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

Curso BCOP

São José do Rio Preto, SP | 6/2/20

PROGRAMA POR UMA INTERNET MAIS SEGURA

CUIDADO COM O QUE SAI DA REDE
SUA INFRAESTRUTURA NÃO DEVE SER UTILIZADA EM ATAQUES

Gilberto Zorello | gzorello@nic.br

registro.br nic.br cgi.br

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, Abrint, Abranet, SindiTelebrasil

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 do 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 [11]**
- Interação com **Associações de Provedores** e seus afiliados para disseminação da **Cultura de Segurança**, adoção de **Melhores Práticas** e **mitigação** de problemas existentes
- **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

Programa por uma Internet mais Segura
Interação com Associações

Atividades com Operadoras e Provedores com apoio das Associações

- Reuniões bilaterais com as Operadoras e ISPs
  - Correção de pontos de contato para notificação (Ação 3 MANRS) [3]
  - Acompanhamento da correção de serviços mal configurados que podem ser abusados para fazer parte de ataques DDoS (recomendação do CERT.br) [5]
  - Adoção de Boas Práticas de roteamento (MANRS) [3]
    - Medidas contra tráfego “spoofado” (Ação 2)
    - Implementação de filtros de anúncios BGP (Ação 1)
    - Publicação das políticas de roteamento em base de dados externa (IRR – Internet Routing Registry) (Ação 4)
  - Hardening de equipamentos e redes

Programa por uma Internet mais Segura
Interação com Associações

Atividades com Operadoras e Provedores com apoio das Associações

- Reuniões bilaterais com as Operadoras e ISPs
  - Correção de pontos de contato para notificação (Ação 3 MANRS) [3]
  - Acompanhamento da correção de serviços mal configurados que podem ser abusados para fazer parte de ataques DDoS (recomendação do CERT.br) [5]

Nome da Empresa	ASN	DNS	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DICOVERY	TFTP	2019-10	2019-11	2019-12	2020-01	MT4145
																			#	
Empresa 1	ASN 1	17	4	1	10	2	0	2	0	0	0	0	0	0	0	512	49	37	36	0
Empresa 2	ASN 2	0	5	9	0	0	0	1	0	0	0	0	1	0	0	16	11	12	16	0
Empresa 3	ASN 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3	0	0
																529	60	52	52	

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Interação com as operadoras e provedores: redução de endereços IP mal configurados que permitem amplificação
  - Em mai/18: 575k grandes operadoras // 148k ISP e ASN corporativos (80/20)
  - **Hoje: 103k grandes operadoras // 168k ISP e ASN corporativos (novos protocolos analisados – UBNT, WS-DISCOVERY, TFTP (38/62)**
  - Redução total dos IPs notificados de 62% desde o início do Programa
    - **Segmentação dos IPs notificados: 61% ISPs, 1% corporativos, 38% operadoras**

Programa por uma Internet mais Segura
Endereços IP e ASNs notificados pelo CERT.br

Brasil	DNS		SNMP		NTP		SSDP		UBNT	
mês	ASNs	IP	ASNs	IP	ASNs	IP	ASNs	IP	ASNs	IP
2019-02	2.905	69.093	2.556	136.401	944	80.838	868	20.689	2.690	180.756
2019-03	2.933	63.895	2.661	111.561	914	72.873	847	18.837	2.042	95.974
2019-04	2.898	59.865	2.662	123.241	997	79.698	886	18.919	1.909	76.666
2019-05	3.045	68.764	2.633	103.204	1.019	77.979	953	18.564	1.797	64.729
2019-06	2.960	69.473	2.744	107.090	961	82.372	928	19.048	1.679	55.732
2019-07	3.012	78.879	2.777	103.289	990	77.374	827	19.597	1.640	50.811
2019-08	3.068	76.143	2.808	90.960	998	78.058	795	14.071	1.625	52.598
2019-09	3.072	67.420	2.833	89.740	1.025	78.037	745	11.746	1.478	39.561
2019-10	3.113	65.922	2.861	81.781	991	72.720	695	8.811	1.442	33.160
2019-11	3.040	61.723	2.824	78.277	985	70.950	659	7.787	1.320	24.565
2019-12	2.962	58.453	2.900	77.952	1.003	72.235	736	10.791	1.374	25.964
2020-01	3.144	69.680	2.881	72.806	1.013	72.862	705	9.386	1.251	19.407

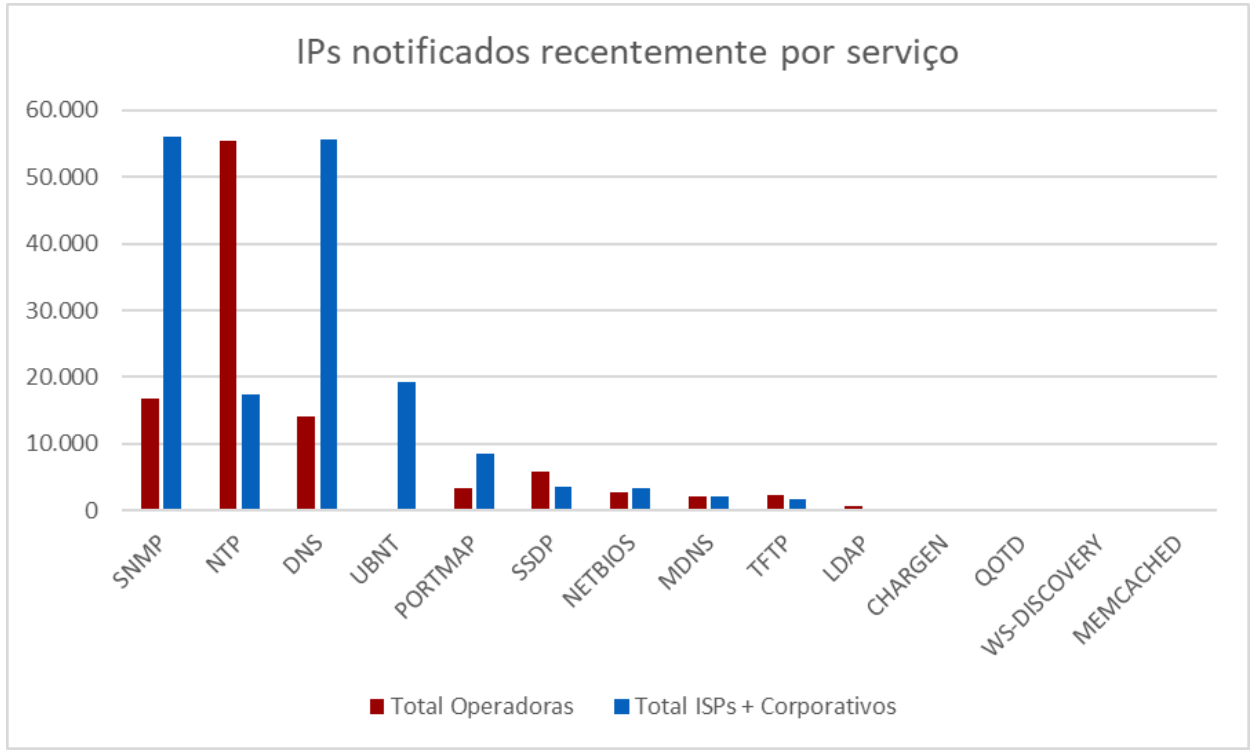
O Brasil está em **quinto** lugar entre os endereços IPs com serviços SNMP mal configurados

- "-" significa que não houve notificação para o protocolo no mês.

Fonte: https://snmpscan.shadowserver.org/ [12]

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Endereços IP notificados recentemente por serviço mal configurado

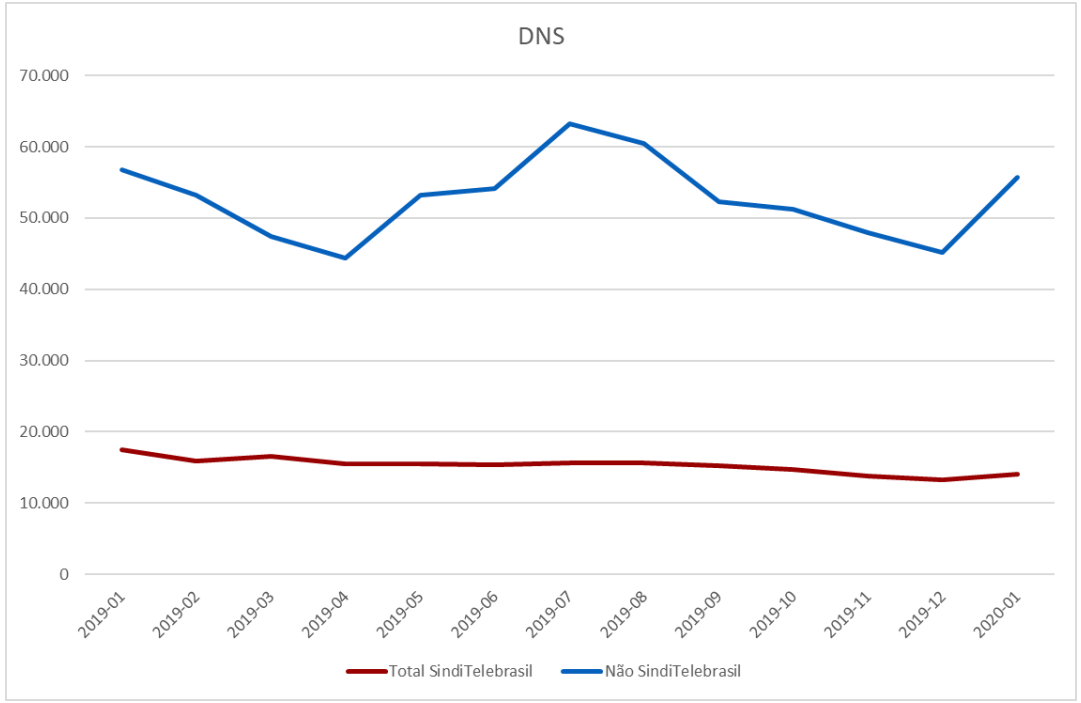


Principais ofensores: **ISPs e ASes corporativos → SNMP, DNS, UBNT e NTP**

Grandes operadoras → NTP, SNMP e DNS

Programa por uma Internet mais Segura
Desenvolvimento do Programa

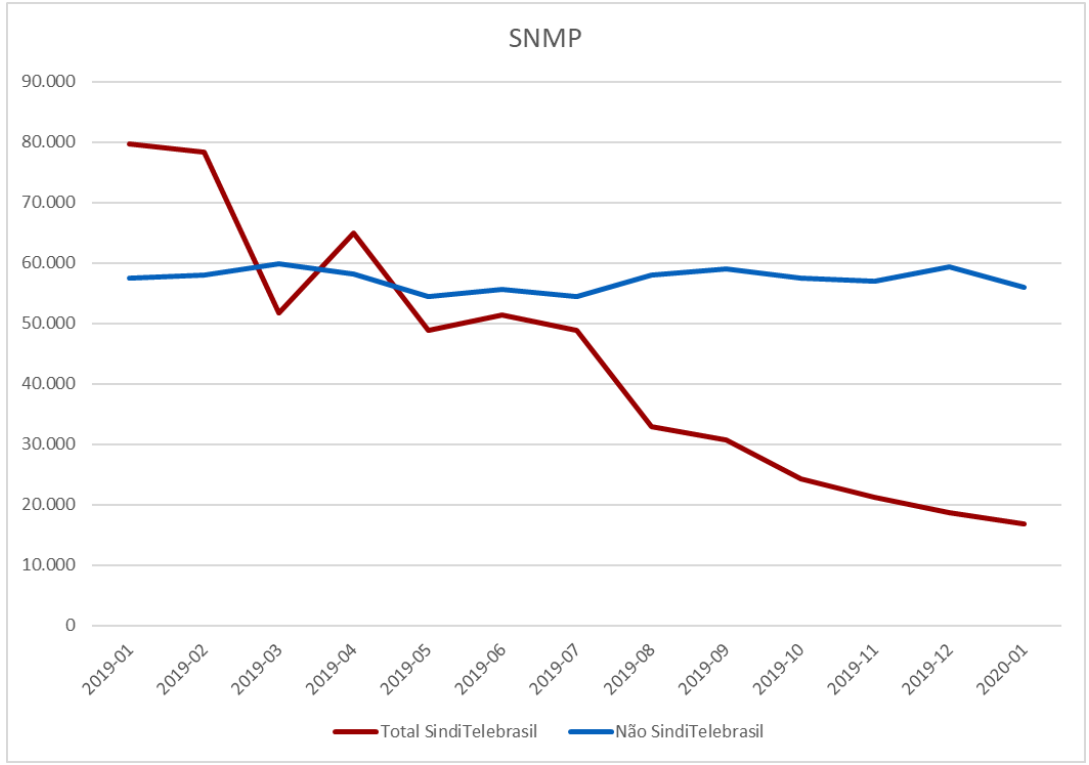
- Ações com as Operadoras, Provedores e AS Corporativos - **DNS**



Os serviços DNS recursivos abertos em redes de ISPs e ASes Corporativos são os mais notificados

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Ações com as Operadoras, Provedores e AS Corporativos - **SNMP**



Hoje são notificados mais serviços SNMP habilitados de ISPs e Ases Corporativos

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

Programa por uma Internet mais Segura
Página WEB

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

Minimum security requirements for CPEs acquisition

O LACNOG BCOP WG e LAC-AAWG, em parceria com M³AAWG e LACNIC, e coordenação NIC.br, desenvolveram um documento que tem como objetivo identificar um conjunto mínimo de requisitos de segurança que devem ser especificados no processo de compra de CPEs pelos ISPs

Visa a aquisição de equipamentos que permitam gerenciamento remoto e que sejam nativamente mais seguros, permitindo:

- Redução dos riscos de comprometimento da rede do provedor e da Internet como um todo
- Redução dos custos e perdas resultantes do abuso dos equipamentos por invasores: degradação ou indisponibilidade de serviços, suporte técnico e retrabalho

O documento foi lançado no LACNIC 31 (maio/19) e está disponível em https://www.m3aawg.org/sites/default/files/lac-bcop-1-m3aawg-v1-portuguese-final.pdf - Documento conjunto LACNOG-M3AAWG: Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinante (CPE) LAC-BCOP-1

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, São Paulo, SP

[2] https://bcp.nic.br/i+seg/ - Programa por uma Internet mais segura

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

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

[5] https://bcp.nic.br/ddos#5 - Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)

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

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

[8] 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

[9] https://www.cert.br/docs/palestras/certbr-forum-anatel2016.pdf - Problemas de Segurança e Incidentes com CPEs e Outros Dispositivos, 20º Fórum de Certificação para Produtos de Telecomunicações, Anatel, 11/2016, Campinas, SP

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

[11] https://www.m3aawg.org/sites/default/files/lac-bcop-1-m3aawg-v1-portuguese-final.pdf - Documento conjunto LACNOG-M3AAWG: Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinante (CPE) LAC-BCOP-1

[12] https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/ - Artigo do ShadowServer sobre os testes de amplificadores

[13] https://cert.br/docs/palestras/certbr-fiesp-deinfra-2019.pdf - Apresentação do CERT.br na Reunião de Telecomunicações do DEINFRA FIESP 23 de outubro de 2019 – São Paulo/SP

Obrigado

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

gzorello@nic.br

6 de fevereiro de 2020

nic.br cgi.br

www.nic.br | www.cgi.br