Segurança da Internet no Brasil e Recomendações do CERT.br

Cristine Hoepers

cristine@cert.br

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

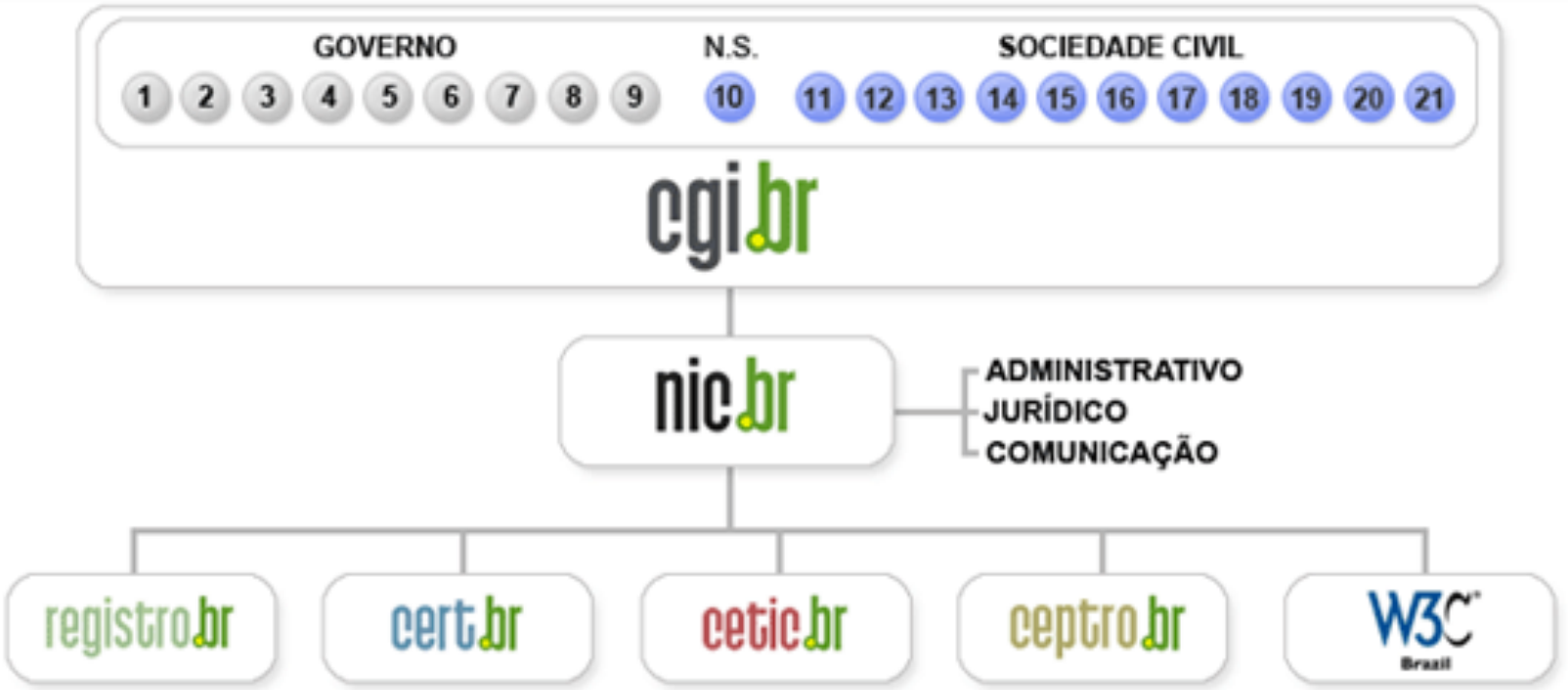
Comitê Gestor da Internet no Brasil – CGI.br

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, 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.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

http://www.cgi.br/sobre-cg/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet
11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

CERT.br

Tratamento de Incidentes

- Articulação
- Apoio à recuperação
- Estatísticas

Treinamento e Conscientização

- Cursos
- Palestras
- Documentação
- Reuniões

Análise de Tendências

- *Honeypots* Distribuídos
- SpamPots

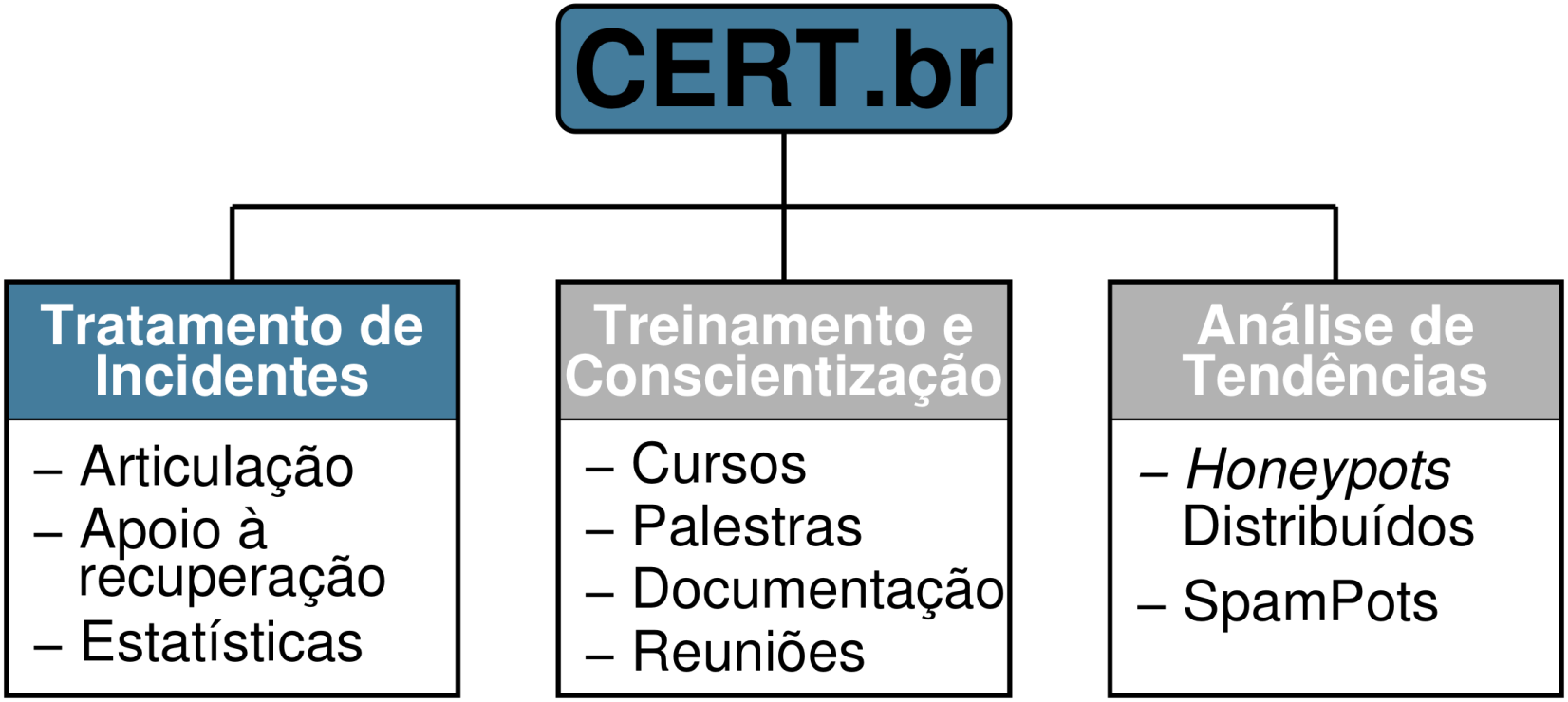
SEIPartner CERT Courses

FIRST Improving Security Together MEMBER

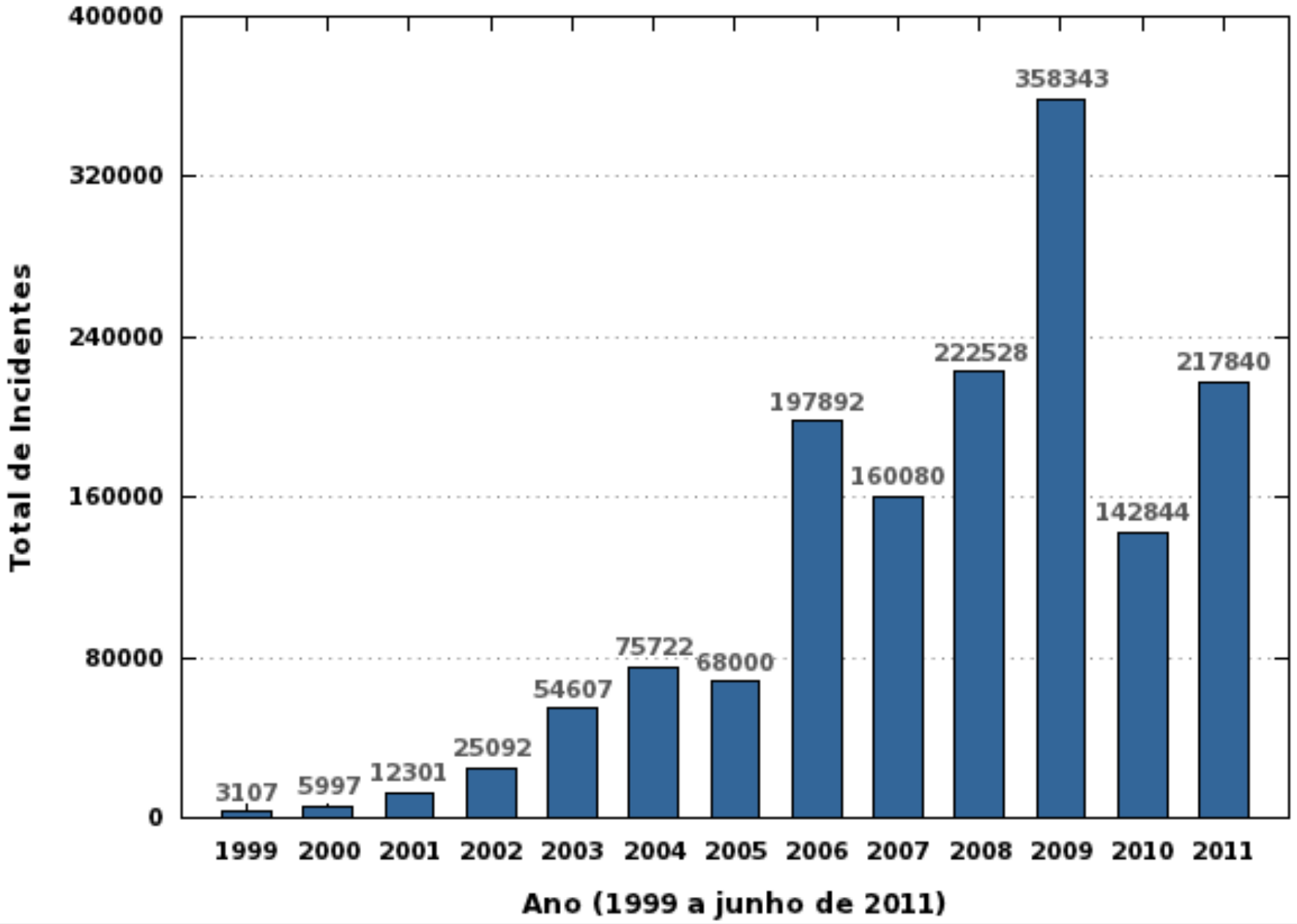
APWG RESEARCH PARTNER www.antiphishing.org

Criado em 1997 para:

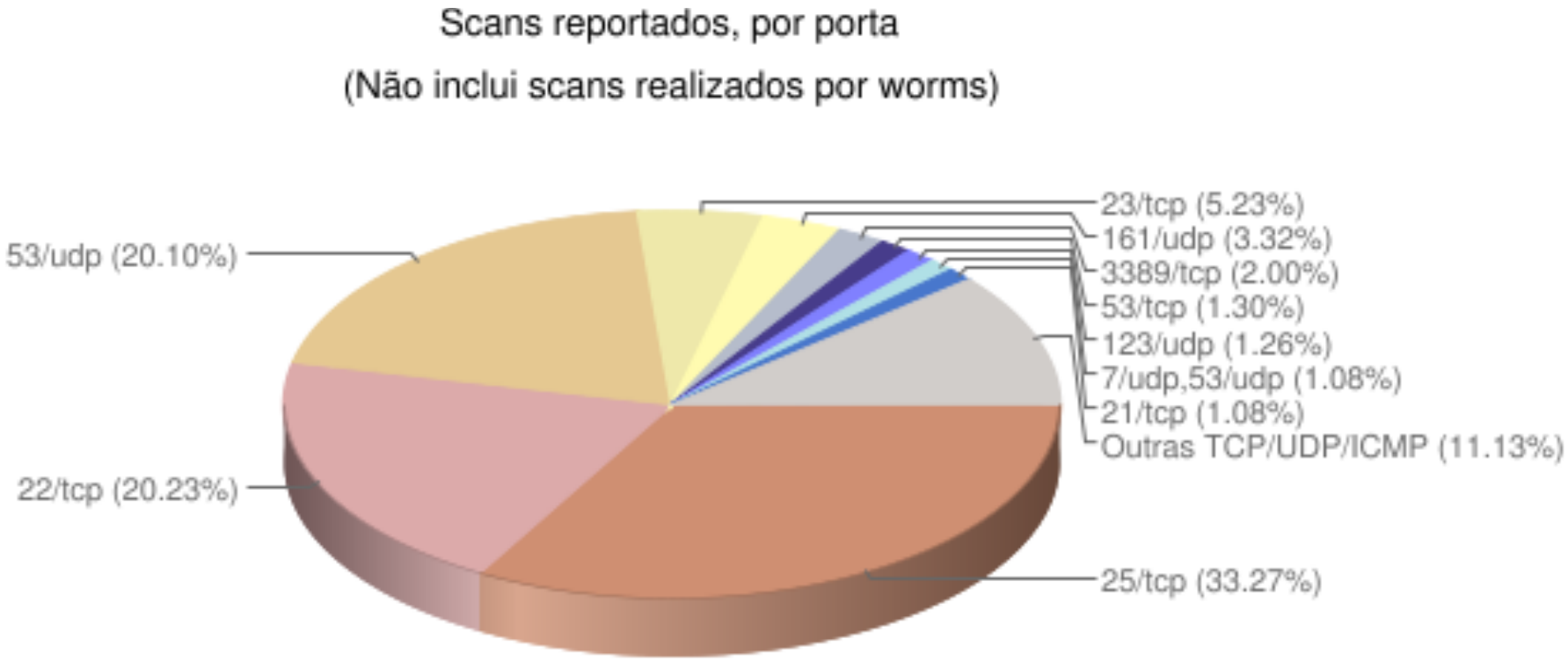
- **Ser um ponto de contato nacional para notificação de incidentes de segurança**
- **Prover a coordenação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades, como os operadores da justiça, provedores de acesso e serviços e backbones**
- **Auxiliar novos CSIRTs a estabelecerem suas atividades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**


CERT.br
Tratamento de Incidentes
– Articulação
– Apoio à recuperação
– Estatísticas
Treinamento e Conscientização
– Cursos
– Palestras
– Documentação
– Reuniões
Análise de Tendências
– *Honeypots* Distribuídos
– SpamPots

Incidentes reportados ao CERT.br por ano

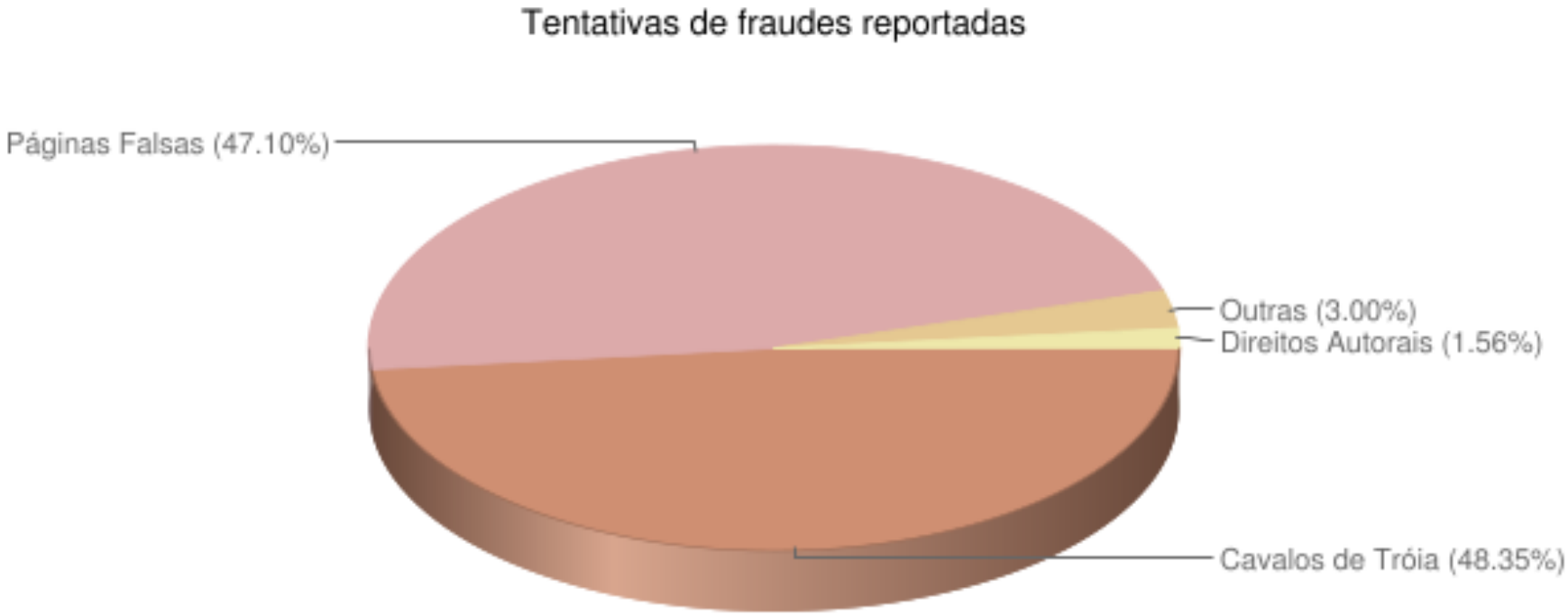


Varreduras Mais Frequentes – 2º Trim/2011



- **Força bruta:**
  - **SSH, TELNET, FTP, VNC, etc**
  - **Alvos:**
    - **senhas fracas, senhas padrão, contas temporárias**
  - **Pouca monitoração permite ao ataque perdurar por horas/dias**
- **Serviço DNS**

Tentativas de Fraude Reportadas – 2º Trim/2011



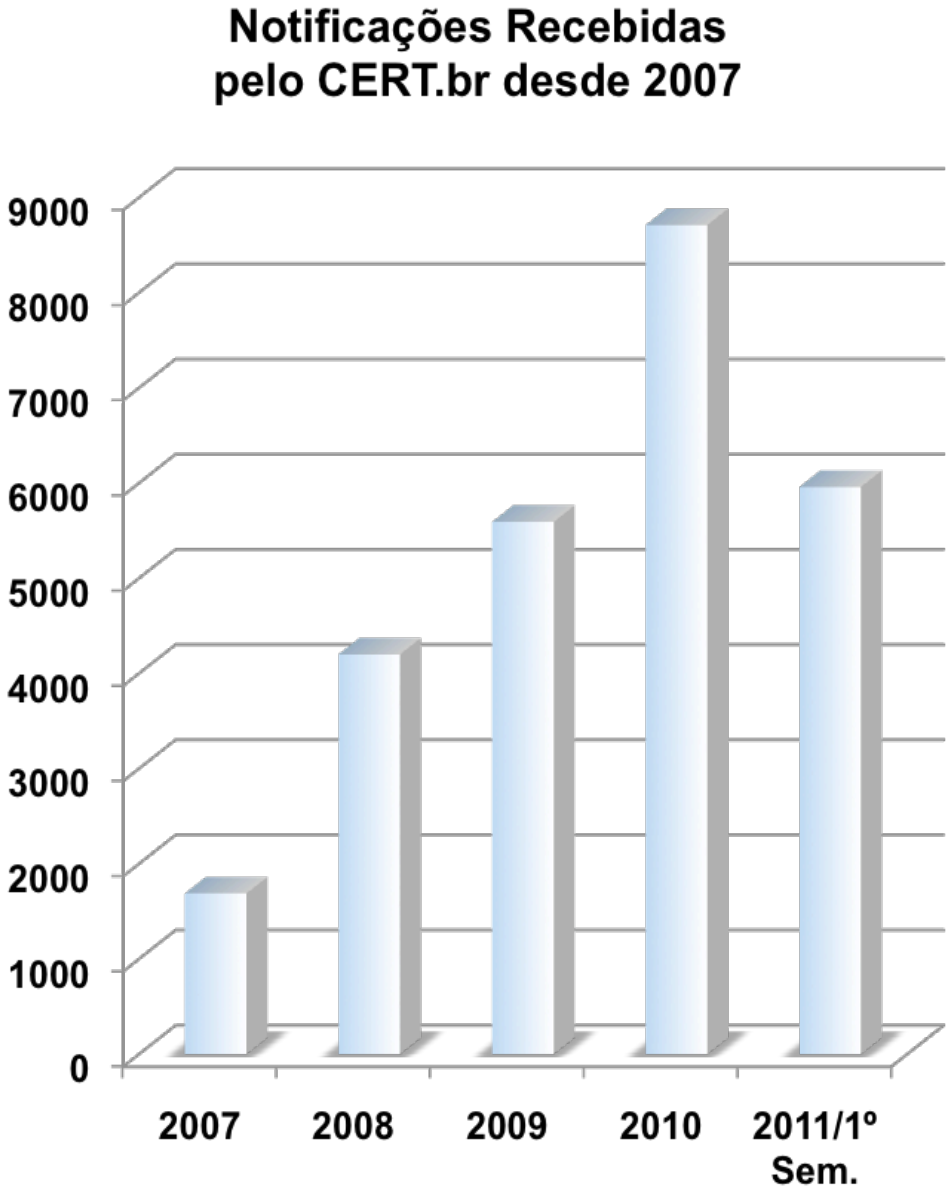
- ***Spams*** **em nome de diversas entidades/temas variados**
  - ***Links*** **para** ***trojans*** **hospedados em diversos** ***sites***
  - **Vítima raramente associa o** ***spam*** **com a fraude**
- **Retorno de páginas falsas**
  - **via** ***spams*** **em nome das instituições financeiras e/ou de comércio eletrônico**
  - **muitas envolvem alteração do arquivo hosts das máquinas**

Tentativas de fraudes reportadas (cont.)

- *Drive-by downloads* intensamente utilizados
  - Via JavaScript, ActiveX, etc, inclusive em grandes *sites*
  - Em conjunto com *malware* modificando:
    - arquivo *hosts*
    - configuração de *proxy* em navegadores (arquivos PAC)
- *Links* patrocinados
- *Malware* para:
  - *Smartphones*
  - Via redes sociais
    - explorando a confiança de seguidores
    - grande uso de *links* curtos
- Furtam diversos tipos de credenciais
  - E-mail, Redes Sociais Windows Live, *login* de consulta ao Serasa
  - Exploram confiança para propagação e vendem serviços

Ataques a servidores *Web*

- A maioria das quebras de segurança nos serviços da "Web 2.0" são por falhas de programação
  - falta de validação de entrada
  - falta de checagem de erros
- Muitas vulnerabilidades de *Software*
  - uso de pacotes prontos
  - falta de atualização dos sistemas e dos pacotes



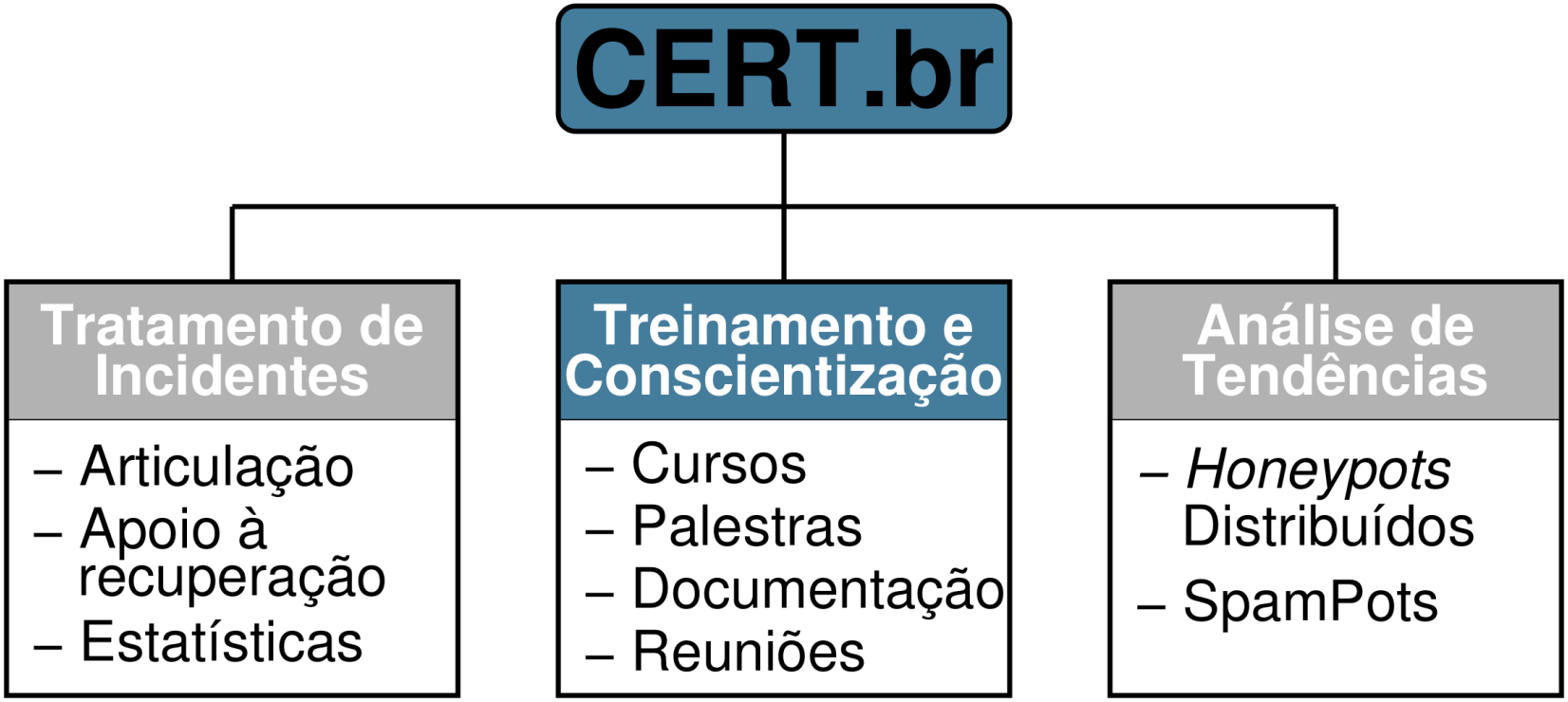
Uso de Botnets

- **Uma base muito grande de computadores com *software* desatualizado/vulnerável sendo ativamente abusada por criminosos**
  - **Especialmente em países em desenvolvimento**
- **Uso de *botnets:***
  - **DDoS**
  - **Extorsão**
  - ***Download* de outros tipos de *malware***
  - **Furto de informações**
  - **Proxies abertos**
    - **envio de *spam***
    - ***navegação anônima***

Uso de *botnets* para DDoS

- **20 PCs domésticos abusando de Servidores DNS Recursivos Abertos podem gerar 1Gbps**
  - **No Brasil temos mais de 13.000 recursivos abertos no momento**
    (Dados do *Measurement Factory* passados ao CERT.br semanalmente)
- **Em março de 2009 foram atingidos picos de 48Gbps**
  - **em média ocorrem 3 ataques de 1Gbps 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**


CERT.br
Tratamento de Incidentes
– Articulação
– Apoio à recuperação
– Estatísticas
Treinamento e Conscientização
– Cursos
– Palestras
– Documentação
– Reuniões
Análise de Tendências
– Honeypots Distribuídos
– SpamPots

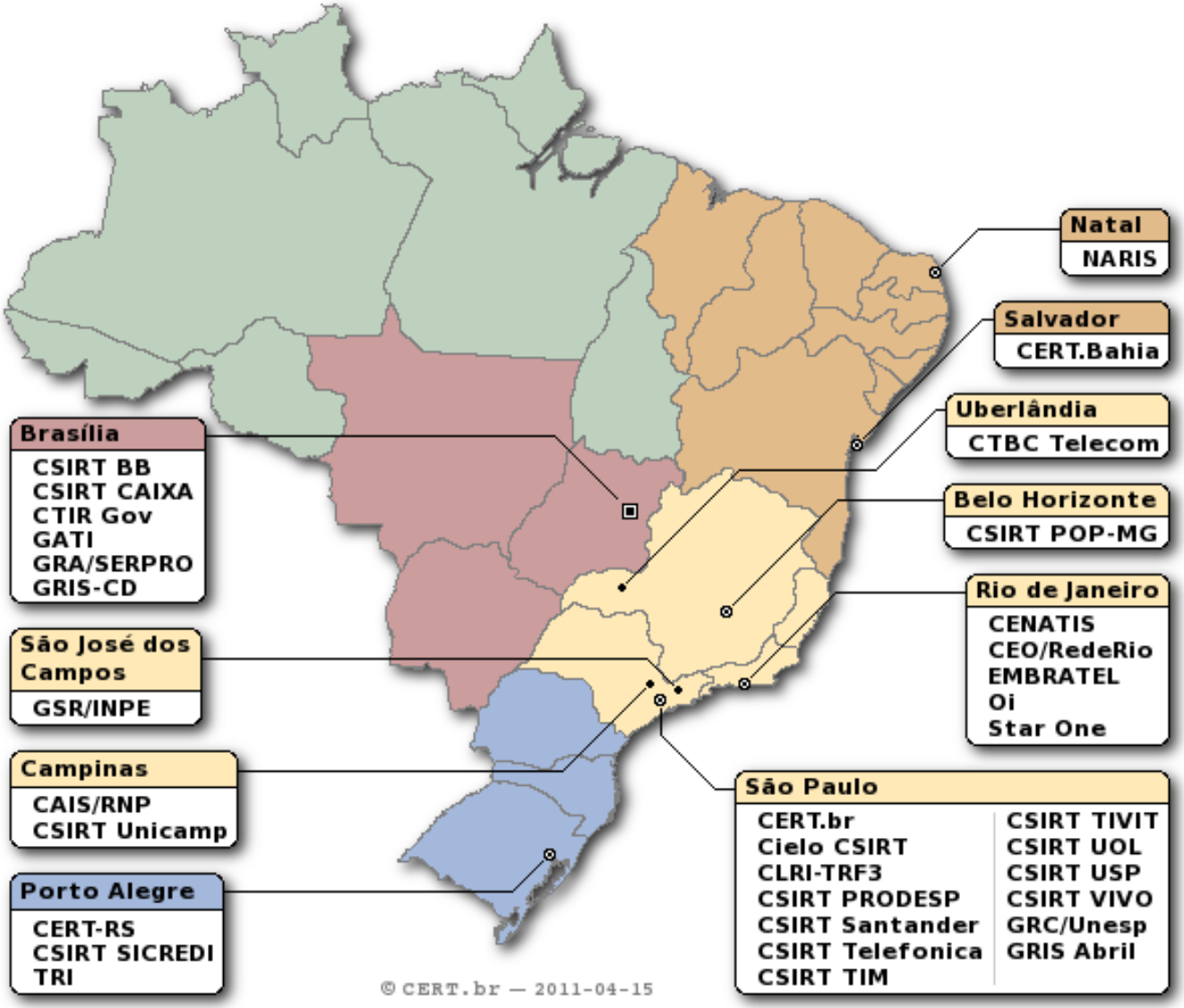
Apoio e Treinamento para Novos CSIRTs

- **Auxílio no estabelecimento das atividades**
  - **Reuniões, palestras, treinamentos, etc**
- ***SEI/CMU Partner* desde 2004, licenciado para ministrar os cursos do *CERT® Program* no Brasil:**
  - **http://www.cert.br/cursos/**
    - ***Overview of Creating and Managing CSIRTs***
    - ***Fundamentals of Incident Handling***
    - ***Advanced Incident Handling for Technical Staff***
  - **400+ profissionais segurança treinados**
    - **máximo de 25 participantes por turma**

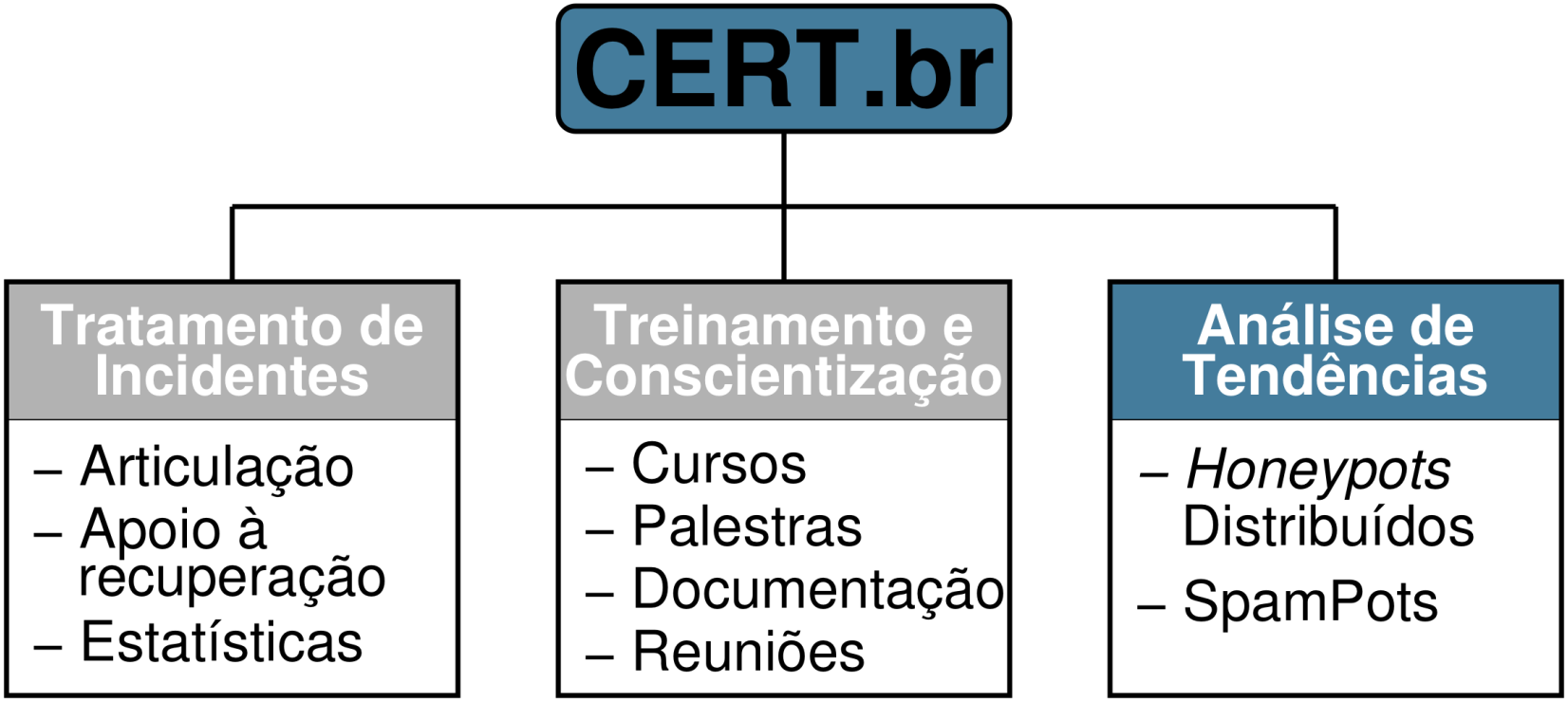
CSIRTs Brasileiros – Julho/2011

34 times com serviços anunciados ao público

Setor	CSIRTs
Escopo Nacional	CERT.br
Governo	CLRI-TRF-3, CSIRT Prodesp, CTIR Gov, GATI, GRA/SERPRO, GRIS-CD
Setor Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, EMBRATEL, StarOne, Oi, CSIRT Telefonica, CSIRT TIM, CSIRT UOL, CSIRT VIVO
Academia	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CERT-Bahia, CSIRT USP, GRC/UNESP, TRI
Outros	CSIRT TIVIT, GRIS Abril



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


CERT.br
Tratamento de Incidentes
– Articulação
– Apoio à recuperação
– Estatísticas
Treinamento e Conscientização
– Cursos
– Palestras
– Documentação
– Reuniões
Análise de Tendências
– Honeypots Distribuídos
– SpamPots

Projeto *Honeypots* Distribuídos

Rede de sensores (*honeypots), instalados em diversas redes conectadas à Internet no Brasil, capazes de observar ataques a eles direcionados**

Objetivo: aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro

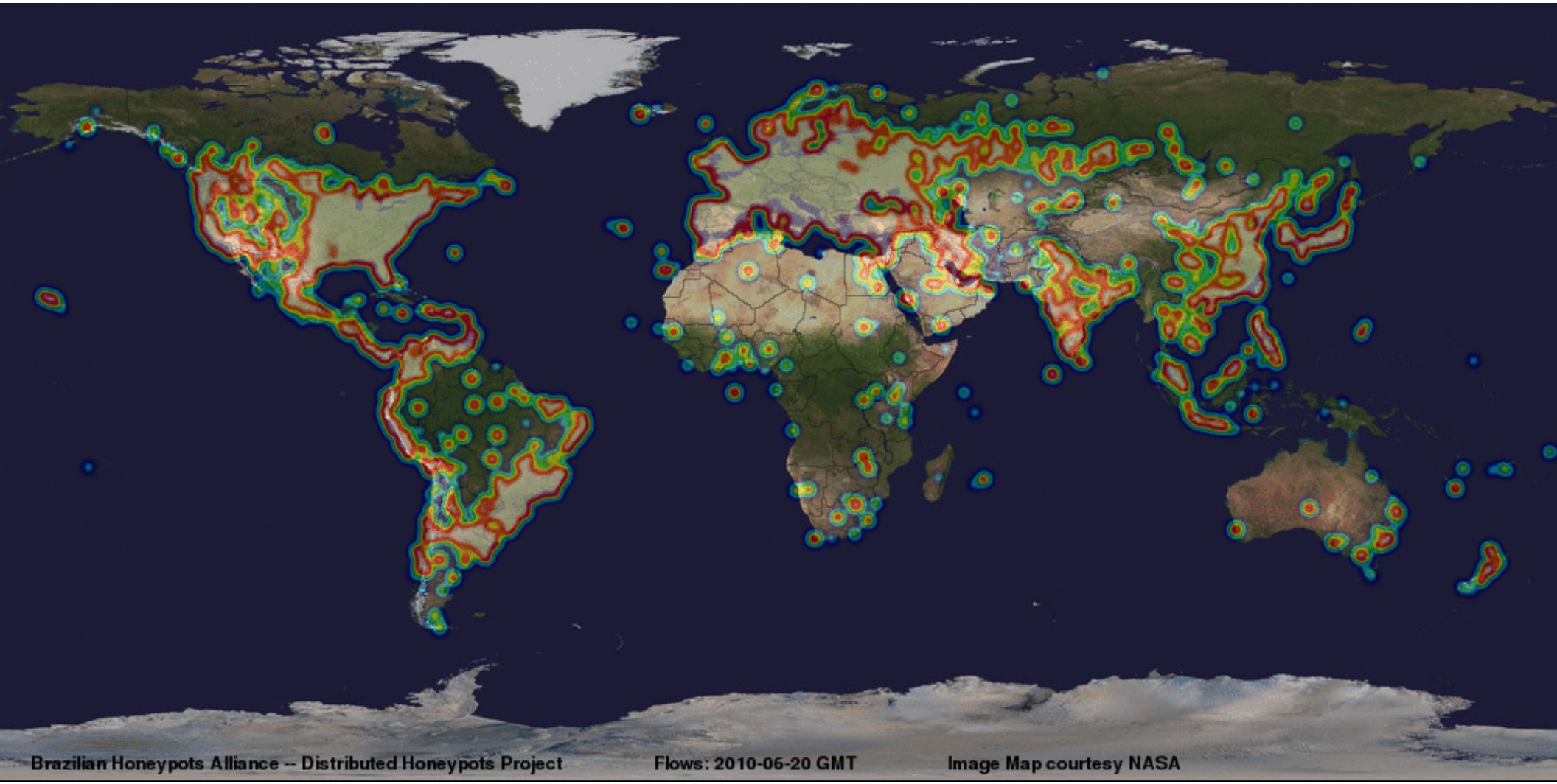
- **47 instituições parceiras, entre academia, governo, indústria, instituições financeiras e redes militares**
- **Baseado em trabalho voluntário**
- **http://honeytarg.cert.br/honeypots/**

Utilização dos dados coletados para:

- **Notificação das redes originadoras dos ataques**
- **Geração de estatísticas públicas**

* *Honeypot* é um tipo de sensor usado para simular serviços e registrar as atividades maliciosas.
Fonte: http://www.cert.br/docs/whitepapers/honeypots-honeynets/

Manutenção de Estatísticas Públicas



Recomendações

Ataques de força bruta (1/2)

- **Boas senhas**
  - Difíceis de serem descobertas (fortes)
  - Fáceis de serem lembradas
- **Não utilizar:**
  - Dados pessoais, palavras que façam parte de dicionários, sequências de teclado
- **Utilizar:**
  - Grande quantidade e diferentes tipos de caracteres
  - Números aleatórios
- **Dicas práticas:**
  - Utilizar as iniciais de uma frase
  - Utilizar uma frase longa
  - Fazer substituições de caracteres

Ataques de força bruta (2/2)

- **Reduzir o número equipamentos com serviço aberto**
  - Quanto mais máquinas expostas maior o risco
  - Implementar rede de gerência
- **Implementar filtragem de origem**
  - Permitir o acesso apenas de máquinas pré-determinadas
- **Mover o serviço para uma porta não padrão**
  - Medida paliativa, não definitiva
  - Permite reduzir a quantidade de ataques
- **Permitir acesso somente via chaves públicas**
- **Aumentar a monitoração**

Sugestões para defesa contra ataques de força bruta para SSH
http://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/

Abuso de máquinas de usuários

- **Definição de política de uso aceitável**
- **Monitoração:**
  - **Pró-ativa de fluxos**
  - **Das notificações de abusos**
- **Ação efetiva junto ao usuário nos casos de:**
  - **Detecção de *proxy* aberto ou**
  - **Máquina comprometida**
- **Gerência de saída de tráfego com destino à porta 25/TCP para redução de *spam***
  - **http://www.antispam.br/admin/porta25/**

Prevenção de Abuso de Serviço DNS

DNS Cache Poisoning

- Instalar as últimas versões dos softwares DNS
  - Correções não eliminam o ataque, apenas retardam seu sucesso
  - Adoção de DNSSEC é uma solução mais definitiva
    http://registro.br/suporte/tutoriais/dnssec.html

DNS Recursivo Aberto

- Duas possíveis soluções:
  - Utilizar o conceito de views do BIND; ou
  - Colocar os servidores DNS em computadores diferentes, com configurações e políticas de acesso diferentes
    - Única solução possível para o Microsoft DNS
  - Detalhes em:
    http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Ataques de DDoS (1/3)

- **Preparação**
  - **Estabelecer contatos e definir procedimentos**
    - **Provedor de acesso, de hospedagem (checar contrato)**
    - **Internos: administradores de rede, de segurança**
  - **Super provisionamento de recursos**
    - **Rede, aplicações, bases de dados, etc.**
  - **Efetuar testes de *stress* e de carga**
  - **Conhecer a rede e aplicações**
    - **Recursos críticos a serem mantidos**
    - **Acessos nacionais/internacionais**
    - **IPs de origem e protocolos prioritários**
  - **Liberar apenas os serviços realmente necessários (*hardening*)**
  - **Implementar filtros em roteadores**
  - **Segmentação de rede**

Ataques de DDoS (2/3)

- **Análise**
  - Monitoramento da rede
    - Tráfego IRC pode indicar máquinas infectadas por *bots*
  - Detectar o incidente e definir o escopo
    - *Logs*, serviços afetados e desempenho (carga, banda, CPU)

- **Mitigação**
  - Não existe receita de bolo
  - Depende do alvo, tipo, escopo do ataque
  - Reduzir os efeitos do ataque
    - Tentar bloquear o tráfego e reduzir a carga de processos
    - Desabilitar serviços desnecessários ou não prioritários
  - Manter canais de comunicação *out-of-band*

Ataques de DDoS (3/3)

- **Após o incidente**
  - **Documentar os detalhes do incidente e as soluções tomadas**
  - **Verificar o que poderia ter sido feito melhor**
  - **Lições aprendidas**
  - **Rever os planos e as defesas**
    - **Contratos**
    - **Contatos**
    - **Infra-estrutura de redes, etc.**

Network DDoS Incident Response Cheat Sheet

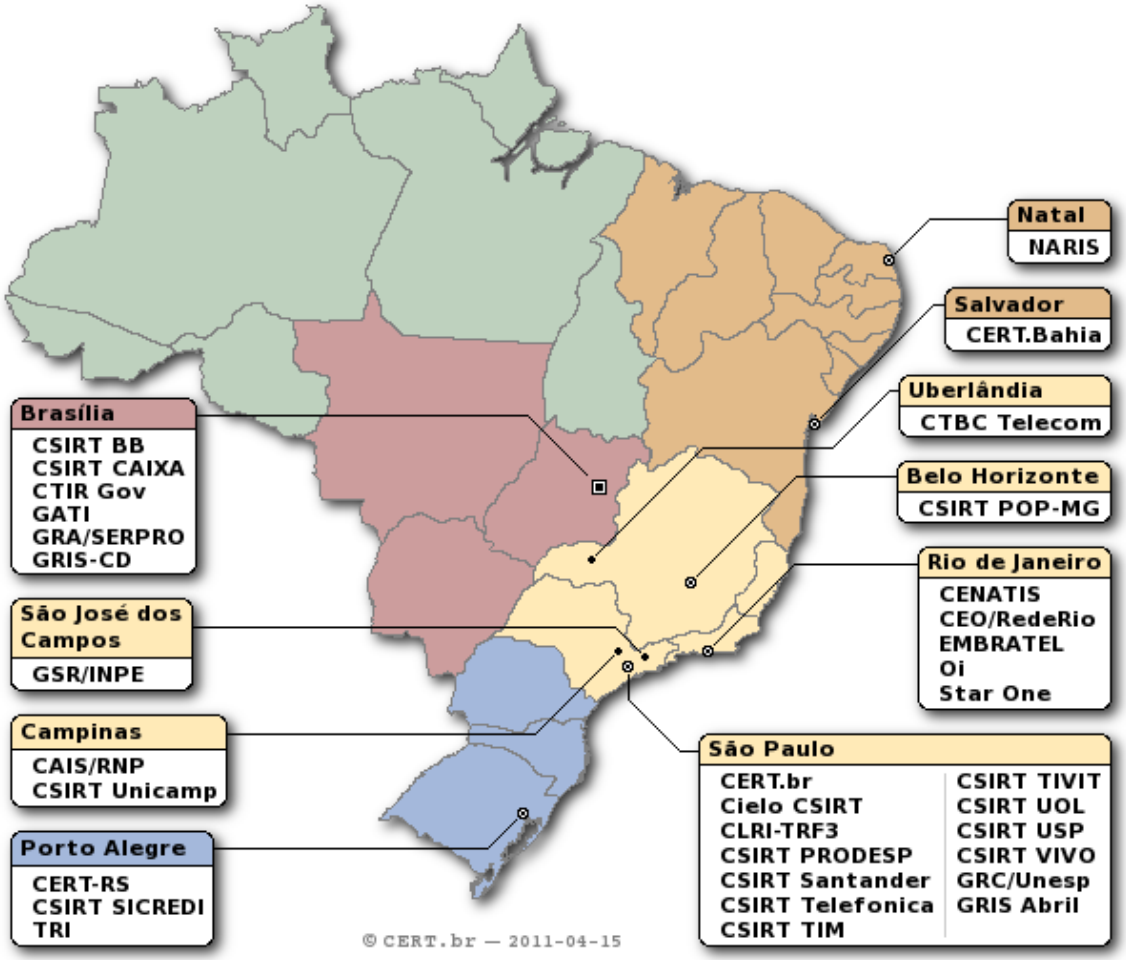
http://zeltser.com/network-os-security/ddos-incident-cheat-sheet.pdf

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
    - saiba para onde redirecionar notificações e reclamações
- Endereço do grupo de resposta a incidentes de segurança deve ser anunciado junto à comunidade
- Contas que recebem notificações de incidentes/abusos não podem barrar mensagens, pois:
  - Antivírus podem impedir a notificação de *malware*
  - Regras anti-*spam* podem impedir notificações de *spam* e *phishing*

Criar um CSIRT (1/2)

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

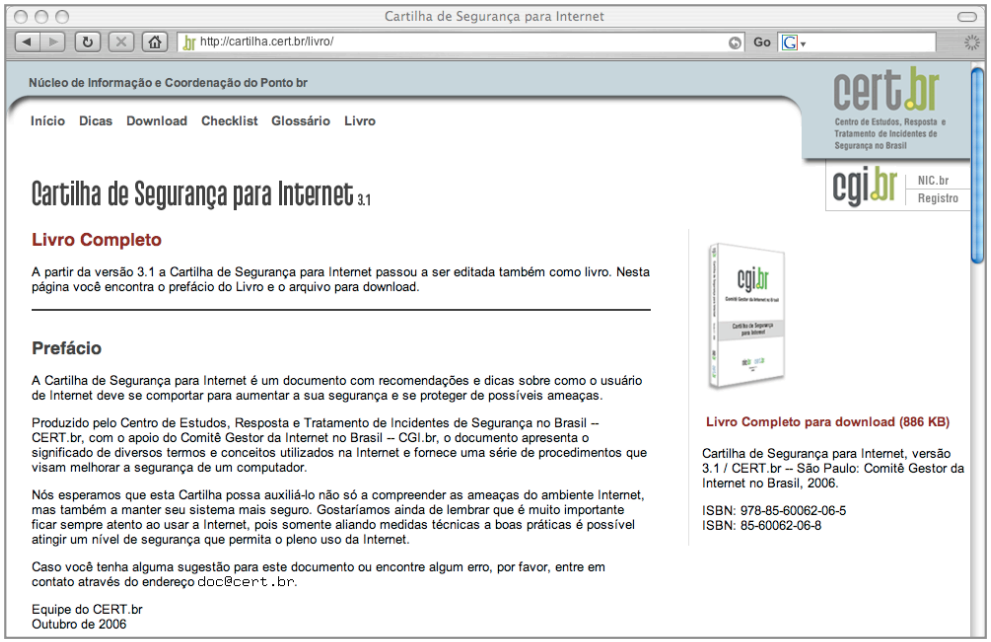


http://www.cert.br/csirts/brasil/

Criar um CSIRT (2/2)

- 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 as vítimas
- 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 a um incidente é a primeira a entrar em contato com as evidências de um possível crime
  - Seguir políticas e preservar evidências

Informar-se e manter-se atualizado (1/2)



http://cartilha.cert.br/

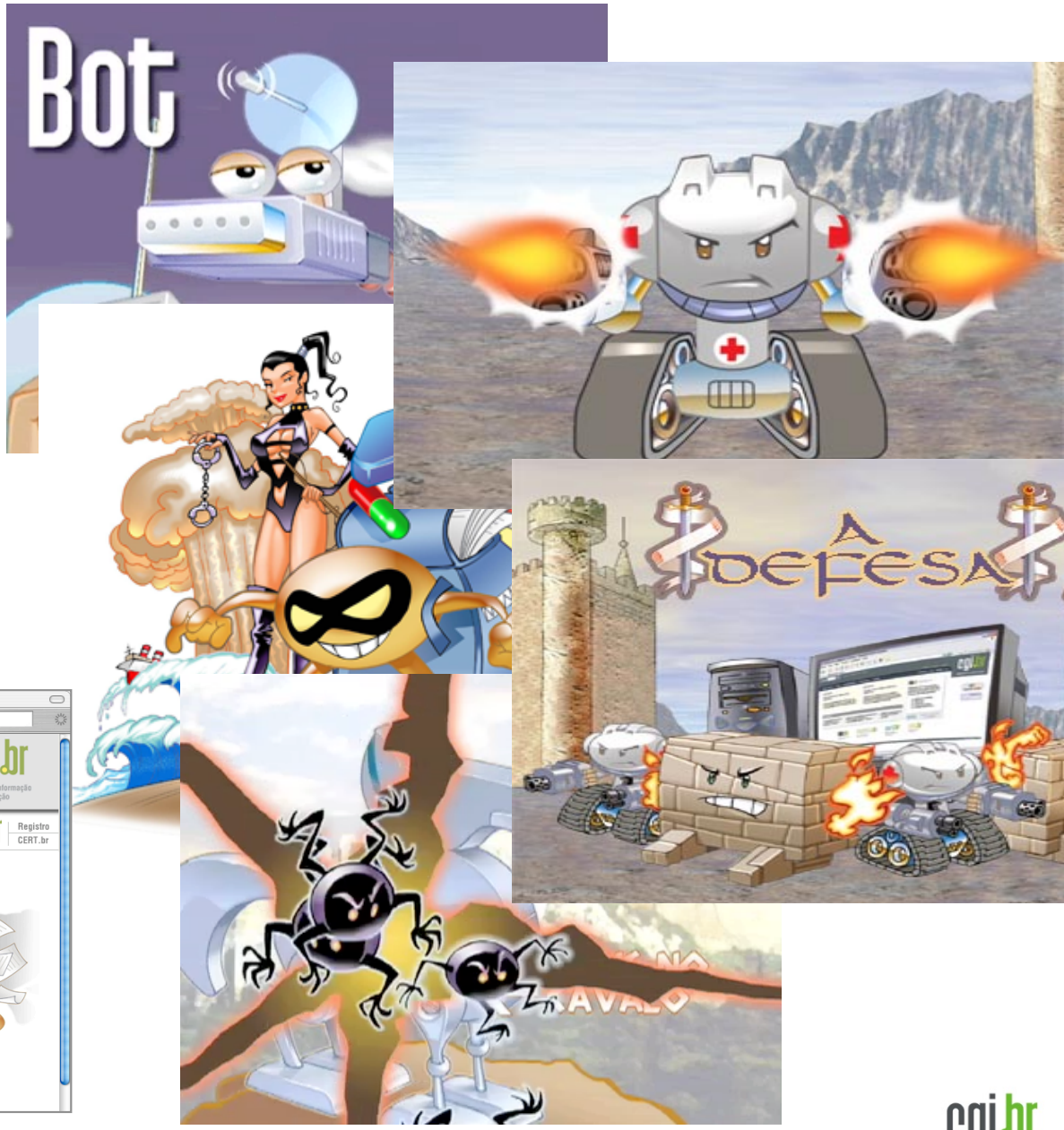
http://www.cert.br/rss/certbr-rss.xml

http://twitter.com/certbr

Informar-se e manter-se atualizado (2/2)

Site Antispam.br – Vídeos Educacionais no escopo das atividades da CT Anti-Spam do CGI.br

http://www.antispam.br/



Desafios (1/2)

- **Só haverá melhorias quando**
  - **O processo de desenvolvimento de *software* incluir**
    - **Levantamento de requisitos de segurança**
    - **Testes que incluam casos de abuso**

      (e não somente casos de uso)
  - ***Desenvolvimento seguro de software* se tornar parte da formação de projetistas e programadores**
    - **Desde a primeira disciplina de programação e permeado em todas as disciplinas**
  - **Provedores de acesso e serviço, operadoras e administradores de redes em geral forem mais pró-ativos**
  - **Os sistemas para usuários finais forem menos complexos**
    - **Mudança total de paradigma de uso da tecnologia**

Desafios (2/2)

- **Há falta de pessoal treinado no Brasil para lidar com Redes e com segurança em IPv4**
  - **A falta de pessoal com essas habilidades em IPv6 é ainda mais gritante**
- **Vencer a cultura de que é melhor investir em tecnologia do que treinamento e implantação de boas políticas**
  - **Quantas instituições realmente implementam tecnologias com base em uma análise de risco?**
- **Ir além do "*compliance*"**

Outras Iniciativas do NIC.br Relacionadas à Segurança

- Manutenção da Hora Oficial do Brasil para sincronia de computadores – NTP.br
- Manutenção dos Pontos de Troca de Tráfego nas áreas metropolitanas – PTT.br
- Manutenção de espelhos de 3 servidores raiz DNS no Brasil
- Adoção de DNSSEC pelo Registro.br
  - Brasil foi o segundo ccTLD a adotar DNSSEC
  - Hoje temos todo o `.br` com possibilidade de uso de DNSSEC
  - Treinamento gratuito online ou presencial
- Manutenção, desde março de 2011, do Portal InternetSegura.br

  reúne as principais iniciativas de segurança da Internet no Brasil em um único local

Links Relacionados

- **CGI.br - Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do Ponto br**
  http://www.nic.br/
- **CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/
- **Esta palestra**
  http://www.cert.br/docs/palestras/