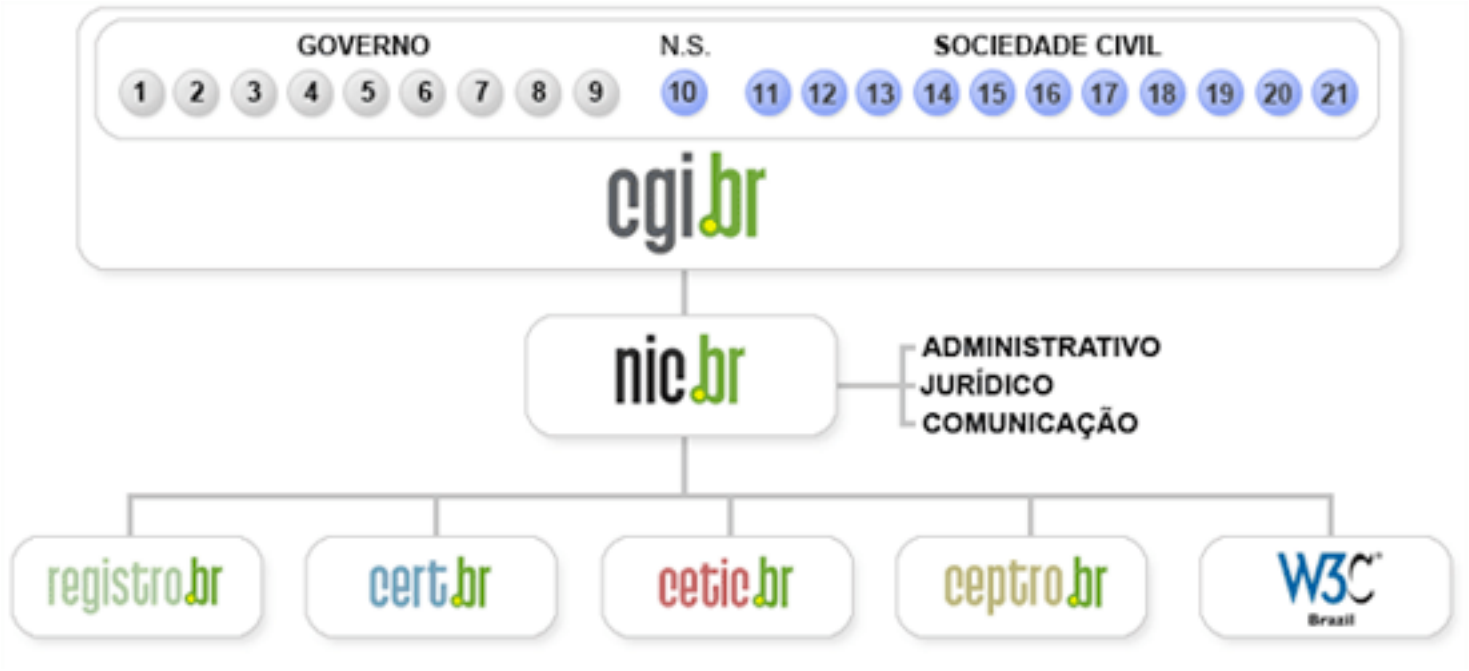
Crimes pela Internet: Aspectos Técnicos

Cristine Hoepers
cristine@cert.br

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

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

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nacional de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

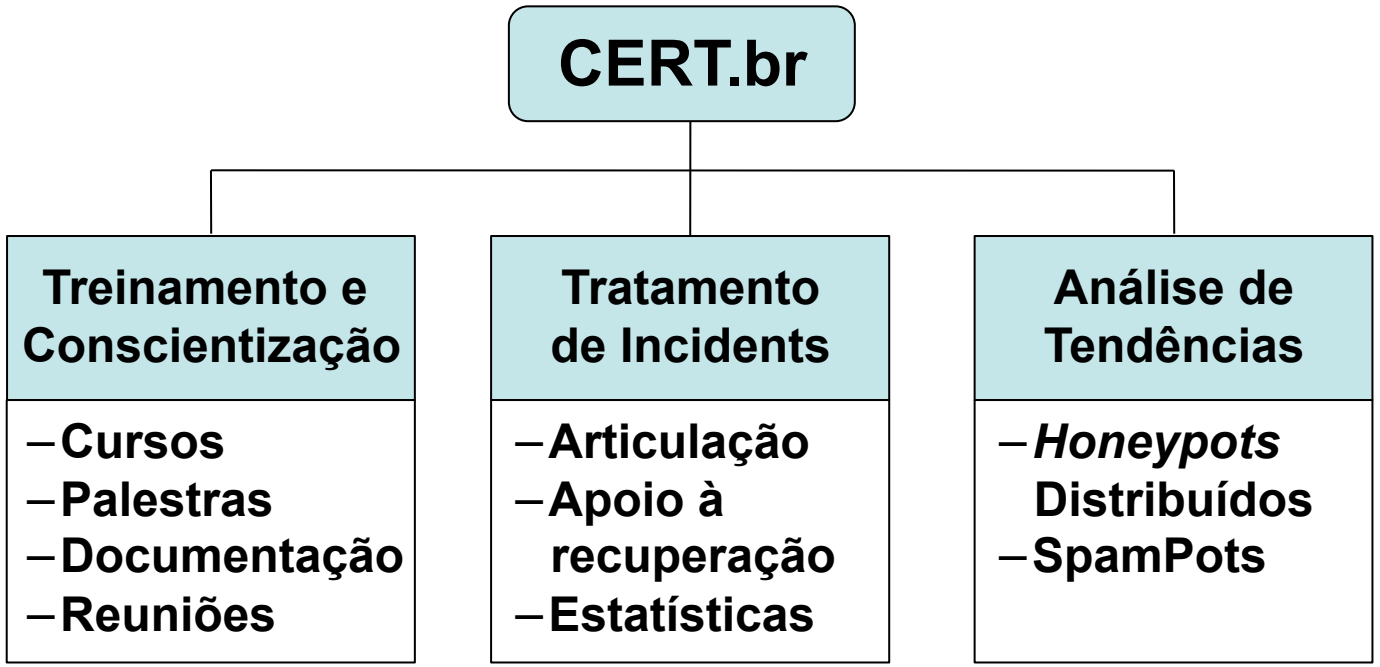
11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Comitê Gestor da Internet no Brasil – CGI.br

Dentre as atribuições 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/



SEIPartner CERT Courses

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

The Honeynet PROJECT®

Criado em 1997 para:

- Ser um **ponto de contato nacional** para notificação de incidentes de segurança
- Prover a **coordenação e o apoio necessários** no processo de resposta a incidentes
- Estabelecer um **trabalho colaborativo com outras entidades**, como os operadores da justiça, provedores de acesso e serviços e backbones
- **Auxiliar novos CSIRTs** a estabelecerem suas atividades
- Aumentar a **conscientização** sobre a necessidade segurança na Internet

Agenda

Contexto

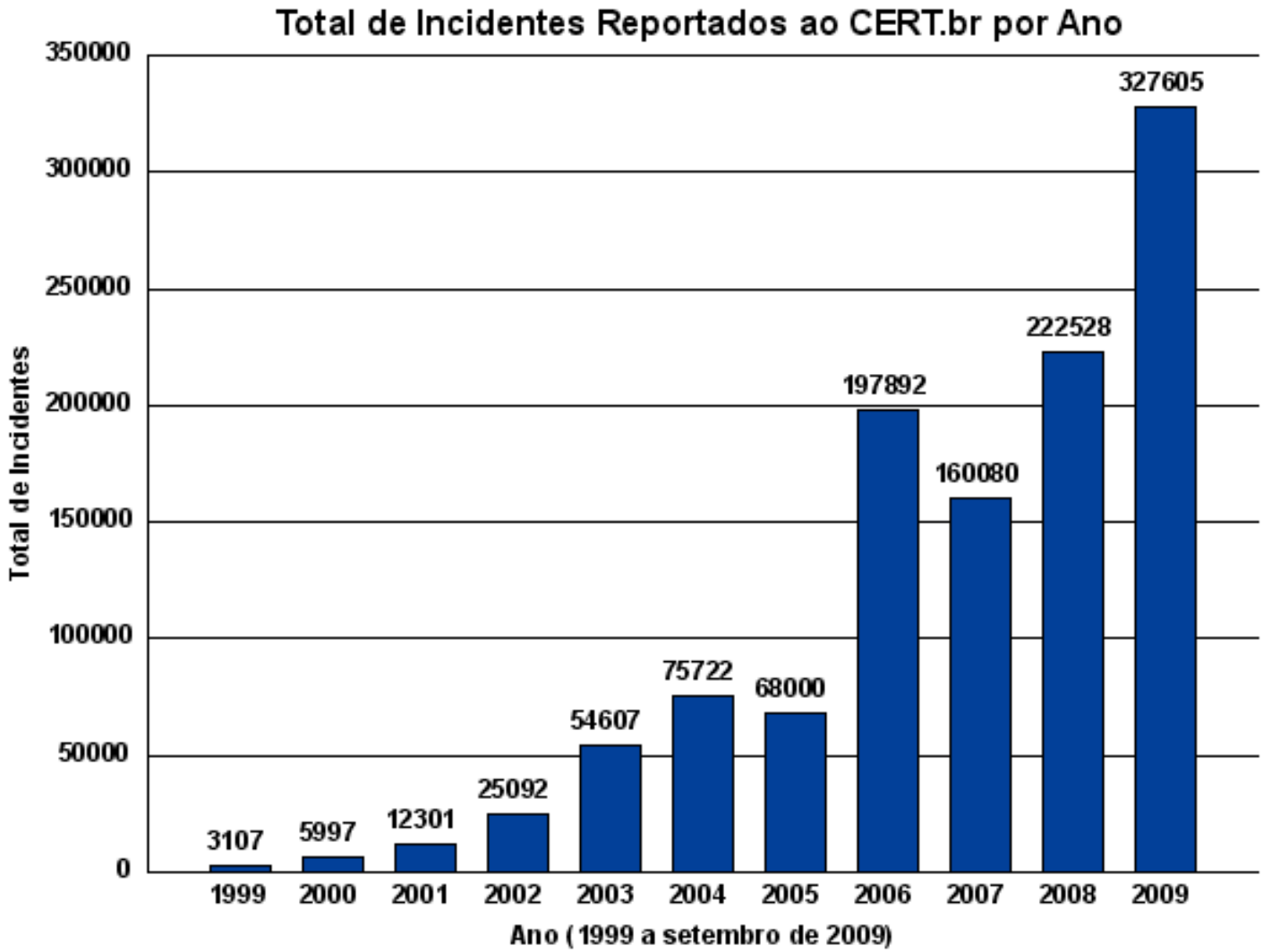
- Perfil dos incidentes mais freqüentes
- Abuso da infra-estrutura das redes

Como lidar com o cenário atual

- Papel das empresas e profissionais de segurança
- Considerações finais

Incidentes Mais Freqüentes

Incidentes Reportados ao CERT.br



http://www.cert.br/stats/incidentes/

Tendências dos Últimos 6 Anos

Mudança no enfoque dos atacantes:

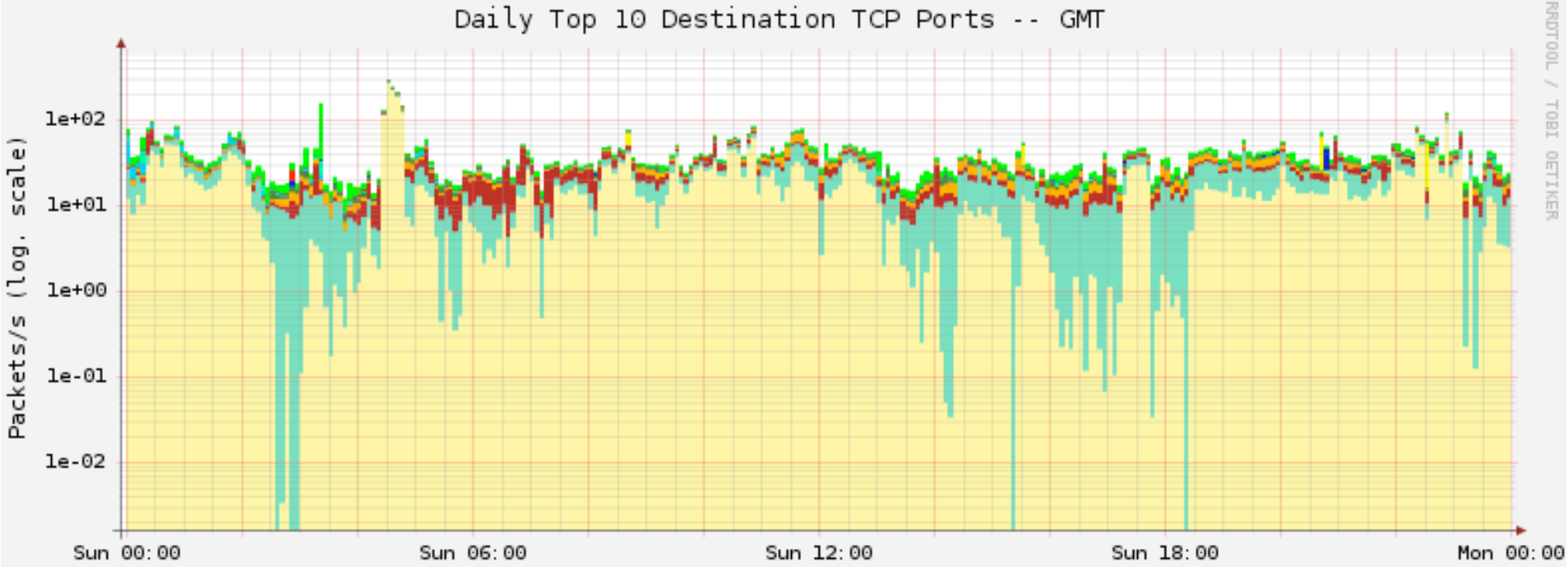
- **Ataques a usuários finais**
  - **fraudes, *bots*, *spyware*, etc**
- **Motivação financeira**

Características das tentativas de fraude:

- **Eventuais violações de direitos autorais**
- **Fraude com objetivos financeiros**
  - **majoritariamente envolve *spams***
    - **em nome das mais variadas instituições e com tópicos diversos**
    - **com *links* (URLs) para códigos maliciosos (cavalos de tróia)**
  - **páginas falsas estão voltando a ter números significativos**
  - ***drive-by downloads* sendo usados intensamente no Brasil**
    - **casos publicados na mídia nos últimos meses incluem: *sites* principais da Vivo, da Oi e da Ambev**

Abuso da Infra-Estrutura de Redes e Efeitos Colaterais

Varreduras mais freqüentes – *Honeypots* Distribuídos

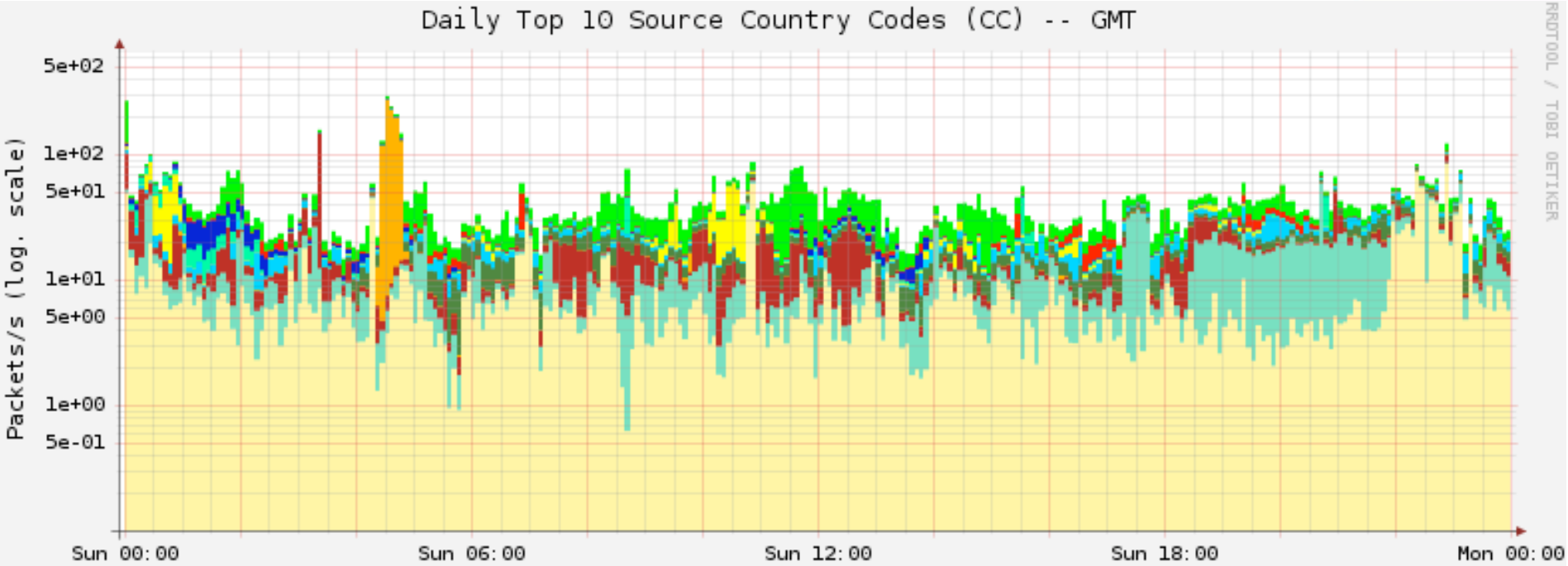


22 445 1433 139 135 1080 21 8080 5900 2967 Others

22	Average:	17.21	pkts/s	Min:	0.00	pkts/s	Max:	270.38	pkts/s
445	Average:	8.39	pkts/s	Min:	2.40	pkts/s	Max:	27.51	pkts/s
1433	Average:	4.89	pkts/s	Min:	0.01	pkts/s	Max:	32.84	pkts/s
139	Average:	2.79	pkts/s	Min:	0.07	pkts/s	Max:	15.01	pkts/s
135	Average:	1.18	pkts/s	Min:	0.00	pkts/s	Max:	5.86	pkts/s
1080	Average:	0.53	pkts/s	Min:	0.00	pkts/s	Max:	26.95	pkts/s
21	Average:	0.45	pkts/s	Min:	0.00	pkts/s	Max:	38.80	pkts/s
8080	Average:	0.42	pkts/s	Min:	0.00	pkts/s	Max:	12.96	pkts/s
5900	Average:	0.30	pkts/s	Min:	0.00	pkts/s	Max:	19.80	pkts/s
2967	Average:	0.22	pkts/s	Min:	0.00	pkts/s	Max:	6.46	pkts/s
Others	Average:	3.69	pkts/s	Min:	1.02	pkts/s	Max:	118.65	pkts/s

http://www.honeypots-alliance.org.br/stats/flows/tcp-udp/

Country Codes de origem – *Honeypots* Distribuídos

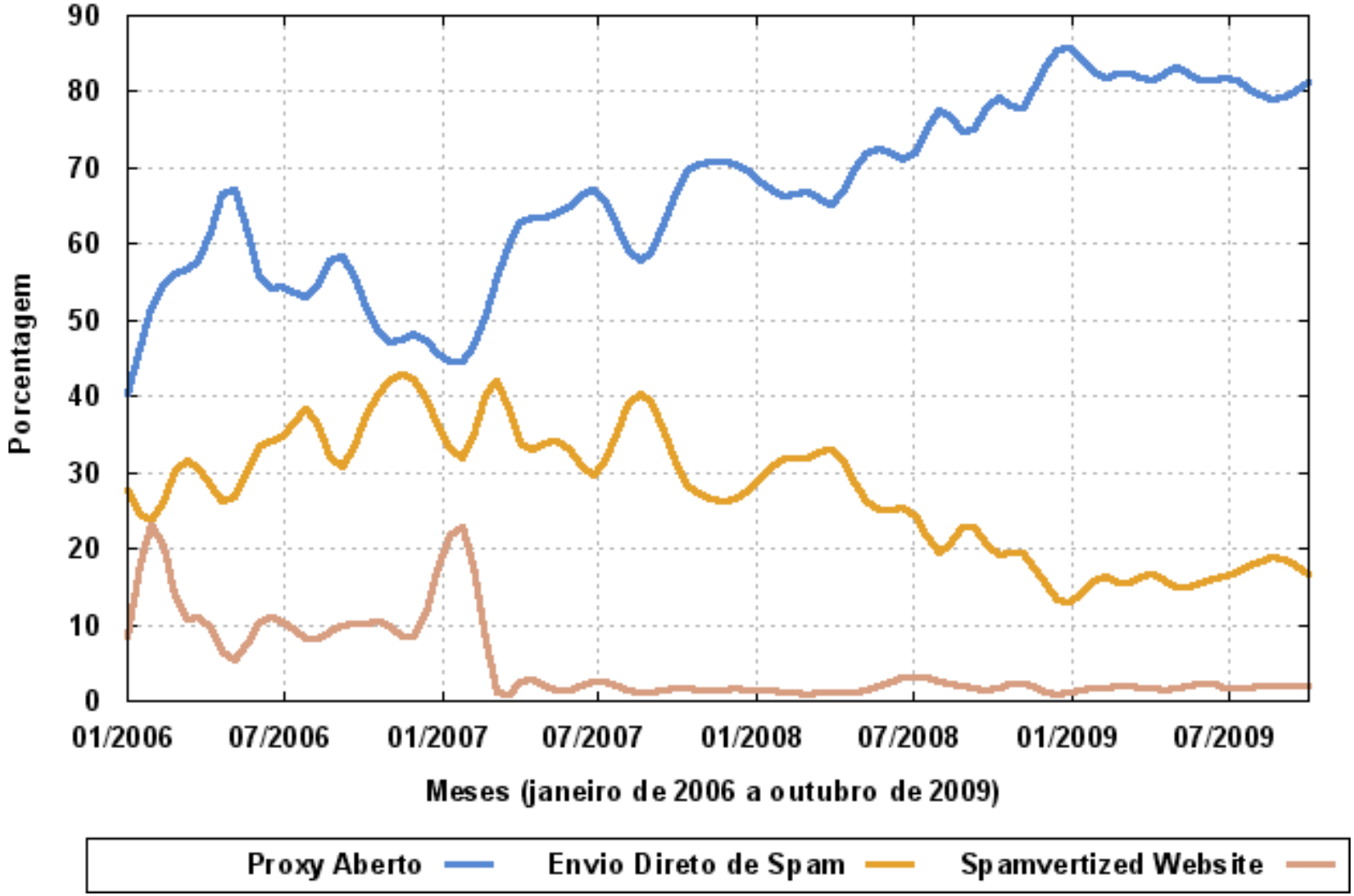


BR	Average:	8.15	pkts/s	Min:	0.62	pkts/s	Max:	83.74	pkts/s
CN	Average:	6.40	pkts/s	Min:	0.65	pkts/s	Max:	53.90	pkts/s
US	Average:	4.78	pkts/s	Min:	0.18	pkts/s	Max:	133.31	pkts/s
MX	Average:	3.20	pkts/s	Min:	0.00	pkts/s	Max:	262.98	pkts/s
VE	Average:	2.93	pkts/s	Min:	0.00	pkts/s	Max:	12.97	pkts/s
AR	Average:	2.37	pkts/s	Min:	0.05	pkts/s	Max:	12.38	pkts/s
FR	Average:	2.19	pkts/s	Min:	0.00	pkts/s	Max:	41.34	pkts/s
RU	Average:	1.38	pkts/s	Min:	0.14	pkts/s	Max:	23.34	pkts/s
JP	Average:	1.17	pkts/s	Min:	0.03	pkts/s	Max:	12.28	pkts/s
TW	Average:	1.05	pkts/s	Min:	0.08	pkts/s	Max:	23.18	pkts/s
Others	Average:	9.16	pkts/s	Min:	1.49	pkts/s	Max:	141.08	pkts/s

http://www.honeypots-alliance.org.br/stats/flows/cc/

Reclamações de Spam ao CERT.br pelo SpamCop

Tipo mais comum é o abuso de proxies abertos.



Brasil na CBL – Reflexo Direto do Abuso de *Proxies*

cert.br

Country Codes com maior número de IPs listados

CC	Total	%	Rank
BR	1.074.484	17,43	01
IN	684.849	11,11	02
VN	414.639	6,73	03
RU	354.970	5,76	04
PL	261.219	4.24	05
TH	241.157	3.91	06
CN	207.356	3,36	07
CO	179.652	2,91	08
UA	151.436	2,46	09
AR	147.432	2,39	10

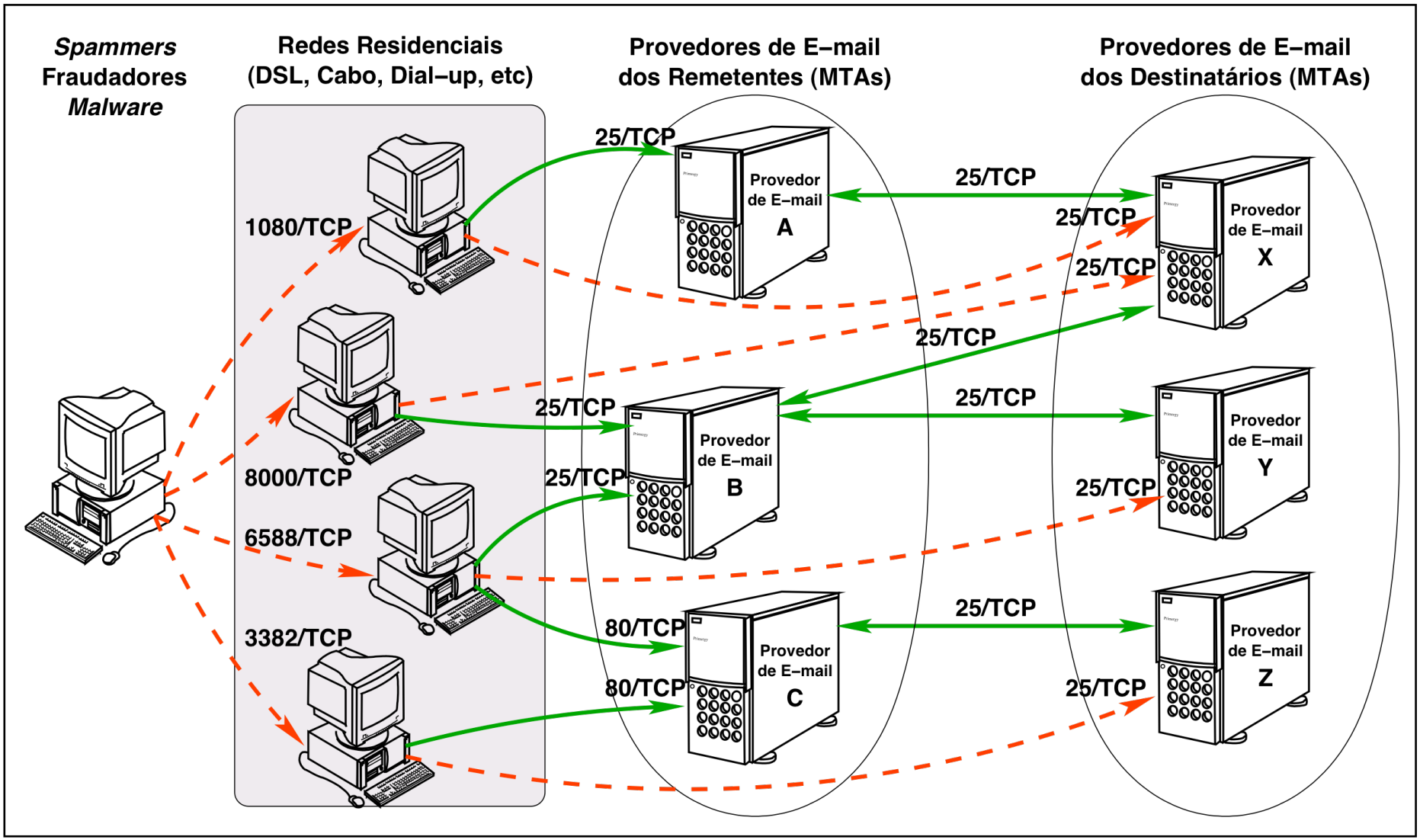
Domínios (DNS reverso) com maior número de IPs listados

Domínio	Total	%	Rank
telebahia.net.br	348.651	5,66	01
brasiltelecom.net.br	213.962	3,47	04
telesp.com.br	187.146	3,04	05
netservicos.com.br	64.033	1,04	20
telet.com.br (claro)	63.002	1,02	21
gvt.net.br	52.443	0,85	26
ig.com.br	50.249	0,82	27
timbrasil.com.br	20.030	0,32	54
ctbctelecom.net.br	19.436	0,32	56
canbrasnet.com.br	11.782	0,19	84

Dados gerados em: `Mon Nov 23 17:45:38 2009 UTC/GMT`
Composite Blocking List http://cbl.abuseat.org/

cgi.br | nic.br

Abuso via *Proxies* Abertos – *Spam*/*Phishing*



Uso de *botnets* para DDoS

- **20 PCs domésticos abusando de Servidores DNS Recursivos Abertos podem gerar 1Gbps**
  - **No Brasil temos mais de 13.000 recursivos abertos no momento**
    (Dados do *Measurement Factory* passados ao CERT.br semanalmente)
- **Em março de 2009 foram atingidos picos de 48Gbps**
  - **em média ocorrem 3 ataques de 1Gpbs por dia na Internet**
- **De 2% a 3% do tráfego de um grande *backbone* é ruído de DDoS**
- **Extorsão é o principal objetivo**
  - **mas *download* de outros *malwares*, *spam* e furto de informações também valem dinheiro e acabam sendo parte do *payload* dos *bots***

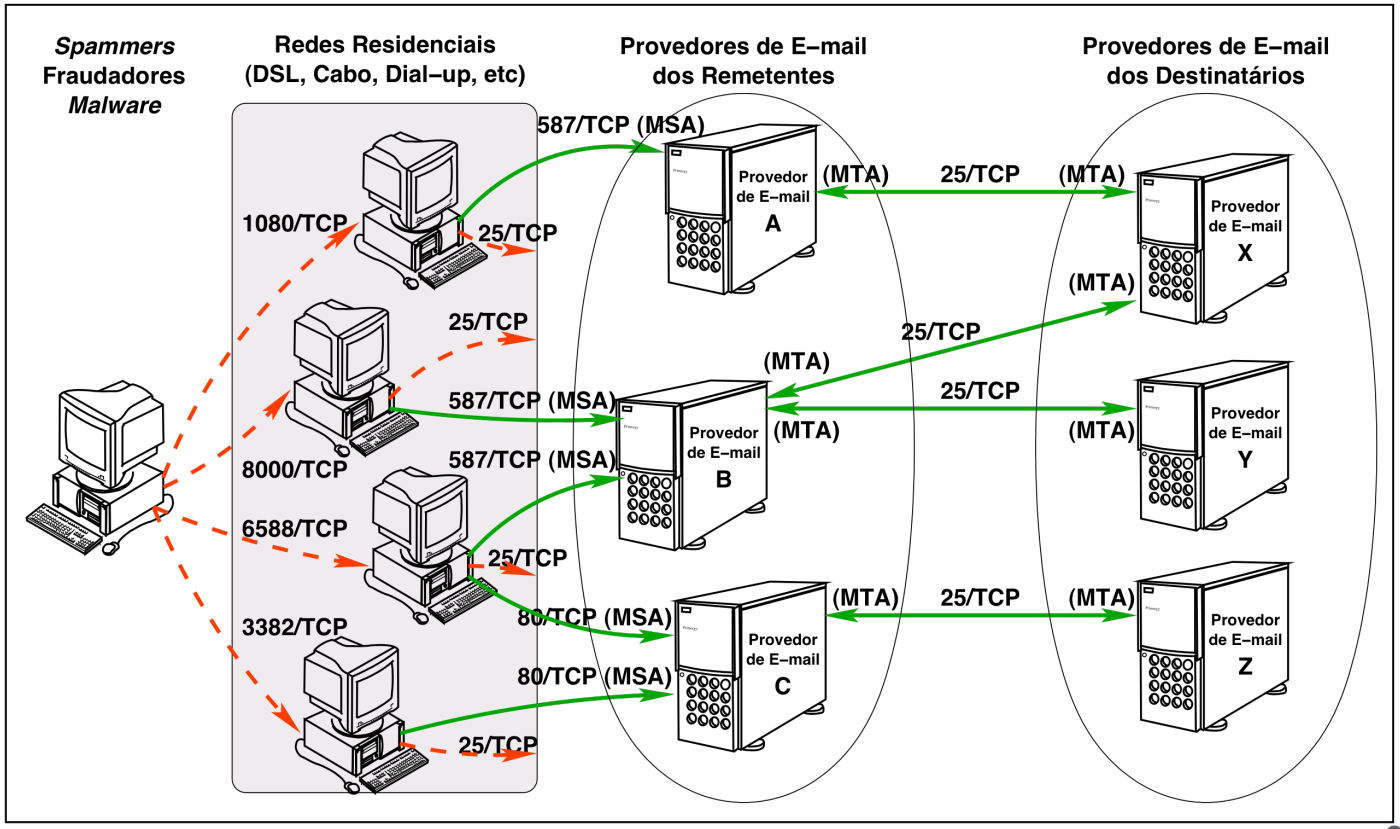
Fonte: ***Global Botnet Underground: DDoS and Botconomics*.**
***Jose Nazario, Ph.D., Head of Arbor* ASERT**
***Keynote* do Evento RioInfo 2009**

Papel das Empresas e Profissionais de Segurança

Implementar Métodos de Prevenção e Mitigação

- **Definir políticas de segurança e uso aceitável**
- **Alertar usuários infectados**
- **Impedir que tráfego malicioso deixe sua rede**

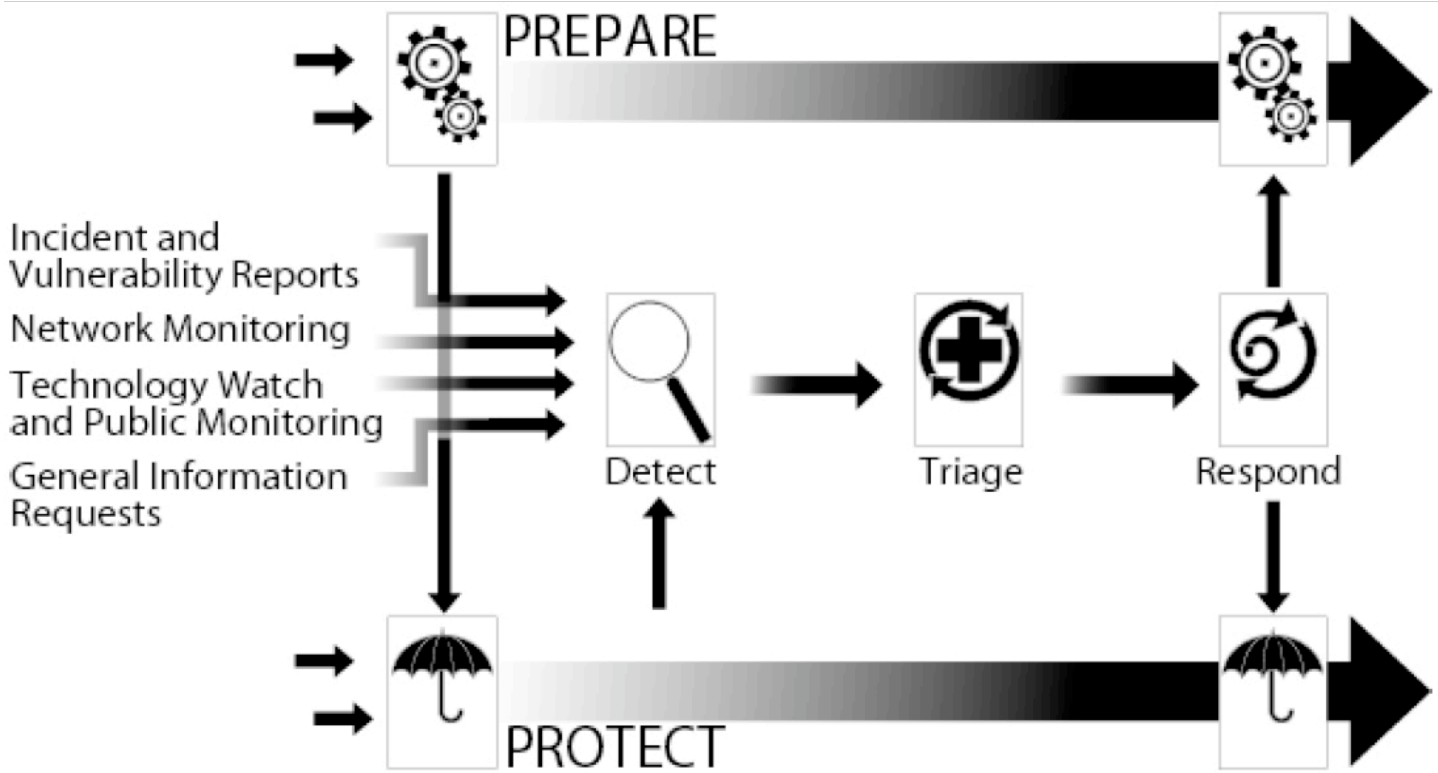
Exemplo: Gerência de Porta 25



Definir uma Estratégia de Tratamento de Incidentes

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

– CERT® Program CSIRT Development Team



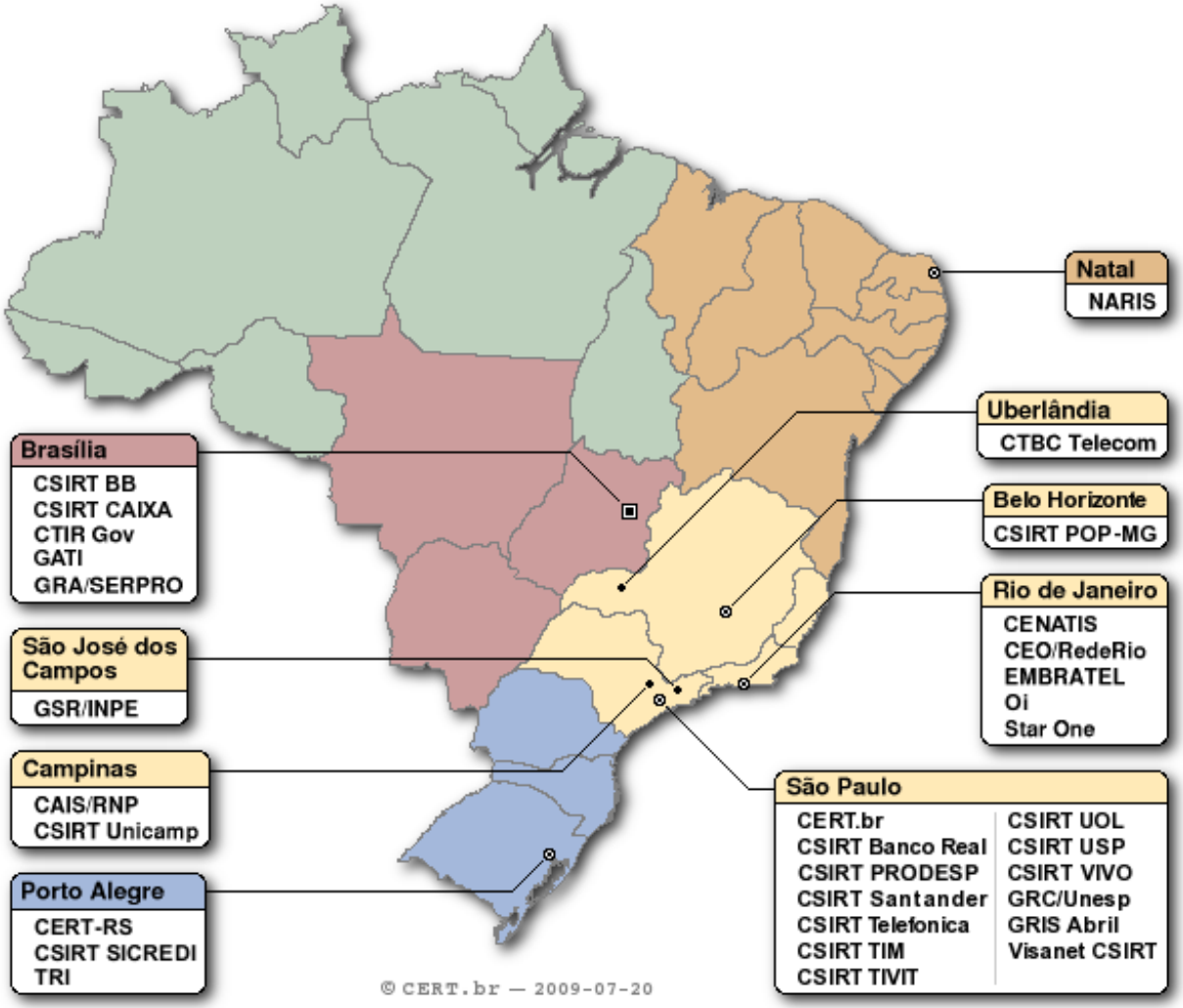
Fonte: ***Defining Incident Management Processes for CSIRTs: A Work in Progress.*** **Figura utilizada com permissão do CERT®/CC e do SEI/CMU.**
http://www.cert.org/archive/pdf/04tr015.pdf

Papel dos CSIRTs Quando se Fala em Crimes

- A pessoa que responde um incidente é a primeira a entrar em contato com as evidências de um possível crime
  - seguir as políticas
  - preservar as evidências
- A redução do impacto é conseqüência da:
  - agilidade de resposta
  - redução no número de vítimas
- O CSIRT não é um investigador
  - A decisão de levar um caso à justiça deve ser da vítima
  - Em uma organização, leia-se: alta administração e setor jurídico
- O sucesso depende da confiabilidade
  - nunca divulgar dados sensíveis nem expor vítimas, por exemplo
- 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

Grupos de Tratamento de Incidentes no Brasil

Setor	CSIRTs
Resposabilidade Nacional	CERT.br
Redes de Governo	CTIR Gov, GATI, GRA/SERPRO, CSIRT Prodesp
Setor Financeiro	CSIRT BB, CSIRT CAIXA, CSIRT Banco Real, CSIRT Sicredi, CSIRT Santander, Visanet CSIRT
Telecom/ISP	CTBC Telecom, EMBRATEL, StarOne, Oi, CSIRT Telefonica, CSIRT TIM, CSIRT UOL, CSIRT VIVO
Redes Acadêmicas e de Pesquisa	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CSIRT USP, GRC/UNESP, TRI
Outros	CSIRT TIVIT, GRIS Abril



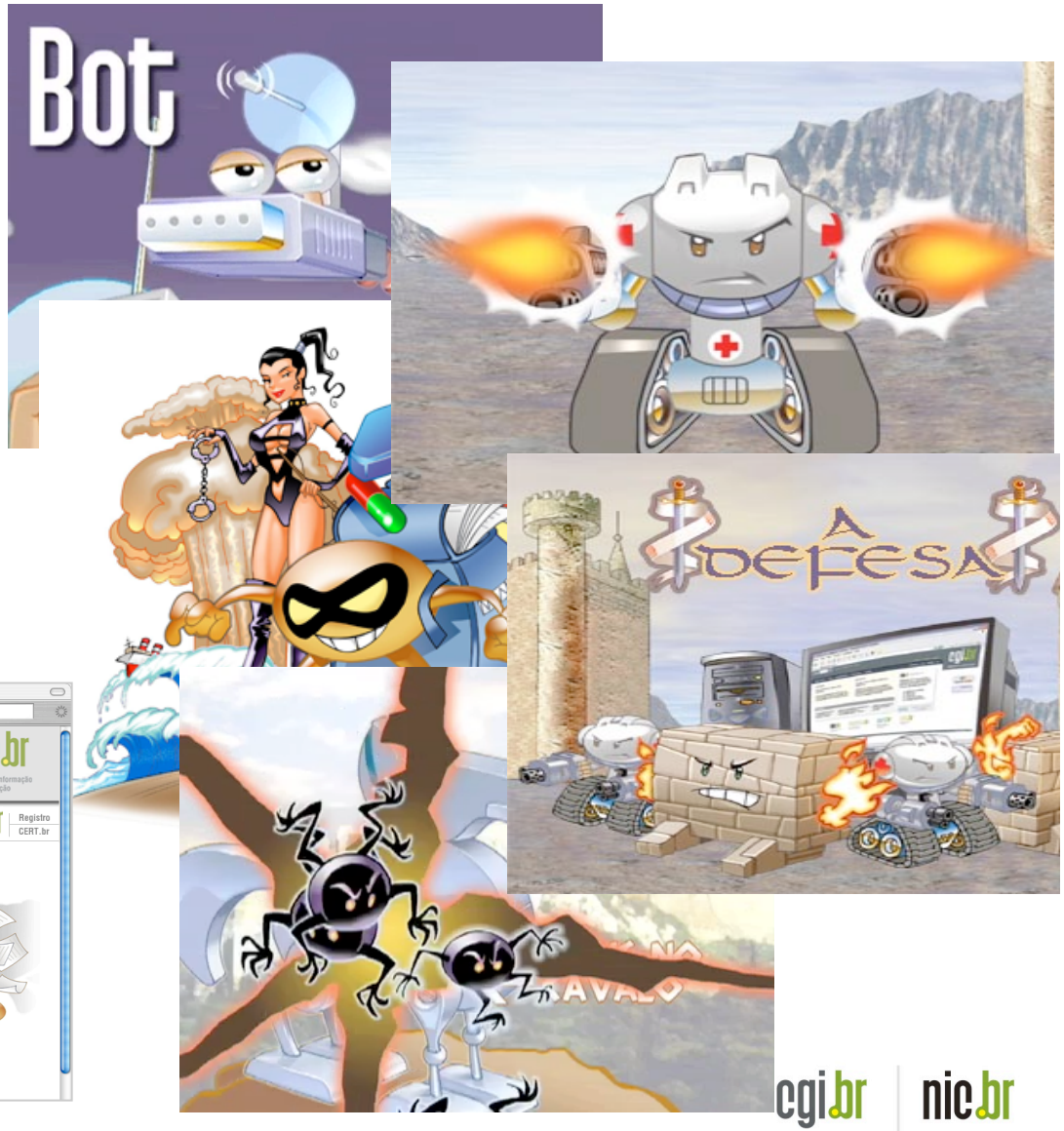
http://www.cert.br/contato-br.html

Auxiliar na Educação de Administradores e Usuários

- **Práticas de Segurança para Administradores de Redes Internet**
  http://www.cert.br/seg-adm-redes/
  - **boas práticas em configuração, administração e operação segura de redes conectadas à Internet**
- **Cartilha de Segurança para Internet**
  http://cartilha.cert.br/

Auxiliar na Educação de Administradores e Usuários

- **Site Antispam.br – Vídeos Educacionais no escopo das atividades da CT Anti-Spam do CGI.br**
  http://www.antispam.br/



Considerações Finais (1/3)

- **Cenário atual é reflexo direto de**
  - ***Softwares* com muitas vulnerabilidades**
  - **Pressão econômica para lançar, mesmo com problemas**
  - **É uma questão de "*Economics and Security*"**
    http://www.cl.cam.ac.uk/~rja14/econsec.html

- **Os criminosos estão apenas migrando para onde os negócios estão**

- **Verdadeiro custo da segurança pode ser a perda de confiança por parte dos usuários**

Considerações Finais (2/3)

- **Só haverá melhorias quando**
  - **O processo de desenvolvimento de *software* incluir**
    - **Levantamento de requisitos de segurança**
    - **Testes com casos de abuso (não somente casos de uso)**
  - ***Secure Software Development* se tornar parte da formação de projetistas e programadores**
    - **desde a primeira disciplina de programação e permeado em todas as disciplinas**
  - **Provedores, operadoras e administradores de redes em geral forem mais pró-ativos na implementação de métodos de mitigação**

Considerações Finais (3/3)

- **Mas é necessário cuidado:**
  - **Nem todas as medidas sendo defendidas ou implantadas são efetivas**
    - **Algumas só reduzem a privacidade, sem aumentar a segurança**
  - **Por conseqüência**
    - **Medidas efetivas acabam sendo "boicotadas" em nome da privacidade, mesmo quando não interferem em nada na privacidade**
- **Não será possível erradicar todos os problemas, precisamos torná-los gerenciáveis**
  - **cada setor precisa fazer a sua parte – isso é cooperação para a solução dos problemas**
  - **a solução não virá de uma ação única**

Counter eCrime Operations Summit IV – Maio/2010

1ª Edição na América Latina

Evento que reúne CSIRTs, academia e especialistas em investigações de crimes pela Internet.

Discute os aspectos técnicos e operacionais de prevenção e combate a crimes pela Internet.

Local: Hotel Blue Tree Morumbi
São Paulo
Data: 11 a 13 de maio de 2010

http://apwg.org/

Links Relacionados

- **CGI.br - Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do Ponto br**
  http://www.nic.br/
- **CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/