Boas Práticas de Segurança

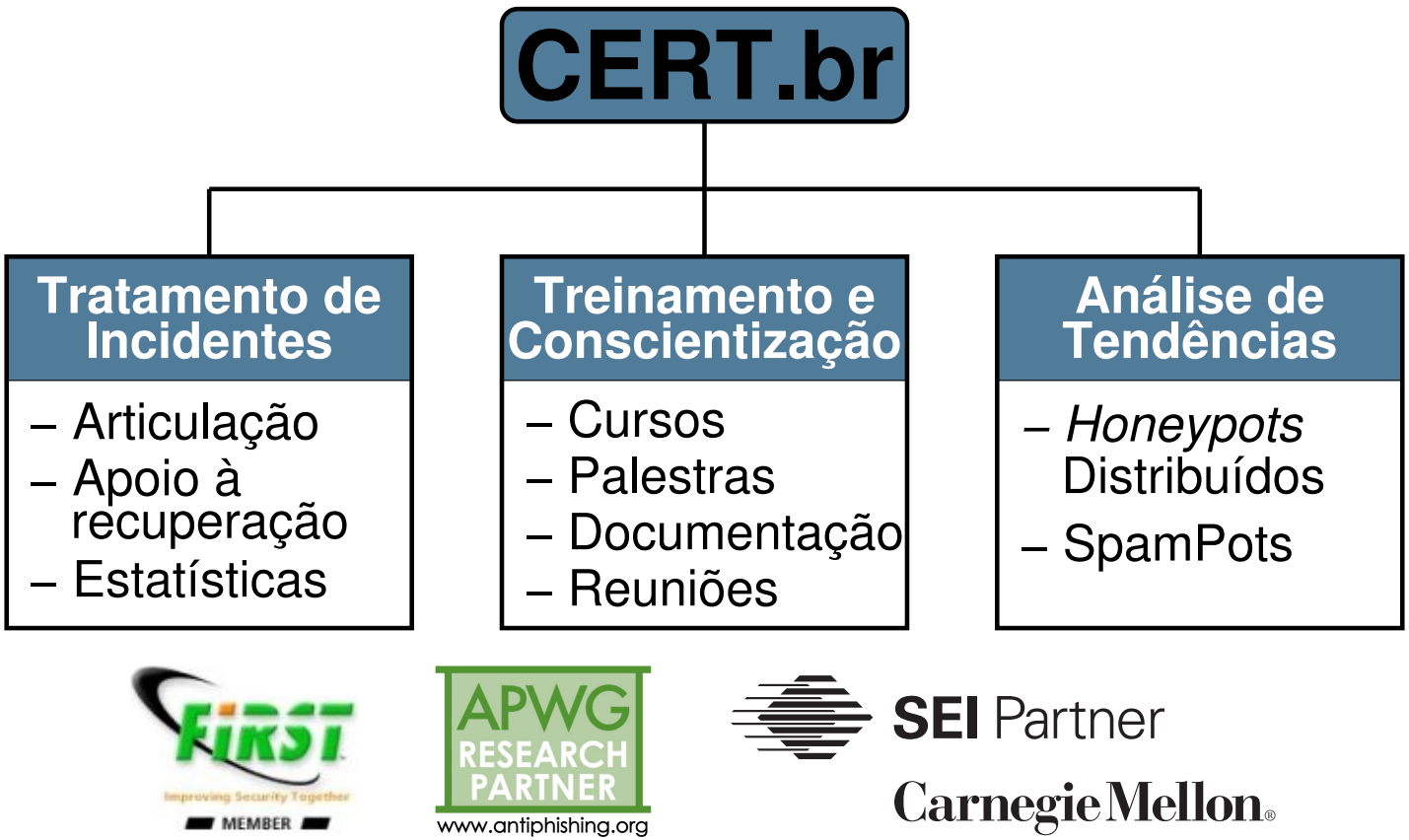
Luiz Eduardo Roncato Cordeiro
cordeiro@cert.br

Esta Apresentação:
http://www.cert.br/docs/palestras/

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto br
Comitê Gestor da Internet no Brasil

Sobre o CERT.br

Criado em 1997 como ponto focal nacional para tratar incidentes de segurançaa relacionados com as redes conectadas à Internet no Brasil



http://www.cert.br/sobre/

Estrutura do CGI.br

01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério do Planejamento, Orçamento e Gestão
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério da Defesa
07- Agência Nacional de Telecomunicações
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas**

Motivação

Objetivos da implementação de boas práticas:

- Reduzir o desperdício de recursos
- Não ser origem de ataques
- Prover um serviço de maior qualidade
- Colaborar para o aumento da segurança da Internet

Não será possível erradicar todos os problemas, precisamos torná-los gerenciáveis

- cada setor precisa fazer a sua parte – cooperação para a solução dos problemas
- a solução não virá de uma ação única

Agenda

Ataques mais Frequentes
    Prevenção e Mitigação

Estruturação e Atuação das Áreas de Segurança

Considerações Finais

Referências

Ataques mais Frequentes e Recomendações para Prevenção e Mitigação

Ataques mais Frequentes

Reportados ao CERT.br no ano de 2010

Ataques mais Frequentes

- de força bruta
  - SSH, FTP, Telnet, VNC, etc
- com contínuo crescimento nos últimos meses:
  - ataques a aplicações Web vulneráveis
  - servidores SIP
- a usuários finais
  - fraudes, *bots*, *spyware*, etc
  - motivação financeira
  - abuso de *proxies*, na maioria instalados por *bots*

Ataques de Força Bruta

Serviço SSH

- Ampla utilização em servidores UNIX
- Alvos
  - senhas fracas
  - contas temporárias
- Pouca monitoração permite que o ataque perdure por horas ou dias

Outros serviços

- FTP
- TELNET
- Radmin
- VNC

Mitigação de Força Bruta SSH

Recomendações:

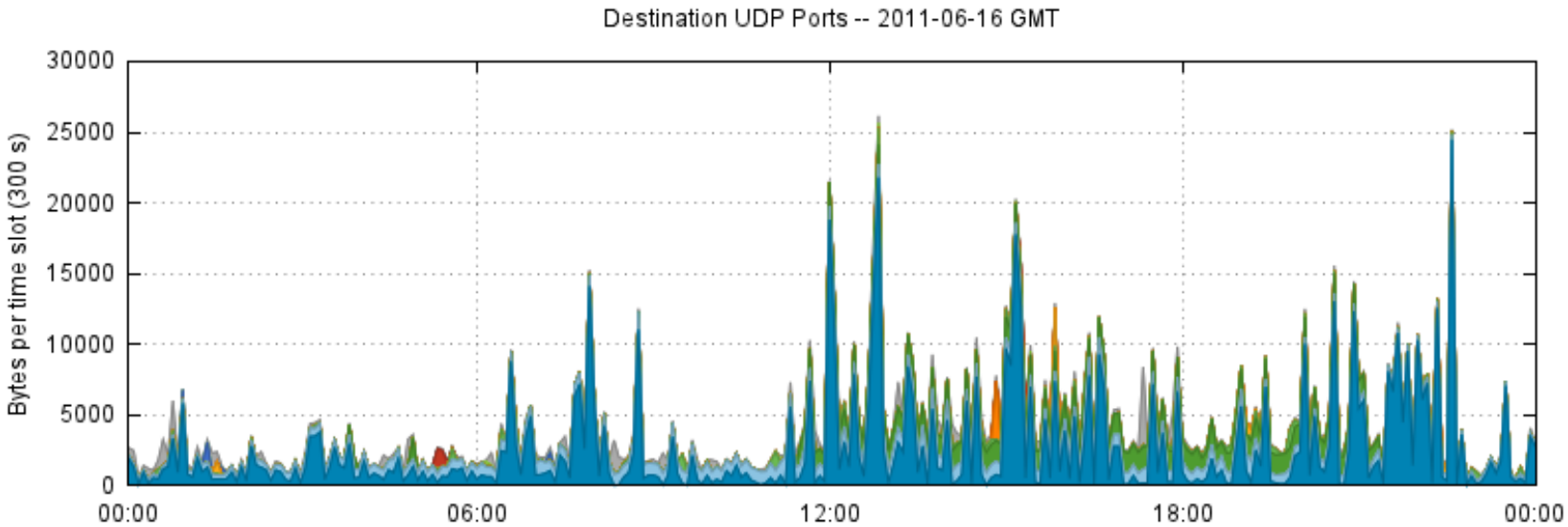
- Senhas fortes
- Redução no número de equipamentos com serviço aberto para Internet
- Filtragem de origem
- Mover o serviço para uma porta não padrão
- Acesso somente via chaves públicas
- Aumento na monitoração

Detalhes em: http://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/

Ataques a Servidores SIP

- Varreduras por dispositivos SIP
- Identificação de ramais válidos
- Tentativas de quebra de senhas de ramais
- Tentativas de realizar ligações
- spit?

Varreduras SIP no Consórcio de Honeypots



#	Key	Port	Name	Total		Max	Avg
01		5060	SIP (Session Initiation Protocol)	715.57 KB	58.10 %	81.53 B/s	8.28 B/s
02		53	DNS (Domain Name System)	206.11 KB	16.74 %	6.52 B/s	2.39 B/s
03		161	SNMP (Simple Network Management Protocol)	169.15 KB	13.73 %	6.03 B/s	1.96 B/s
04		137	NETBIOS Name Service	32.21 KB	2.62 %	4.70 B/s	0.37 B/s

SIP: REGISTER

```
2010-10-20 05:57:55 IP: 211.103.141.180, method: REGISTER,
from: "123", to: "123", CSeq: "1 REGISTER", user-agent: "friendly-scanner"

[...] from: "1234", to: "1234", [...]
[...] from: "12345", to: "12345", [...]
[...] from: "123456", to: "123456", [...]
[...] from: "sip", to: "sip", [...]
[...] from: "admin", to: "admin", [...]
[...] from: "pass", to: "pass", [...]
[...] from: "password", to: "password", [...]
[...] from: "testing", to: "testing", [...]
[...] from: "guest", to: "guest", [...]
[...] from: "voip", to: "voip", [...]
[...] from: "account", to: "account", [...]
[...] from: "passwd", to: "passwd", [...]
[...] from: "qwerty", to: "qwerty", [...]
[...] from: "654321", to: "654321", [...]
[...] from: "54321", to: "54321", [...]
[...] from: "4321", to: "4321", [...]
[...] from: "abc123", to: "abc123", [...]
[...] from: "123abc", to: "123abc", [...]
```

Mitigação de Ataques SIP

Recomendações:

- Senhas fortes
- Redução no número de equipamentos com serviço aberto para Internet
- Filtragem de origem
- Aumento na monitoração
- Leituras recomendadas
  - Asterisk: `README-SERIOUSLY.bestpractices.txt`
  - *Seven Steps to Better SIP Security*: http://blogs.digium.com/2009/03/28/sip-security/
  - *Asterisk VoIP Security (webinar)*: http://www.asterisk.org/security/webinar/

Tentativas de Fraude Financeira

- *Spams* em nome de diversas entidades/temas variados
  - *links* para cavalos de tróia hospedados em diversos *sites*
  - vítima raramente associa o *spam* com a fraude financeira
- Páginas falsas estão voltando a ter números significativos
  - *drive-by downloads* sendo usados intensamente no Brasil
    - via JavaScript, ActiveX, etc, inclusive em grandes *sites*
  - em conjunto com *malware* modificando:
    - arquivo *hosts*
    - configuração de *proxy* em navegadores (arquivos PAC)
- *Malware* se registrando como *Browser Helper Objects* (BHO) em navegadores
- *Malware* validando, no *site* real, os dados capturados

Uso de *botnets* para DDoS

- 20 PCs domésticos abusando de Servidores DNS Recursivos Abertos podem gerar 1Gbps
- Em 2010 foi atingida a marca de 100Gbps
  - aumento de 102% em relação a 2009
  - 1000% desde 2005
  - em média ocorrem 3 ataques de 1Gpbs por dia na Internet
- De 2% a 3% do tráfego de um grande backbone é ruído de DDoS
- Extorsão é o principal objetivo
  - mas *download* de outros *malwares*, *spam* e furto de informações também valem dinheiro e acabam sendo parte do payload dos *bots*

Fonte: *Global Botnet Underground: DDoS and Botconomics*
Jose Nazario, Ph.D., Head of Arbor ASERT
Keynote do Evento RioInfo 2009.

Fonte: *Worldwide Infrastructure Security Report*
2010 Report, ARBOR Network

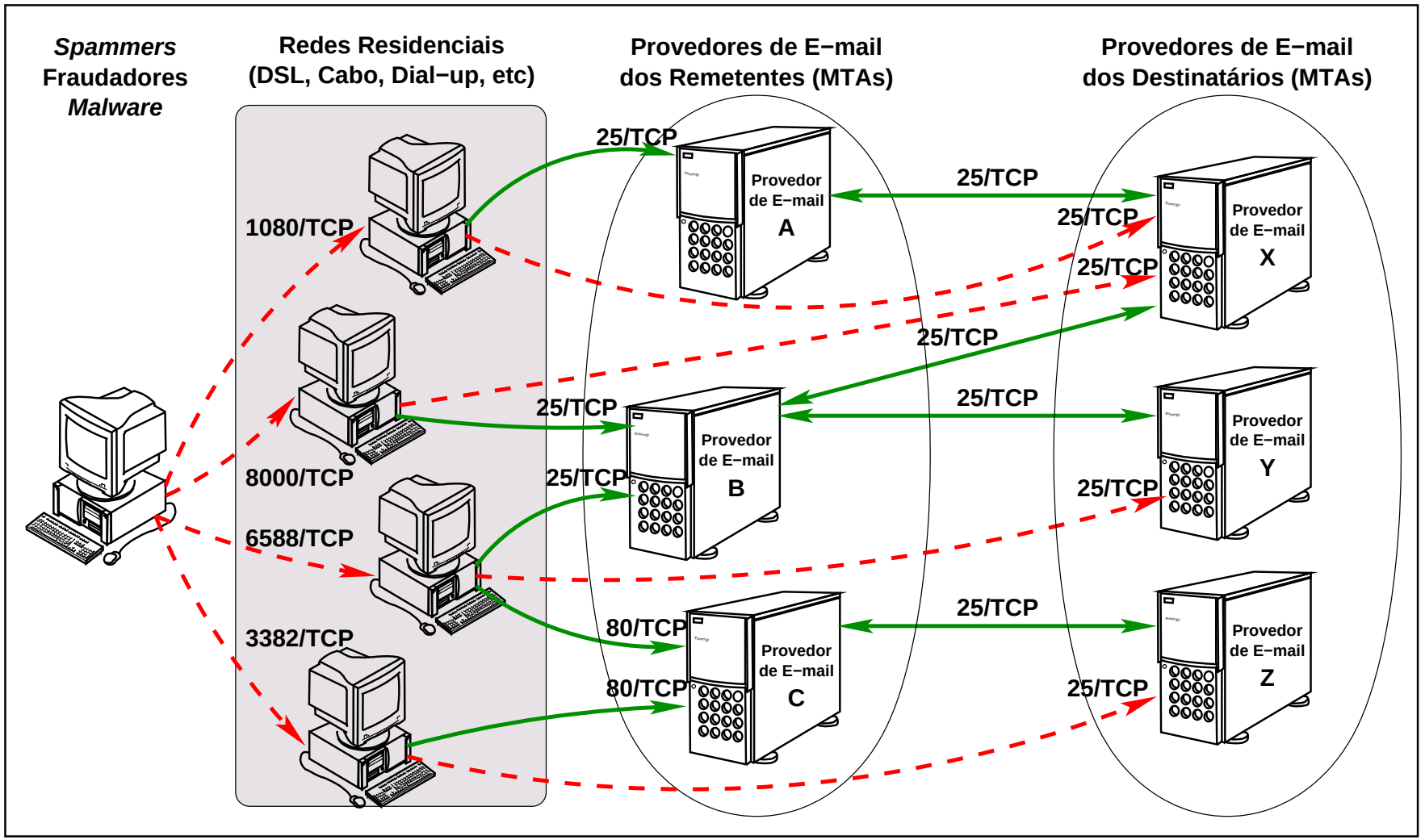
Brasil na CBL

	País	Endereços IP	% do Total	Taxa de Infecção (%)
1	Índia (IN)	1.503.169	16,47	5,609
2	Brasil (BR)	737.421	8,08	1,334
3	Alemanha (DE)	588.689	6,45	0,547
4	Vietnã (VN)	584.421	6,40	3,576
5	Rússia (RU)	443.737	4,86	1,172
6	Indonésia (ID)	405.342	4,44	3,639
7	Paquistão (PK)	359.352	3,94	8,555
8	Itália (IT)	269.670	2,95	0,595
9	Ucrânia (UA)	199.703	2,19	1,942
10	Arábia Saudita (SA)	197.834	2,17	3,374

Fonte: CBL, uma lista de endereços IP de computadores que comprovadamente enviaram *spams* nas últimas 24 horas e estavam infectados.

Dados gerados em: `Wed Jun 8 17:21:49 2011 UTC/GMT`
Composite Blocking List `http://cbl.abuseat.org/`

Abuso de Máquinas Infectadas para Envio de Spam



Mitigação do Abuso das Máquinas de Usuários

- definição de políticas de uso aceitável;
- monitoração proativa de fluxos;
- monitoração das notificações de abusos;
- ação efetiva junto ao usuário nos casos de detecção de *proxy* aberto ou máquina comprometida;
- *egress filtering*;
- gerência de saída de tráfego com destino à porta 25/TCP.

Gerência de Porta 25

Diferenciar a submissão de *e-mails* do cliente para o servidor, da transmissão de *e-mails* entre servidores.

Implementação depende da aplicação de medidas por provedores e operadoras:

- Provedores de serviços de correio eletrônico:
  - Implementar o padrão de *Message Submission*, tipicamente na porta 587/TCP (RFC 4409), e implementar SMTP autenticado
- Operadoras de banda larga/*dial up* de perfil residencial (usuário final):
  - Impedir envio direto de mensagens eletrônicas (através da filtragem da saída de tráfego com destino à porta 25/TCP)

Detalhes em: http://www.antispam.br/admin/porta25/

Benefícios da Gerência de Porta 25

- Saída de listas de bloqueio
- Diminuição de reclamações de usuários
- Dificulta o abuso da infra-estrutura da Internet para atividades ilícitas (fraudes, furto de dados, etc)
- Aumento de rastreabilidade em caso de abuso
- Atua na submissão, antes da mensagem entrar na infra-estrutura de *e-mail*
- Diminuição do consumo de banda por *spammers*
- Diminuição de custos operacionais
  - spam foi o mais apontado como responsável pela demanda de recursos operacionais no "*2008 Worldwide Infrastructure Security Report*"

    http://www.arbornetworks.com/report

Outras Recomendações

Prevenção de DNS *Cache Poisoning*

- Instalar as últimas versões dos *softwares* DNS
  - Correções usam portas de origem aleatórias nas consultas
  - Não eliminam o ataque, apenas retardam seu sucesso
- Adoção de DNSSEC é uma solução mais definitiva
  http://registro.br/suporte/tutoriais/dnssec.html

Correção de DNS Recursivo Aberto

Duas possíveis soluções:

- Colocar os servidores DNS em computadores diferentes, com configurações e políticas de acesso diferentes; ou
  - única solução possível para o Microsoft DNS
- Utilizar o conceito de *views* do BIND

Detalhes em: http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Cuidados com o uso de IPv6 (1/2)

- Regras de filtragem em *firewall* são diferentes
  - não assumir que as regras utilizadas para IPv4 funcionam em IPv6
  - verificar se as regras funcionam em IPv6
  - Roteiro do laboratório de firewall
    http://www.ipv6.br/pub/IPV6/MenuIPv6CursoPresencial/roteiro-lab-firewall.pdf
- Túneis IPv6 podem não estar sendo filtrados
  - túneis: *Teredo*, *HE*, *Sixxs*, etc
  - com o túnel implementado pode haver conexões entrantes
- Windows (a partir do Vista) cria túneis automaticamente
  - pode haver tráfego IPv6 em sua rede hoje sem que seja notado

Cuidados com o uso de IPv6 (2/2)

- ICMPv6 é importante para o funcionamento do protocolo
  - RFC4890:
    Recommendations for Filtering ICMPv6 Messages in Firewalls

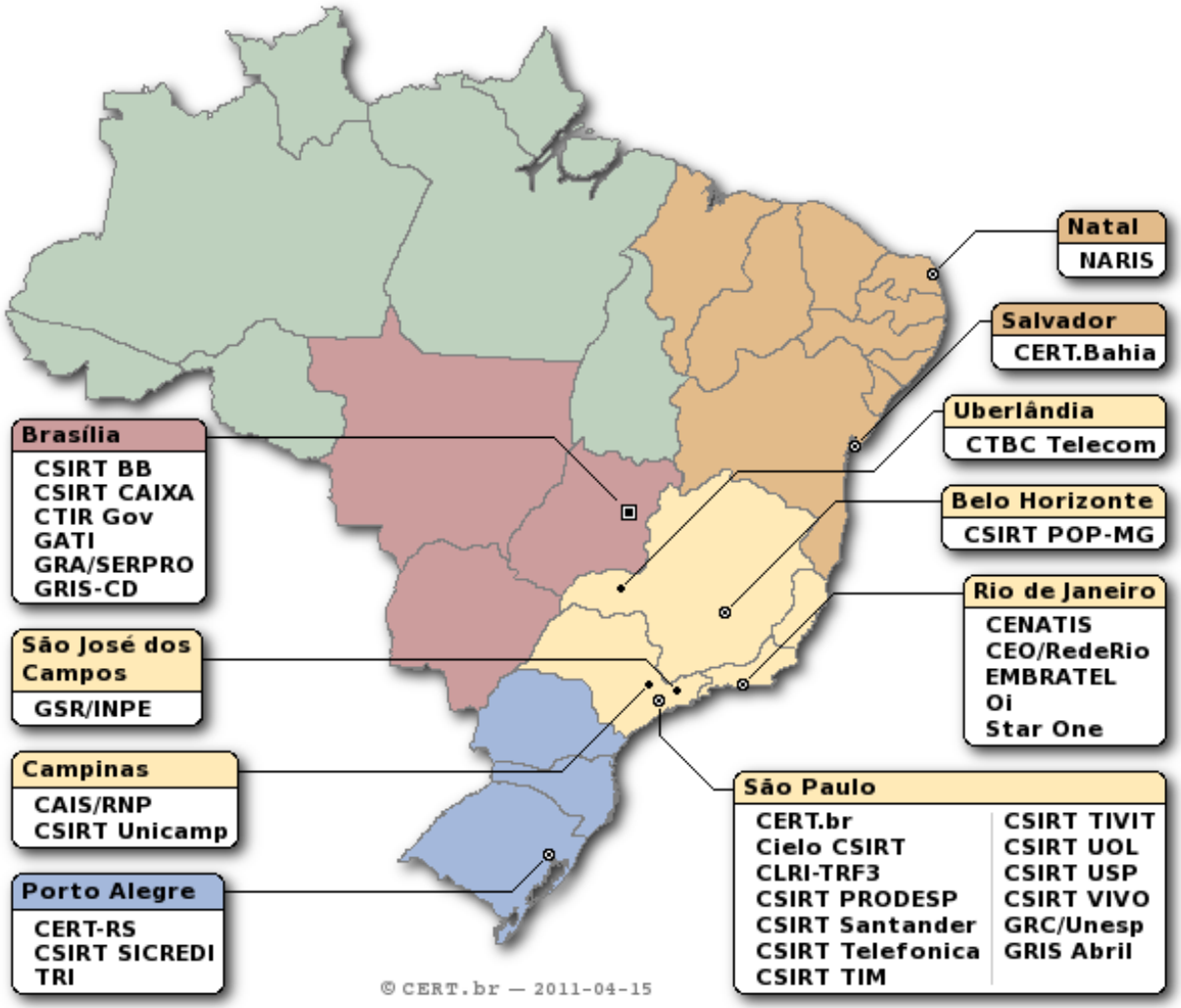
- Tutorial: Seguridad IPv6
  http://www.gont.com.ar/talks/lacnicxv/
  fgont-lacnicxv-tutorial-seguridad-ipv6.pdf

- Security Assessment of Neighbor Discovery for IPv6
  http://www.gont.com.ar/talks/lacsec2011/
  fgont-lacsec2011-nd-security.pdf

Acompanhamento de Notificações

- Criar *e-mails* da RFC 2142 (`security@`, `abuse@`)
- Manter os contatos de Whois atualizados
- O contato técnico deve ser um profissional que tenha contato com as equipes de abuso
  - ou, ao menos, saber para onde redirecionar notificações e reclamações
- Redes com grupos de resposta a incidentes de segurança devem anunciar o endereço do grupo junto à comunidade
- As contas que recebem notificações de incidentes ou abusos não podem barrar mensagens
  - antivírus podem impedir uma notificação de *malware*
  - regras anti-spam podem impedir notificações de *spam* e de *phishing*

Criar um Grupo de Tratamento de Incidentes



http://www.cert.br/csirts/brasil/

"Um CSIRT provê serviços de suporte para prevenção, tratamento e resposta a incidentes de segurança em computadores."

Papel dos CSIRTs

- A redução do impacto de um incidente é consequência da:
  - agilidade de resposta
  - redução no número de vítimas
- O sucesso depende da confiabilidade
  - nunca divulgar dados sensíveis nem expor vítimas, por exemplo
- O papel do CSIRT e dos profissionais de segurança é:
  - auxiliar a proteção da infra-estrutura e das informações
  - prevenir incidentes e conscientizar sobre os problemas
  - responder incidentes – retornar o ambiente ao estado de produção
- A pessoa que responde um incidente é a primeira a entrar em contato com as evidências de um possível crime
  - seguir as políticas
  - preservar as evidências

Considerações Finais

Considerações Finais

- Monitore o tráfego de saída de sua rede
- Tenha um ponto de contato para assuntos de segurança e abuso
  - atue e dê algum tipo de resposta a quem entrou em contato
- Mantenha-se informado
  - listas dos fabricantes de *software*
  - *sites*, blogs e listas de segurança
- Cada um é responsável por uma parte da segurança da Internet

Referências

- Esta Apresentação:
  http://www.cert.br/docs/palestras/
- CERT.br
  http://www.cert.br/
- NIC.br
  http://www.nic.br/
- CGI.br
  http://www.cgi.br/