Segurança: Tendências Atuais e Recomendações do NBSO

Cristine Hoepers
cristine@nic.br

Klaus Steding-Jessen
jessen@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

- CGI.br e NBSO
- Outros CSIRTs
- Tendências atuais
- Desafios para o profissional
- Honeypots como ferramentas de auxílio
- Recomendações

CGI.br e 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

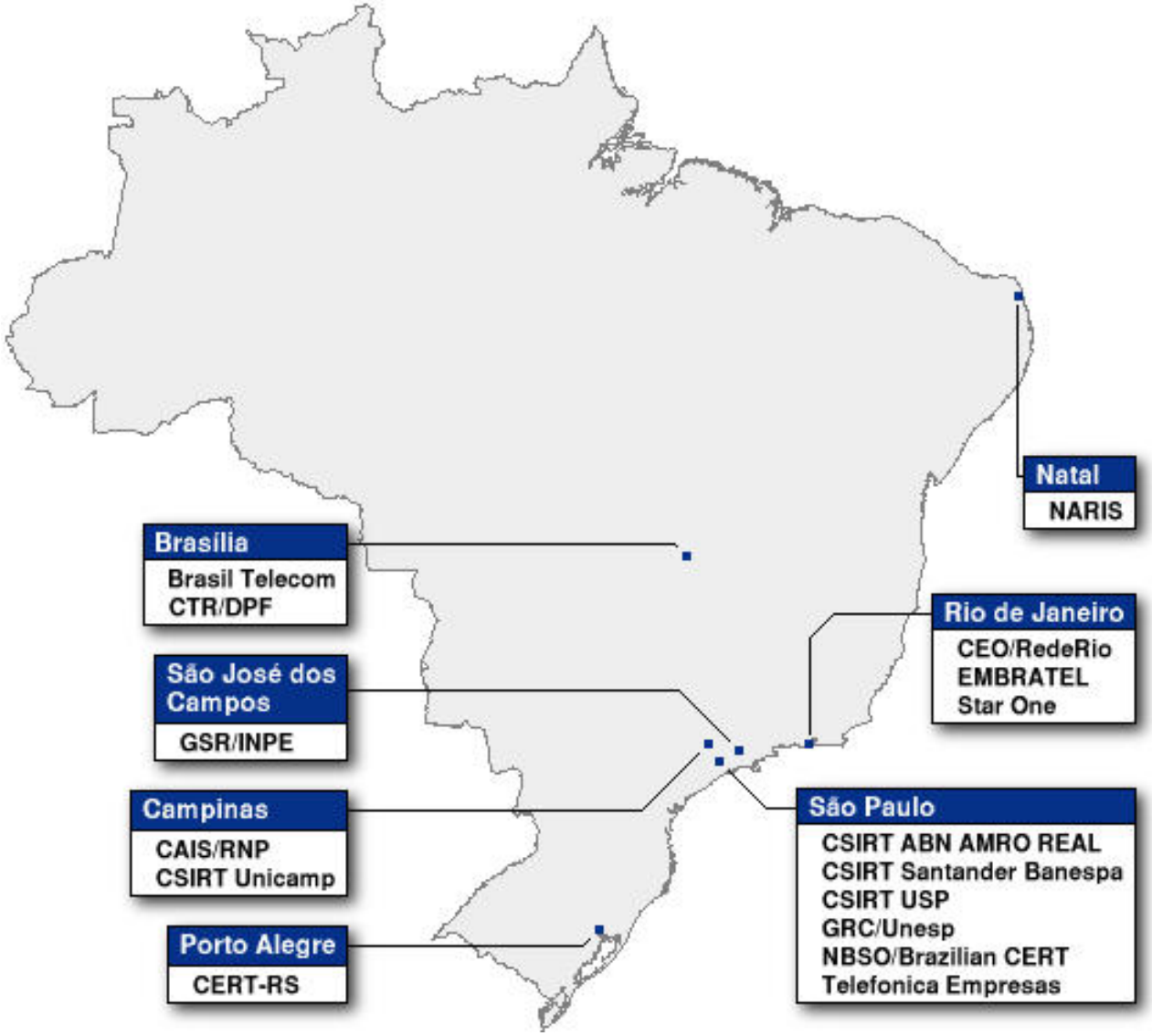
Missão do NBSO

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

CSIRTs Brasileiros



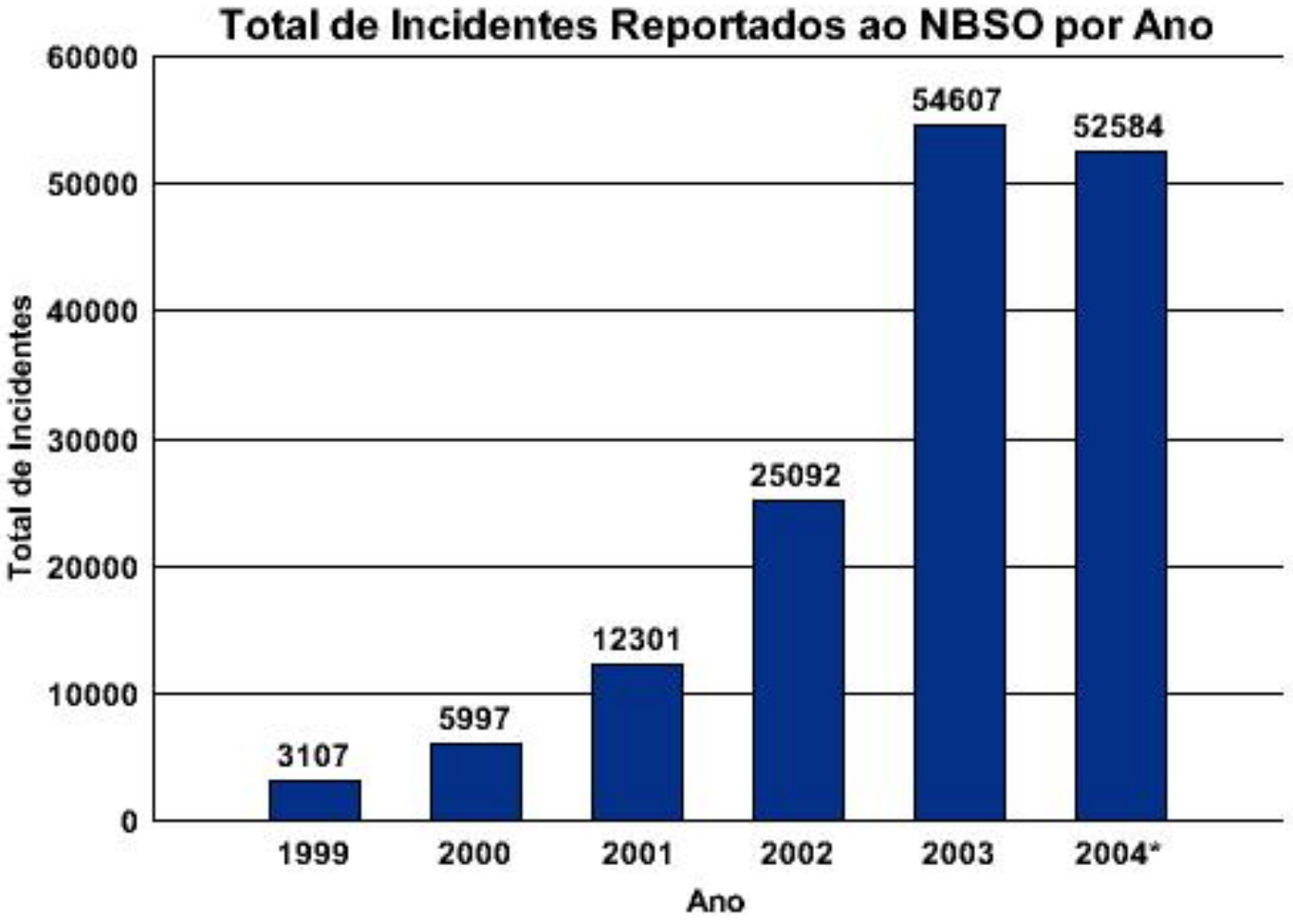
http://www.nbso.nic.br/contato-br.html

CSIRTs no Mundo

- Existem centenas de CSIRTs espalhados pelo mundo
- Um mapa com os nomes e localizações destes CSIRTs é mantido pelo CERT/CC:
  - http://www.cert.org/csirts/csirt-map.html

Tendências e Desafios

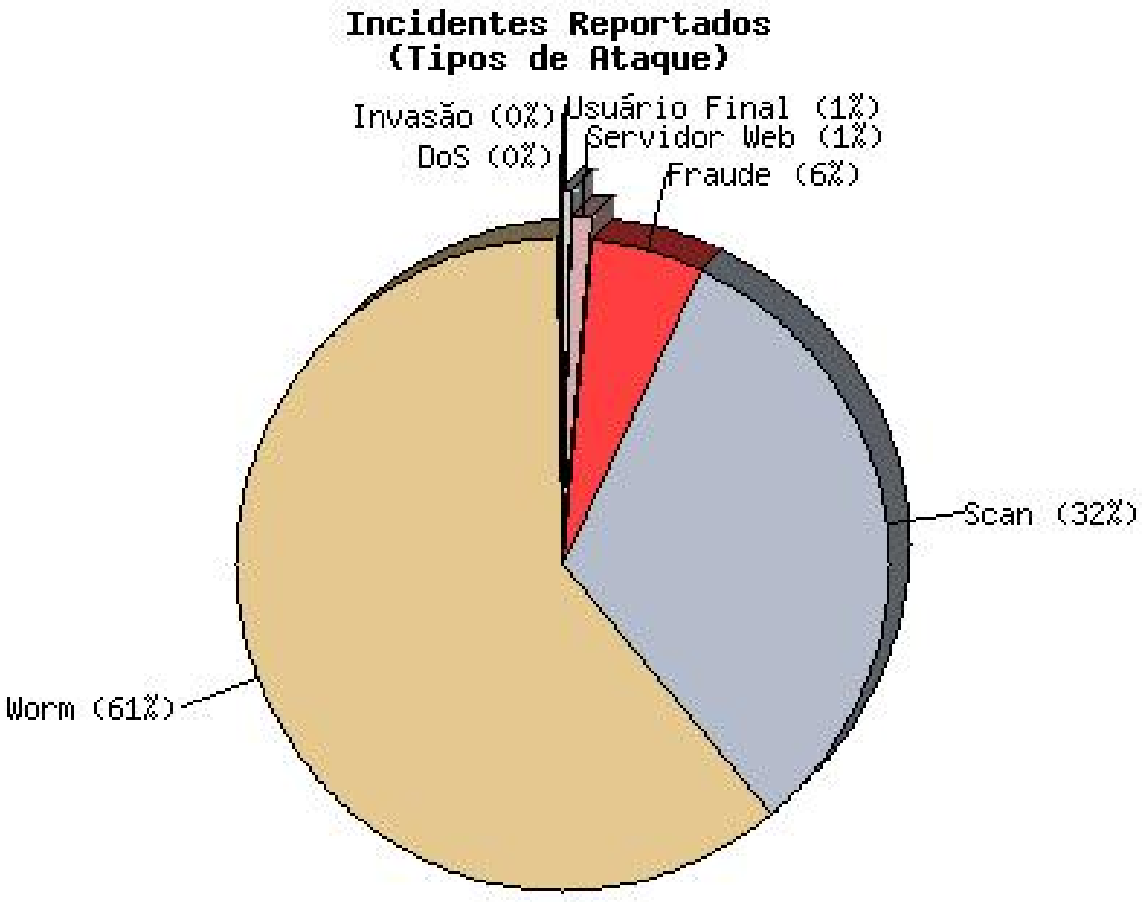
Incidentes Reportados ao NBSO



* Dados até setembro de 2004

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

Incidentes Reportados ao NBSO (cont.)



Dados de julho a setembro de 2004
http://www.nbso.nic.br/stats/incidentes/

Fraudes

- Grande crescimento
  - 2003: 593 (anual)
  - 2004: 2.340 (até setembro)
- engenharia social é a base
  - cavalos de tróia
  - scams
  - phishing scams

Worms

- Código malicioso que:
  - procura por máquinas vulneráveis
  - explora as vulnerabilidades
  - se copia para a máquina comprometida
  - reinicia o ciclo
- Exemplos:
  - Code Red, Nimda, Slammer, Slapper, Sasser

Worms (cont.)

- Bots:
  - procuram por máquinas vulneráveis
  - exploram múltiplas vulnerabilidades
  - se copiam para a máquina comprometida
  - instalam backdoors e se conectam em um canal de IRC
  - permitem administração remota
  - reiniciam o ciclo
- Exemplos:
  - Phatbot, Agobot, Gaobot

Worms (cont.)

- Botnets:
  - rede de bots controlada através de IRC
  - normalmente composta por centenas ou milhares de bots
- Utilização (geralmente por aluguel):
  - ataques de negação de serviço
  - envio de spam
  - realização de ataques diversos

Outras Tendências

- Defacements (geralmente via PHP)
  - aumentar o “zone-h score”
  - extorsão
  - score + fraude
- ataques de força bruta de ssh
  - senhas fracas
- carders + spammers + invasores + crime

Causas?

- softwares mal projetados e implementados
- crescimento da Internet comercial
- mudança de perfil dos usuários
- disseminação de banda larga
- softwares desatualizados
- falta de aplicação das correções
- uso inadequado de firewalls e antivírus

Desafios dos Próximos Anos

- Ataques cada vez mais automatizados
- Tempo entre a descoberta de uma vulnerabilidade e o lançamento de um exploit reduzindo dramaticamente
- Volume dos dados a serem analisados aumentando
- Parque de máquinas e complexidade crescentes

Honeypots Como Ferramentas de Auxílio

Honeypots – definições

- recursos computacionais dedicados a serem sondados, atacados ou comprometidos
- registro e controle dessas atividades
- todo tráfego destinado a um honeypot é anômalo ou malicioso
- menor quantidade de dados e falsos-positivos se comparados com firewalls e IDS tradicionais

Honeypots – tipos

Alta interatividade

- possui serviços legítimos
- permite monitorar atividades do invasor
- coleta de ferramentas
- difícil de manter
- maior risco

Honeypots – tipos (cont)

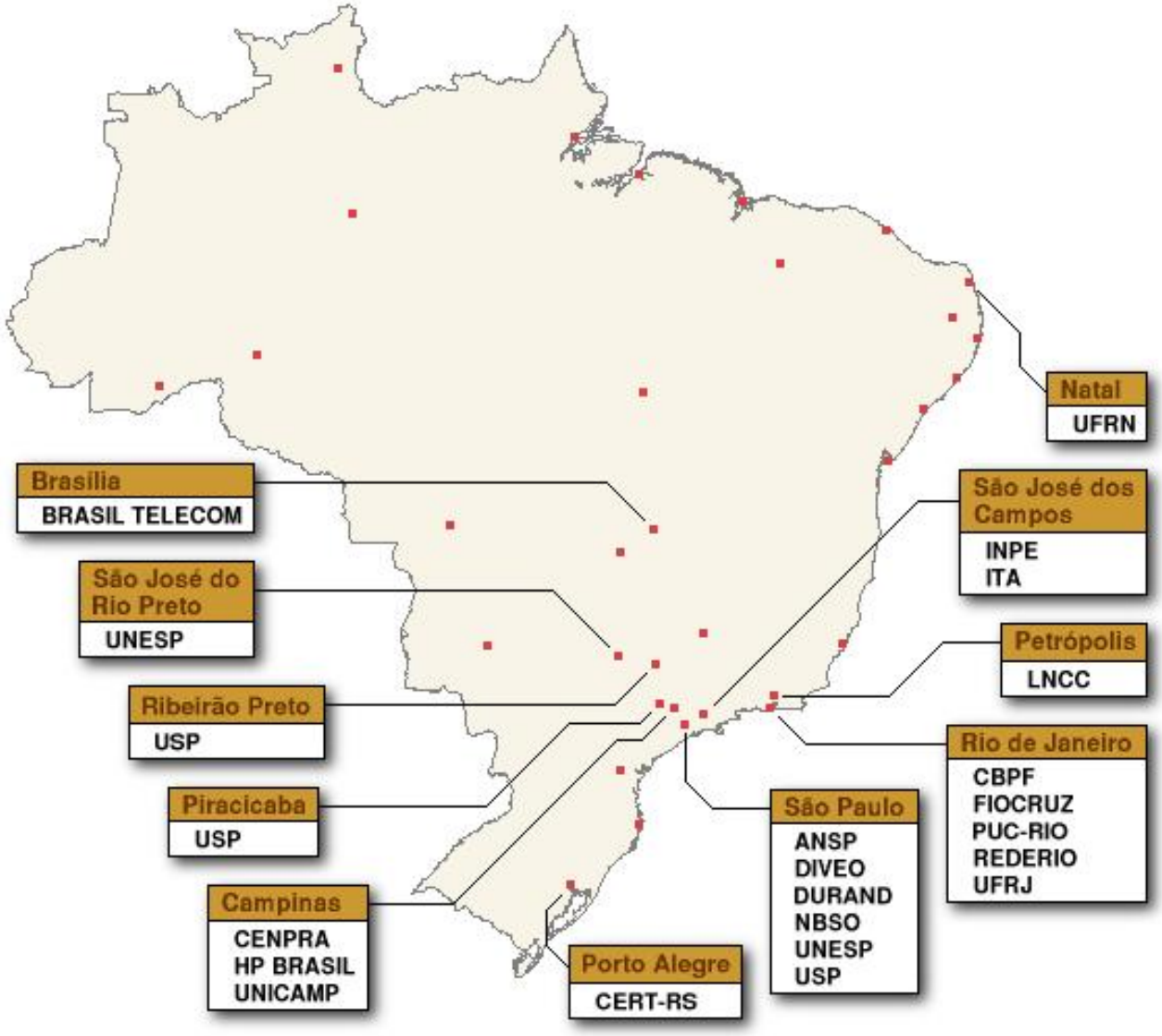
Baixa interatividade

- emulam serviços, não existe serviço real a ser atacado
- o atacante não pode comprometer o honeypot
- adequados para redes de produção

Consórcio Brasileiro de Honeypots

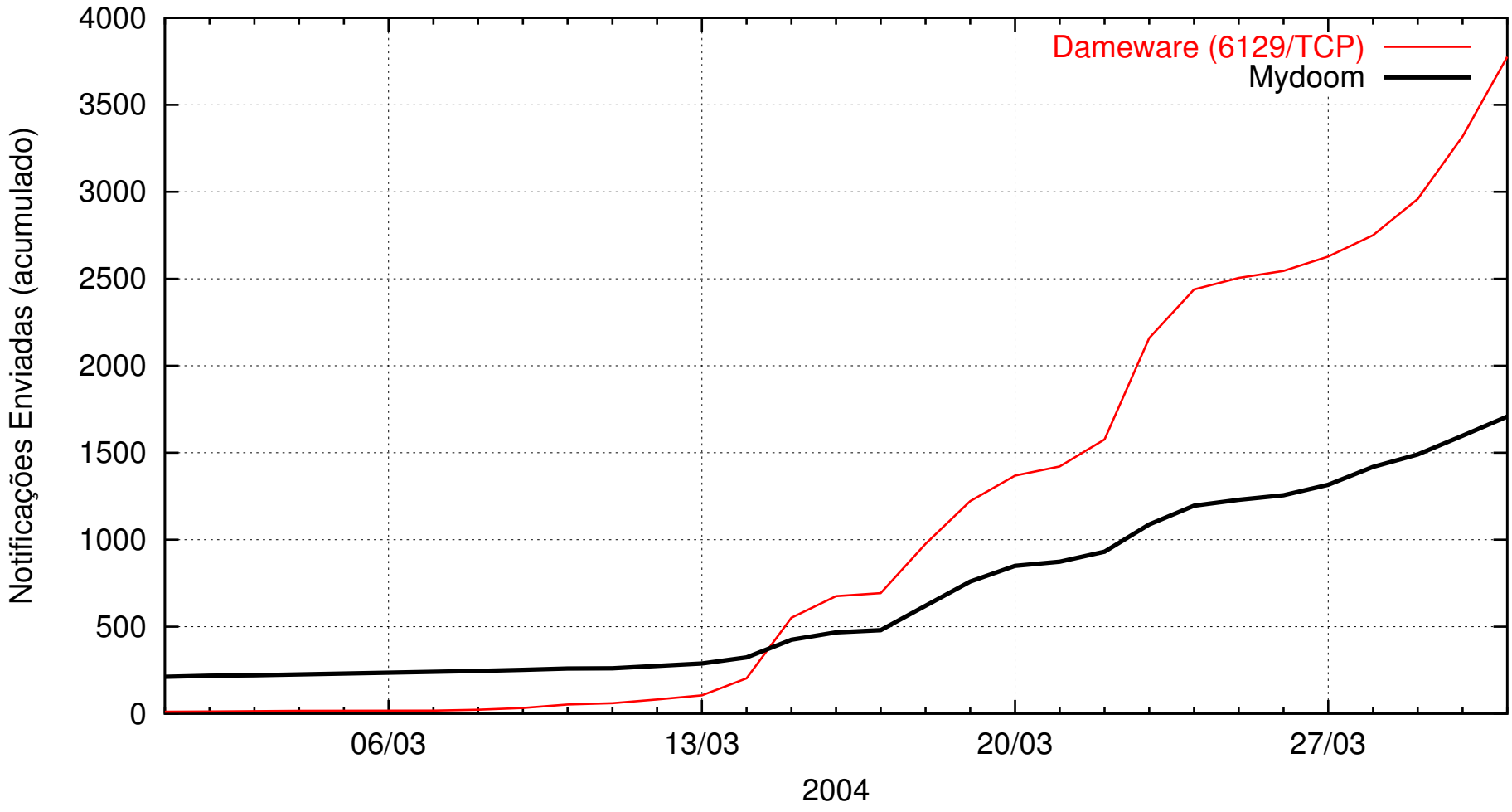
- Honeypots de baixa interatividade mantidos pelas instituições consorciadas
- Objetivo de aumentar, no espaço Internet brasileiro, a capacidade de:
  - detecção de incidentes
  - correlação de eventos
  - determinação de tendências de ataques
- Utilização dos dados por grupos de resposta a incidentes

Membros do Projeto

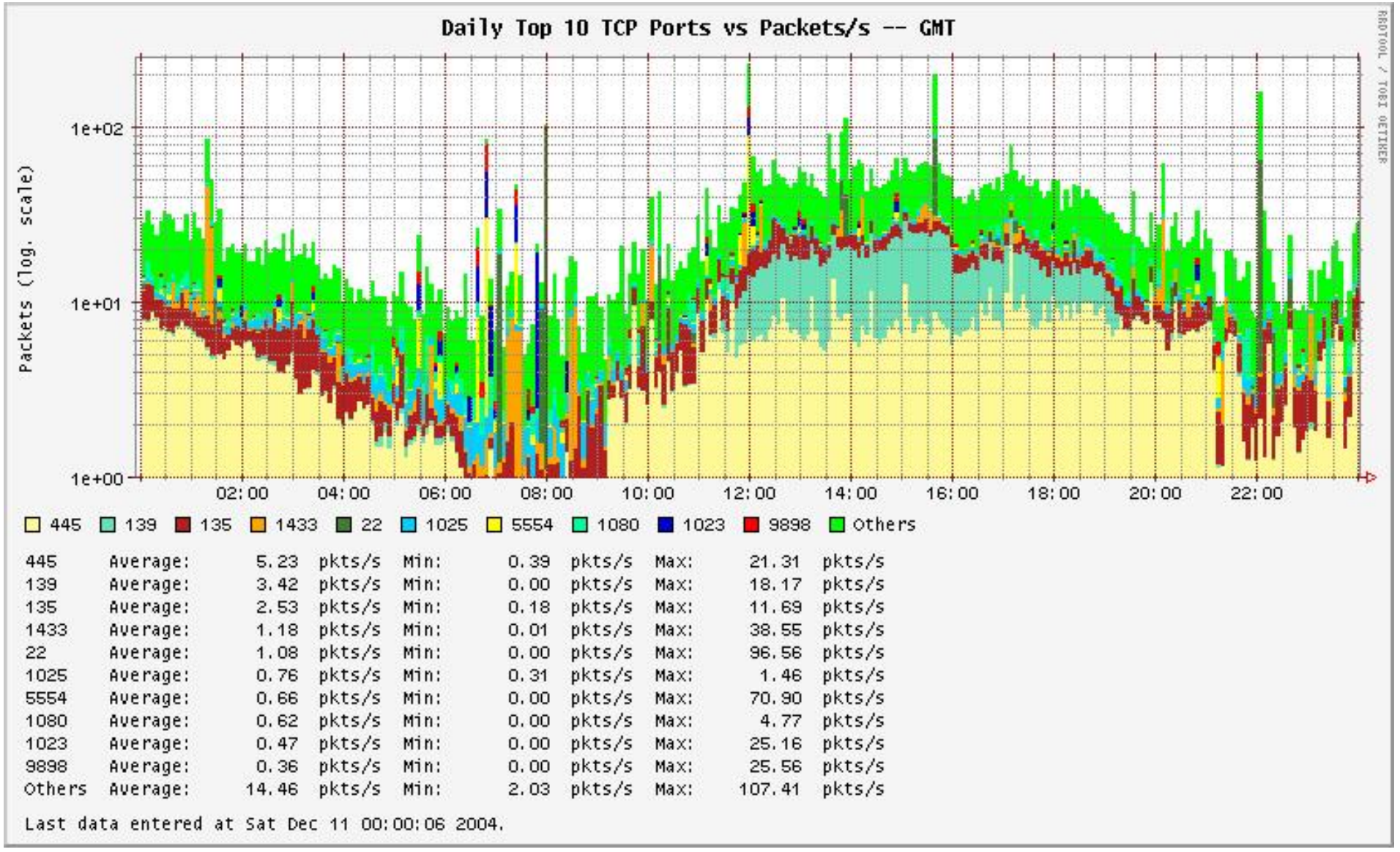


http://www.honeypots-alliance.org.br/

Identificação de Tendências



Atividades Maliciosas



Utilidade para o Administrador

- identificação de máquinas infectadas/comprometidas na instituição
- correlação com logs de outros equipamentos
- novas tendências
- comparação com outras instituições
- domínio de uma nova tecnologia
- modesto investimento em tempo e equipamento

Recomendações

Administradores

- Ter (e seguir) uma política de segurança
- Pensar em segurança desde o princípio
  - projeto da rede
  - planejamento da instalação
  - instalação do sistema
- Ter política de atualização e correção
- Implantar ferramentas de apoio e defesa
  - firewalls, IDSs, análise de flows, honeypots

Administradores (cont.)

- Manter-se atualizado – o grande desafio
  - trocar informações com outros administradores
  - manter relacionamento com CSIRTs próximos
  - assinar listas de discussão
  - ir a conferências, workshops, cursos
- Educar seus usuários
- Práticas de Segurança para Administradores de Redes Internet
  http://www.nbso.nic.br/docs/seg-adm-redes/

Usuários

- Mudar a postura ao utilizar a Internet
  - não seguir links, não executar anexos, não confiar em todas as informações
- manter o sistema atualizado
- utilizar firewall pessoal e antivírus
- Cartilha de Segurança para Internet
  http://www.nbso.nic.br/docs/cartilha/

Referências

- Esta palestra
  http://www.nbso.nic.br/docs/palestras/
- 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/
- Consórcio Brasileiro de Honeypots
  Projeto Honeypots Distribuídos
  http://www.honeypots-alliance.org.br/
- Ferramentas
  http://www.nbso.nic.br/tools/
- Cursos do CERT/CC ministrados pelo NBSO
  http://www.nbso.nic.br/cursos/