
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 ptt.br ceweb.br

Aumentando a segurança do seu provedor e da infraestrutura da Internet

ceptro.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 3 ações muito simples…

Interessados?

GINSU 2000

The Deluxe 10 Piece Set • Cet ens. de luxe comprend 10 pièces

AS SEEN ON TV
TEL QU'ANNONCÉ À LA TV

Nossa

Agenda

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

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e SOCIEDADE CIVIL — 10 11 12 13 14 15 16 17 18 19 20 21

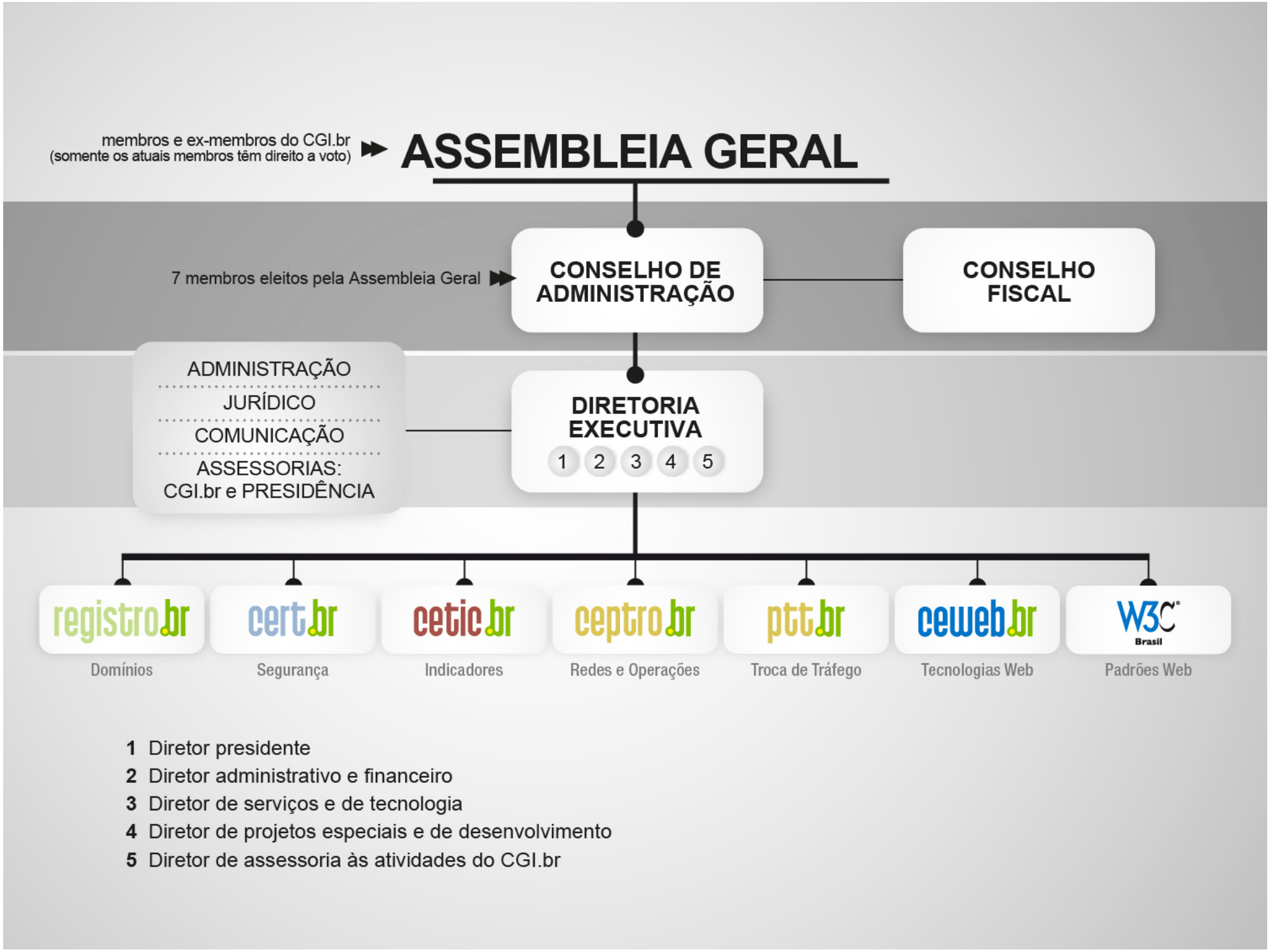
Representantes do Governo:

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

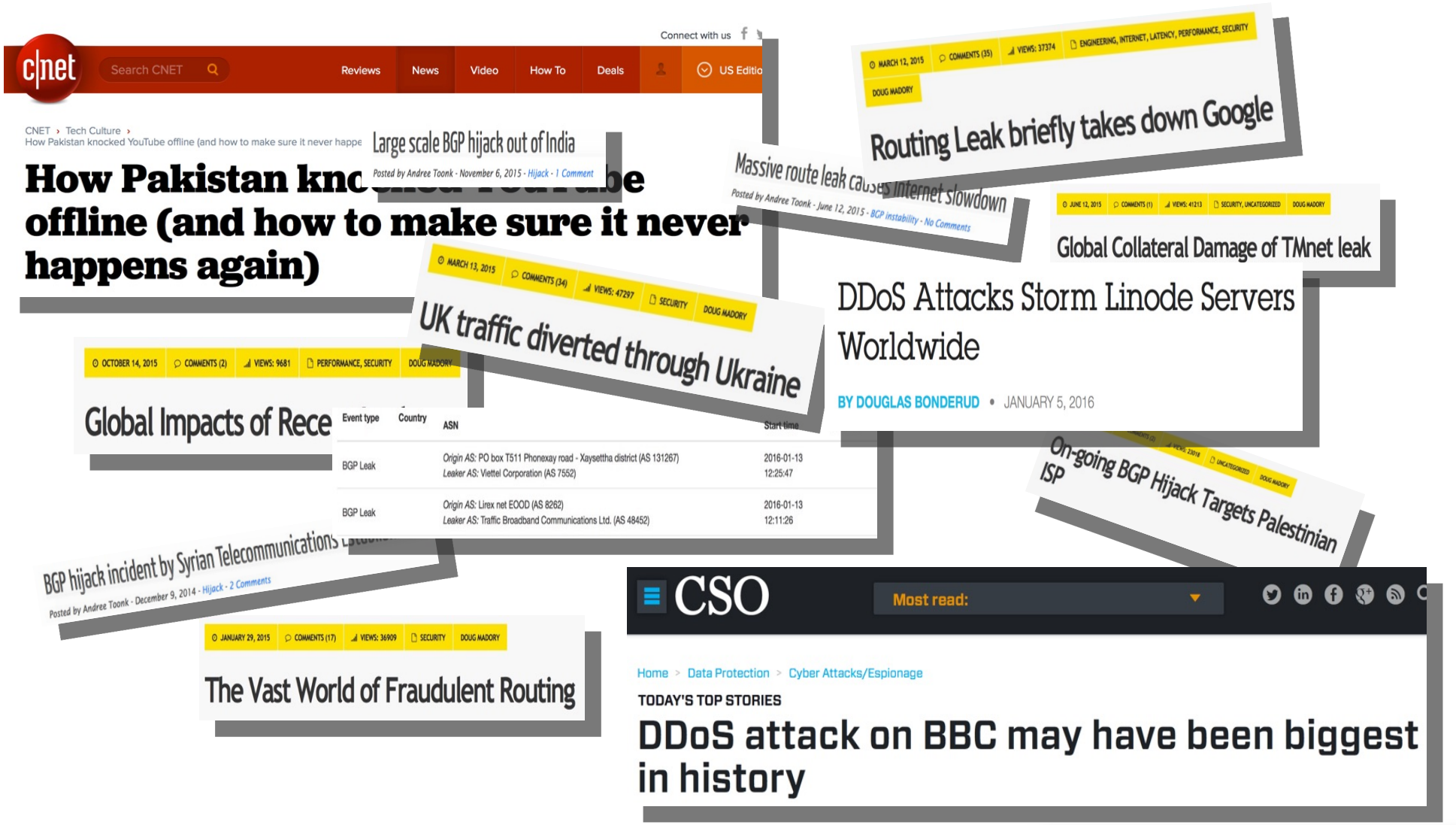


1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

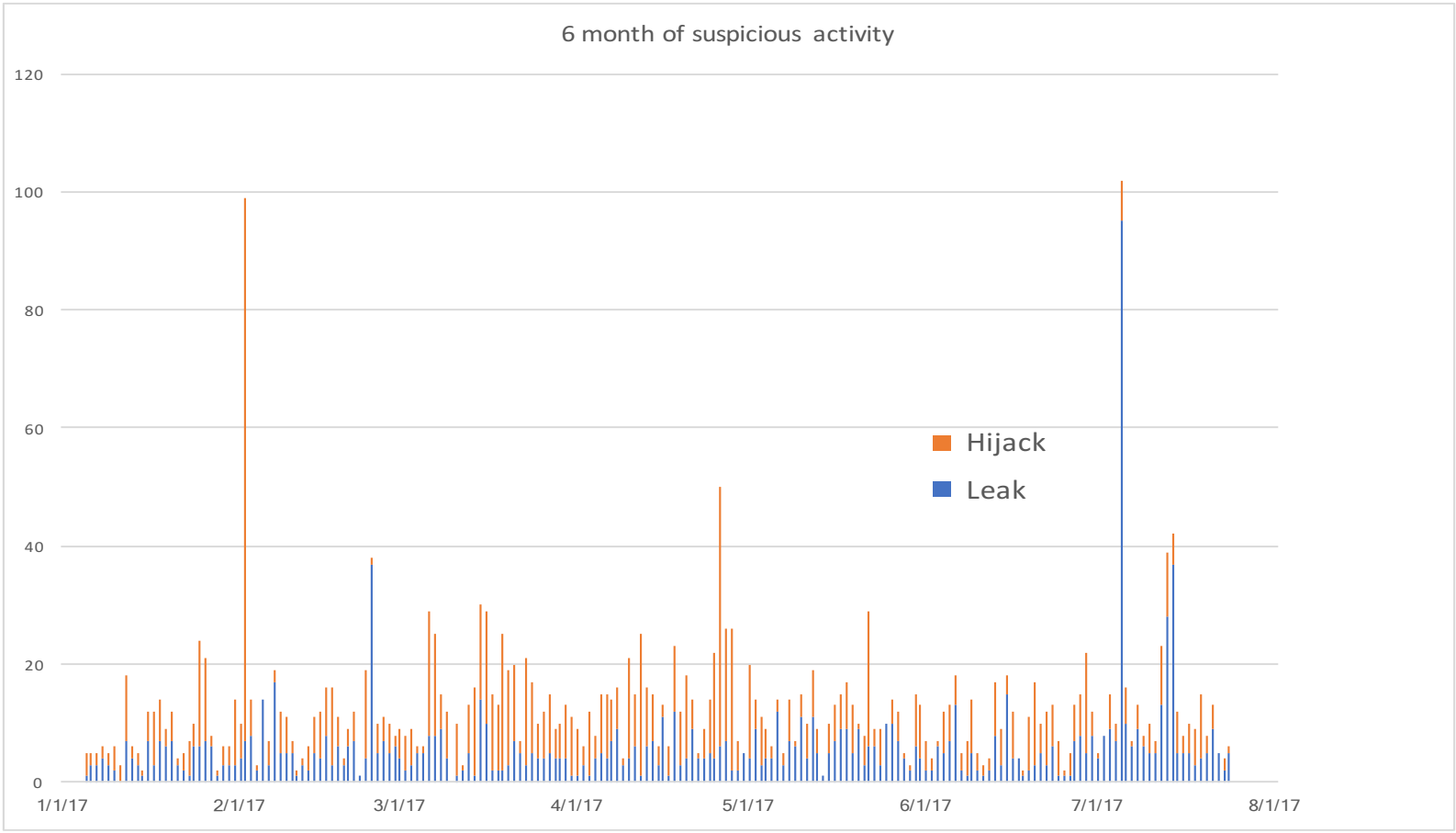
A Internet funciona com base na **Cooperação entre Sistemas Autônomos**

- A Internet é uma **'rede de redes'**
- São quase **60.000 redes diferentes**, sob gestões técnicas e administrativas diferentes.
- A estrutura de **roteamento BGP** funciona com base em cooperação e confiança.

O BGP não tem
Validação para os dados



Segurança e estabilidade da Internet
Nenhum dia sem um incidente



http://bgpstream.com/

Segurança e estabilidade da Internet
Problemas de segurança

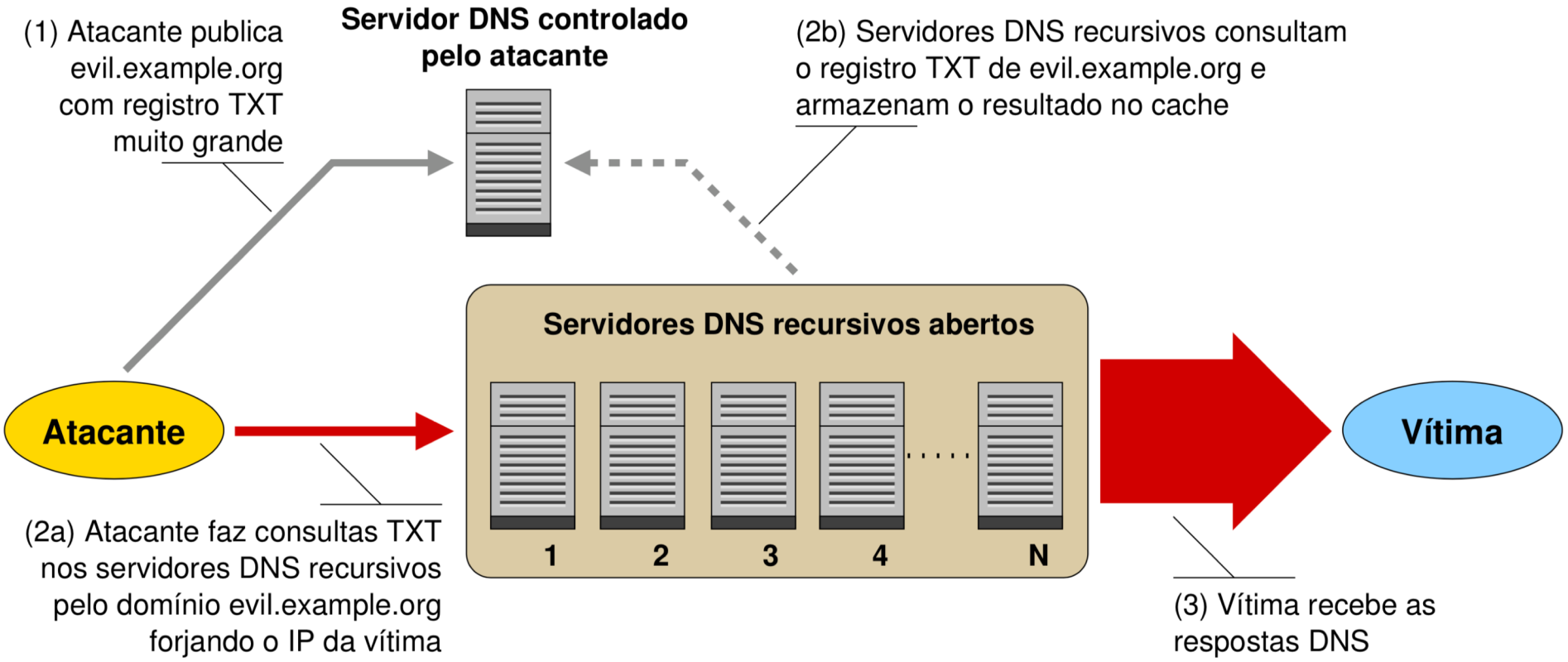
- CERT.br afirma que em 2016 **300Gbps foi o novo 'normal'** em ataques DDOS, ataques até 1Tbps reportados
- Tentativas de invasão por **força bruta**: telnet (23), ssh (22), outras (2323, 23231, 2222)
- Busca por protocolos que permitem **amplificação:**
  - UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, QuotD, mDNS, LDAP

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

	DNS		SNMP		NTP		SSDP	
month	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
2017-08	2.347	72.677	2.018	554.457	872	108.168	891	27.209
2017-09	2.307	62.283	1.791	406.015	800	89.603	-	-
2017-10	2.328	67.066	1.886	343.674	845	108.605	902	32.056
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

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

Segurança e estabilidade da Internet
Problemas de segurança



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.**

Segurança e estabilidade da Internet
MANRS

1. Garantir que **seus anúncios BGP** sejam anúncios **dos seus blocos IP e dos blocos de seus clientes**

- **Como? Definição de 'políticas'** (saber e divulgar o que vai exportar e importar) **e filtros** (para verificar e forçar as 'políticas') **no BGP**

2. Garantir que os **IPs de origem** dos pacotes que **saem da sua rede não sejam falsificados**

- **Como? Implantando antispoofing** (ver bcp.nic.br)

3. Garantir que seus **contatos estejam atualizados** e sejam acessíveis por terceiros

- **Como? Atualizando o whois do Registro.br** (www.registro.br), IRRs, PeeringDB, etc
- **Como? Usando o INOC-DBA-br** (inoc.nic.br)

Segurança e estabilidade da Internet
MANRS

- **Estamos juntos nisso!**
- Os operadores de rede têm **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/manrs

Outras
Recomendações

- 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.
  - Acompanhe com atenção, contribua, utilize...

- O SIMET realiza também testes relacionados à segurança:
  - BCP38 (antispoofing)
  - Gerência da Porta 25

- O provedor pode utilizar o SIMETBox, ou incentivar os usuários a utilizarem o SIMET Móvel (Android/iOS) ou SIMET Web
  - Acesso aos dados dos testes
  - Mapa de qualidade

Outras
Recomendações

- 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).
  - Cuidado com o NTP porque muitos clientes usam a porta 123 UDP também como porta de origem, recebendo respostas nessa porta
  - Para gerência de rede, permitir apenas blocos de redes de gerência da própria operadora.

Hardening

Autenticação

- Um usuário para cada funcionário
  - Não deixe os funcionários usarem uma mesma conta padrão no acesso aos sistemas.
  - Contas padrão podem ser utilizadas para backups e emergências
- Use senhas fortes
  - Verifique as recomendações do CERT.br
- Armazene suas senhas criptografadas
  - Nunca em texto puro
- Use autenticação em 2 fatores
  - Coisas que sei (senha) / coisas que sou (biometria) / coisas que possuo (chave)

Hardening

Autorização

- Cada usuário deve ter permissões no equipamento adequadas ao trabalho que realiza
  - Não forneça acesso de administrador para todos
  - Pode-se usar grupos para facilitar a atribuição de privilégios
  - Em alguns sistemas é possível escalar privilégios

Hardening

Auditoria

- Manter um **registro de cada usuário com suas respectivas permissões**
- **Registrar as ações** de cada usuário no sistema
- Diferenciar **níveis de criticidade**: informativo, aviso, critico
- Tipos de Registros: documentos, logs, backups de configurações
- Data e Hora certas usando NTP (atenção também aos fusos horários)

Hardening
Acesso

- Usar apenas protocolos seguros
  - Se houver protocolos inseguros habilitados, desative-os (telnet, ftp, http, winbox)
  - Se o protocolo inseguro for o único meio de acesso ao dispositivo, restrinja o alcance via uma rede de gerência apartada e protegida
  - Exemplos de protocolos seguros: ssh, https, sftp, winbox (secure mode)
- Adicione uma mensagem de login
  - “Roteador pertencente a empresa X, acessos não autorizados serão monitorados, investigados e entregues às autoridades responsáveis”
- Armazene logs para auditoria: ações, tentativas de acesso
- Force o logout depois de um tempo de inatividade ou se desconectar o cabo
- Use Port Knocking se possível

Hardening
Sistema

- Desative as interfaces não utilizadas
- Desative serviços não usados, inseguros, e que podem ser utilizados para amplificação
  - Testador de banda
  - DNS recursivo
  - Servidor NTP
- Remova ou desative pacotes com funções extras não utilizadas
  - Ex.: pacote wireless.
- Desabilite protocolos de descoberta de vizinhança
  - Ex.: CDP, MNDP, LLDP
- Mantenha o sistema e pacotes atualizados, na versão estável. Aplique todos os patches de segurança.

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.

Obrigado

www.nic.br

moreiras@nic.br