



nie.br

Núcleo de Informação
e Coordenação do
Ponto BR

egi.br

Comitê Gestor da
Internet no Brasil

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

nic.br egi.br

registro.br

Futurecom 2018 – 20 Anos
São Paulo, SP | 15/10/18

AUMENTANDO A SEGURANÇA DOS PROVEDORES E DA PRÓPRIA DA INTERNET

Gilberto Zorello

gzorello@nic.br

registro.br nic.br cgi.br

Segurança e estabilidade da Internet
Querem saber?

Como...

RESOLVER DEFINITIVAMENTE

**OS PRINCIPAIS PROBLEMAS DE SEGURANÇA
da INTERNET (e do seu provedor)???**

**Incluindo ataques DDOS, SPAM
e 'roubo de prefixos'!**

Segurança e estabilidade da Internet
Querem saber?

Isso tudo gastando praticamente

NADA, ZERO, NOTHING! ~~\$\$\$\$~~

Com apenas 4 ações muito simples...

Interessados?

Nossa Agenda

- NIC.br e CGI.br
- Problemas de segurança na Internet
- Programa por uma Internet mais segura
- MANRS – ações para resolver os problemas de segurança na infraestrutura de roteamento da Internet
- Outras ações importantes



1 2 3 4 5 6 7 8 9

GOVERNO

10 11 12 13 14 15 16 17 18 19 20 21

SOCIEDADE CIVIL

e

Representantes do Governo:

- 1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
- 2 Casa Civil da Presidência da República
- 3 Ministério das Comunicações
- 4 Ministério da Defesa
- 5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
- 6 Ministério do Planejamento, Orçamento e Gestão
- 7 Agência Nacional de Telecomunicações
- 8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
- 9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

- 10 Notório saber em assunto da Internet
- 11 a 14 Representantes do setor empresarial
 - provedores de acesso e conteúdo da Internet
 - provedores de infra-estrutura de telecomunicações
 - indústria de bens de informática, de bens de telecomunicações e de software
 - setor empresarial usuário
- 15 a 18 Representantes do terceiro setor
- 19 a 21 Representantes da comunidade científica e tecnológica

Organograma do NIC.br

membros e ex-membros do CGI.br
(somente os atuais membros têm direito a voto) ➔

ASSEMBLEIA GERAL

7 membros eleitos pela Assembleia Geral ➔

**CONSELHO DE
ADMINISTRAÇÃO**

**CONSELHO
FISCAL**

ADMINISTRAÇÃO
.....
JURÍDICO
.....
COMUNICAÇÃO
.....
ASSESSORIAS:
CGI.br e PRESIDÊNCIA

**DIRETORIA
EXECUTIVA**

1 2 3 4 5

registro.br

Domínios

cert.br

Segurança

cetic.br

Indicadores

ceptro.br

Redes e Operações

ceweb.br

Tecnologias Web

ix.br

Troca de Tráfego

W3C
Brasil

Padrões Web

- 1 Diretor presidente
- 2 Diretor administrativo e financeiro
- 3 Diretor de serviços e de tecnologia
- 4 Diretor de projetos especiais e de desenvolvimento
- 5 Diretor de assessoria às atividades do CGI.br

Programa por uma Internet mais Segura

Como Resolver os problemas

A Internet funciona com base na cooperação entre Sistemas Autônomos:

- É uma “**rede de redes**”.
- São quase **60.000 redes diferentes**, sob gestões técnicas diferentes.
- 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



CNET > Tech Culture >
How Pakistan knocked YouTube offline (and how to make sure it never happens again)

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

Massive route leak causes internet slowdown

Posted by Andree Toonk - June 12, 2015 - BGP instability - No Comments

Routing Leak briefly takes down Google

MARCH 12, 2015 COMMENTS (35) VIEWS: 37374 ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY DOUG MADORY

Global Collateral Damage of TMnet leak

JUNE 12, 2015 COMMENTS (1) VIEWS: 41213 SECURITY, UNCATEGORIZED DOUG MADORY

DDoS Attacks Storm Linode Servers Worldwide

BY DOUGLAS BONDERUD • JANUARY 5, 2016

UK traffic diverted through Ukraine

MARCH 13, 2015 COMMENTS (34) VIEWS: 47297 SECURITY DOUG MADORY

Global Impacts of Recent BGP Leaks

Event type	Country	ASN	Start time
BGP Leak		Origin AS: PO box T511 Phonexay road - Xaysettha district (AS 131267) Leaker AS: Viettel Corporation (AS 7552)	2016-01-13 12:25:47
BGP Leak		Origin AS: Lirex net EOOD (AS 8262) Leaker AS: Traffic Broadband Communications Ltd. (AS 48452)	2016-01-13 12:11:26

BGP hijack incident by Syrian Telecommunications

Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments

The Vast World of Fraudulent Routing

JANUARY 29, 2015 COMMENTS (17) VIEWS: 36909 SECURITY DOUG MADORY

CSO

Most read:

Home > Data Protection > Cyber Attacks/Espionage

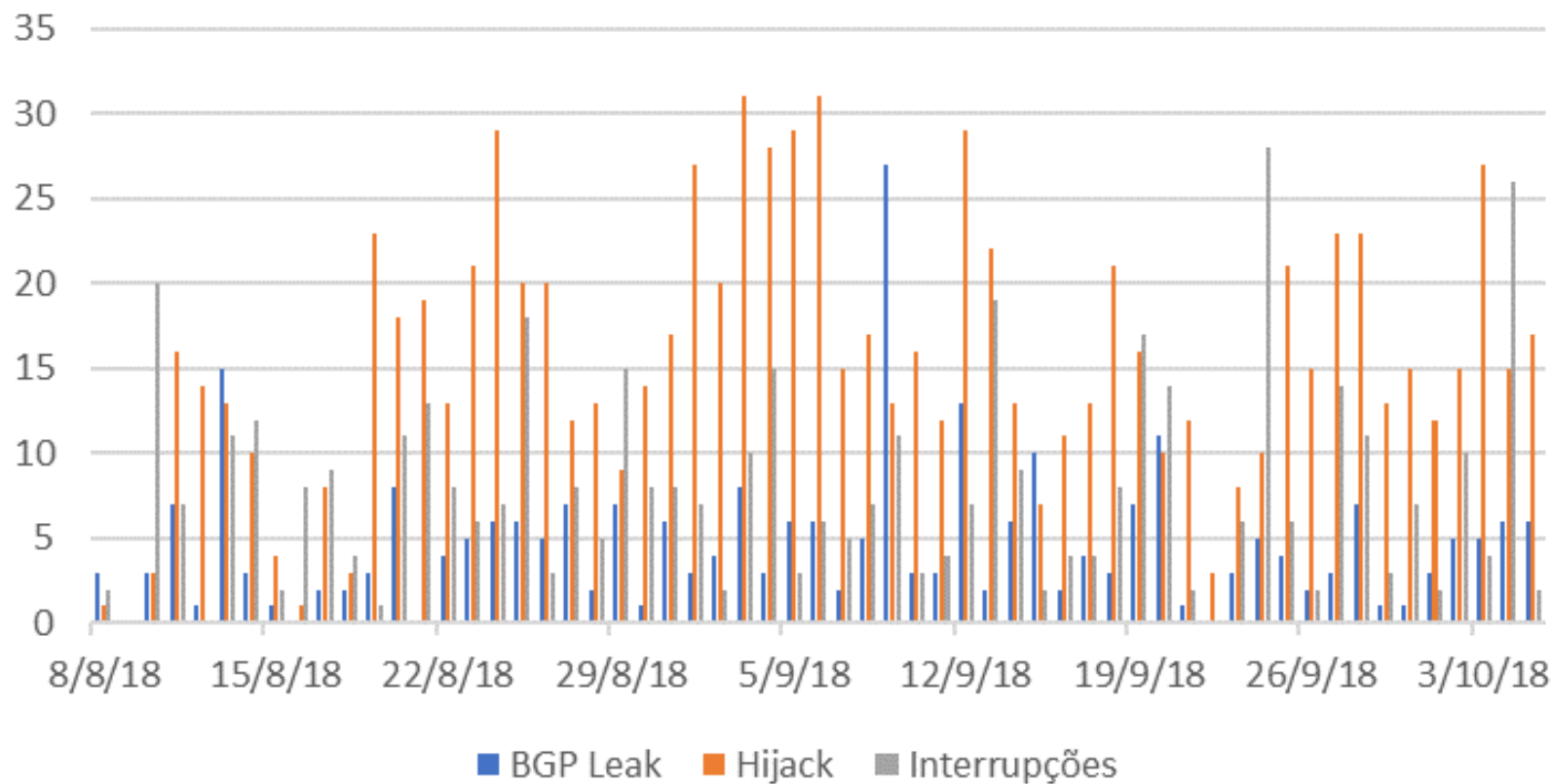
TODAY'S TOP STORIES

DDoS attack on BBC may have been biggest in history

Segurança na Internet

Nenhum dia sem um incidente

60 dias de atividades suspeitas



<http://bgpstream.com/>

Segurança na Internet

Panorama Atual

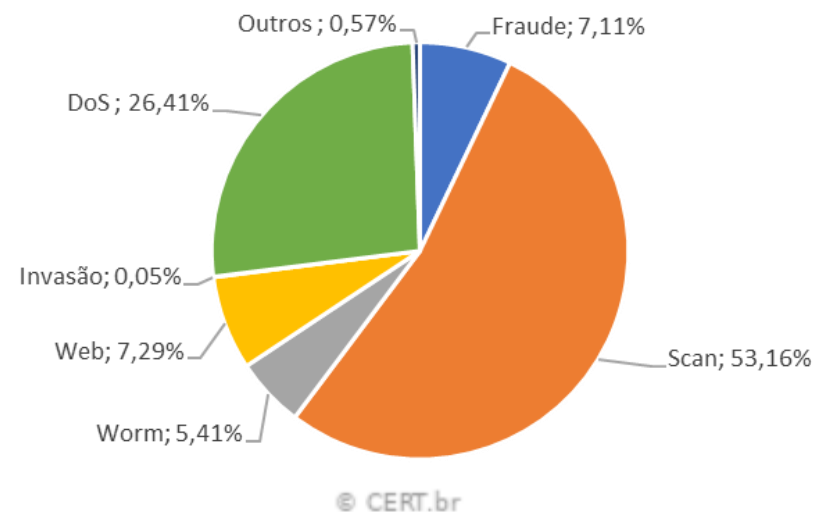
Ataques à infraestrutura e aos serviços disponíveis na Internet estão cada vez mais comuns.

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

- Tratamento de incidentes de segurança.
- **Medições em “honeypots” distribuídos na Internet.**
- Medições no IX.

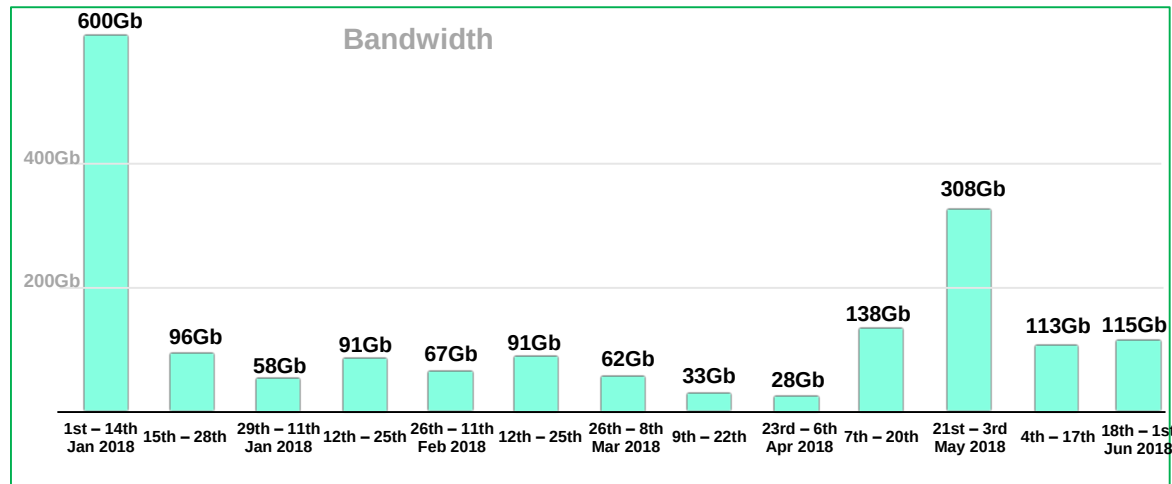
Constata-se um ritmo crescente de notificações de varreduras, fraudes e DDoS.

Ataques Reportados ao CERT (%) - 2017



Segurança na Internet

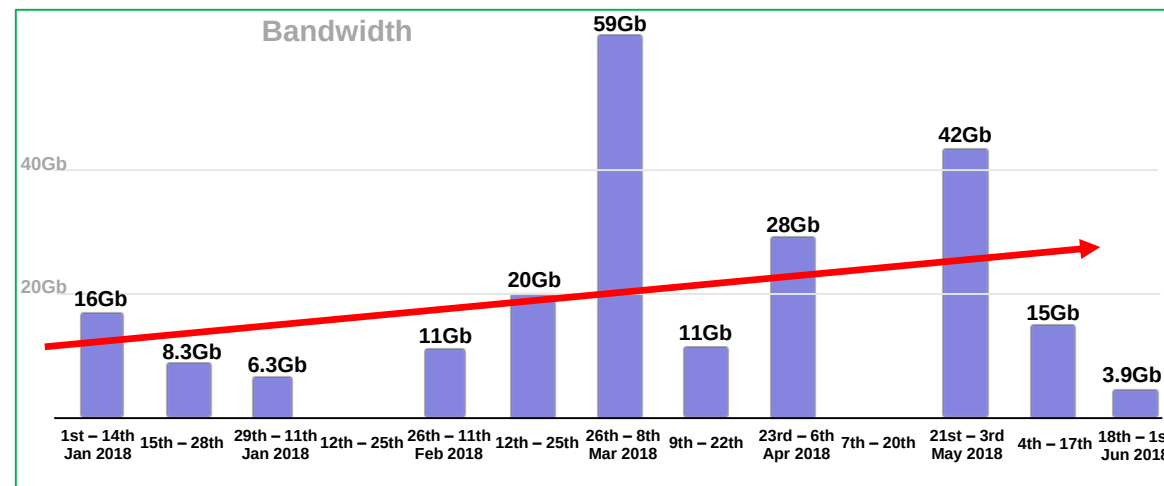
Panorama Atual



Origem mundo destino Brasil

Ataques DDoS com origem no exterior e destino ao Brasil

Ataques DDoS com origem no Brasil e destino ao Brasil



Origem Brasil destino Brasil

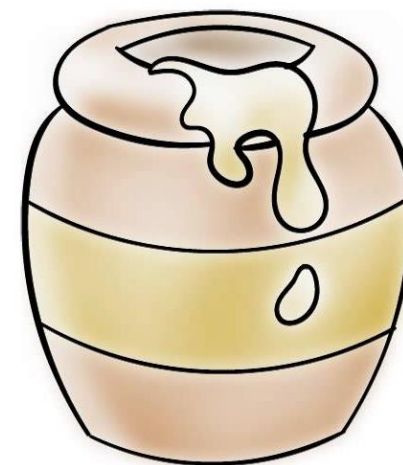
Fonte: <https://br.arbornetworks.com/asert-blog/um-balanco-dos-ataques-ddos-ao-brasil-no-primeiro-semester-deste-ano/>, em 06/08/18 11:39.

Segurança na Internet

Panorama Atual

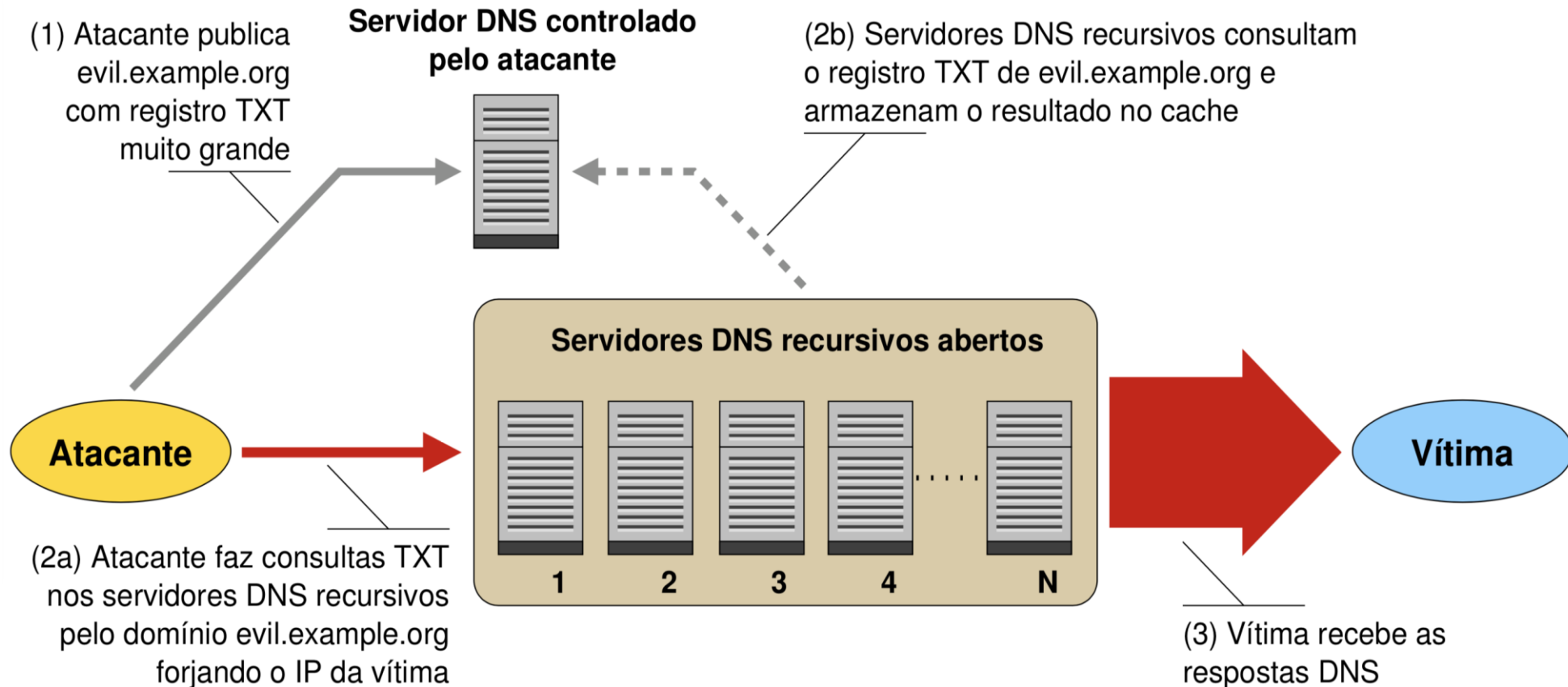
Os honeypots detectam principalmente:

- **Ataques de força bruta a serviços do tipo Telnet, SSH, RDP.**
- Portas exploradas pela botnet Mirai para CPEs.
- **Busca por protocolos que permitem amplificação: UDP, DNS, SNMP, NTP, SSDP.**
- Para reduzir o impacto e a viabilidade destes ataques, as comunidades da Internet devem **mobilizar-se em conjunto** e executar ações para diminuir tais atividades maliciosas.



Segurança e estabilidade da Internet

Problemas de segurança



Visão geral do ataque de negação de serviço utilizando servidores DNS recursivos abertos

Panorama Atual

Endereços IP e ASN notificados pelo CERT.

	DNS		SNMP		NTP		SSDP	
month	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
2017-11	2.279	61.281	-	-	821	100.801	863	26.999
2017-12	2.436	62.758	2.001	460.519	-	-	845	27.828
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	na	na	2.383	163.987	856	85.911	789	20.233

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

Observações:

- "na" significa que o protocolo ainda não foi notificado no mês;
- "-" significa que não houve notificação para o protocolo no mês.

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

Programa por uma Internet mais Segura Iniciativa

Lançado pelo CGI.br e NIC.br.

Painel do IX Fórum 11 em dez/17 [1].



Apoio: ISOC, ABRANET, SindiTelebrasil, ABRINT.



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

- **Redução de ataques de Negação de Serviço originados nas redes brasileiras.**
- Redução das vulnerabilidades e falhas de configuração presentes nos elementos de rede.
- **Criar uma cultura de segurança.**
- Aproximar as diferentes equipes responsáveis pela segurança e estabilidade da rede.

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 estabelecimento de boas práticas:
 - **especificação, configuração e operação de CPE em suas respectivas redes.**
 - implantação das ações básicas para melhorar a Segurança na Internet, preconizadas pelo MANRS [2].
- **Implementação de filtros de rotas no IX.br, que pode contribuir para a melhora do cenário geral.**
- Estabelecimento de métricas e acompanhamento da efetividade das ações.

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 Programa MANRS [2], apoiado pela ISOC, preconiza a Segurança e Estabilidade na Internet.

- **Estamos todos juntos nisso!!**
- Os operadores de rede têm a responsabilidade em assegurar uma infraestrutura de roteamento robusta, confiável!
- **A segurança da sua rede depende das demais redes!**
- A segurança das outras redes depende da sua rede!
- **Implemente as ações do MANRS e junte-se à iniciativa.**
- **Quanto mais operadores de rede trabalharem juntos menos problemas todos terão!**





MANRS

Mutually Agreed Norms for Routing Security

Saiba mais em:

<http://manrs.org>

<http://bcp.nic.br>

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 demandem que estas ações sejam aplicadas pelos seus provedores de serviços.**



MANRS



Sequestro de Prefixos
Vazamento de Rotas
Falsificação de IP de Origem

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).**



MANRS



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

Recomendações Adicionais

Receber e tratar notificações que são enviadas [5]:

- 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.



Reduzir ataques DDoS saindo de sua rede [4]:

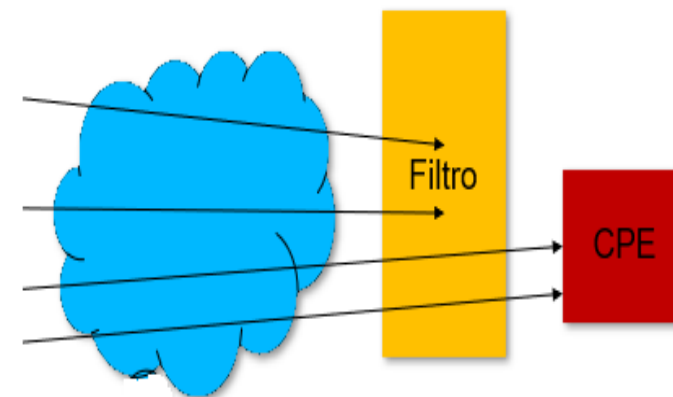
- Análise proativa do tráfego que sai da rede utilizando netflows.
- Configurar os CPEs para não ter serviços abertos que permitam amplificação e ter política de senhas seguras (hardening).

Programa por uma Internet mais Segura

Recomendações Adicionais

Filtrar **tráfego de entrada** 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

Minimum security requirements for CPEs acquisition

O LACNOG está desenvolvendo um documento que tem como objetivo identificar um conjunto mínimo de requisitos de segurança que devem ser especificados no processo de compra de CPEs por 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.

Assim que o documento estiver liberado, será disponibilizado para a Comunidade Técnica da Internet pelo site <https://bcp.nic.br>.

- Acompanhe com atenção, contribua, utilize...



Programa por uma Internet mais Segura

Minimum security requirements for CPEs acquisition

Em geral, as vulnerabilidades incluem:

- credenciais padrão para vários dispositivos.
- credenciais que não podem ser modificadas.
- uso de protocolos e algoritmos obsoletos e inseguros.
- acessos não documentados (backdoors).
- falta de atualizações e correções de segurança.
- serviços desnecessários e / ou inseguros habilitados por padrão.
- serviços que não podem ser desativados.
- ausência de gerenciamento remoto e mecanismos seguros de atualização.

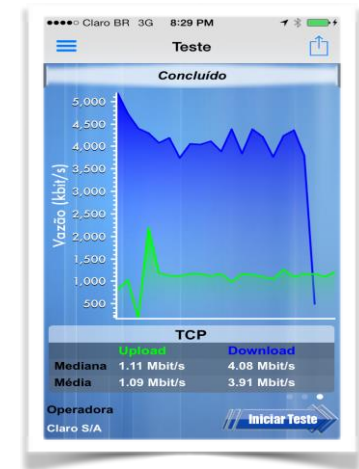
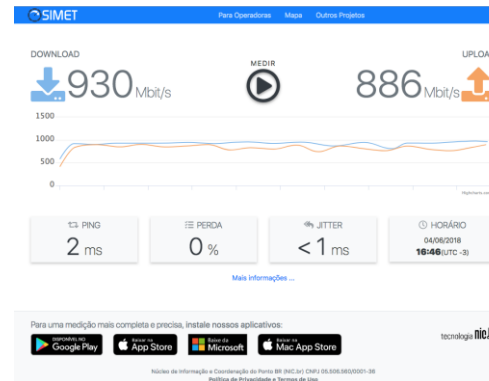
nic.br



Programa por uma Internet mais Segura

SIMET - Sistema de Medição de Qualidade da Internet

- SIMET WEB
 - Widget
 - Lista de Provedores
- SIMET Mobile
 - Android
 - iOS
- SIMETBox
 - Testes BCP 38
 - Teste Porta 25



Programa por uma Internet mais Segura

SIMET - Sistema de Medição de Qualidade da Internet

- Testes realizados do usuário até um dos PTTs do IX.br, fora da rede medida.
 - Rede ASN 14026 (uso só para medição de participantes do IX.br).
- Quem não tem acesso a algum PTT (fora do Brasil) usa os servidores localizados no ASN 22548 (NIC.br).
- Medições com IPv4 e IPv6.
- Medições BCP 38, testes:
 - Mesmo IP
 - Mesma rede
 - Outra rede
 - Endereço privado



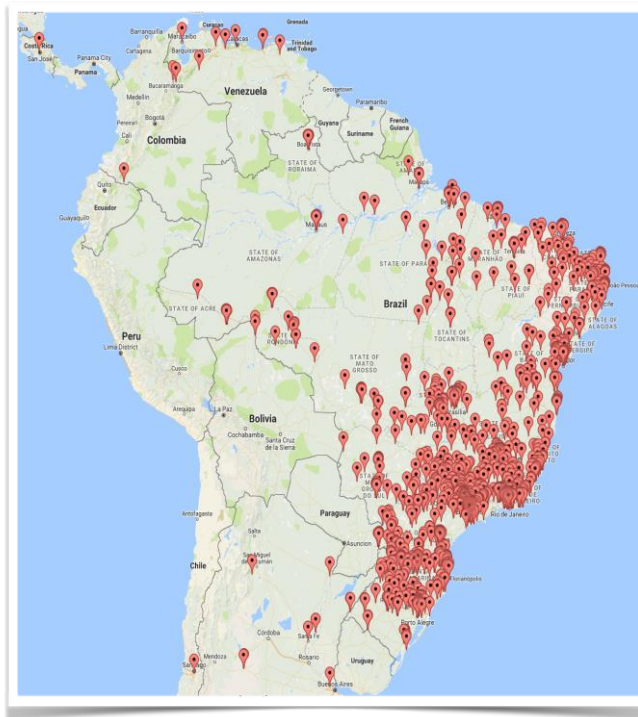
Programa por uma Internet mais Segura

SIMET - Sistema de Medição de Qualidade da Internet



Adquira Roteadores para atender seus usuários (SOHO) com as seguintes características:

- Compatível com OpenWRT, destravado para permitir troca do firmware
- **64 MiB RAM e 8 MiB FLASH**
- No mínimo com padrão de rede wi-fi IEEE 802.11 b/g/n para geolocalização
- **CPU compatível com a velocidade do circuito, OpenWRT muitas vezes não usa aceleração por hardware**



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

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(a)
www.site.br

@ gzorello@nic.br

15 de outubro de 2018

nic.br **cgi.br**
www.nic.br | www.cgi.br