Boas Práticas de Segurança

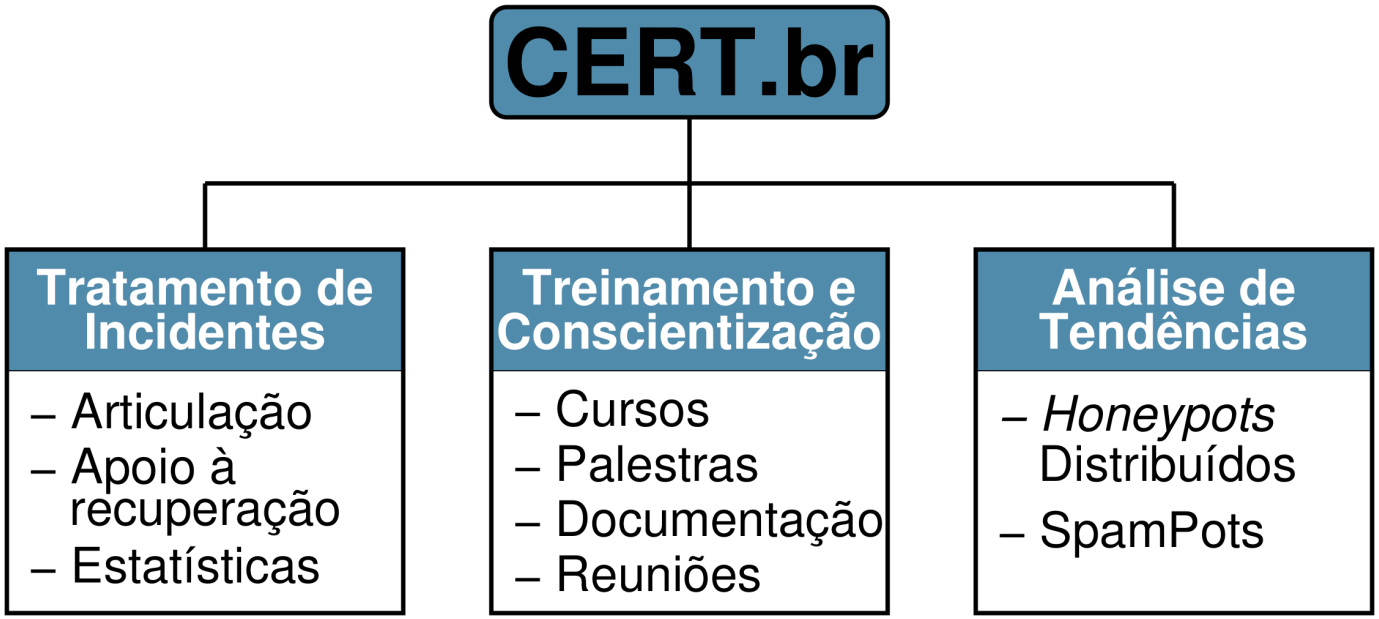
Miriam von Zuben
miriam@cert.br

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

NIC.br - Núcleo de Informação e Coordenação do Ponto br
CGI.br - Comitê Gestor da Internet no Brasil

Sobre o CERT.br

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



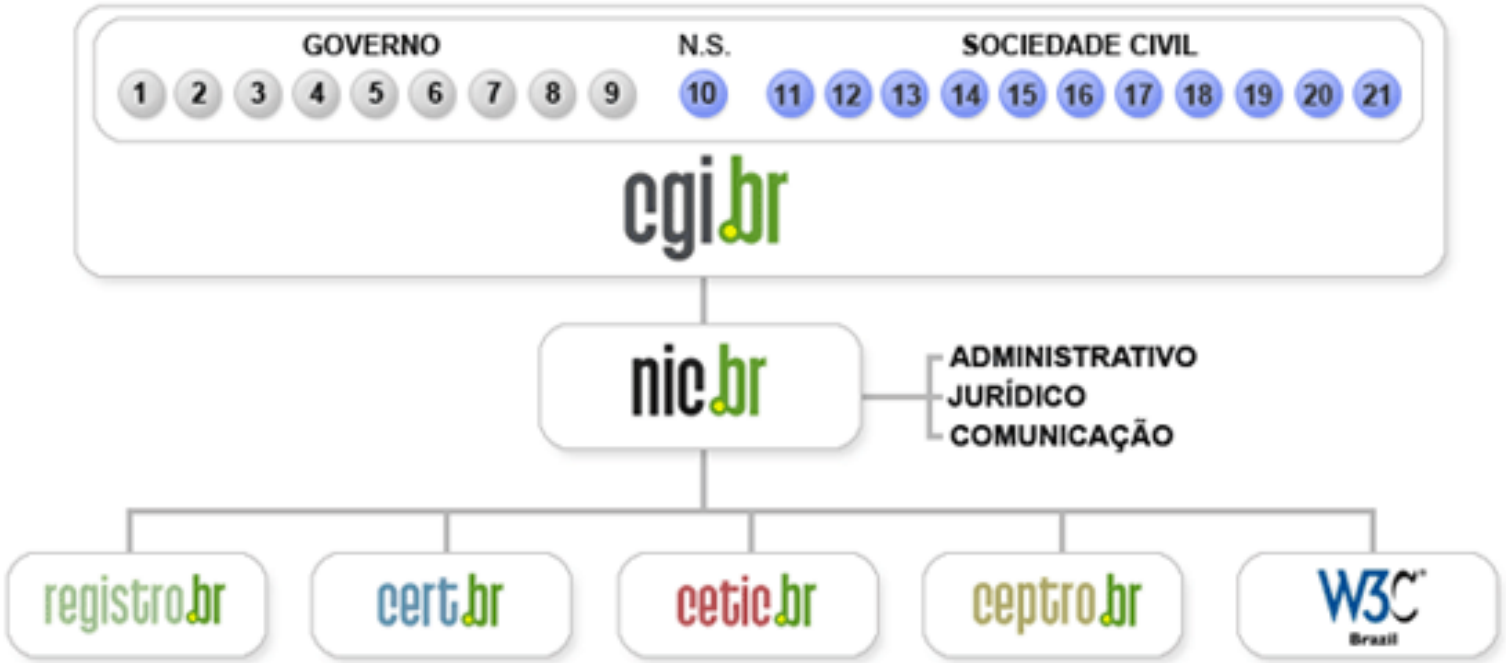
FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon

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**

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

Motivação (1/2)

- **Implementação de boas práticas pode auxiliar a:**
  - **Reduzir o desperdício de recursos**
    - **banda**
    - **tempo e pessoas**
    - ***hardware***
  - **Não ser origem/vítima de fraudes e ataques**
  - **Evitar problemas como:**
    - **perda de produtividade**
    - **danos à imagem**
  - **Reduzir perdas financeiras**
  - **Prover serviços de maior qualidade**
  - **Colaborar para o aumento da segurança da Internet**

Motivação (2/2)

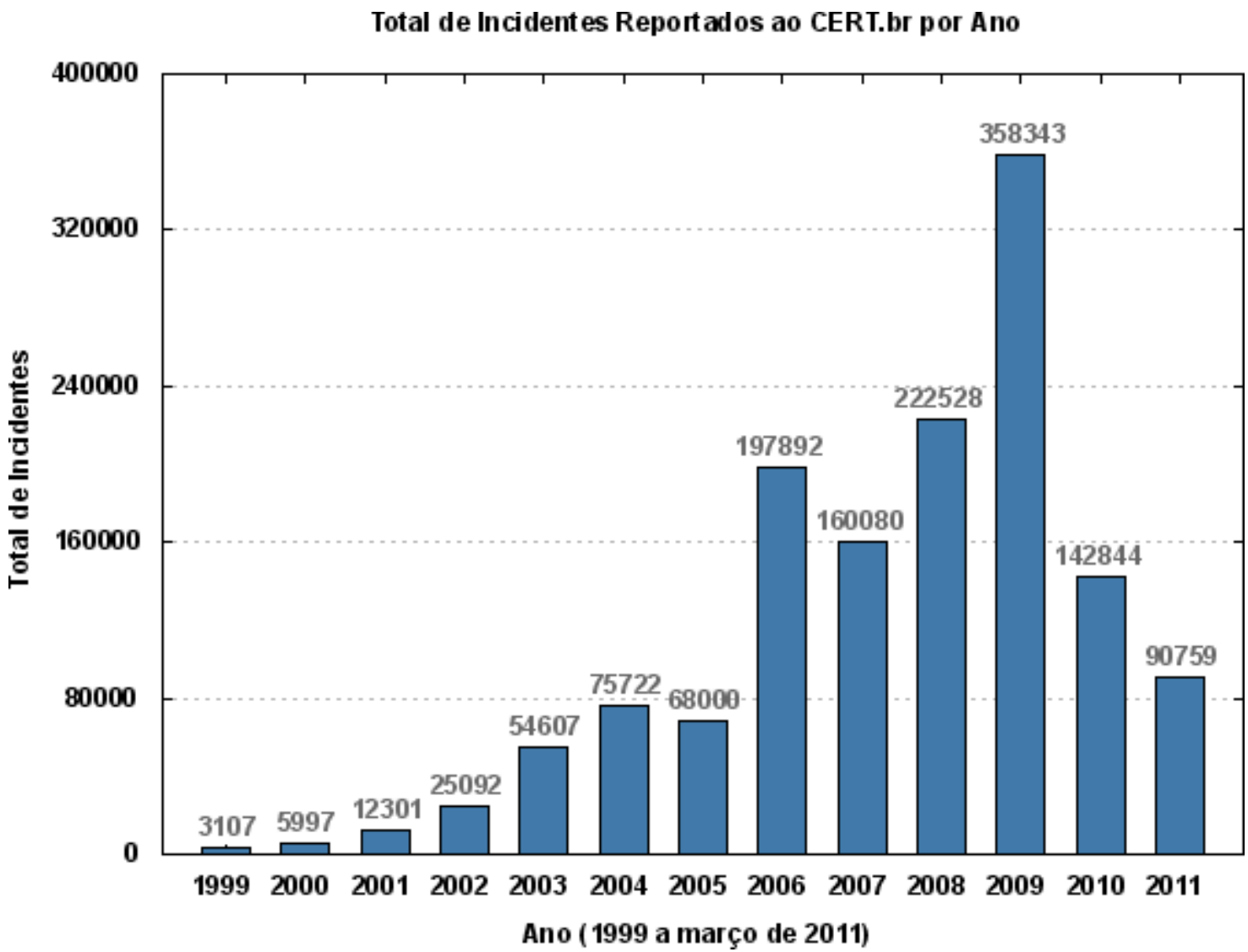
- **Não é possível erradicar todos os problemas**
- **Mas é possível:**
  - **Minimizá-los**
  - **Torná-los gerenciáveis**
- **Cada setor precisa fazer a sua parte**
  - **A solução não virá de uma ação única**
  - **Necessidade de cooperação para a solução dos problemas**

Agenda

- **Contexto**
  - **Incidentes de segurança mais frequentes**
- **Recomendações para prevenção e mitigação**
- **Considerações finais**
- **Referências**

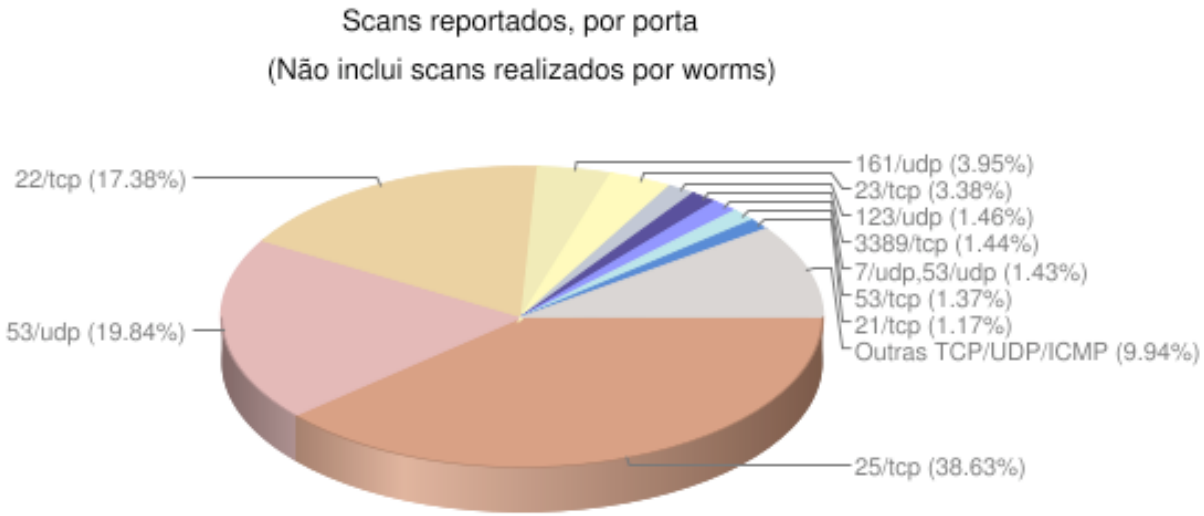
Contexto - Incidentes de segurança mais frequentes

Incidentes reportados ao CERT.br por ano



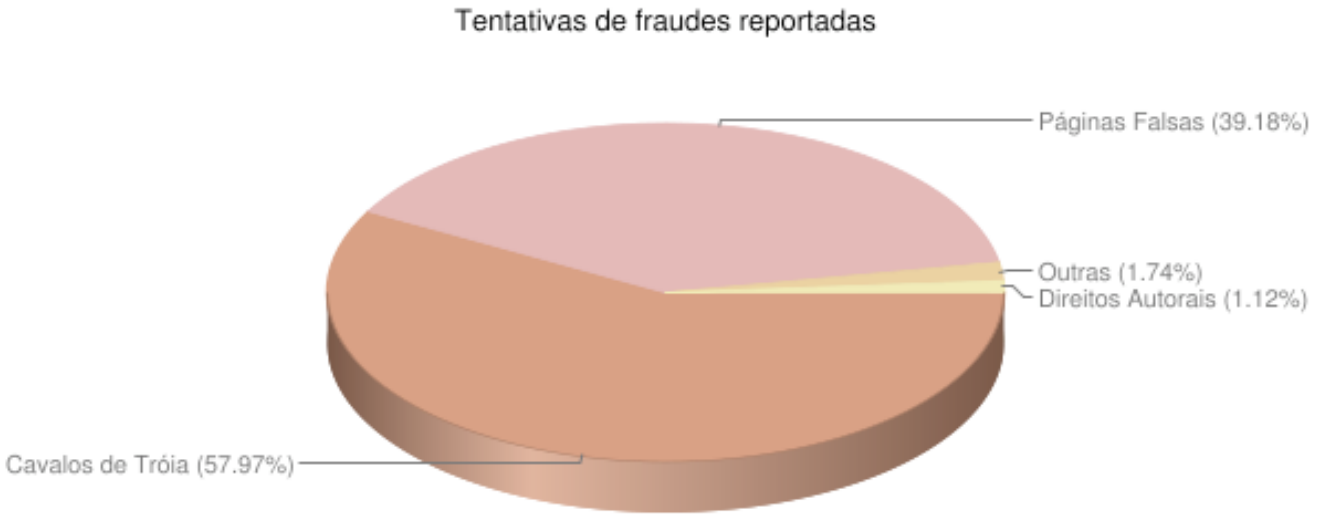
Incidentes reportados ao CERT.br em 2010

Scans reportados, por porta



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

Tentativas de fraudes reportadas (1/3)



- **A usuários finais**
  - **Fraudes, *bots*, *spyware*, etc**
  - **Motivação financeira**
  - **Abuso de *proxies*, na maioria instalados por *bots***

Tentativas de fraudes reportadas (2/3)

- ***Spams* em nome de diversas entidades/temas variados**
  - ***Links* para *trojans* hospedados em diversos *sites***
  - **Vítima raramente associa o *spam* com a fraude**
- **Ataques a servidores *Web***
- ***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**

Tentativas de fraudes reportadas (3/3)

- *Malware* para:
  - *Smartphones*
  - Via redes sociais
    - explorando a confiança de seguidores
    - grande uso de *links* curtos
- Uso de *botnets:*
  - DDoS
  - Extorsão
  - *Download* de outros tipos de *malware*
  - Furto de informações
  - Proxies abertos
    - envio de *spam*
    - *navegação anônima*

Brasil na CBL

	País	Endereços IP	% do Total	Taxa de Infecção (%)
1	Índia (IN)	1.459.837	17.23	5.391
2	Brasil (BR)	738.297	8.71	1.342
3	Vietnã (VN)	625.005	7.38	3.584
4	Rússia (RU)	456.519	5.39	1.202
5	Indonésia (ID)	401.537	4.74	3.562
6	Paquistão (PK)	364.081	4.30	8.744
7	China (CN)	221.266	2.61	0.067
8	Ucrânia (UA)	215.126	2.54	2.091
9	Romênia (RO)	204.329	2.41	2.165
10	Arábia Saudita (SA)	201.154	2.37	3.418

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

Dados gerados em Tue Jun 21 05:16:18 2011 UTC/GMT
Composite Blocking List - http://cbl.abuseat.org

Recomendações para prevenção e mitigação

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***

Gerência de porta 25

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

Cuidados com o uso de IPv6

- **Regras de filtragem em *firewall* são diferentes**
  - **Não assumir que as regras utilizadas em IPv4 funcionam em IPv6**
  - **Túneis IPv6:**
    - **podem não estar sendo filtrados**
    - **com o túnel implementado pode haver conexões entrantes**
    - **criados automaticamente no Windows (a partir do Vista)**
    - **pode já haver tráfego IPv6 na rede IPv4**
- **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

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.**

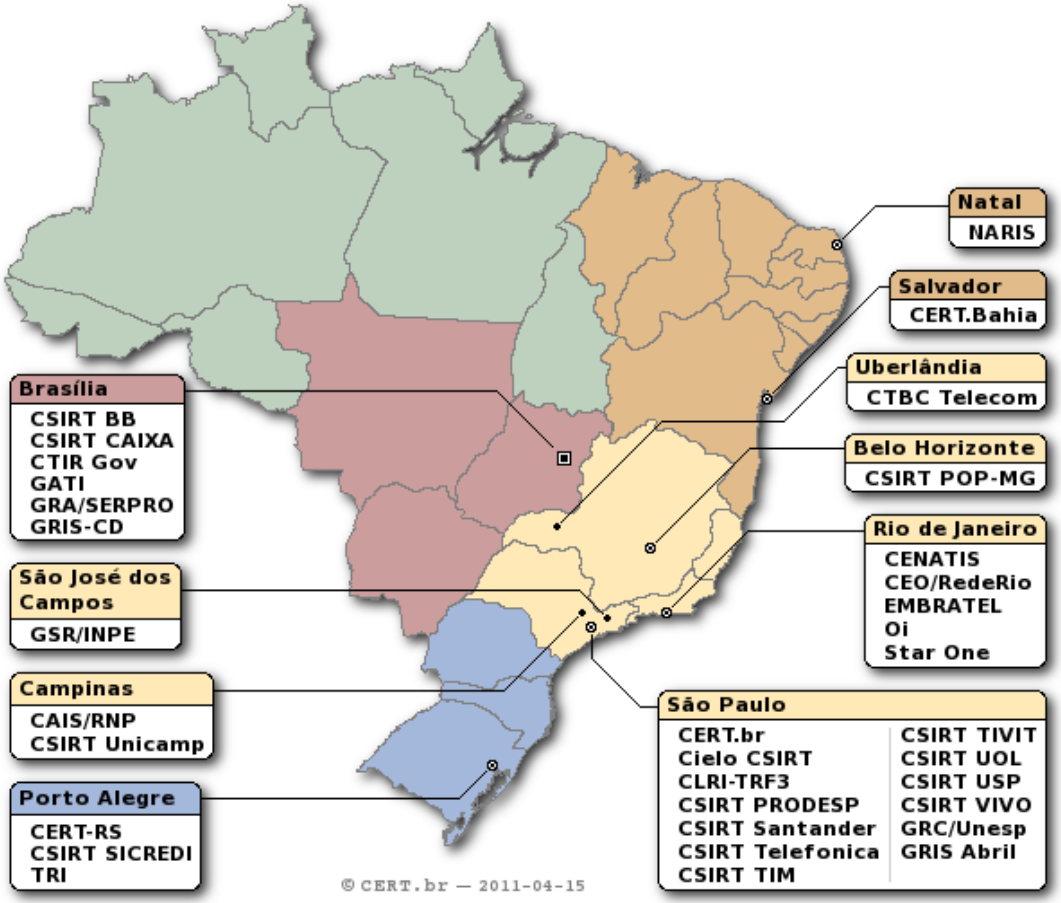
Network DDoS Incident Response Cheat Sheet

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)



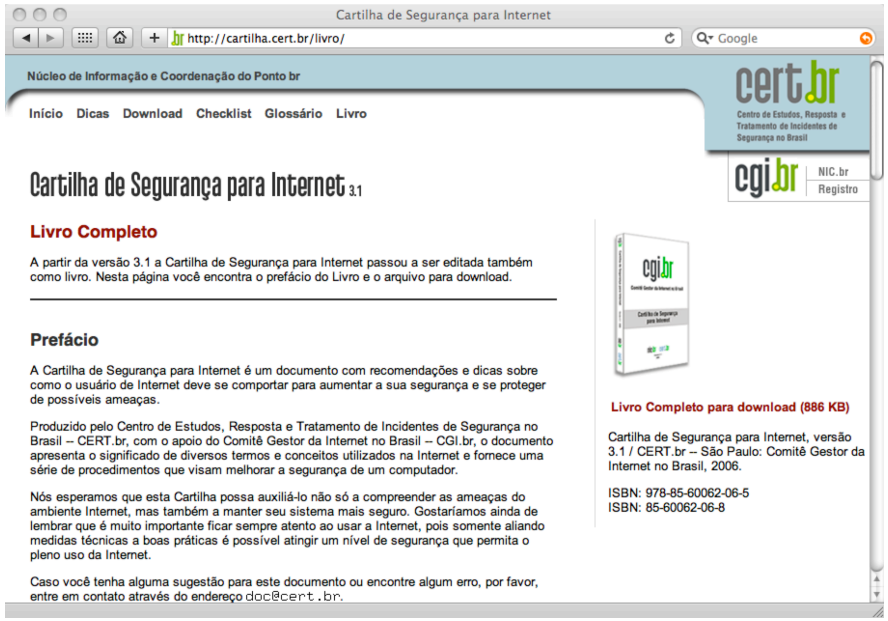
http://www.cert.br/csirts/brasil/

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

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/

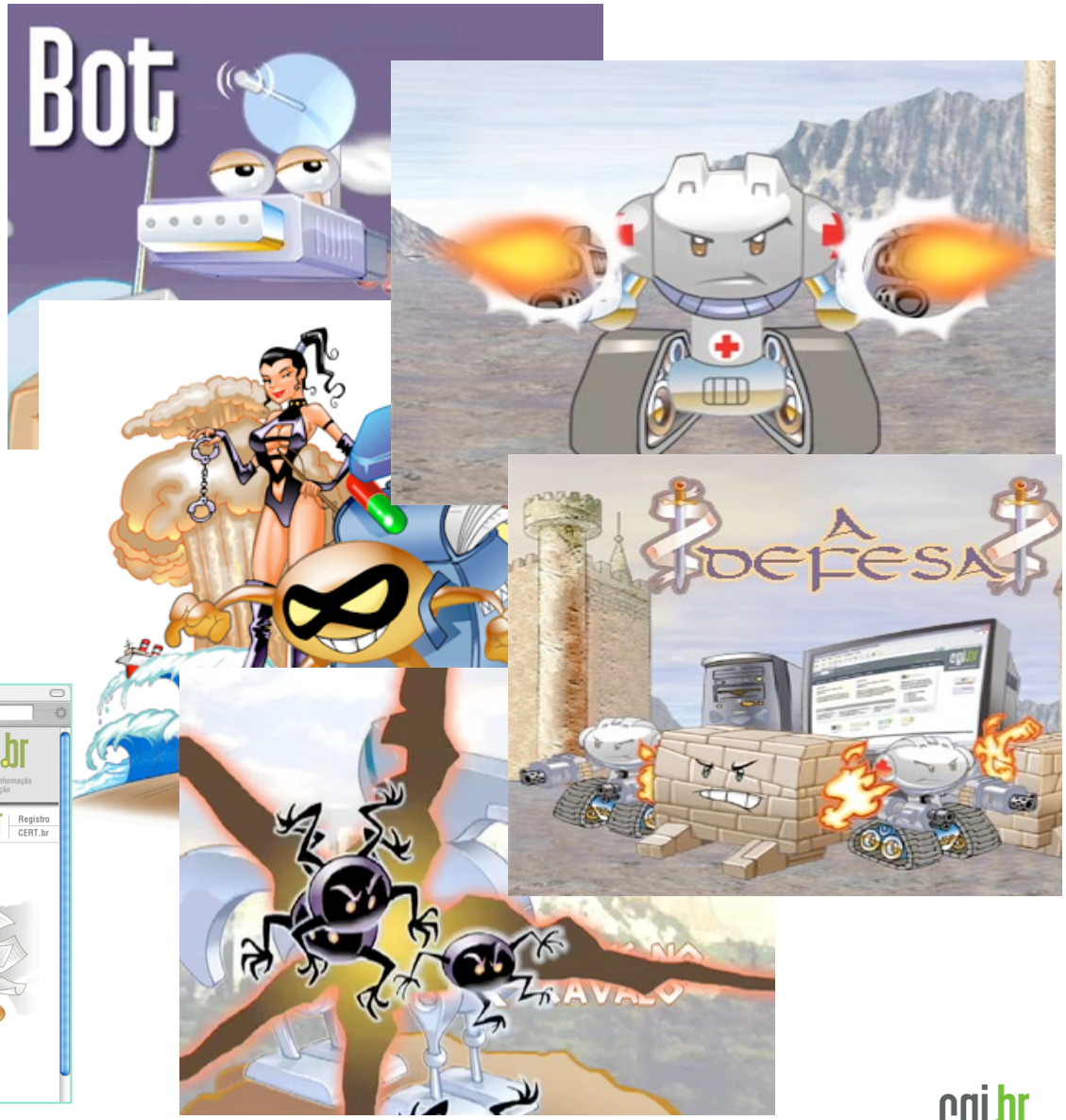
http://www.cert.br/rss/certbr-rss.xml

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/



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 de 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/

Miriam von Zuben

miriam@cert.br