Novas Ameaças na Internet e Iniciativas do CERT.br e CGI.br para Combatê-las

Klaus Steding-Jessen
jessen@cert.br

Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil – CERT.br
http://www.cert.br/
Comitê Gestor da Internet no Brasil – CGI.br
http://www.cgi.br/

Roteiro

- Sobre o CGI.br e o CERT.br
- Situação atual
- Principais ameaças
- Formas de proteção
  - políticas de atualização
  - segurança em camadas
  - proteção da rede interna
  - acompanhar as tendências de ataques
  - educação de usuários
- Considerações finais

Sobre o CGI.br (cont)

Comitê Gestor da Internet no Brasil

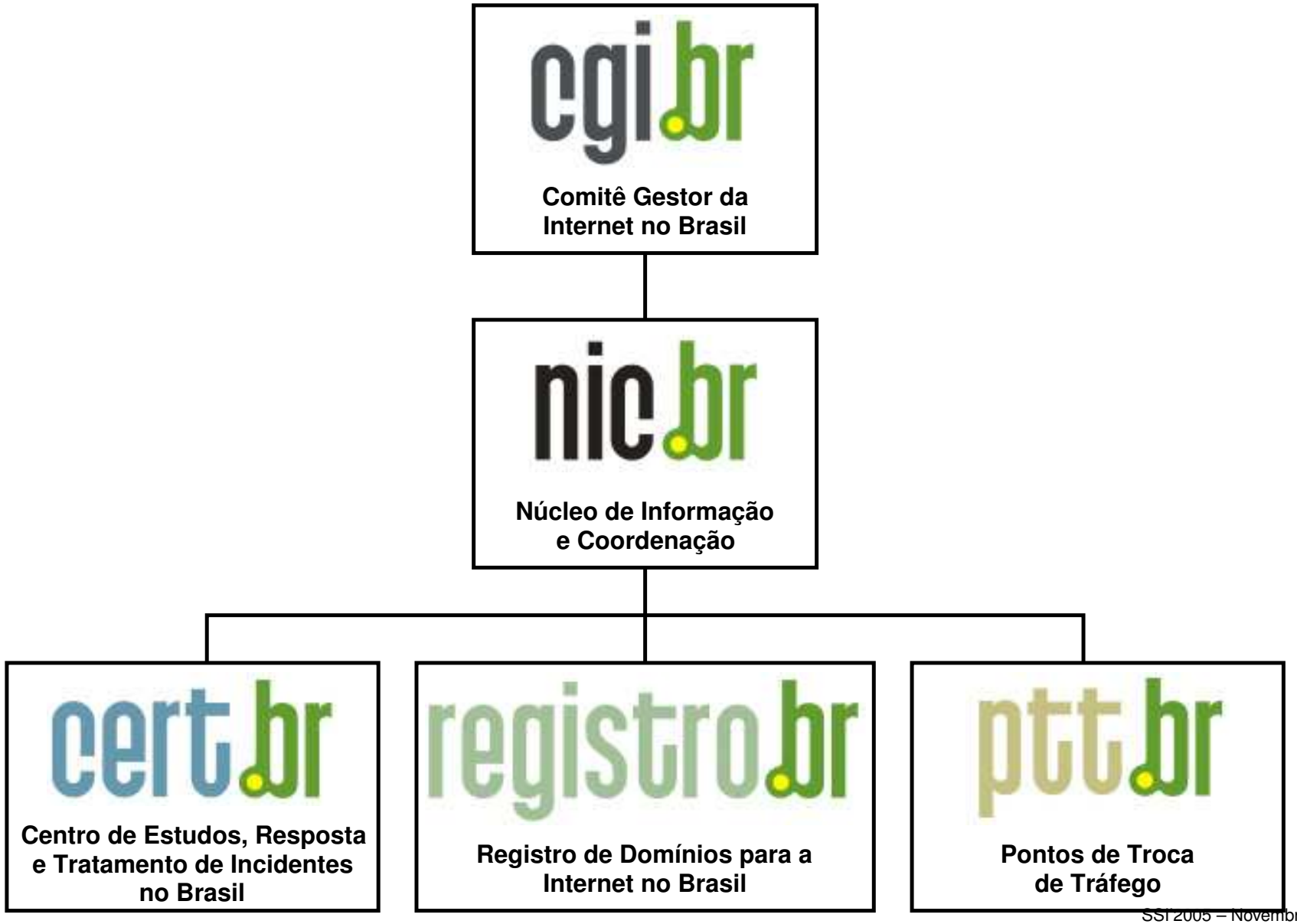
- Comitê criado pela Portaria Interministerial 147 de 31/05/1995, alterada pelo Decreto Presidencial 4.829 de 03/09/2003
  - 9 representantes do Governo Federal
  - 4 representantes do setor empresarial
  - 4 representantes do terceiro setor
  - 3 representantes da comunidade científica e tecnológica
  - 1 representante de notório saber em assuntos de Internet

Sobre o CGI.br (cont)

Algumas atribuições:

- 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.

Sobre o CGI.br / NIC.br



Sobre o CERT.br

Atividades do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (antigo NBSO)

- articulação das ações para resposta a incidentes envolvendo redes brasileiras
- manutenção de estatísticas sobre incidentes de segurança
- desenvolvimento de documentação sobre segurança para usuários de Internet e administradores de redes
- fomento à criação de novos Grupos de Resposta a Incidentes (CSIRTs) no Brasil
- cursos do CERT/CC sobre tratamento de incidentes
- coordena o Consórcio Brasileiro de Honeypots – Projeto Honeypots Distribuídos

Ameaças Atuais

Principais Ameaças

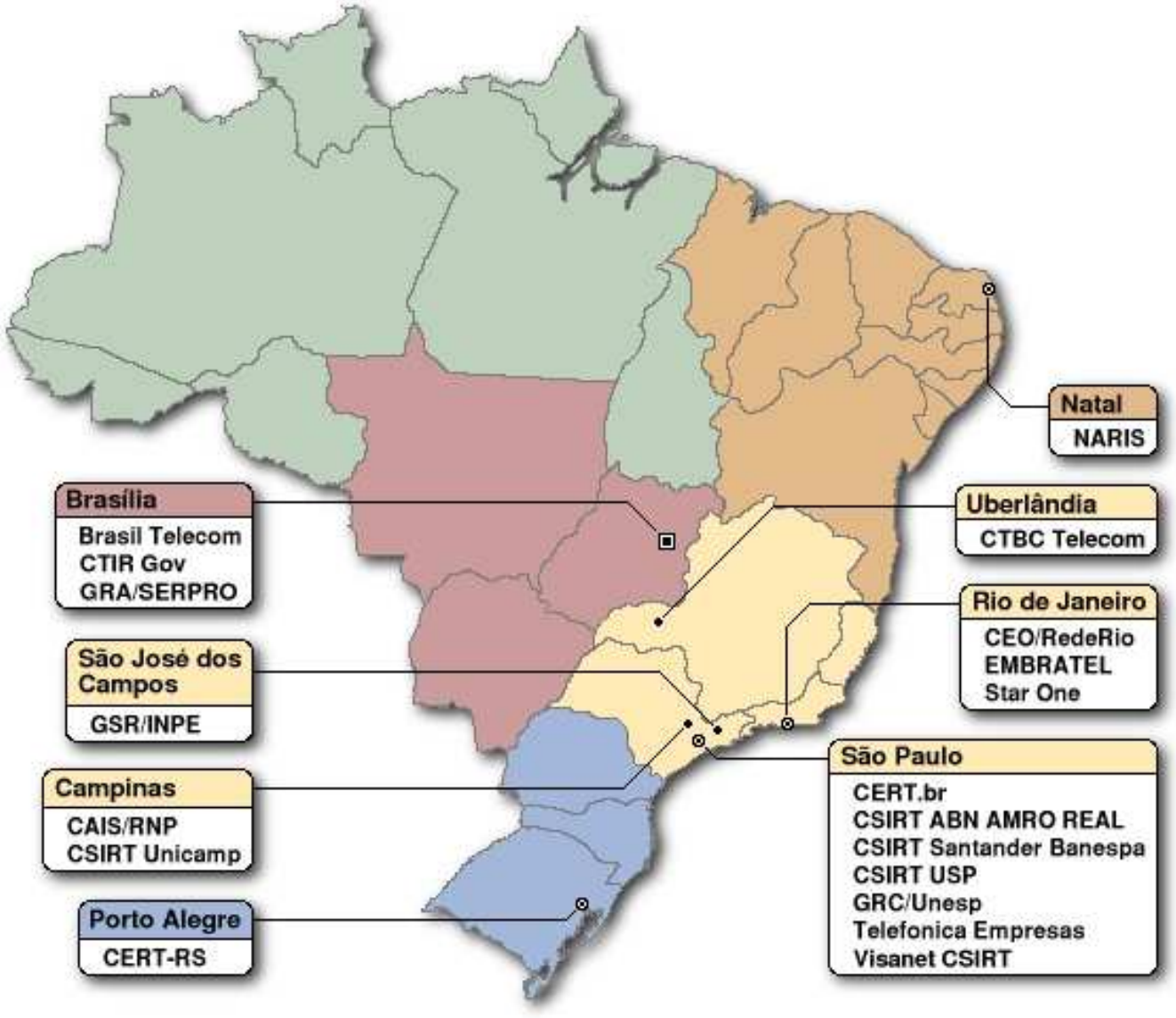
- vulnerabilidades freqüentes
- códigos maliciosos explorando essas vulnerabilidades, em curto espaço de tempo
- ferramentas automatizadas de ataque
- atacantes + spammers
- ataques de força bruta
- Redes mal-configuradas sendo abusadas para realização de todas estas atividades – sem o conhecimento dos donos

Principais Ameaças (cont)

- Botnets
  - usadas para envio de scams, phishing, invasões, esquemas de extorsão
- Alvo migrando para usuários finais
- fraudes / scams / phishing
- Crime Organizado
  - aliciando spammers e invasores
  - injetando dinheiro na “economia underground”

Iniciativas de Combate

Integração dos Grupos de Resposta



http://www.cert.br/contato-br.html

Integração dos Grupos de Reposta (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 (reconhecidos pelo CERT.br)

iNOC-DBA (Internet Network Operation Centers – Dial By AS Number), a global hotline phone system which directly interconnects the Network Operations Centers and Security Incident Response Teams

Acompanhamento de Tendências

Projeto Honeypots Distribuídos

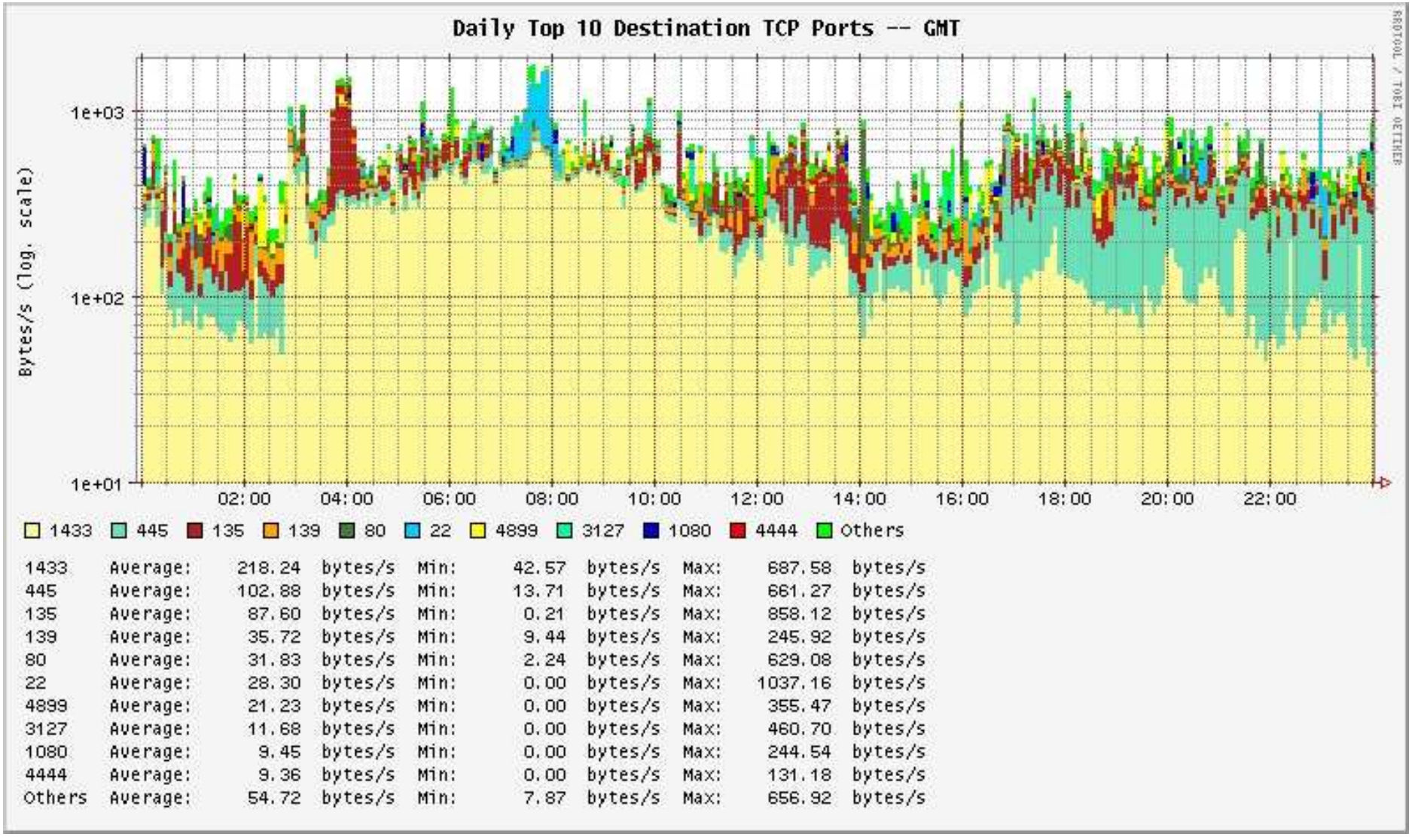
- coordenação: CenPRA/MCT e CERT.br
- 27 instituições parceiras:
  - academia, governo, teles, empresas
- honeypots distribuídos no Brasil
  - em diversos AS e em diferentes localidades
- com base em trabalho voluntário
- mantém estatísticas públicas
  - flows diários das atividades combinadas dos honeypots

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

Acompanhamento de Tendências (cont.)

Cidades onde os honeypots estão localizados.

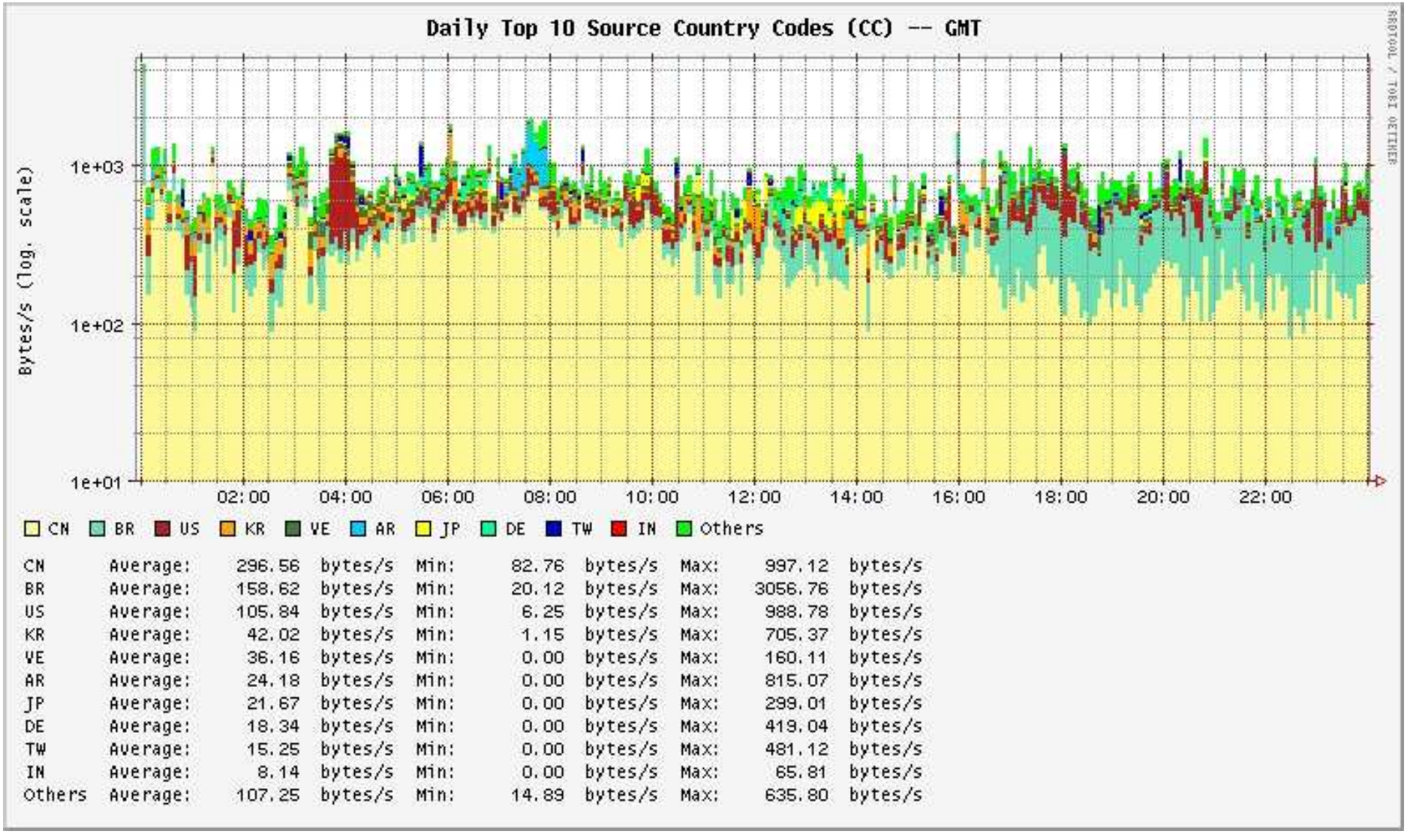
Acompanhamento de Tendências (cont.)



1433	Average:	218.24	bytes/s	Min:	42.57	bytes/s	Max:	687.58 bytes/s
445	Average:	102.88	bytes/s	Min:	13.71	bytes/s	Max:	661.27 bytes/s
135	Average:	87.60	bytes/s	Min:	0.21	bytes/s	Max:	858.12 bytes/s
139	Average:	35.72	bytes/s	Min:	9.44	bytes/s	Max:	245.92 bytes/s
80	Average:	31.83	bytes/s	Min:	2.24	bytes/s	Max:	629.08 bytes/s
22	Average:	28.30	bytes/s	Min:	0.00	bytes/s	Max:	1037.16 bytes/s
4899	Average:	21.23	bytes/s	Min:	0.00	bytes/s	Max:	355.47 bytes/s
3127	Average:	11.68	bytes/s	Min:	0.00	bytes/s	Max:	460.70 bytes/s
1080	Average:	9.45	bytes/s	Min:	0.00	bytes/s	Max:	244.54 bytes/s
4444	Average:	9.36	bytes/s	Min:	0.00	bytes/s	Max:	131.18 bytes/s
Others	Average:	54.72	bytes/s	Min:	7.87	bytes/s	Max:	656.92 bytes/s

Estatísticas do Projeto Honeypots Distribuídos – 05/11/2005.

Acompanhamento de Tendências (cont.)



Estatísticas do Projeto Honeypots Distribuídos – 05/11/2005.

Projeto Honeypots Distribuídos (cont.)

Uso, pelo CERT.br, dos dados dos honeypots em Tratamento de Incidentes

- identificação de assinaturas de atividades maliciosas/abusivas conhecidas
  - worms, bots, scans, spam e outros
- notificação dos responsáveis pelas redes de IPs alocados ao Brasil
  - fornecidas dicas de recuperação

Acompanhamento de Tendências (cont.)

- outros projetos *Early Warning* internacionais
  - http://www.arakis.pl/
  - http://www.jpcert.or.jp/isdas/index-en.html
  - http://www.ecsirt.net/
  - http://www.cymru.com/Darknet/

Ações Antifraude

- trabalho conjunto entre algumas instituições financeiras e o CERT.br
- trocas de informações sobre técnicas e sites hospedando páginas clonadas ou códigos maliciosos
- CERT.br é um Anti-Phishing Working Group Research Partner (http://www.antiphishing.org/)
  - notifica os sites hospedando os malwares
  - interage com sites internacionais para agilizar retirada de malwares do ar
  - envia novos exemplares para mais de 20 fabricantes de antivírus

CT-Spam do CGI.br

Missão da Comissão de Trabalho sobre Spam:

- propor uma estratégia nacional de combate ao spam
- articular as ações entre os diferentes atores
- documentos escritos:
  - “Tecnologias e Políticas para Combate ao Spam”
  - “Análise Técnica de Algumas Legislações sobre Spam”
- desenvolver um site anti-spam
  - dicas para usuários
  - melhores práticas para administradores de redes

http://www.cgi.br/eventos/int-ctspam.htm

Recomendações Gerais

Segurança em Camadas

Não há uma solução única para resolver todos os problemas.

- combinar soluções
- firewall, IDS, sistemas atualizados, antivírus
- múltiplas plataformas
- treinamento, atualização dos profissionais

Proteção da Rede Interna

grande risco: propagação de códigos maliciosos de dentro para fora (worms e bots)

- compartimentalização da rede
- política de atualização e correção
- política de conexão de equipamentos na rede interna
  - terceirizados
  - notebooks de funcionários, etc

Ataques de Força Bruta Contra SSH

Dicas para defesa:

- utilizar senhas fortes em todas as contas
- reduzir o número de equipamentos com esse serviço exposto
- restringir a origem das conexões
- acessar via chaves públicas
- monitorar, monitorar, monitorar...

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

Mais Informações sobre Boas Práticas

Práticas de Segurança para Administradores de Redes Internet

http://www.cert.br/docs/seg-adm-redes/

- recomendações para obter o mínimo necessário de segurança
- planejada nova versão para o primeiro trimestre de 2006

Educação dos usuários

- usuários podem ser um risco para a organização
- vetores de disseminação de worms/vírus
- alvos de:
  - ataques de engenharia social
  - phishing/scam
  - cavalos de tróia
  - furto de informações

Educação dos usuários (cont)

Cartilha de Segurança: documento com recomendações e dicas para aumentar a segurança e proteção do usuário de ameaças na Internet.

- 2000: primeira versão, em conjunto com a Abranet
- 2003: segunda versão: ampliada, dividida em partes e disponível também em HTML
- 2005: terceira versão

http://cartilha.cert.br/

http://cartilha.cert.br/

Links de Interesse

- Cursos do CERT.br

  http://www.cert.br/cursos/

- Cartilha de Segurança para Internet

  http://cartilha.cert.br/

- Práticas de Segurança para Administradores de Redes Internet

  http://www.cert.br/docs/seg-adm-redes/

- Consórcio Brasileiro de Honeypots

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