Panorama atual

Gilberto Zorello
Coordenação do Programa

Segurança e estabilidade da Internet
Estrutura da Internet atual

A Internet funciona com base na cooperação entre Sistemas Autônomos:

- É uma **“rede de redes”**
- São mais de **64.500 redes diferentes**, sob gestões técnicas independentes
- **A estrutura de roteamento BGP funciona com base em cooperação e confiança**
- O BGP não tem validação dos dados.
- **Resultado: não há um dia em que não ocorram incidentes de Segurança na Internet**

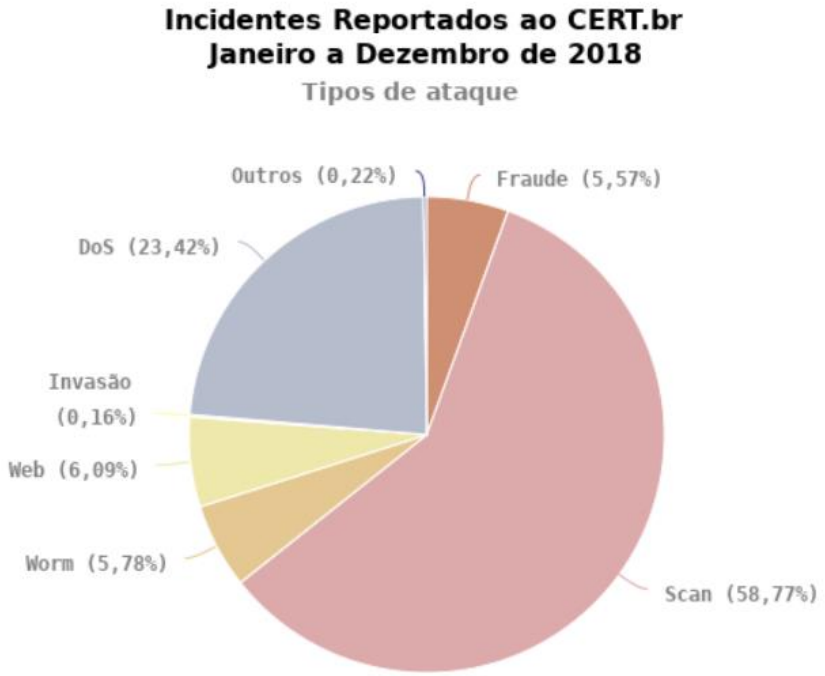
O BGP não tem
Validação para os dados

Segurança e estabilidade da Internet
Panorama Atual

Ataques à infraestrutura e aos serviços disponíveis na Internet estão cada vez mais comuns.

O NIC.br analisa a tendência dos ataques com dados obtidos por:

- Incidentes de segurança reportados
- **Medições em "honeypots" distribuídos na Internet**
- Medições no IX.



https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html

Constata-se um ritmo crescente de notificações de varreduras, fraudes e DoS

Como resolver os problemas

Programa por uma Internet mais Segura

Iniciativa

Lançado pelo CGI.br e NIC.br

Painel do IX Fórum 11 em dez/17

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 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**
- 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

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

Programa por uma Internet mais Segura
Ações necessárias da comunidade técnica

- **Configurar corretamente serviços que podem ser abusados em ataques de amplificação**
  - **Conforme as notificações do CERT**
- **Implementar as ações preconizadas pelo MANRS**
  - **Filtragem de rotas e de endereços de origem falsos (antispoofing) e informações para ações colaborativas entre os operadores da rede**
- **Realizar o hardening de equipamentos e redes**
  - **Mapear ameaças, mitigar riscos e adotar ações corretivas**

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Cursos de Boas Práticas Operacionais p/ Sistemas Autônomos – BCOP
- Tutoriais sobre melhores práticas de roteamento e hardening
- Palestras sobre o Programa e o MANRS nos eventos do NIC.br e Associações parceiras
- Interação com grandes operadoras: redução de endereços IP mal configurados
  - Em mar/18: 581k grandes operadoras // 144k ISP e AS corporativos
  - Hoje: 150k grandes operadoras // 214k ISP e AS corporativos.
- Ações com as maiores Associações de Provedores de Internet
- Ações com a indústria

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

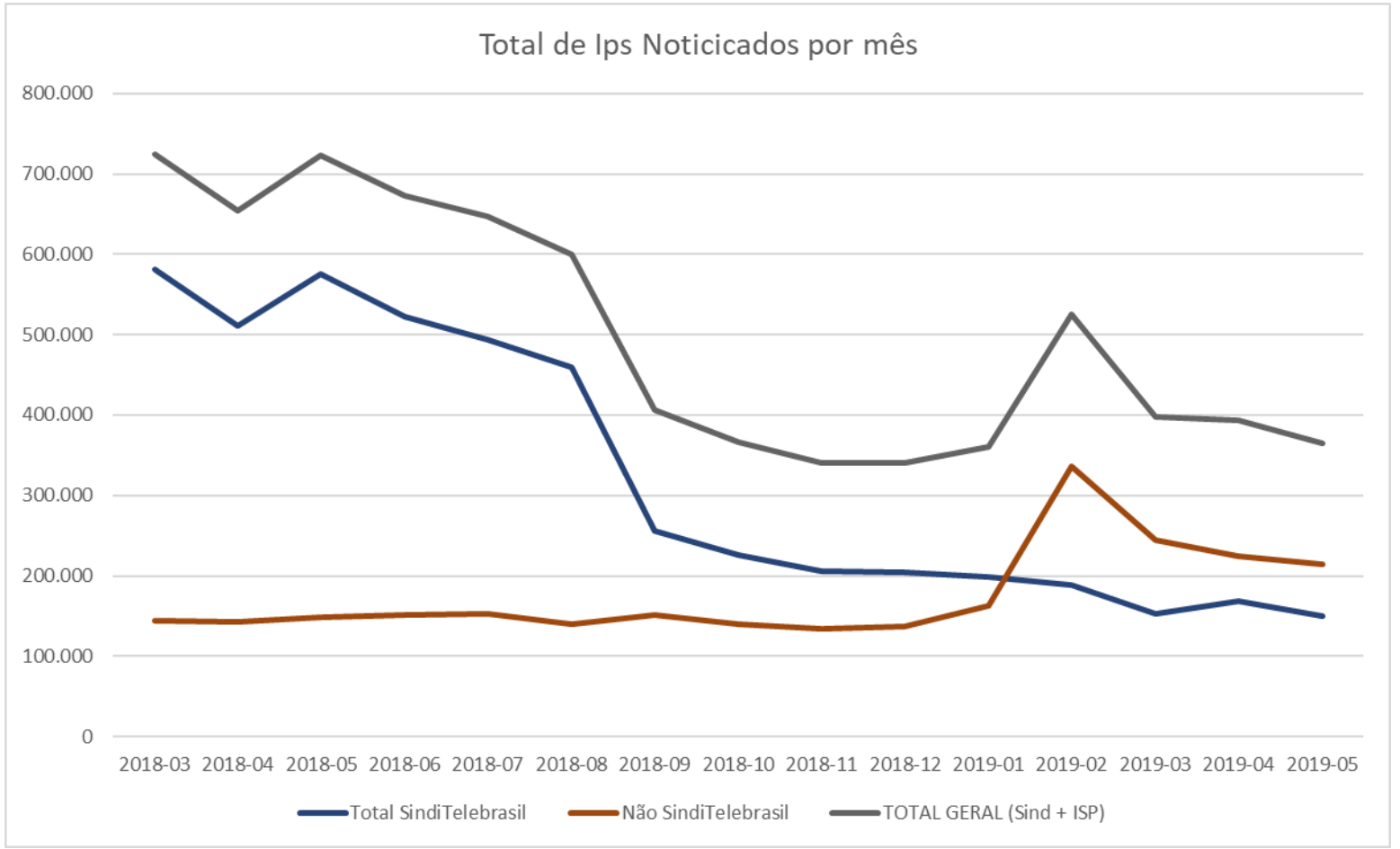
Brasil	DNS		SNMP		NTP		SSDP		UBNT	
mês	ASNs	IP	ASNs	IP	ASNs	IP	ASNs	IP	ASNs	IP
2018-05	2.343	65.270	2.390	502.861	870	88.788	846	23.174	0	0
2018-06	2.629	70.188	2.284	447.411	805	87.408	817	23.340	0	0
2018-07	2.721	68.415	2.436	431.907	881	89.484	787	17.255	0	0
2018-08	2.459	56.555	2.411	397.622	895	89.353	613	11.855	0	0
2018-09	2.767	62.942	2.366	193.432	772	87.378	836	21.836	0	0
2018-10	2.806	64.912	2.383	163.987	856	85.911	789	20.233	0	0
2018-11	2.604	60.937	2.376	137.331	851	87.155	814	20.124	0	0
2018-12	2.849	64.649	2.361	137.463	719	82.610	832	21.704	0	0
2019-01	2.960	74.257	2.583	137.253	923	89.567	840	17.348	0	0
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

O Brasil está em **terceiro** lugar entre os endereços IPs com serviço SNMP aberto

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

Programa por uma Internet mais Segura

Total de endereços IP notificados por mês



Obrigado

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

gzorello@nic.br

24 de maio de 2019

nic.br cgi.br

www.nic.br | www.cgi.br