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

AUMENTANDO A SEGURANÇA NA INTERNET NO BRASIL

Encontro Nacional ABRINT 2018

São Paulo - 5/06/2018

Gilberto Zorello
gzorello@nic.br

nic.br

Programa por uma Internet mais Segura
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.

Programa por uma Internet mais Segura
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.

Dispositivos / Serviços que permitem amplificação que tiveram ASNs e IPs Notificados (totais para o Brasil) [5]

	DNS		SNMP		NTP		SSDP	
	ASN	IP	ASN	IP	ASN	IP	ASN	IP
janeiro-17	2.133	87.953	-	-	981	97.423	-	-
fevereiro-17	2.066	67.159	1.681	573.373	-	-	805	37.459
março-17	-	-	1.805	604.805	915	104.665	-	-
abril-17	2.191	72.124	-	-	861	92.120	812	27.233
maio-17	2.280	69.957	1.869	573.400	-	-	839	40.814
junho-17	2.183	64.179	1.948	596.348	860	91.257	812	33.805
julho-17	-	-	1.963	551.953	841	107.097	-	-
agosto-17	2.347	72.677	2.018	554.457	872	108.168	891	27.209
setembro-17	2.307	62.283	1.791	406.015	800	89.603	-	-
outubro-17	2.328	67.066	1.886	343.674	845	108.605	902	32.056
novembro-17	2.279	61.281	-	-	-	-	863	26.999
dezembro-17	2.436	62.758	2.001	460.519	-	-	845	27.828
	ASN	IP	ASN	IP	ASN	IP	ASN	IP
janeiro-18	2.412	61.875	2.130	479.247	823	97.075	888	25.982
fevereiro-18	2.438	72.185	2.324	559.784	849	93.801	778	20.210
março-18	2.476	63.811	2.278	515.345	844	84.483	544	11.431
abril-18	2.509	66.371	2.280	436.702	850	85.549	794	21.686
maio-18	2.343	65.270	2.390	502.861	870	88.788	846	23.174

Legenda: “-” significa que não foi realizada notificação desta categoria no referido mês.

Programa por uma Internet mais Segura **Iniciativa**

Lançado pelo cgi.br e nic.br.

Painel do IX Fórum 11 em dez/17.

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.

Programa por uma Internet mais Segura
Como Resolver os problemas

Solução para ataques DDoS, SPAM e Sequestro de Blocos IPs:

- **Três ações muito simples que podem ser executadas em sua rede.**
- Baixo custo de implantação: não precisa comprar equipamentos, softwares ou serviços.

Conceito:

- Bloquear o tráfego que entra na rede é complexo.
- ***Avaliar o que sai indevidamente da rede resolve os problemas.***

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.**

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, definir políticas e filtros e garantir que as políticas definidas estão sendo 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].**

   - Impede que os computadores infectados de seus usuários iniciem ataques de amplificação.

3. **Garantir que seus contatos estejam atualizados e acessíveis por terceiros: Whois do registro.br, IRR, PeeringDB.**

   - Permite que equipes de segurança de outras redes te avisem sobre problemas que detectam na sua rede.

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!
- **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
Recomendações Adicionais

Receber e tratar notificações que são enviadas:

- Manter e-mail de contato abuse-c do ASN no Whois atualizado.
- Certificar-se de que os e-mails de abuse ou do grupo de incidentes estão sendo tratados.

Reduzir ataques DDoS saindo de sua rede:

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

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.

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 provedores de acesso.

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 primeiro draft estiver liberado, o documento será disponibilizado para as Associações de Provedores para contribuições.

Programa por uma Internet mais Segura
Minimum security requirements for CPEs acquisition

"Customer premises equipment (CPE)" são os equipamentos usados para conectar os assinantes à rede do provedor de serviços de Internet (ISP).

- Exemplos: modems (cabo, DSL, fibra), roteadores Wi-Fi, entre outros.

Devido a inúmeras vulnerabilidades no software incorporado e nas configurações, os CPEs têm sido alvo de uma série de abusos:

- exploração de serviços mal configurados.
- comprometimento por malwares, com o objetivo de realizar ataques e fraudes, especialmente ataques de negação de serviço.
- propagação de malware, spam, roubo de credenciais, entre outros.

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.

Programa por uma Internet mais Segura
Minimum security requirements for CPEs acquisition

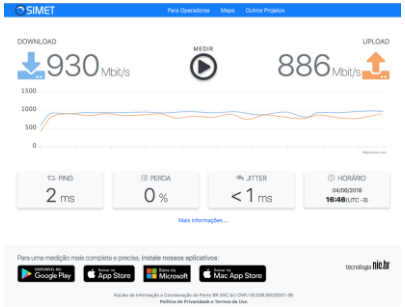
Formato do documento:

- Requisitos gerais (GR).
- Requisitos de segurança de software (SS).
- Atualização e requisitos de gerenciamento (MR).
- Requisitos funcionais (FR).
- Requisitos de configuração inicial (IR).
- Requisitos do fornecedor (VR).

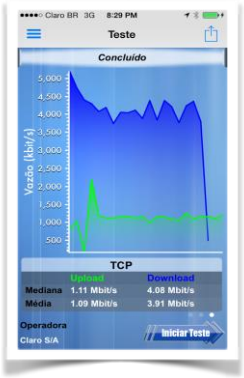
Programa por uma Internet mais Segura

SIMET - Sistema de Medição de Qualidade da Internet

- SIMET WEB
  - Widget
  - Lista de Provedores



- SIMET Mobile
  - Android
  - iOS



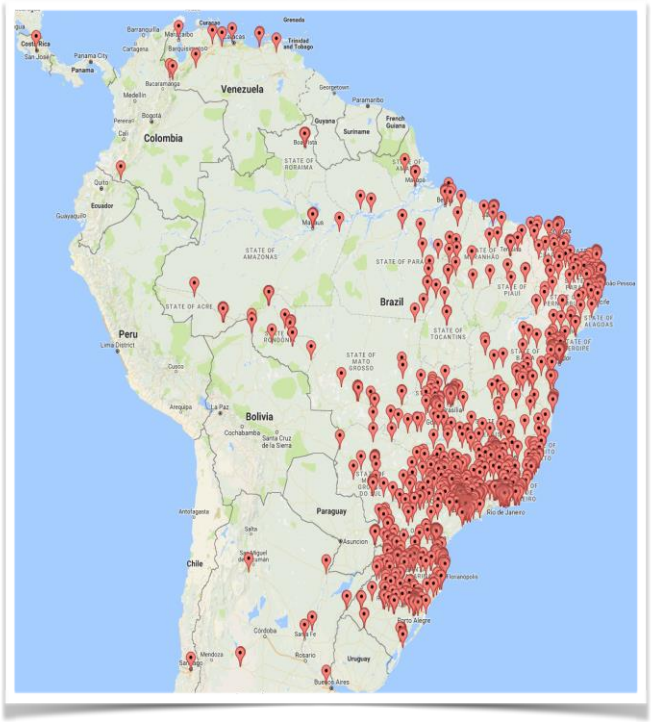
- SIMETBox
  - Testes BCP38
  - Teste Porta 25

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

SIMETBox



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

Cursos BCOP, IPv6 e IX Fóruns Regionais

Cursos IPv6

- O **curso presencial básico sobre IPv6 formou mais de 5000 profissionais** entre 2009 a 2016, provenientes dos principais provedores, Sistemas Autônomos e empresas relacionadas à Internet. Em 2017 lançamos o curso de IPv6 Básico a distância (EaD).

- Em 2018 os **cursos IPv6 presenciais serão retomados** em uma modalidade avançada, com 24 horas/aula (três dias), **abordando conteúdos que não estão presentes no curso a distância (EaD)**, como: segurança IPv6, distribuição de IPv6 nas redes com SLAAC e DHCPv6, última milha IPv6 para provedores de acesso e técnicas de transição IPv6.

- **Um dos pré-requisitos para a matrícula será o aluno ter concluído, com sucesso, o curso a distância (EaD)**

IPv6.br

Cursos BCOP, IPv6 e IX Fóruns Regionais

Cursos BCOP

- O curso de Boas Práticas Operacionais para Sistemas Autônomos, foi criado em 2013 para **difundir boas práticas na operação da Internet**, em particular boas práticas no roteamento BGP. Em 2017 tivemos 16 cursos no total com 540 profissionais treinados.

- **Em 2018, os cursos BCOP** passarão a ter 24 horas/aula (três dias), com uma **atenção maior para tópicos básicos sobre segurança**, como *hardening* de equipamentos de rede, gerenciamento adequado de senhas, técnicas de *antispoofing*, monitoramento da rede com *flows*, etc. O curso continuará abordando a configuração de BGP na Internet, com acesso a múltiplos provedores e a *Internet Exchanges*.

- **O aluno ter concluído o curso a distância (EaD) será considerado como um diferencial para a seleção dos alunos do curso BCOP.**

Cursos BCOP, IPv6 e IX Fóruns Regionais

IX Fórum Regionais

- O **IX Fórum Regional**, reunião aberta de provedores realizada desde 2017 em conjunto com os cursos, tem por objetivo incentivar o diálogo entre os participantes, abordando o uso dos Pontos de Troca de Tráfego e a interconectividade, além de incluir tópicos técnicos e temas relacionados, buscando estratégias para promover o desenvolvimento da Internet em cada localidade.

- Além de palestras do próprio NIC.br e de um espaço para o debate sobre a conectividade local e os PTTs com os participantes, outras empresas e entidades são convidadas a fazer suas apresentações nessas reuniões. Os IX Fóruns Regionais incentivam o diálogo e o desenvolvimento da Internet regionalmente, promovendo o peering e a participação nos PTTs. Em 2017 tivemos 17 IX Fóruns Regionais com 900 participantes no total. Em 2018 eles continuarão a ser promovidos.

Cursos BCOP, IPv6 e IX Fóruns Regionais

Calendário 2018

- 14 a 18 de maio - **São Paulo/SP** - BCOP + IX Fórum Regional
- 11 a 15 de junho - **Teresina/PI** - BCOP + IX Fórum Regional
- 25 a 29 de junho - **Belo Horizonte/ MG** - BCOP + IX Fórum Regional
- 09 a 13 de julho - **Goiânia/GO** - BCOP + IX Fórum Regional
- 13 a 17 de agosto - **Fortaleza/CE** - BCOP + IX Fórum Regional
- 27 a 31 de agosto - **São Paulo/SP** - IPv6 Avançado
- 10 a 14 de setembro - **Natal/RN** - IPv6 Avançado + IX Fórum Regional
- 17 a 21 de setembro - **Aracaju/SE** - BCOP + IX Fórum Regional
- 01 a 05 de outubro - **Salvador/BA** - IPv6 Avançado + IX Fórum Regional
- 22 a 26 de outubro - **Florianópolis/SC** - BCOP + IX Fórum Regional
- 05 a 09 de novembro - **Porto Alegre/RS** - IPv6 Av. + IX Fórum Regional
- 12 a 14 de novembro - **São Paulo/SP** - IPv6 Avançado
- 03 a 07 de dezembro - **São Paulo/SP** - BCOP

Obs: Muitas das datas coincidem com o calendário dos WTRs, da RNP. Nesses casos os eventos serão realizados em conjunto. Todas as datas estão sujeitas à confirmação.

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.nic.br

gzorello@nic.br @ComuNICbr Facebook.com/nic.br/

27 de abril de 2018

nic.br cgi.br

www.nic.br | www.cgi.br