Principais Ameaças na Internet e Recomendações para Prevenção

Cristine Hoepers
cristine@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
- Principais ameaças
- Recomendações para estruturação e atuação das áreas de segurança
- Considerações finais

Sobre o CGI.br (cont)

Comitê Gestor da Internet no Brasil

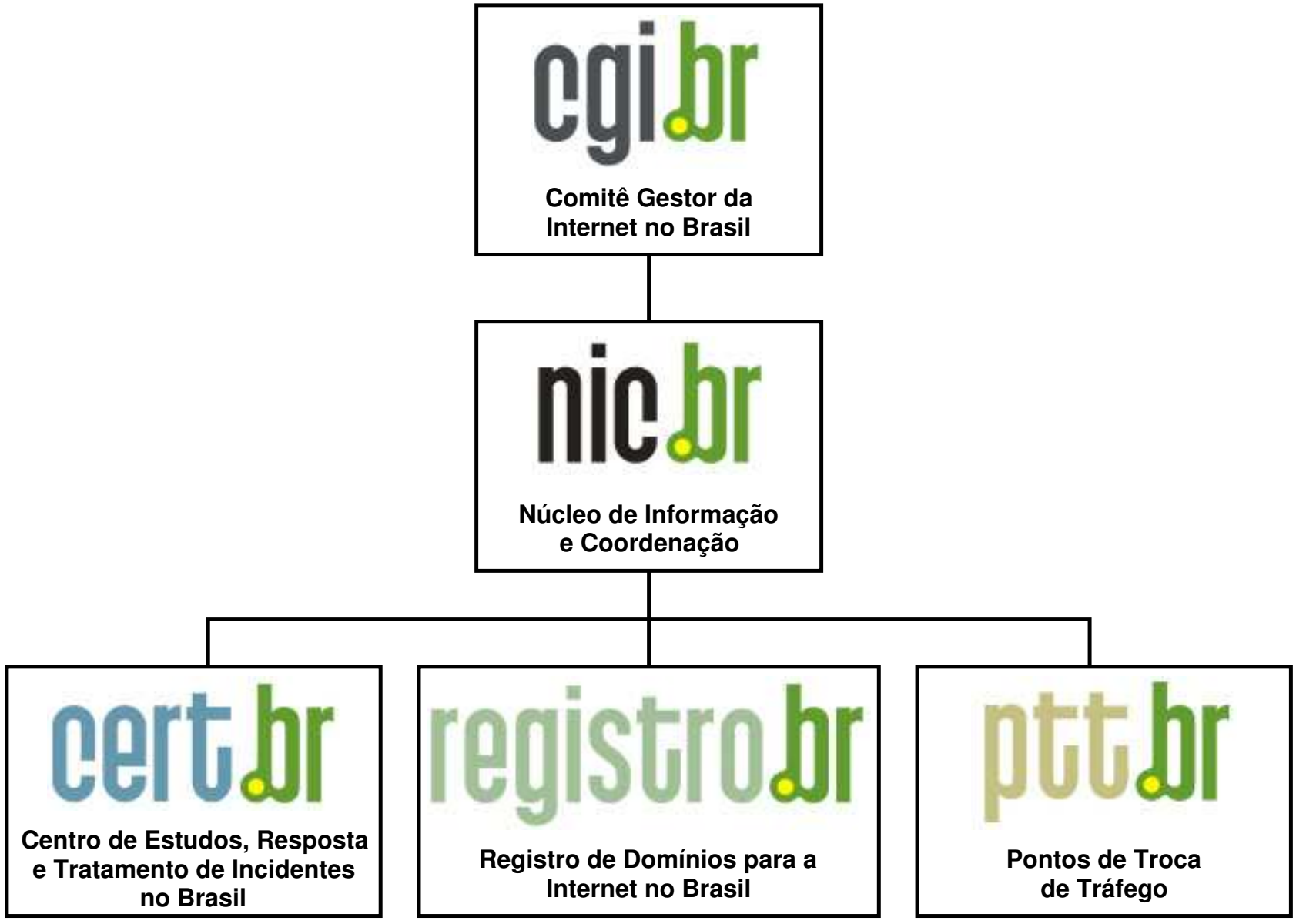
- Comitê criado pela Portaria Interministerial 147 de 31/05/1995, que foi alterada pelo Decreto Presidencial 4.829 de 03/09/2003
  - 9 representantes do Governo Federal
  - 4 representantes do setor empresarial
  - 4 representantes do terceiro setor
  - 3 representantes da comunidade científica e tecnológica
  - 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
- coordenação do Consórcio Brasileiro de Honeypots – Projeto Honeypots Distribuídos

Principais Ameaças

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)

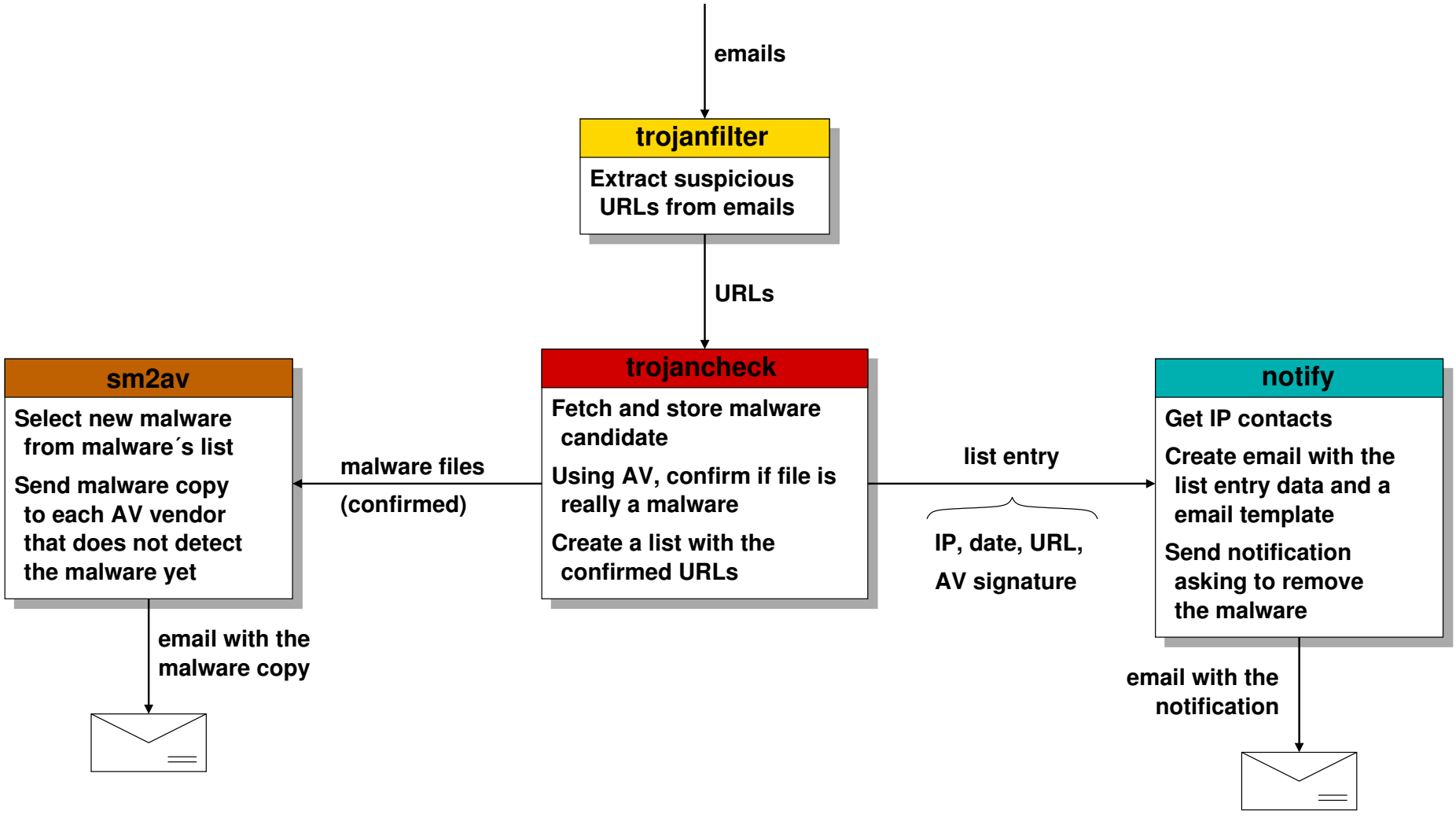
- Botnets
  - usadas para envio de scams, phishing, invasões, DoS, esquemas de extorsão
- Alvo migrando para usuários finais
- Fraudes / scams / phishing
- Crime Organizado
  - aliciando spammers e invasores
  - injetando dinheiro na “economia underground”

Atuação do CERT.br contra Fraudes

- Cooperação com algumas instituições financeiras
- CERT.br é um Anti-Phishing Working Group (APWG) Research Partner
  - 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

http://www.antiphishing.org/

Atuação do CERT.br contra Fraudes (cont.)



Estatísticas de Fraudes do CERT.br

Enviados 11262 exemplares de trojans para empresas de antivírus (06/04/2005 a 31/12/2005).

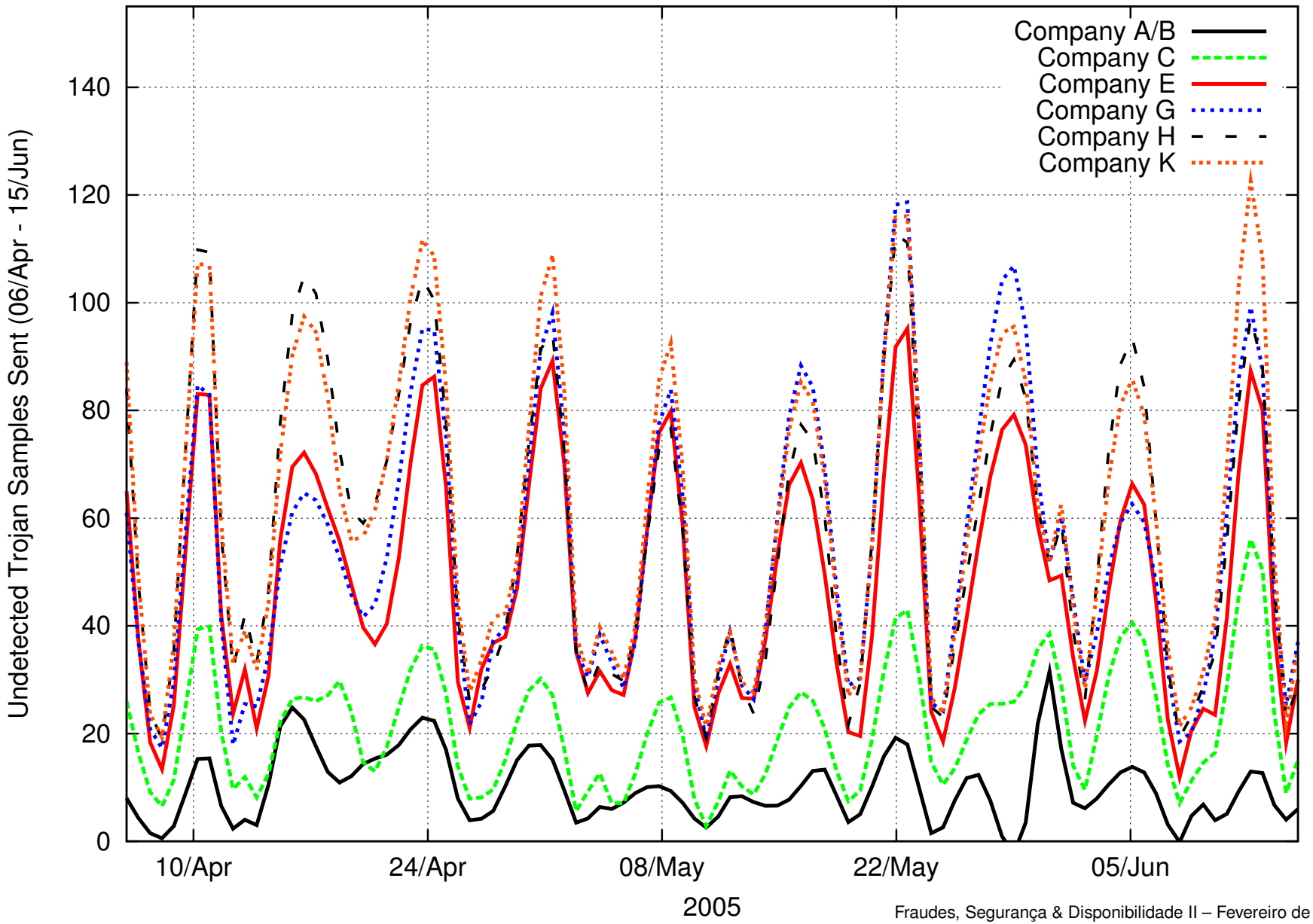
Antivírus	trojans enviados	porcentagem de detecção
Company A	1241	88.98 %
Company B	1241	88.98 %
Company D	4062	63.93 %
Company C	4155	63.11 %
Company E	7300	35.18 %
Company F	7405	34.25 %
Company G	8088	28.18 %
Company H	8297	26.33 %
Company I	8405	25.37 %
Company J	8913	20.86 %
Company K	10050	10.76 %
Company L	10537	6.44 %

Estatísticas de Fraudes do CERT.br (cont)

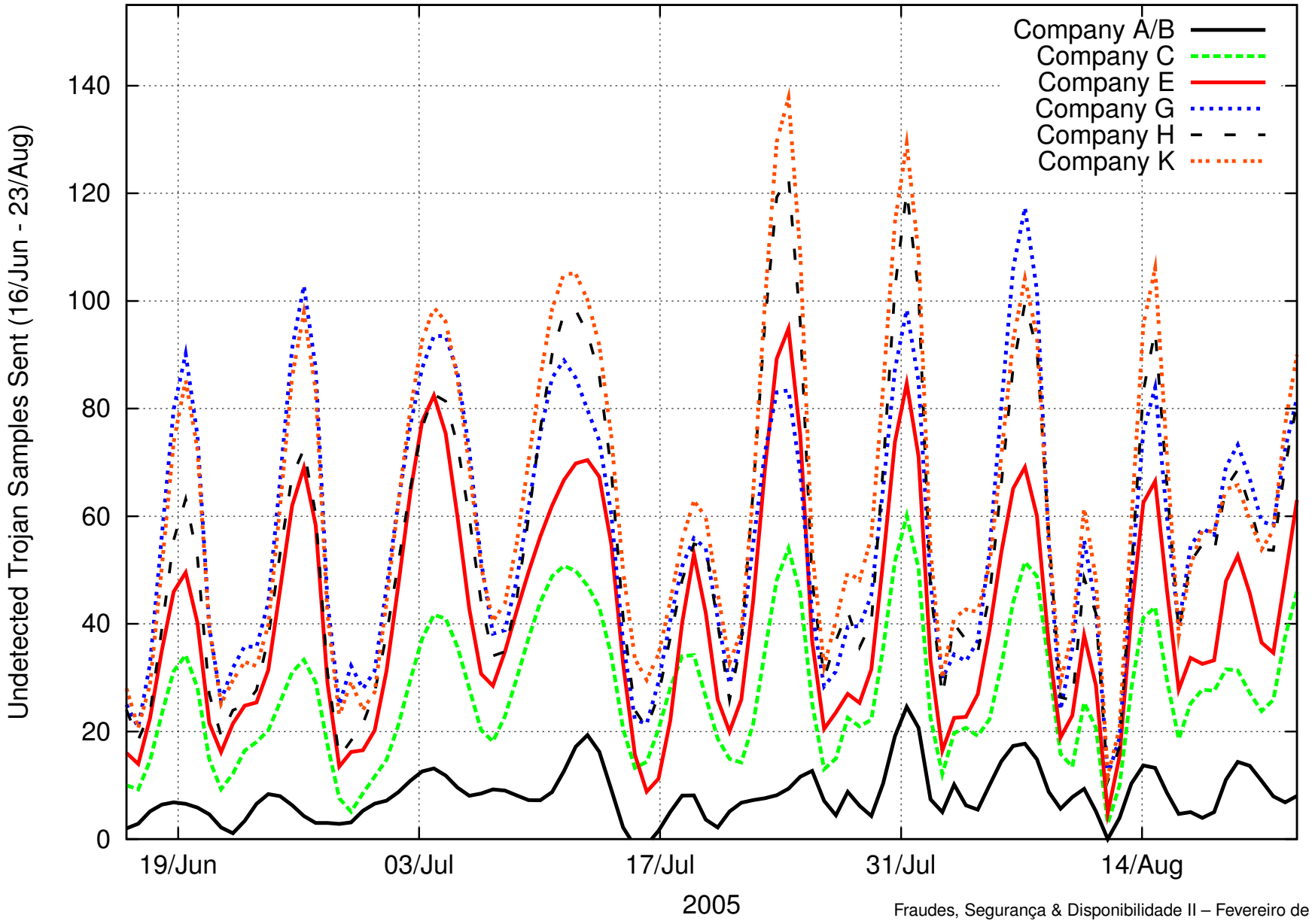
Enviados 2848 exemplares de trojans para empresas de antivírus (01/01/2006 a 16/02/2006).

Antivírus	trojans enviados	porcentagem de detecção
Company A	264	90.73 %
Company B	264	90.73 %
Company E	542	80.97 %
Company D	1088	61.80 %
Company C	1275	55.23 %
Company J	2016	29.21 %
Company F	2030	28.72 %
Company G	2056	27.81 %
Company H	2263	20.54 %
Company I	2613	8.25 %
Company K	2615	8.18 %
Company L	2628	7.72 %

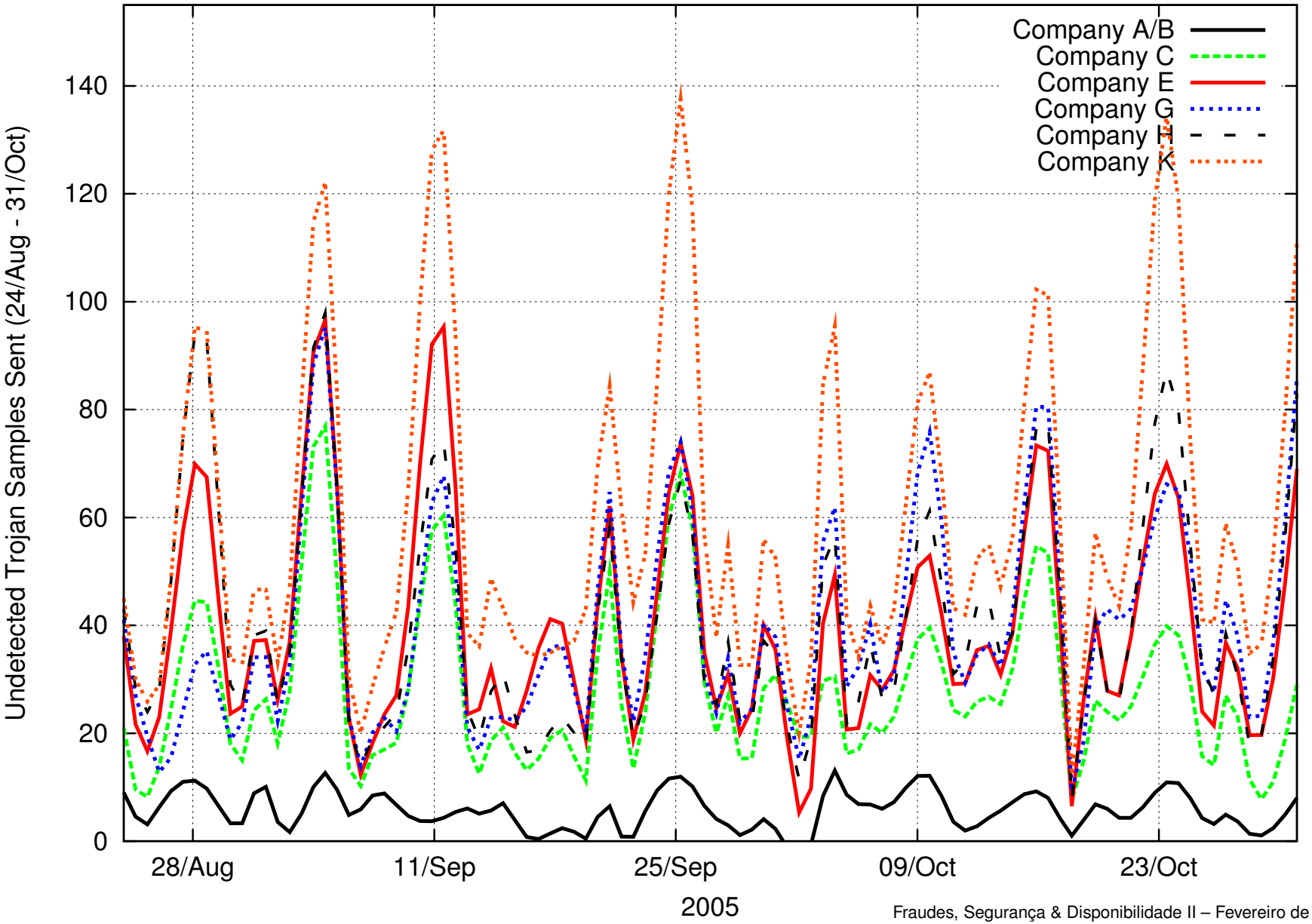
Estatísticas de Fraudes do CERT.br (cont)



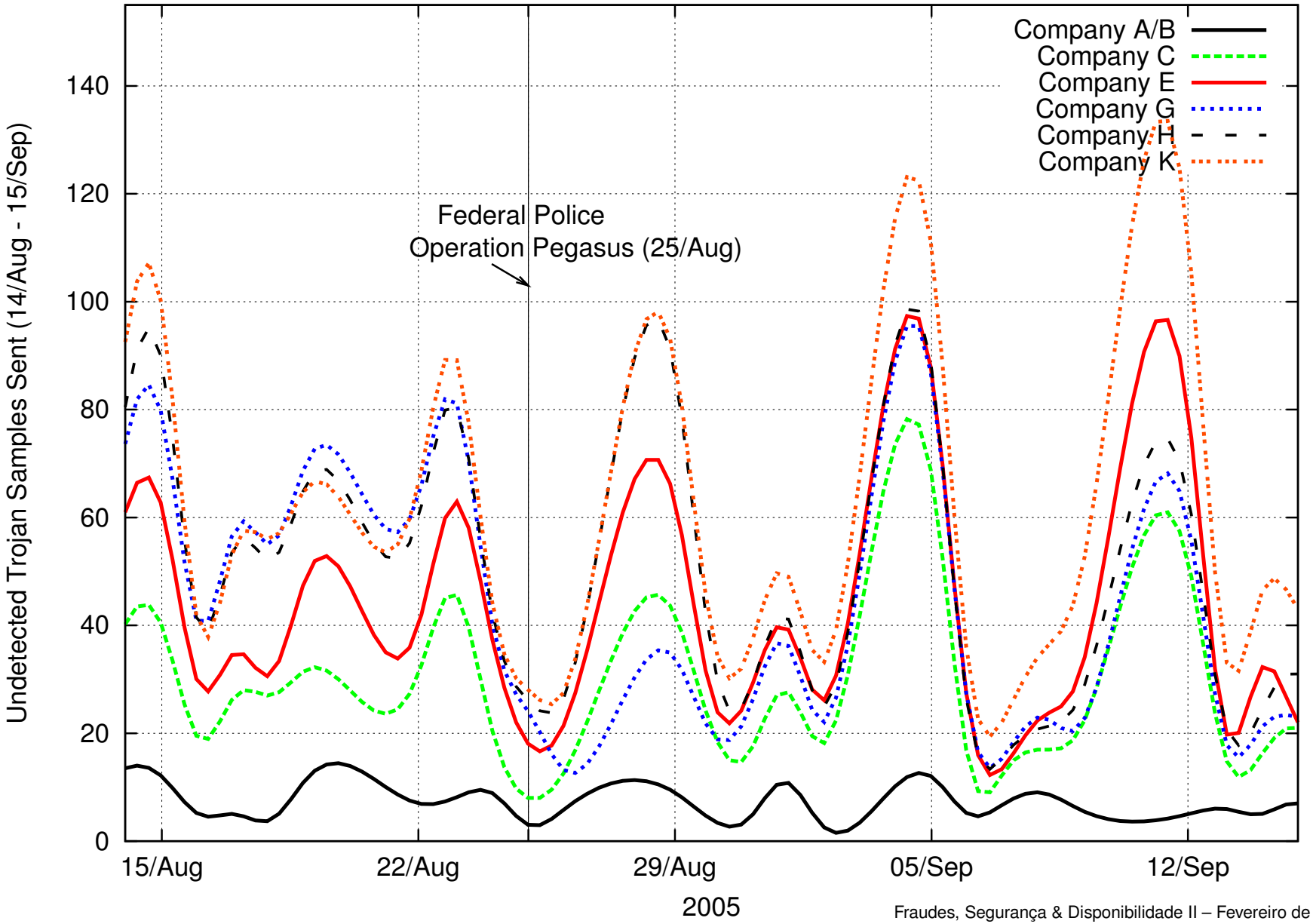
Estatísticas de Fraudes do CERT.br (cont)



Estatísticas de Fraudes do CERT.br (cont)



Estatísticas de Fraudes do CERT.br (cont)



Estatísticas de Fraudes do CERT.br (cont)

Domínios que mais receberam notificações por hospedarem cavalos de tróia (2005):

total	domínio
3451	aol.co.uk
2699	gratisweb.com
1606	netscape.com
927	aol.com.au
614	aol.com
435	americaonline.com.ar
287	hometown.aol.de
268	webcindario.com
229	telepolis.com
214	terra.com.br
213	uol.com.br
212	perso.wanadoo.es
165	aol.com.br
160	100free.com

Estatísticas de Fraudes do CERT.br (cont)

Domínios que mais receberam notificações por hospedarem cavalos de tróia (2006):

total	domínio
1155	gratisweb.com
414	aol.com.au
326	aol.com
203	americaonline.com.ar
162	webcindario.com
130	rapidupload.com
122	200.96.232.42
116	perso.wanadoo.es
96	zupload.com
89	loveni.com
83	filesxfer.com
76	82.88.114.91
71	telepolis.com
61	hometown.aol.de

Estatísticas de Fraudes do CERT.br (cont)

Extensões e países de origem mais freqüentes (2005):

total	(%)	extensão
14954	75.27	exe
4081	20.54	scr
431	2.17	zip
221	1.11	jpg
30	0.15	rar
29	0.15	com
21	0.11	gif
15	0.08	js & php
14	0.07	html
12	0.06	txt
10	0.05	bmp

total	(%)	CC
3112	45.41	US
1244	18.15	BR
293	4.28	KR
271	3.95	ES
248	3.62	DE
203	2.96	GB
187	2.73	IT
187	2.73	RU
179	2.61	CA
137	2.00	FR
131	1.91	CN

Estatísticas de Fraudes do CERT.br (cont)

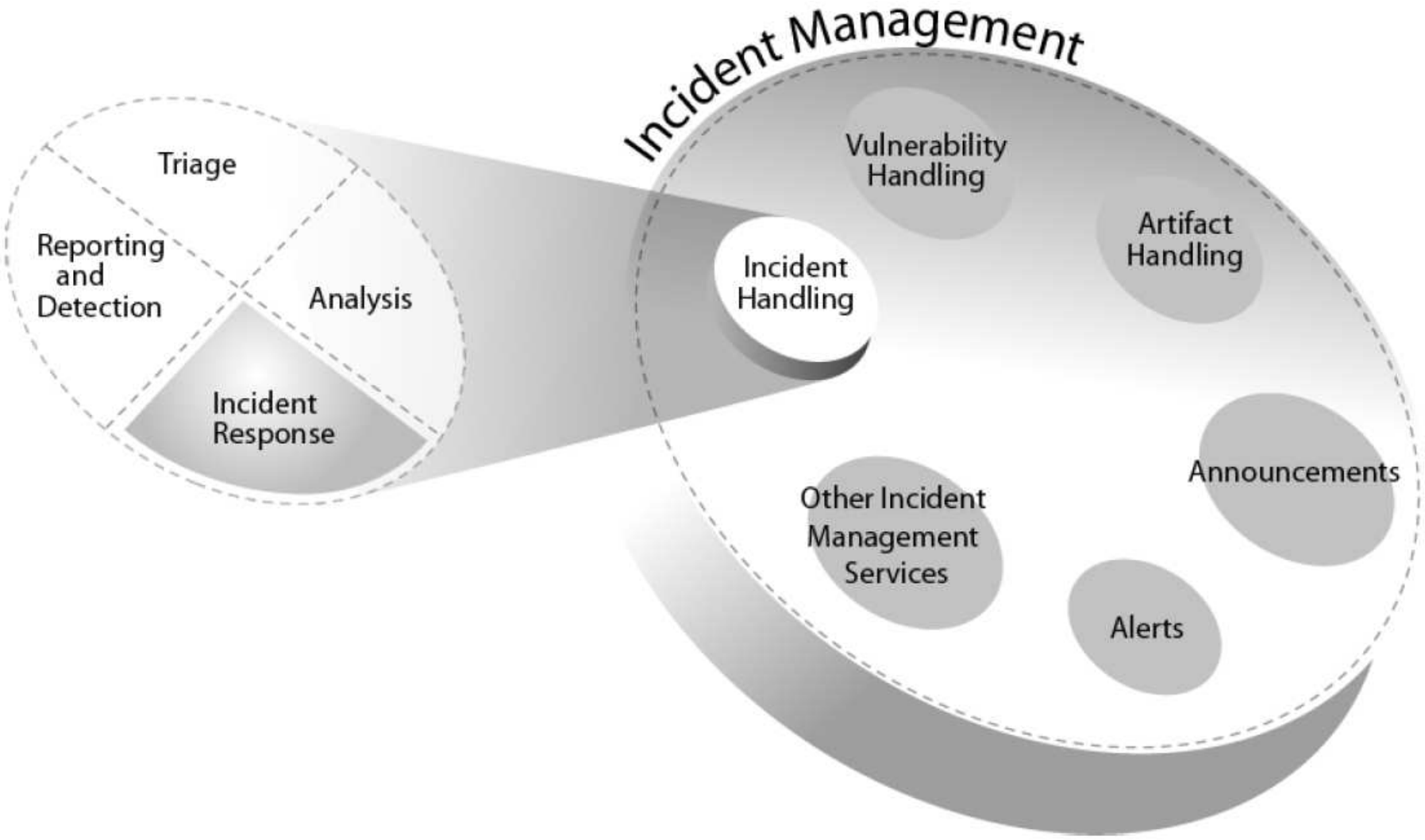
Extensões e países de origem mais freqüentes (2006):

total	(%)	extensão
3298	63.69	exe
1241	23.97	scr
320	6.18	php
97	1.87	zip
68	1.31	cmd
51	0.98	bmp
39	0.75	jpg
22	0.42	com
11	0.21	kbc
10	0.19	klg
7	0.14	rar

total	(%)	CC
857	48.09	US
227	12.74	BR
96	5.39	RU
80	4.49	DE
64	3.59	KR
54	3.03	CN
46	2.58	CA
44	2.47	ES
41	2.30	IT
39	2.19	FR
30	1.68	AR

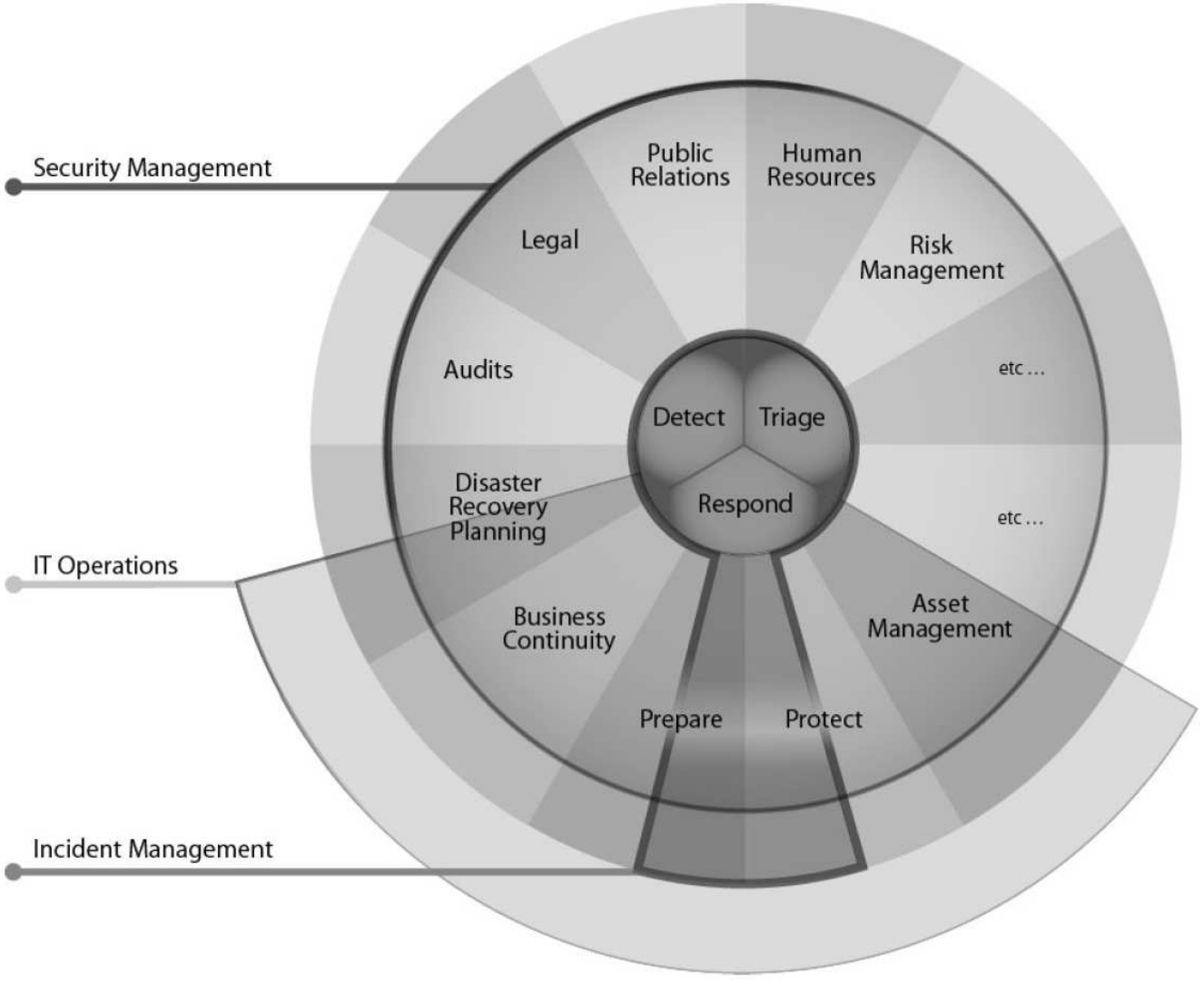
Recomendações para Estruturação e Atuação das Áreas de Segurança

Investir em Gestão de Incidentes



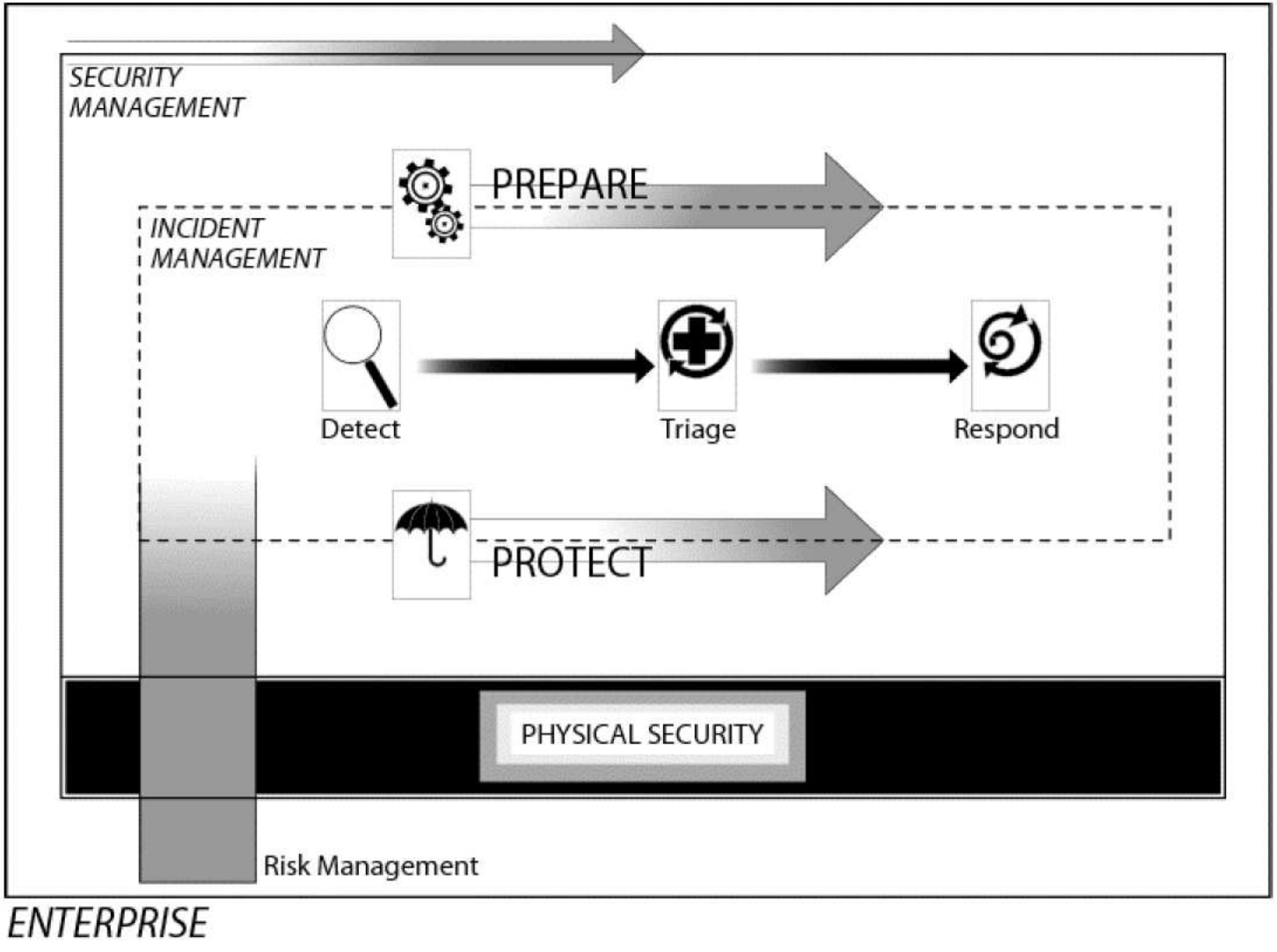
Fonte: Defining Incident Management Processes for CSIRTs: A Work in Progress.
Figura utilizada com permissão do CERT/CC e do SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Gestão de Incidentes x Gestão de Segurança



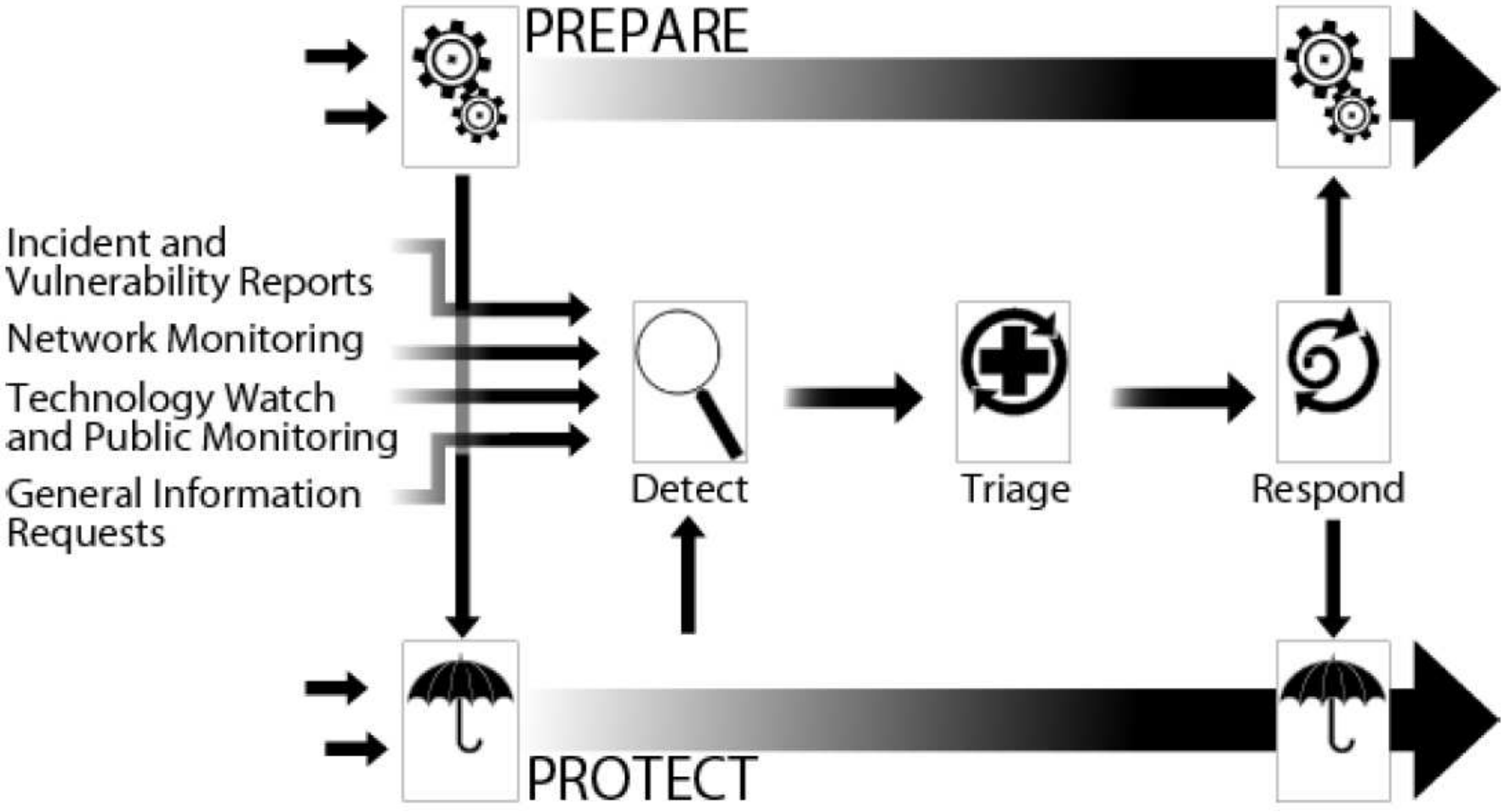
Fonte: Defining Incident Management Processes for CSIRTs: A Work in Progress.
Figura utilizada com permissão do CERT/CC e do SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Gestão de Incidentes x Gestão de Segurança (cont.)



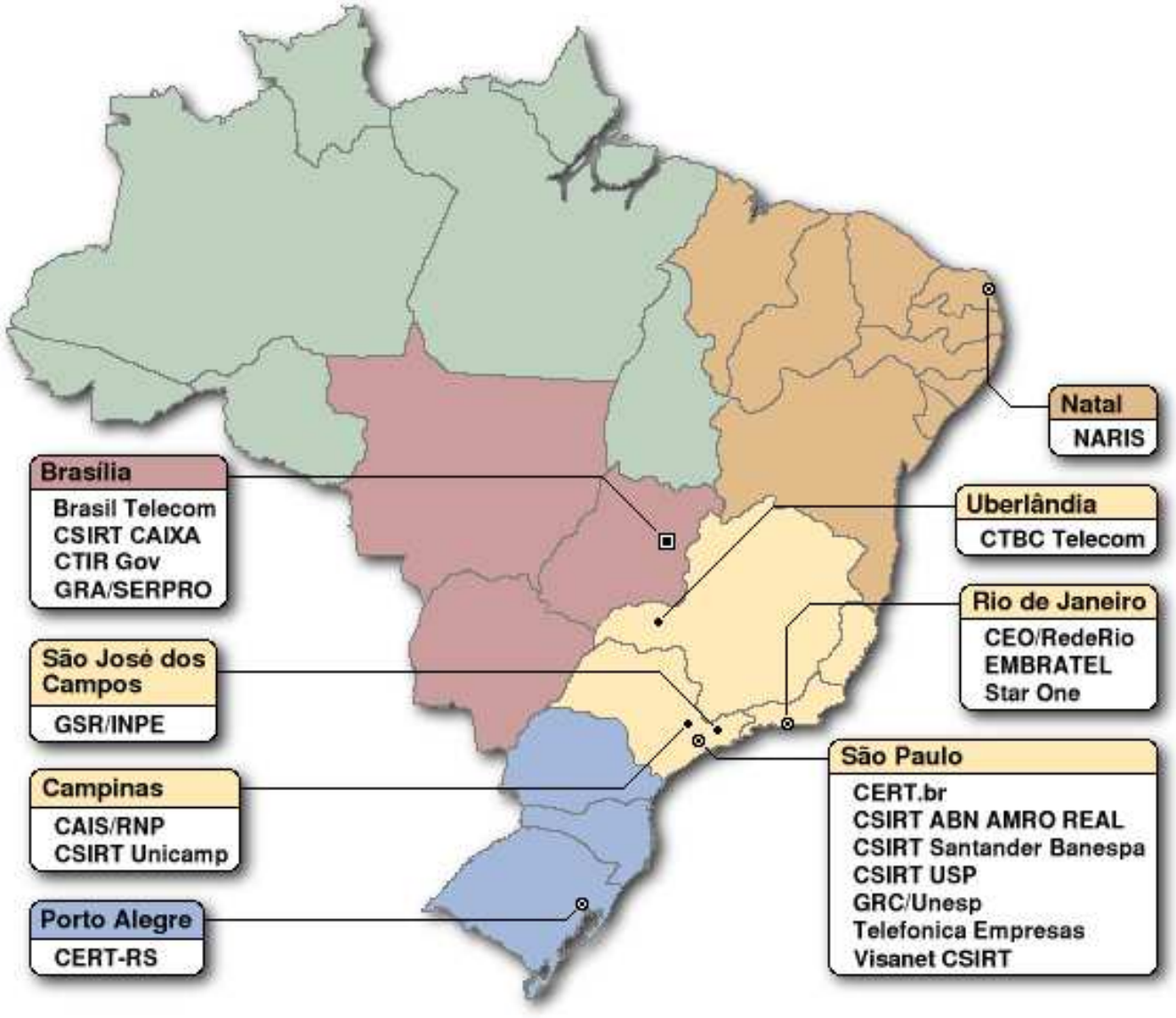
Fonte: Defining Incident Management Processes for CSIRTs: A Work in Progress.
Figura utilizada com permissão do CERT/CC e do SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Interação entre os Processos da Gestão de Incidentes (cont.)



Fonte: Defining Incident Management Processes for CSIRTs: A Work in Progress.
Figura utilizada com permissão do CERT/CC e do SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Cooperação com outros CSIRTs



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

Acompanhamento de Tendências

- Projetos de *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/
- Projeto de *Early Warning* Nacional:
  - Projeto Honeypots Distribuídos

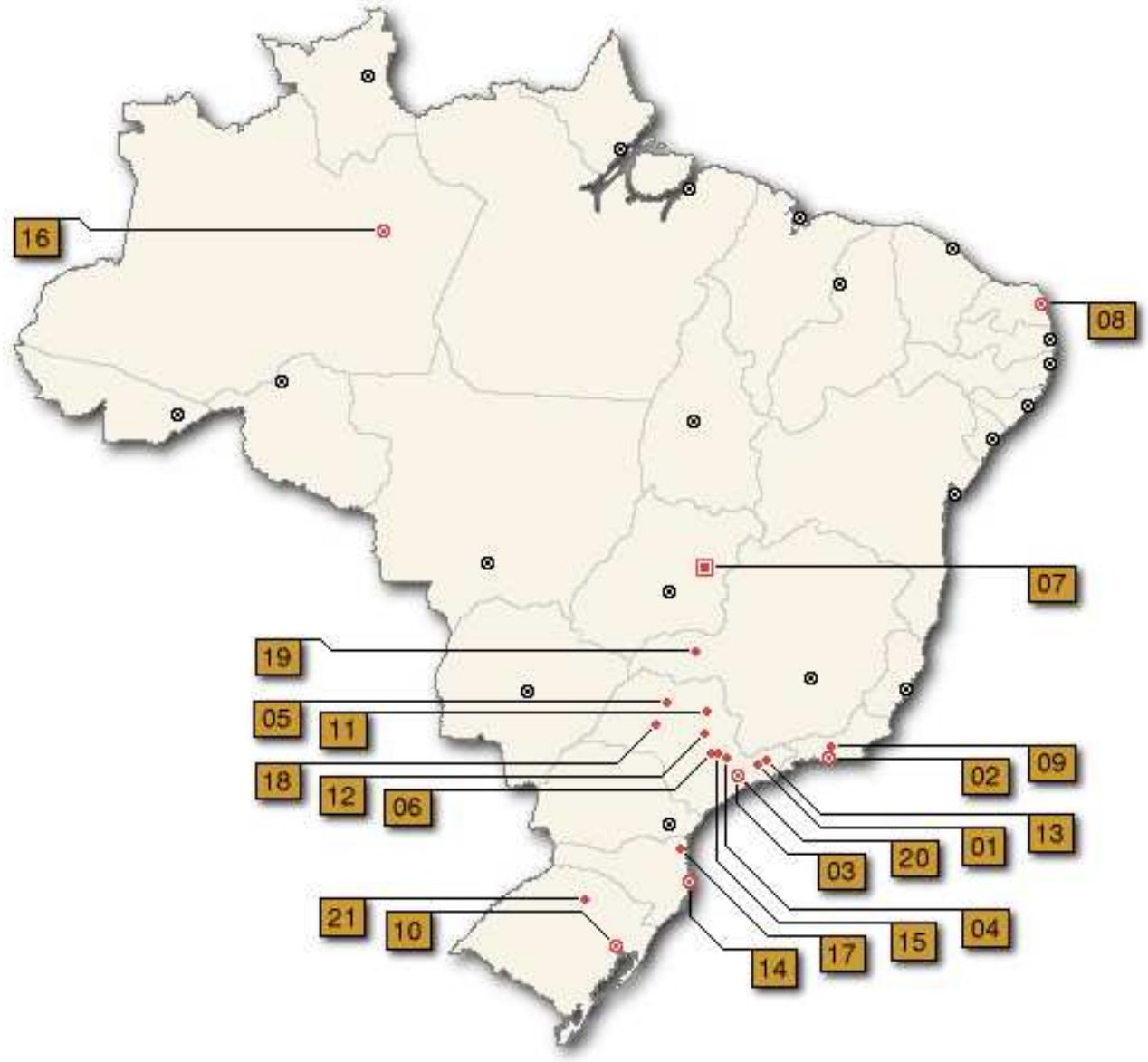
    http://www.honeypots-alliance.org.br/

Acompanhamento de Tendências (cont.)

Projeto Honeypots Distribuídos

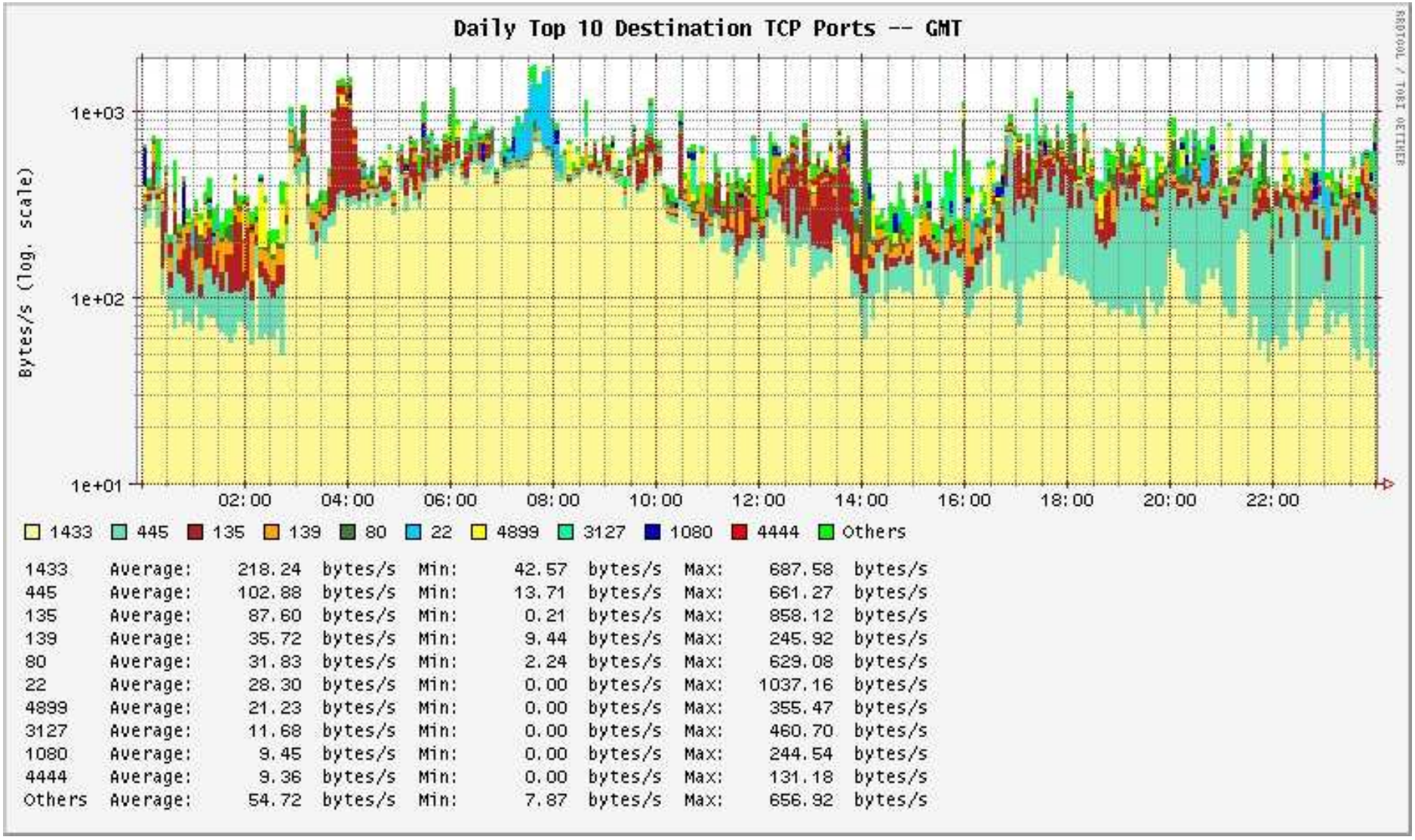
- coordenação: CERT.br e CenPRA/MCT
- 34 instituições parceiras
- honeypots em diversas redes e cidades
- mantém estatísticas públicas
- detecção rápida de:
  - novos worms/bots
  - servidores comprometidos
  - erros de configuração de rede
- coleta de novas assinaturas para IDSs e de novos exemplares de malware

Acompanhamento de Tendências (cont.)



Cidades onde os honeypots estão localizados.

Acompanhamento de Tendências (cont.)



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

Considerações Finais

Não há uma solução única para resolver todos os problemas:

- combinar soluções
- treinamento, atualização dos profissionais
- política de conexão de equipamentos na rede interna

Usuários podem ser um risco para a organização:

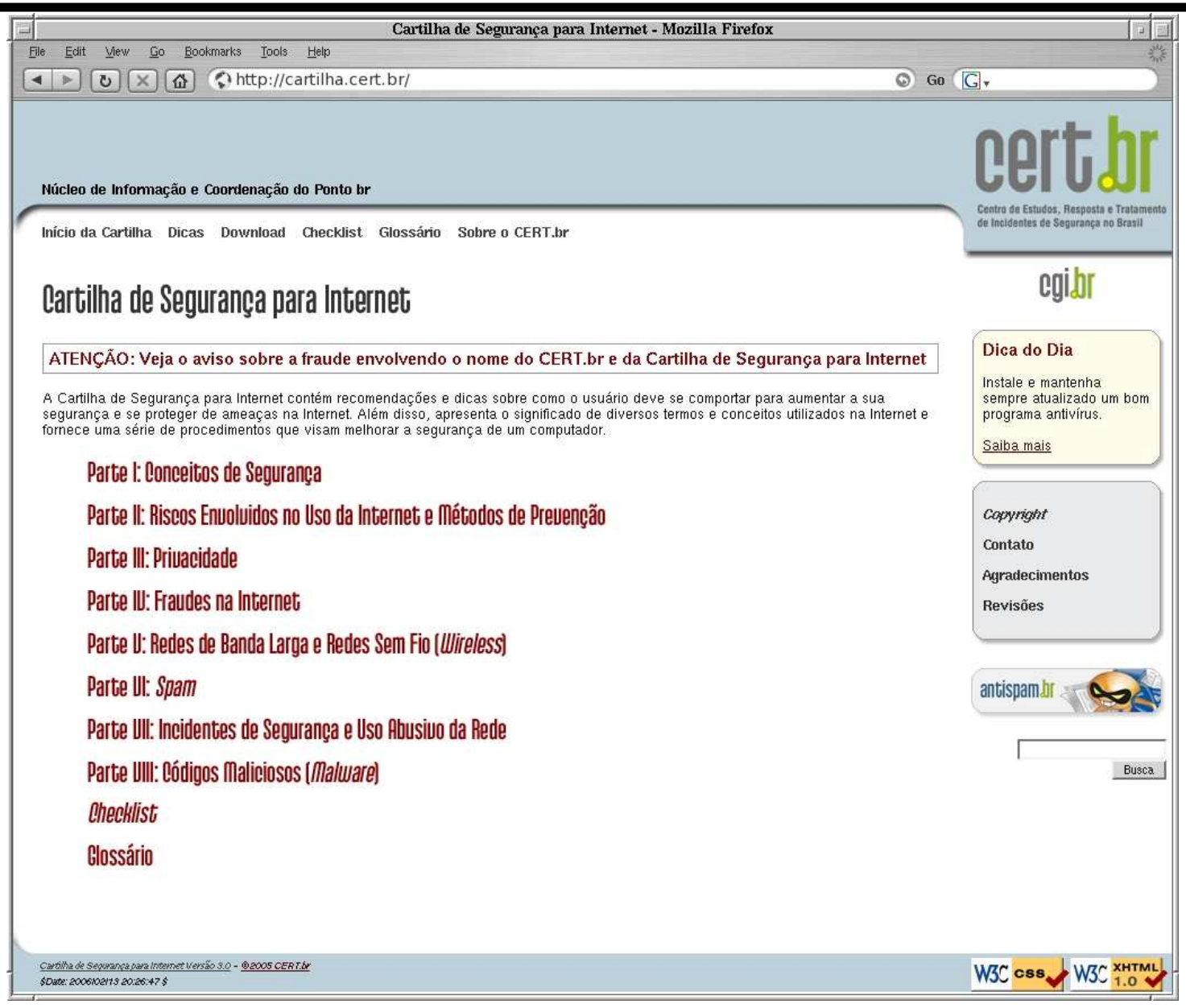
- vetores de disseminação de worms/vírus
- alvos de:
  - ataques de engenharia social
  - phishing/scam
  - cavalos de tróia
  - furto de informações

Educação dos usuários

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/



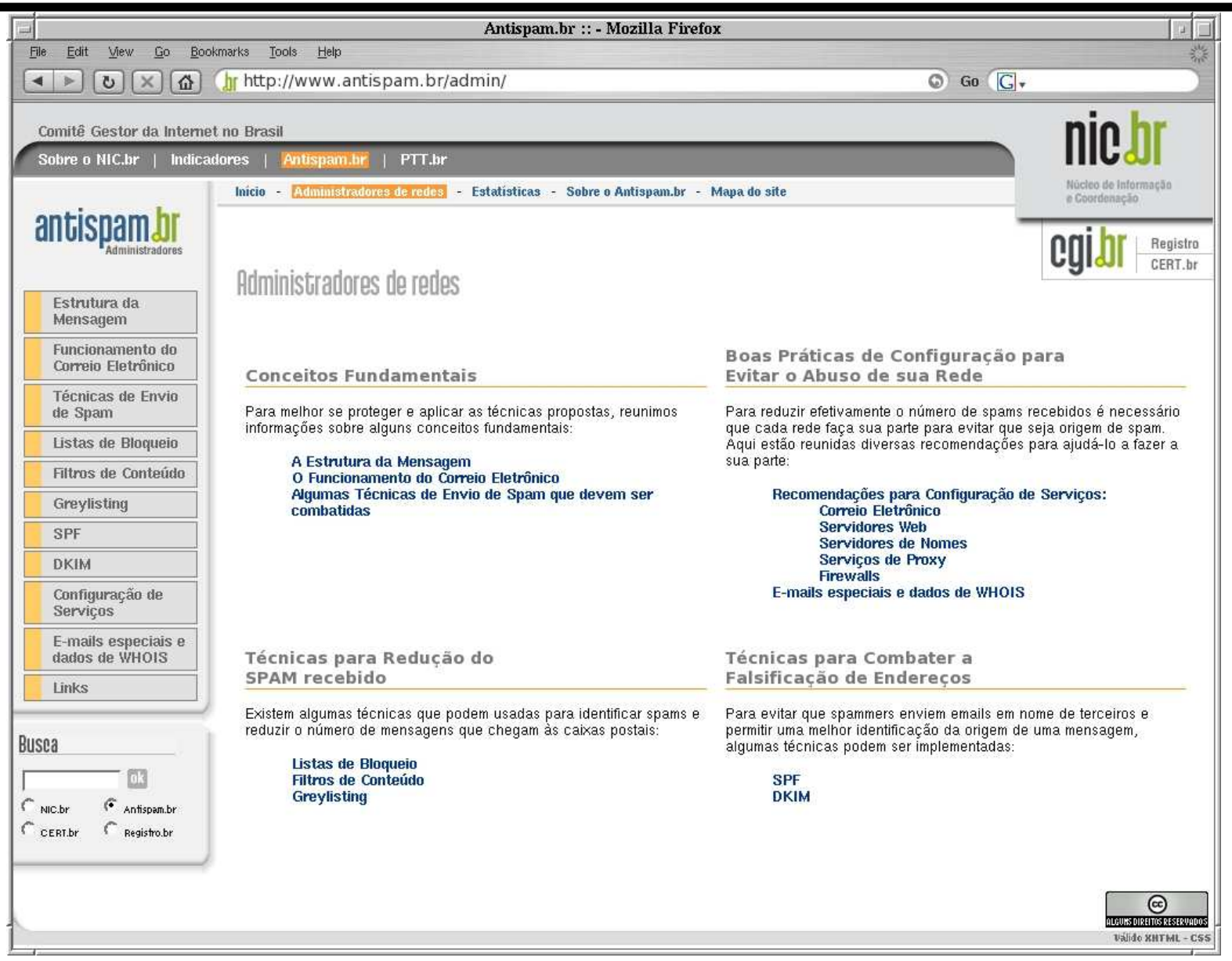
Educação dos usuários (cont)

Antispam.br: objetiva informar o usuário e o administrador de redes sobre o combate ao spam, suas implicações e formas de proteção.

- Iniciativa da Comissão de Trabalho Anti-Spam do CGI.br (http://www.cgi.br/sobre-cg/antispam.htm)
- Possui recomendações para Administradores de Redes:
  - Redução no envio de spam a partir de redes mal configuradas
  - Aumento da rastreabilidade e redução de fraudes (SPF e DKIM)

http://www.antispam.br/

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



http://www.antispam.br/tipos/

Adesão à Campanha

http://www.antispam.br/campanha/

Adesão à Campanha (cont.)

Adesão à Campanha (cont.)

Links de Interesse

- Esta Palestra
  http://www.cert.br/docs/palestras/
- Antispam.br
  http://www.antispam.br/
- 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/

Links de Interesse

- Material de Apoio para Criação e Operação de CSIRTs
  http://www.cert.br/csirts/
- Consórcio Brasileiro de Honeypots
  http://www.honeypots-alliance.org.br/
- Comitê Gestor da Internet no Brasil
  http://www.cgi.br/
- Cursos do CERT.br
  http://www.cert.br/cursos/