Grupos de Resposta a Incidentes:

Definição, Importância, Situação Atual e o Papel do NBSO

Marcelo H. P. C. Chaves
mhp@nic.br

NIC BR Security Office – NBSO
Brazilian Computer Emergency Response Team
http://www.nbso.nic.br/

Comitê Gestor da Internet no Brasil
http://www.cg.org.br/

Roteiro

- Breve Histórico
- CSIRTs: definição, tipos, autoridade, serviços, cooperação, cenário internacional
- História do CGI.br e do NBSO
- Cenário Nacional de CSIRTs
- Resposta a Incidentes
- Iniciativas e Projetos do NBSO

Breve Histórico

- Final dos Anos 60 – Internet
  - projeto não considera implicações de segurança
  - comunidade de pesquisadores
  - confiança
- 1986
  - “Cookoo’s Egg”
  - diferença de U$0.75 na contabilidade
  - 30+ sistemas invadidos
  - contas/senhas óbvias
  - vulnerabilidades em software
  - tempo e persistência

Breve Histórico (cont.)

- 1988
  - Internet Worm – Robert Morris Jr.
  - 6000+ computadores atingidos
  - vulnerabilidades do sendmail e finger
  - uso do arquivo .rhosts
  - mobilização em torno do tema segurança
  - criação do primeiro CSIRT: CERT/CC

Incidente de Segurança

*Um **incidente de segurança** pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.*

Exemplos:

- tentativas de ganhar acesso não autorizado;
- ataques de negação de serviço;
- uso ou acesso não autorizado a um sistema;
- modificações em um sistema, sem o conhecimento ou consentimento prévio do dono;
- desrespeito à Política de Segurança ou à PUA.

Computer Emergency Response Team

Um grupo ou organização que provê serviços e suporte para um público bem definido, para prevenção, tratamento e resposta a Incidentes de Segurança.

- Ponto central de contato
- Provê informações para o seu público
- Troca informações com outros CSIRTs

Papel do CSIRT

- Fornececer informações confiáveis
  - reduzir as informações que chegam aos administradores de redes e usuários
- Prover recomendações e estratégias
- Determinar o impacto de incidentes
- Prover meios para recuperação rápida
- Ser o ponto de contato com outros grupos, polícia, mídia, etc

Tipos de CSIRT e Autoridade

Tipos:

- Empresas
- Países
- Backbones
- Órgaos Governamentais

Autoridade:

- Completa
- Parcial
- Indireta
- Sem autoridade

Serviços de um CSIRT

Proativos

- Filtragem e repasse de informações
- Disseminação da cultura de segurança
- Desenvolvimento de documentação
- Treinamentos e orientação a usuários
- Configuração e manutenção dos sistemas
- Desenvolvimento de ferramentas

Serviços de um CSIRT (cont.)

Reativos

- Tratamento de Incidentes
- Coordenação de ações
- Detecção e rastreamento de invasões
- Preservação de evidências
- Análise de artefatos
- Análise de vulnerabilidades

Perfil do Profissional

- Integridade e discrição
- Sem prévio envolvimento com atividades de “hacking”
- Conhecimentos:
  - TCP/IP
  - ambiente de TI da instituição
  - comunicação (oral e escrita)

Cooperação entre CSIRTs

- Essencial para a operação
  - permite acesso a informações relevantes
  - permite correlação de eventos
  - facilita a resolução de incidentes
- Não existe fórmula mágica, o grupo necessita
  - construir sua reputação
  - ganhar a confiança de outros grupos

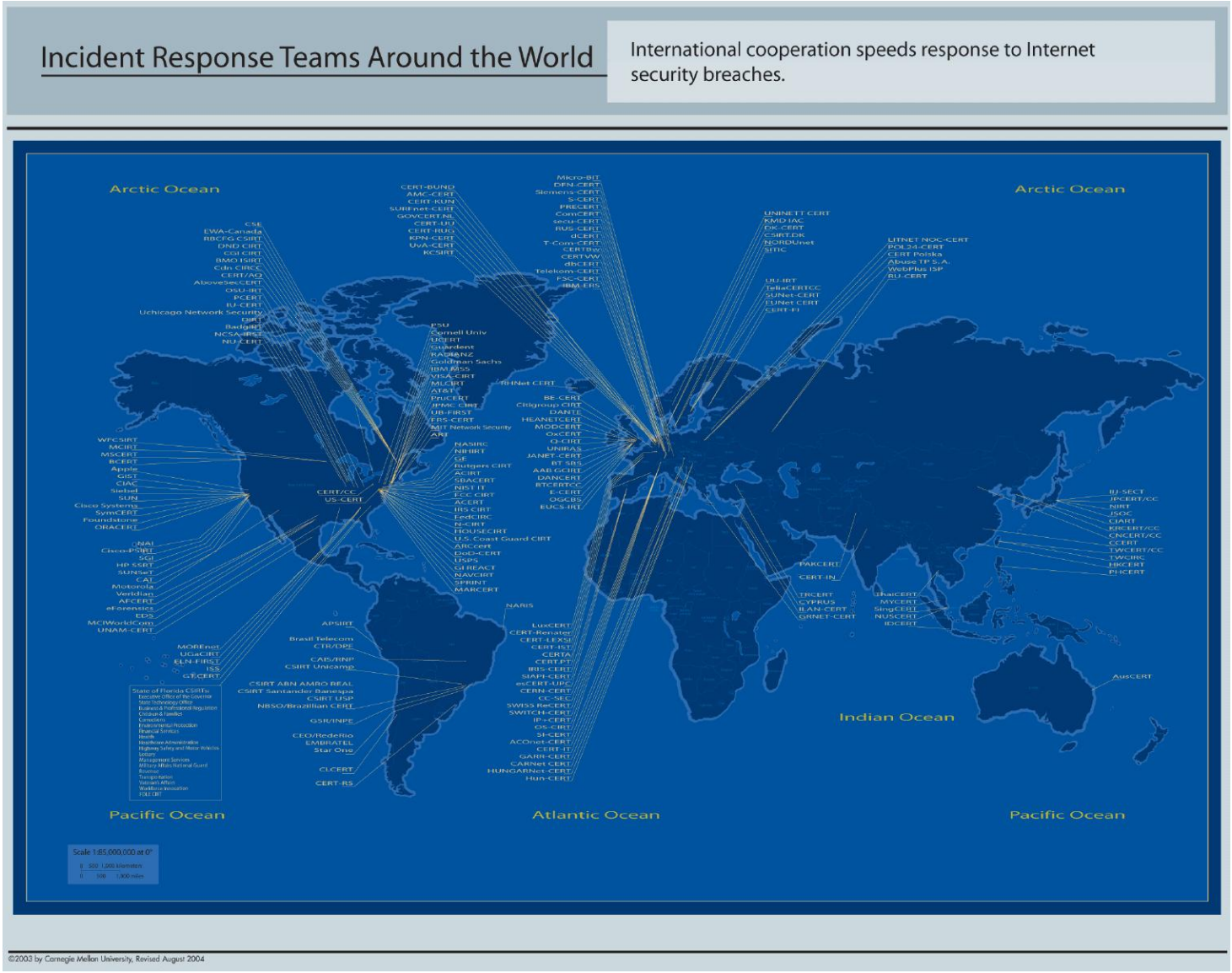
Cooperação entre CSIRTs (cont.)

Como conhecer outros CSIRTs:

- Durante o processo de resposta a incidentes
- Participando de conferências
- FIRST (Forum of Incident Response and Security Teams)
  - reúne CSIRTs de todo o mundo
  - promove e facilita a comunicação

http://www.first.org/

CSIRTs no Mundo



Fonte: CERT Coordination Center

Histórico e Atuação do NBSO

Comitê Gestor da Internet no Brasil – CGI.br

- Criado por portaria interministerial MCT/MC 147, de 31 de maio de 1995.
  - recomendar padrões e procedimentos técnicos e operacionais para a Internet no Brasil;
  - coordenar a atribuição de endereços Internet, o registro de nomes de domínios, e a interconexão de *backbones*;
  - coletar, organizar e disseminar informações sobre os serviços Internet.

---

http://www.cg.org.br/sobre-cg/historia.htm

CGI.br (cont.)

Decreto Nº 4.829, de 3 de setembro de 2003:

- Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.
- Composição: 21 membros – MCT, Casa Civil, MC, Defesa, MDIC, MP, Anatel, representantes da comunidade acadêmica e empresarial, entre outros.

---

http://www.cg.org.br/regulamentacao/

Criação do NBSO

Agosto/1996, documento: “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil”, apontando a necessidade de:

- Um ponto central de contato
- Manutenção de estatísticas sobre incidentes na Internet Brasileira
- Neutralidade para coordenar ações entre redes envolvidas em incidentes
- Representação junto a órgãos internacionais de segurança

Junho/1997: criado o NBSO

---

http://www.cg.org.br/grupo/historico-gts.htm

Missão do NBSO

CSIRT responsável por receber, analisar e responder a incidentes de segurança em computadores envolvendo redes conectadas à Internet Brasileira. Atua:

- no trabalho de conscientização sobre os problemas de segurança
- no auxílio ao estabelecimento de novos CSIRTs no Brasil
- no desenvolvimento de documentação
- na coordenação do tratamento de incidentes

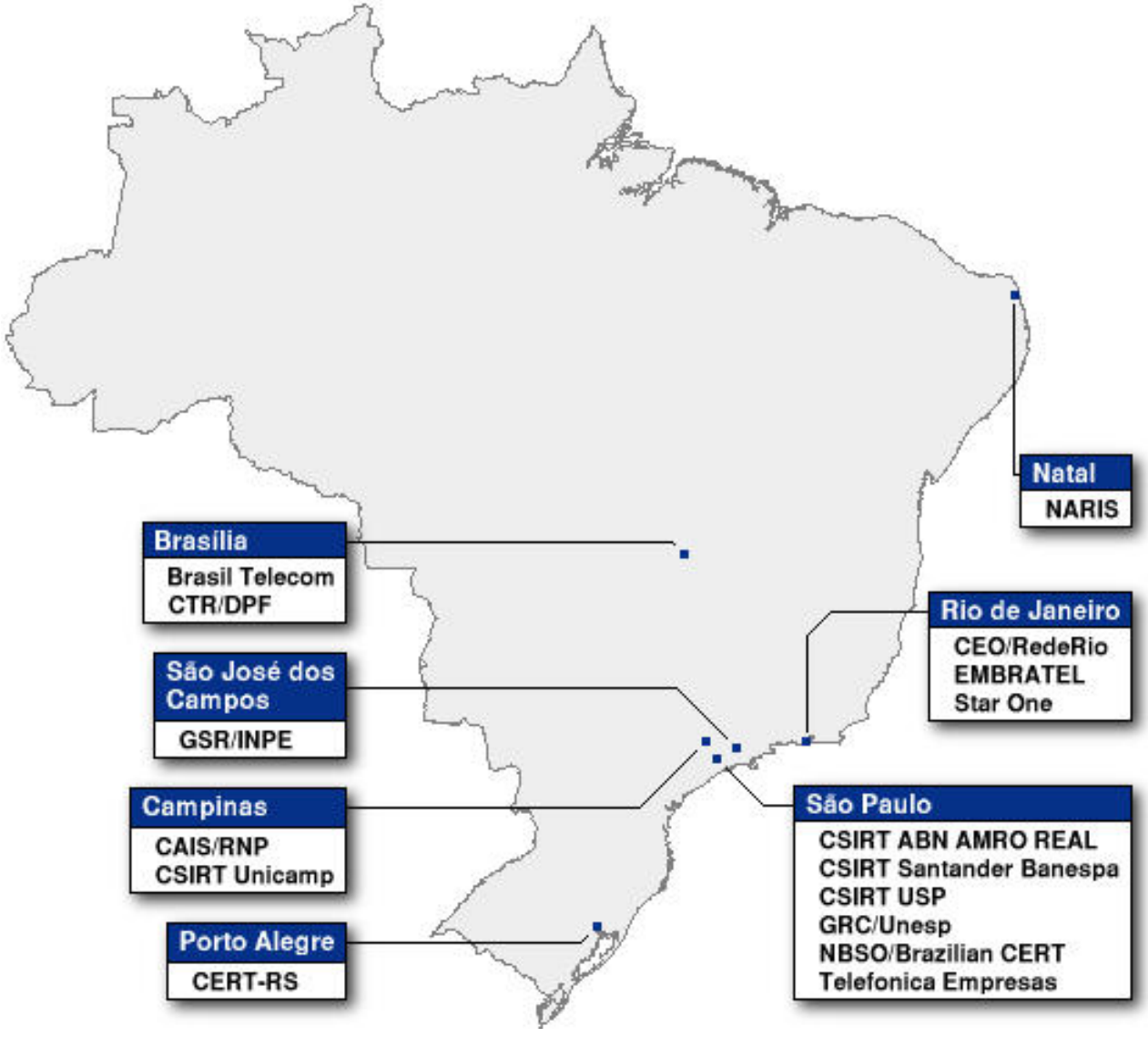
---

http://www.nbso.nic.br/missao.html

Coordenação do Tratamento de Incidentes

- Ponto central de contato para a Internet no Brasil
- Facilitação de ações entre redes envolvidas em incidentes
  - colocar as partes em contato
  - prover apoio necessário para recuperação e análise de sistemas comprometidos
- Trabalho colaborativo com outras entidades, como as polícias, provedores, *backbones* e setor financeiro

CSIRTs Brasileiros



http://www.nbso.nic.br/contato-br.html

CSIRTs Brasileiros (cont.)

Grupos não listados na página do NBSO:

- CSIRT Banco do Brasil
- CSIRT Bradesco
- Citibank
- GRA Caixa Econômica Federal
- GRA SERPRO
- Itaú
- Telemar

CSIRTs Brasileiros (cont.)

Projeto INOC-DBA* BR

Sistema de comunicação imediata entre operadores de redes e CSIRTs, baseado em telefonia IP.

- 120 telefones IP distribuídos pelo CGI.br para:
  - 100 maiores AS (*Autonomous Systems*) do Brasil
  - 20 CSIRTs (nomeados pelo NBSO)

---

* INOC-DBA (Internet Network Operation Centers – Dial By AS Number) Hotline Phone System – http://www.pch.net/inoc-dba/

Resposta a Incidentes

Resposta a Incidentes

Recebimento de notificações de incidentes:

- Quase totalidade por email
  - forma mais usada pela comunidade de CSIRTs
- Origem variada
  - administradores de redes, usuários, outros
  - CSIRTs
- Natureza das notificações:
  - varreduras, tentativas de comprometimento;
  - violação de direitos autorais
- Ações tomadas
  - checagem dos contatos, notificações de outros sites;
  - acompanhamento e estatísticas

Resposta a Incidentes (cont.)

Outras atividades relacionadas:

- Apoio a recuperação de incidentes
- Correlação de eventos de segurança observados com outras fontes
- Dúvidas sobre segurança: usuários, administradores e mídia

Iniciativas e Projetos do NBSO

Documentos em Português

Produção de Documentos

- Cartilha de Segurança para Internet
  - I: Conceitos de Segurança
  - II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção
  - III: Privacidade
  - IV: Fraudes na Internet
  - V: Redes de Banda Larga e Redes Sem Fio (Wireless)
  - VI: Spam
  - VII: Incidentes de Segurança e Uso Abusivo da Rede
  - Checklist
  - Glossário

http://www.nbso.nic.br/docs/cartilha/

Documentos em Português (cont.)

Produção de Documentos

- Práticas de Segurança para Administradores de Redes

  http://www.nbso.nic.br/docs/seg-adm-redes/

- Tradução de Documentos do CERT/CC
  - Advisories

    http://www.nbso.nic.br/certcc/advisories/
  - Documentos sobre CSIRTs

    http://www.nbso.nic.br/csirts/

Formação e Capacitação de CSIRTs

Enfoque no aumento da capacidade nacional de resposta a incidentes de segurança

- Carnegie Mellon Software Engineering Institute Partner
- Cursos do CERT Coordination Center:
  - Fundamentals of Incident Handling
  - Advanced Incident Handling for Technical Staff

---

http://www.nbso.nic.br/cursos/

Notificações

- Consultas regulares em bases mundiais de abuso
- Identificação de IPs brasileiros
- Envio de notificações para os responsáveis das redes
- Alguns exemplos:
  - The Open Relay DataBase (ORDB.org)
  - Smurf Amplifier Registry (SAR)

Notificações de Spam

Controle e Acompanhamento de Notificações de Spam

- Recebidos via SpamCop
- Notificações e estatísticas
- Perfil do spam no Brasil: tipo mais comum e origem
- Ajudar redes brasileiras a direcionar esforços
- **Não** usar para blacklist

---

http://www.nbso.nic.br/stats/spam/

Estatísticas de Incidentes

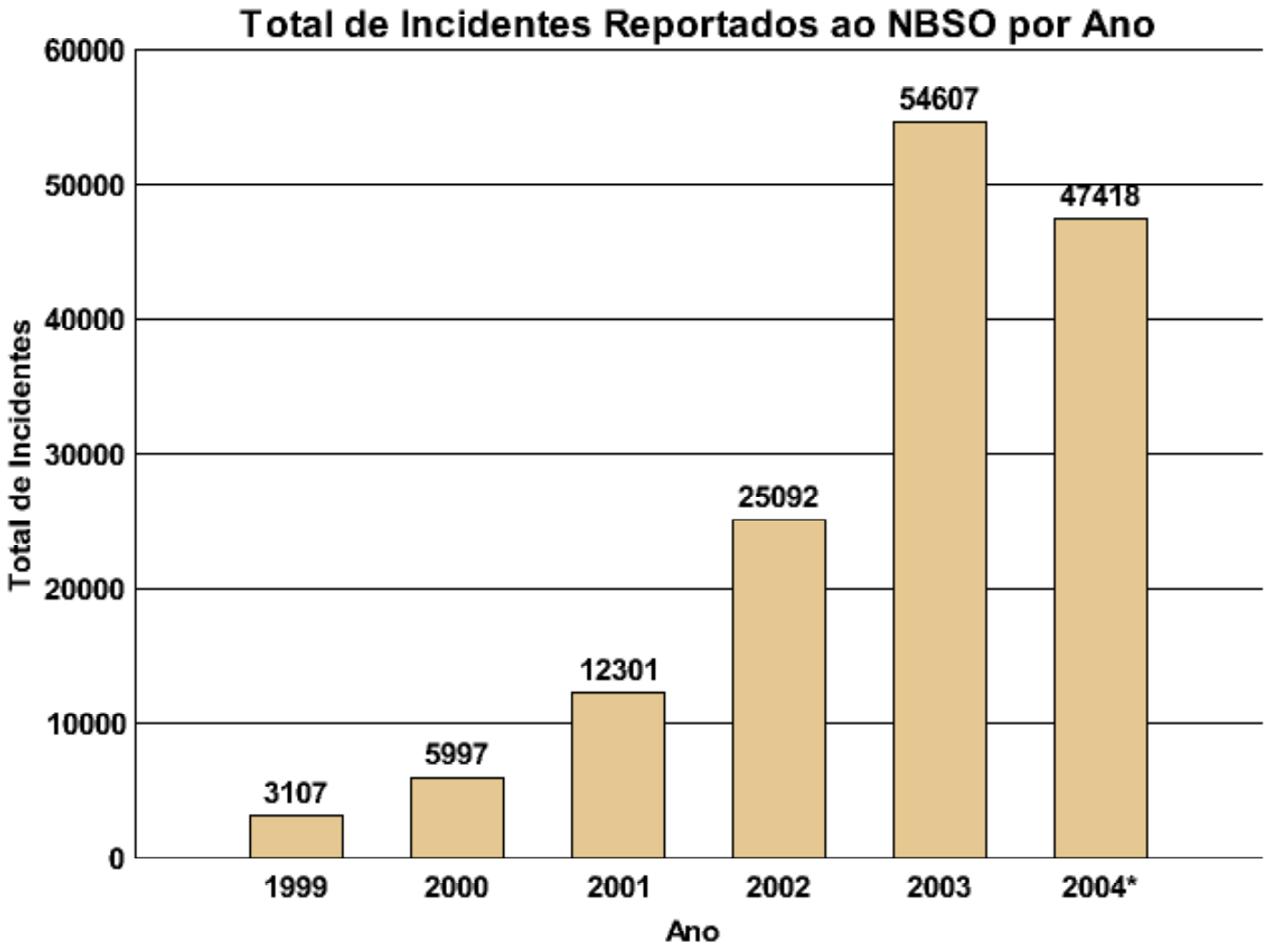
Anunciadas trimestralmente

- apenas os incidentes reportados ao NBSO
- divididos por categoria (varredura, fraudes, invasões, etc)
- Determinação de novas tendências de ataques

---

http://www.nbso.nic.br/stats/incidentes/

Estatísticas de Incidentes (cont.)



* Incidentes reportados ao NBSO até o mês de agosto.

Consórcio Brasileiro de Honeypots

- Honeypots são mantidos pelas instituições consorciadas
- Objetivo de aumentar, no espaço Internet brasileiro, a capacidade de:
  - detecção de incidentes, correlação de eventos;
  - determinação de tendências de ataques.
- Utilização dos dados por grupos de resposta a incidentes
- Uso dos dados pelo NBSO:
  - Identificação de ataques conhecidos: detecção de servidores comprometidos realizando varreduras;
  - Detecção de worms/vírus:mostram um número enorme de máquinas vulneráveis, facilmente exploráveis;
  - Comparação com incidentes reportados voluntariamente.

http://www.honeypots-alliance.org.br/

Referências

- NBSO - NIC BR Security Office
  Brazilian Computer Emergency Response Team
  http://www.nbso.nic.br/
- Comitê Gestor da Internet no Brasil
  http://www.cg.org.br/
- Material de Apoio para CSIRTs
  http://www.nbso.nic.br/csirts/
- Cursos do CERT/CC ministrados pelo NBSO
  http://www.nbso.nic.br/cursos/
- Documentação sobre Segurança e Administração de Redes
  http://www.nbso.nic.br/docs/

Referências (cont.)

- Estatísticas de Notificações de Spam Reportadas ao NBSO
  http://www.nbso.nic.br/stats/spam/
- Estatísticas de Incidentes Reportadas ao NBSO
  http://www.nbso.nic.br/stats/incidentes/
- Documentos, RFCs e sites relacionados
  http://www.nbso.nic.br/links/
- Material desta apresentação
  http://www.nbso.nic.br/docs/palestras/
- Consórcio Brasileiro de Honeypots
  http://www.honeypots-alliance.org.br/