



nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

cgib.br

Comitê Gestor da
Internet no Brasil



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

PROJETO INICIATIVA INTERNET SEGURA

Gilberto Zorello
gzorello@nic.br

nic.br

Projeto Iniciativa Internet Segura [1]

Motivação

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

As notificações de incidentes, análise de sensores na Internet (honeypots) e análise do perfil de tráfego no IX permitem analisar o que está ocorrendo na rede.

Existem muitas notificações de varreduras, fraudes e DDoS (em ritmo crescente).

DDoS é um tipo de ataque pouco reportado, mas afeta diretamente a operação das empresas [4].

Os sensores passivos distribuídos na Internet detectam principalmente:

- **Ataques de força bruta em serviços do tipo Telnet, SSH, RDP, POP3.**
- Portas exploradas pela botnet Mirai para CPEs: TCP 7547, 5555, 37777.
- **Busca por protocolos que permitem amplificação: UDP, DNS, SNMP, NTP, SSDP.**

Na referência [7] há uma palestra sobre Ataques Mais Significativos e Como Melhorar o Cenário.

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: Totais no Brasil para ASNs e IPs Notificados [5]

2017	DNS		SNMP		NTP		SSDP	
	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
Janeiro	2.133	87.953	–	–	981	97.423	–	–
Fevereiro	2.066	67.159	1.681	573.373	–	–	805	37.459
Março	–	–	1.805	604.805	915	104.665	–	–
Abril	2.191	72.124	–	–	861	92.120	812	27.233
Maiο	2.280	69.957	1.869	573.400	–	–	839	40.814
Junho	2.183	64.179	1.948	596.348	860	91.257	812	33.805
Julho	–	–	1.963	551.953	841	107.097	–	–
Agosto	2.347	72.677	2.018	554.457	872	108.168	891	27.209
Setembro	2.307	62.283	1.791	406.015	800	89.603	–	–
Outubro	2.328	67.066	1.886	343.674	845	108.605	902	32.056
Novembro	2.279	61.281	–	–	–	–	863	26.999
Dezembro	2.436	62.758	2.001	460.519	–	–	845	27.828
2018	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
Janeiro	2.412	61.875	2.130	479.247	823	97.075	888	25.982
Fevereiro	2.438	72.185	2.324	559.784	849	93.801	778	20.210
Março	2.476	63.811	2.278	515.345	844	84.483	544	11.431

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

Projeto Iniciativa Internet Segura

Plano de Ação

Para solucionar os problemas de segurança, as ações devem ser realizadas pelos operadores dos Sistemas Autônomos (ASs) que formam a Internet no Brasil, em particular pelos provedores de Internet, com ajuda 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 as Associações de provedores e seus afiliados para estabelecimento de boas práticas para:
 - **especificação, configuração e operação de CPE em suas respectivas redes.**
 - **implantação das ações básicas para melhorar a Segurança na Internet, preconizadas pelo MANRS [2].**
- Estabelecimento de métricas.
- **Implementação de filtros de rotas no IX.br, que pode contribuir para a melhora do cenário geral.**

Projeto Iniciativa Internet Segura

Como Resolver os problemas



Solução para os problemas de segurança da Internet e de seu provedor envolvendo 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.
- **Bloquear o tráfego que entra na rede é complexo.**
- Avaliar o que sai indevidamente da rede resolve os problemas.

Projeto Iniciativa Internet Segura Como Resolver os problemas

A Internet funciona com base na cooperação entre Sistemas Autônomos:

- **A Internet 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 ocorrem incidentes de Segurança na Internet.**



Projeto Iniciativa Internet Segura Como Resolver os problemas



MANRS

Todos devem implementar estas recomendações [9]:

- 1. Garantir que seus anúncio BGP sejam de seus próprios blocos IP e de seus clientes definindo políticas e filtros para garantir que as políticas estão sendo seguidas.**
 - Dificulta sequestro de blocos IP e redirecionamento de tráfego.
- 2. Garantir que os IP de origem que sai 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.

Projeto Iniciativa Internet Segura MANRS



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>

Projeto Iniciativa Internet Segura

Recomendações Adicionais

Receber e tratar notificações que são enviadas:

- E-mail de contato abuse-c do ASN no Whois
- 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 e ter política de senhas segura (hardening).

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 do própria operadora.

Projeto Iniciativa Internet Segura [1]

Referências Adicionais

- [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/spoofers/> - 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](https://twitter.com/ComuNICbr)

 [Facebook.com/nic.br/](https://www.facebook.com/nic.br/)

27 de abril de 2018

nic.br **cgi.br**

www.nic.br | www.cgi.br