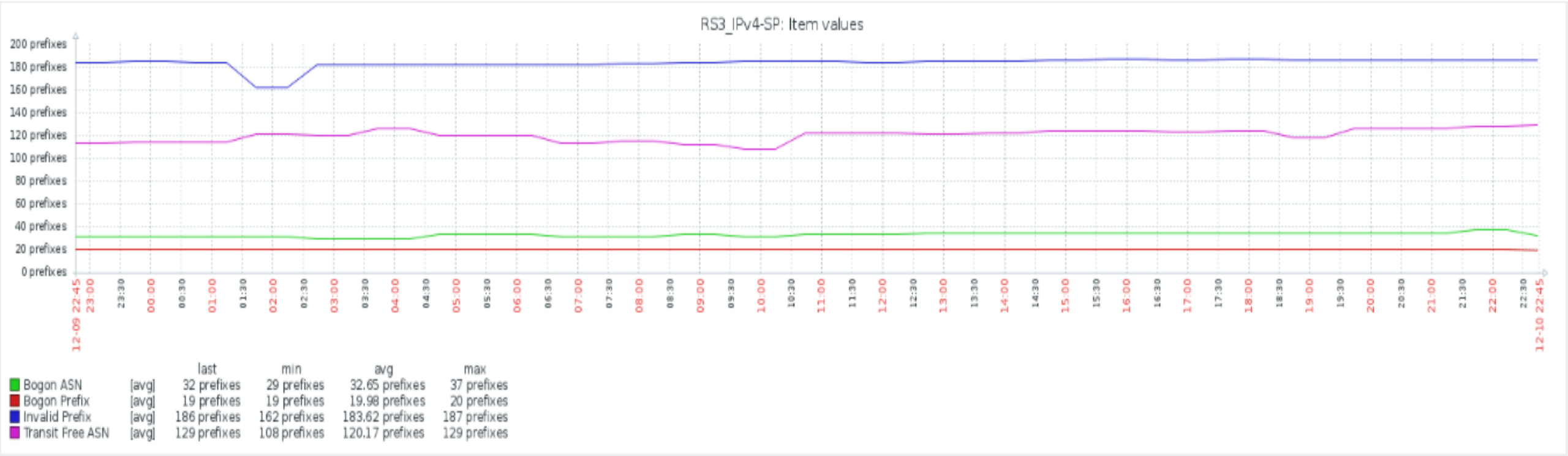
- Proteger os Servidores de Rotas (Route Servers)
- Publicamos um documento com o objetivo de obter feedback da comunidade técnica. Duas rodadas de consultas antes de liberar a versão final (4 meses).
- Objetivos:
  - Validações básicas: Comprimento de prefixo, prefixos bogon, prefixos IX.br, ASNs bogon, ASNs com trânsito livre (Tier-1)
  - Validação de origem:
    - ✓ RDAP / Whois ou equivalente
    - ✓ IRRs
    - ✓ RPKI
  - Validação da política de roteamento:
    - ✓ ASNs brasileiros STUB (ligados diretamento ao IX.br)
    - ✓ Validação do AS-SET
  - Buraco Negro (Black Hole) para os ASNs STUBs brasileiros

Iniciativa Internet Segura no IX.br

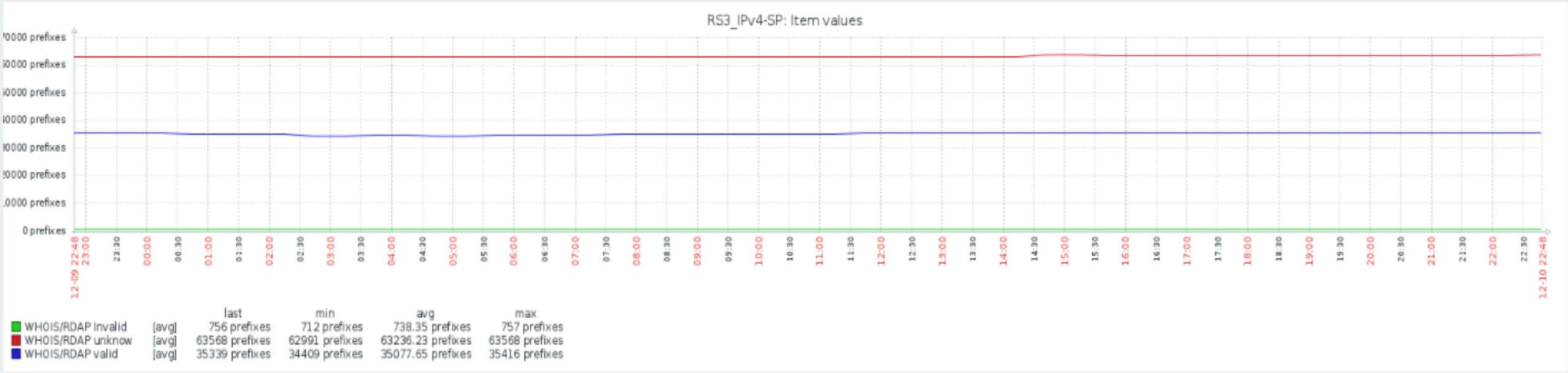
- Atividades foram classificadas de acordo com o tempo para implementação:
  - ✓ EM USO
  - ✓ CURTO (45 dias)
  - ✓ MÉDIO (120 dias)
  - ✓ LONGO (12 a 18 meses)
- São utilizadas Communities BGP para registrar o resultado das validações

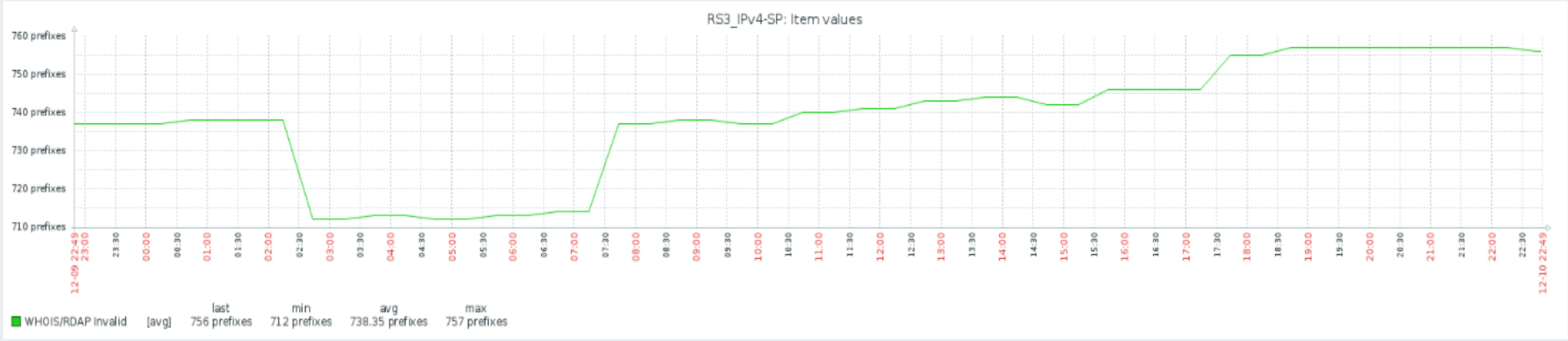


IX.br – Validação de Prefixos

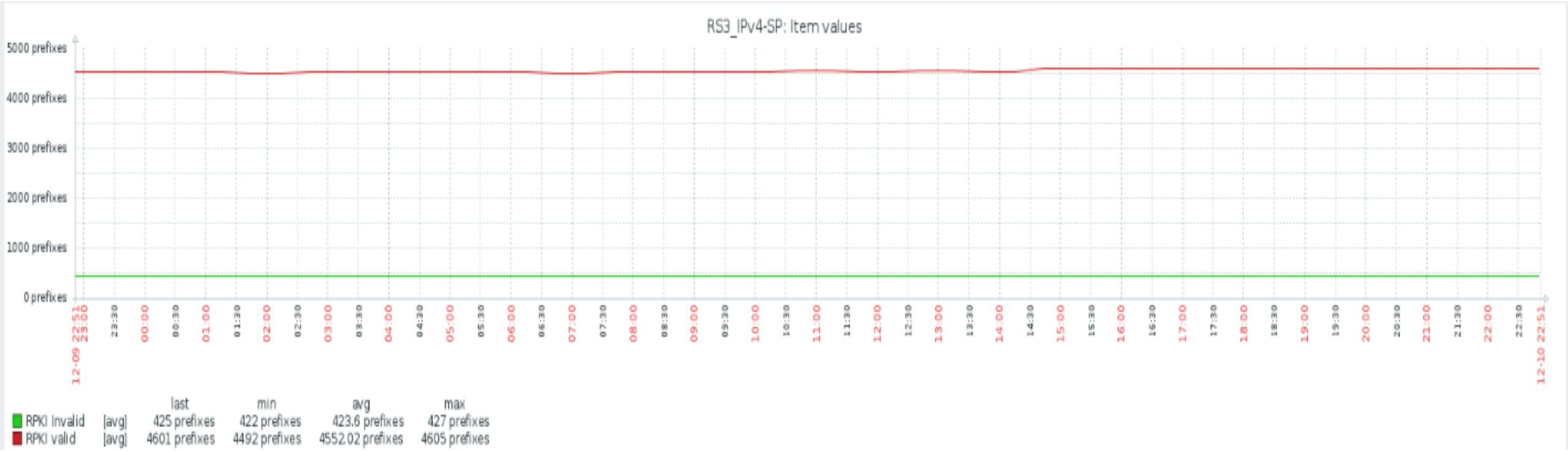


IX.br – Whois / RDAP ou equivalente





IX.br – RPKI


RS3_IPv4-SP: Item values
5000 prefixes
4000 prefixes
3000 prefixes
2000 prefixes
1000 prefixes
0 prefixes
12-09 22:51
23:00
23:30
00:00
00:30
01:00
01:30
02:00
02:30
03:00
03:30
04:00
04:30
05:00
05:30
06:00
06:30
07:00
07:30
08:00
08:30
09:00
09:30
10:00
10:30
11:00
11:30
12:00
12:30
13:00
13:30
14:00
14:30
15:00
15:30
16:00
16:30
17:00
17:30
18:00
18:30
19:00
19:30
20:00
20:30
21:00
21:30
22:00
22:30
12-10 22:51
last
min
avg
max
RPKI Invalid [avg] 425 prefixes 422 prefixes 423.6 prefixes 427 prefixes
RPKI valid [avg] 4601 prefixes 4492 prefixes 4552.02 prefixes 4605 prefixes

LG Web

Sao Paulo/SP | 152.84.66.0/24 | Pesquisar

Prefix	AS Path	Communities	Neighbor IP Address	Next Hop	Metric	Last Modified
152.84.66.0/24	1916 2715	26162:1916 26162:65011 26162:65110 26162:65181 65000:1251 65000:52888 65000:262742	187.16.216.253	187.16.220.208	20	10/12/2018 20:05
152.84.66.0/24	1916 2715	26162:1916 26162:65011 26162:65110 26162:65181 65000:1251 65000:52888 65000:262742	187.16.223.253	187.16.220.208	20	10/12/2018 20:06
152.84.66.0/24	1916 2715	26162:1916 26162:65011 26162:65110 26162:65181 65000:1251 65000:52888 65000:262742	187.16.216.254	187.16.220.208	20	10/12/2018 20:06
152.84.66.0/24	1916 2715	26162:1916 26162:65011 26162:65110 26162:65181 65000:1251 65000:52888 65000:262742	187.16.223.254	187.16.220.208	20	10/12/2018 22:40

Próximos passos

- Análise e adequação para o uso da base publicada pelo registro.br no ftp público
- Publicação da nova versão do documento com a descrição das Communities BGP (português + inglês)
- Envio de notificação para os ASNs com resultado INVÁLIDO na validação de origem via base do registro.br ou RPKI
- Ativação dos filtros
- Nova versão do Looking Glass Web

Programa por uma Internet mais Segura
Referências

[1] https://youtu.be/TIVrx3QoNU4?t=7586 - Painel sobre Programa para uma Internet mais Segura, IX (PTT) Fórum 11, dia 1, parte 1, São Paulo, SP

[2] https://www.manrs.org/manrs/ - MANRS for Network Operators

[3] https://bcp.nic.br/antispoofing - Boas Práticas de Antispoofing

[4] https://bcp.nic.br/ddos - Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)

[5] https://bcp.nic.br/notificacoes - Recomendações para Notificações de Incidentes de Segurança

[6] https://www.caida.org/projects/spoofer/ - Tool to access and report source address validation

[7] Ataques Mais Significativos e Como Melhorar o Cenário, IX Fórum Regional, 10/2017

https://www.cert.br/docs/palestras/certbr-ix-forum-sp-2017-10-20.pdf

https://youtu.be/R55-cTBTLcU?t=2h36m25s

[8] Problemas de Segurança e Incidentes com CPEs e Outros Dispositivos, 20º Fórum de Certificação para Produtos de Telecomunicações, Anatel, 11/2016, Campinas, SP

https://www.cert.br/docs/palestras/certbr-forum-anatel2016.pdf

[9] http://www.nic.br/videos/ver/como-resolver-os-problemas-de-seguranca-da-internet-e-do-seu-provedor-ou-sistema-autonomo/

Obrigado

www.site.br

gzorello@nic.br

14 de dezembro de 2018

nic.br cgi.br

www.nic.br | www.cgi.br