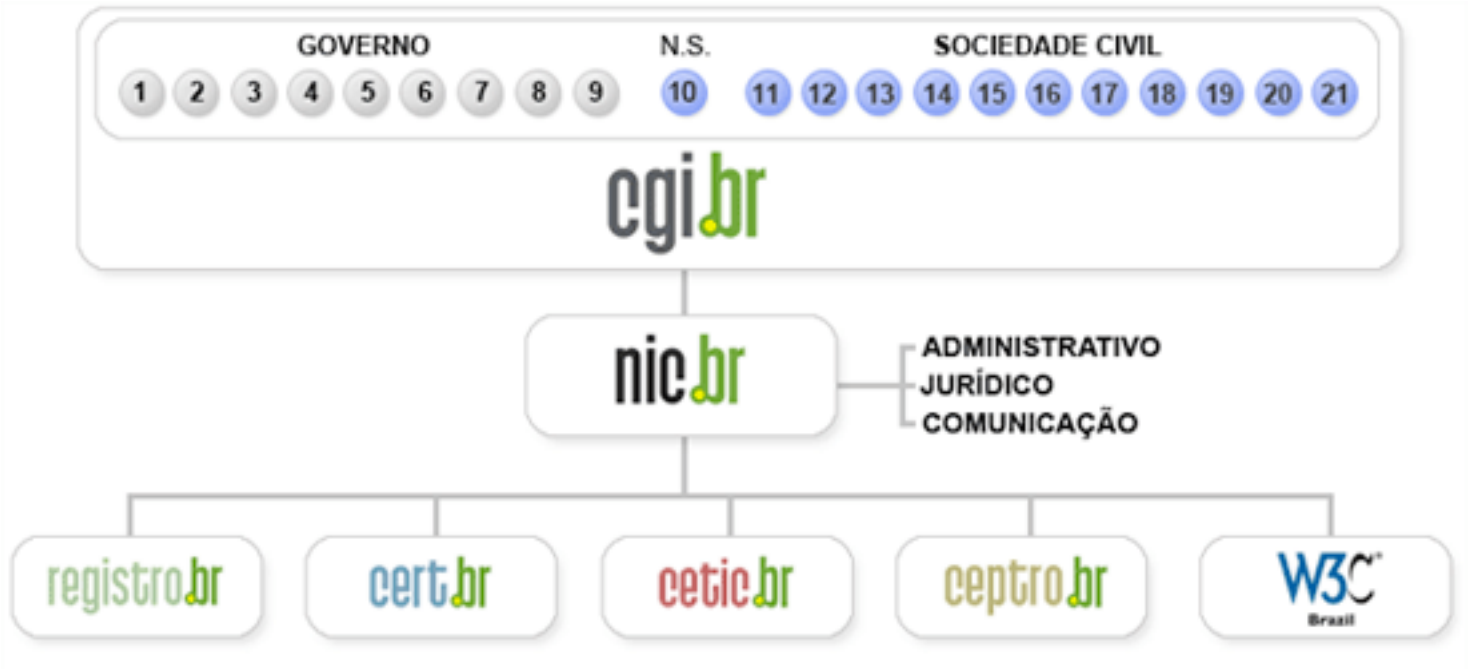
Crimes pela Internet: Aspectos Técnicos e o Papel dos Grupos de Tratamento de Incidentes

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/

Agenda

Contexto

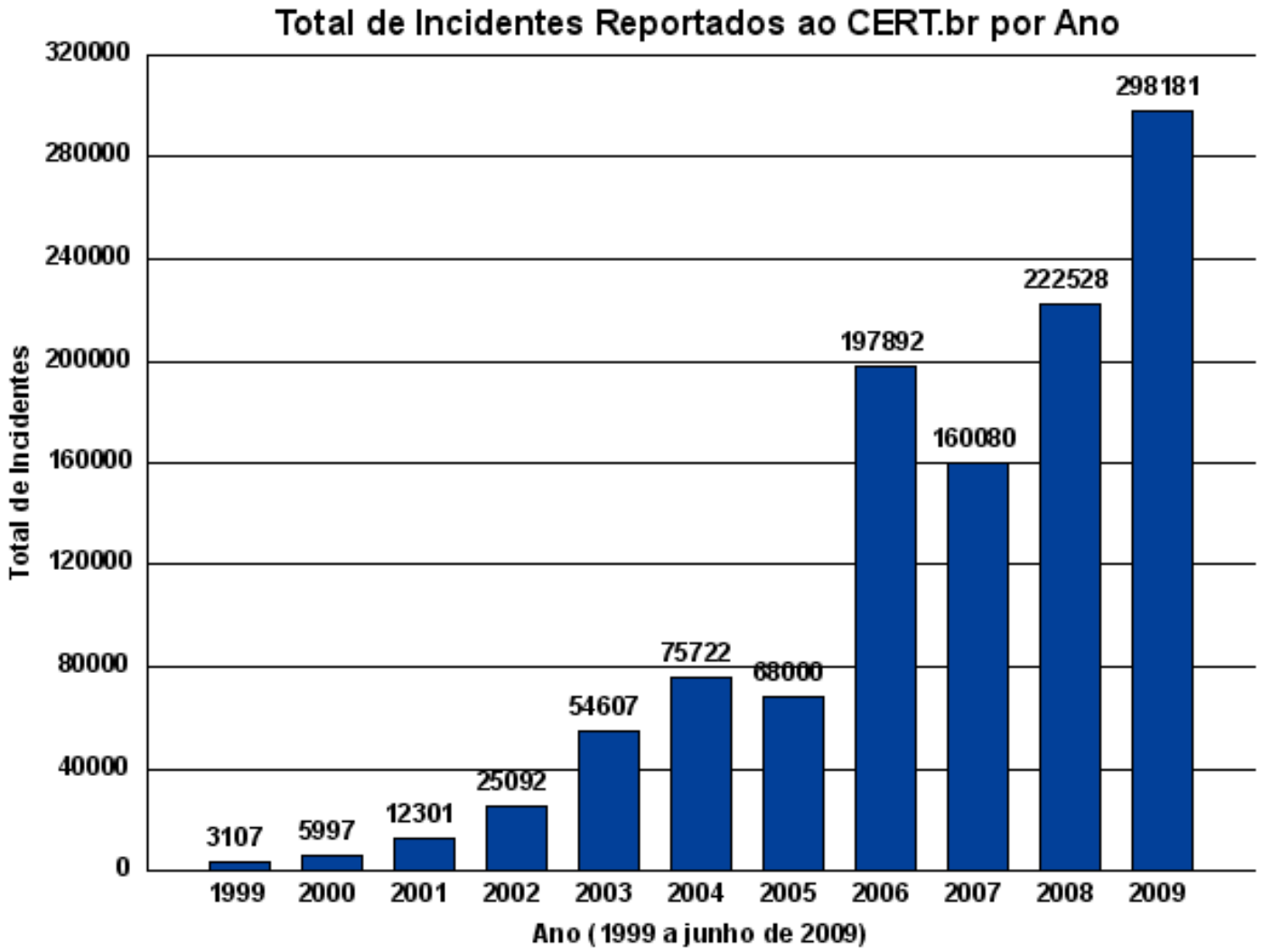
- Perfil dos incidentes mais freqüentes
- Abuso da infra-estrutura das redes

Como lidar com o cenário atual

- Papel dos CSIRTs e dos Profissionais de Segurança
- Evolução dos CSIRTs no Brasil
- Considerações finais

Incidentes Mais Freqüentes

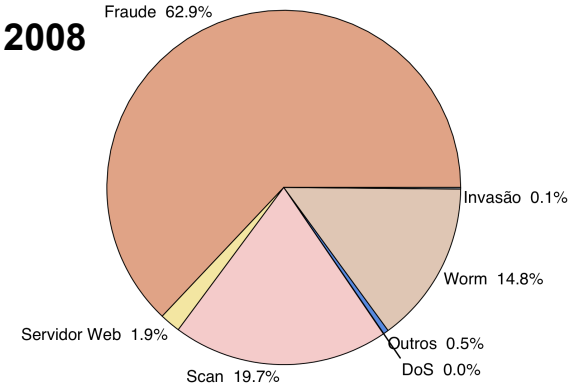
Incidentes Reportados ao CERT.br



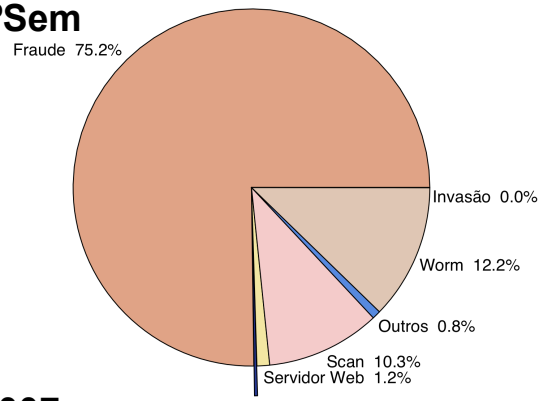
http://www.cert.br/stats/incidentes/

Distribuição entre as categorias nos últimos 6 anos

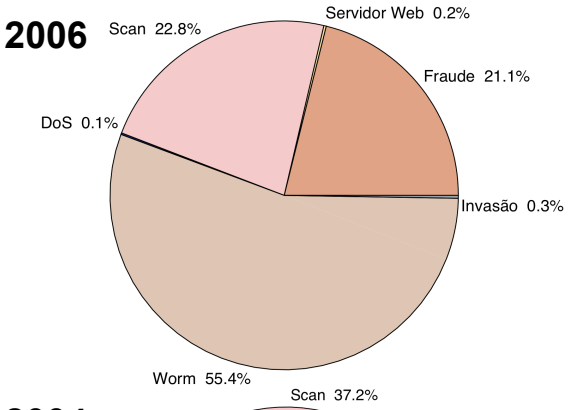
2008



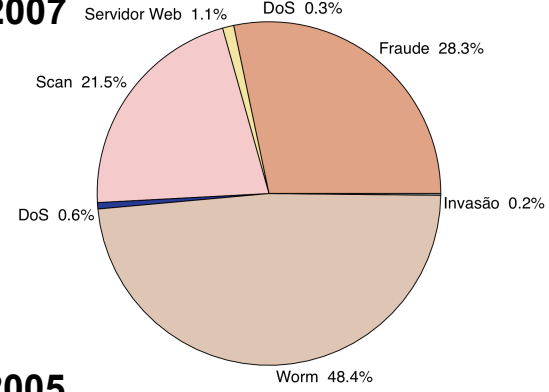
2009 1ºSem



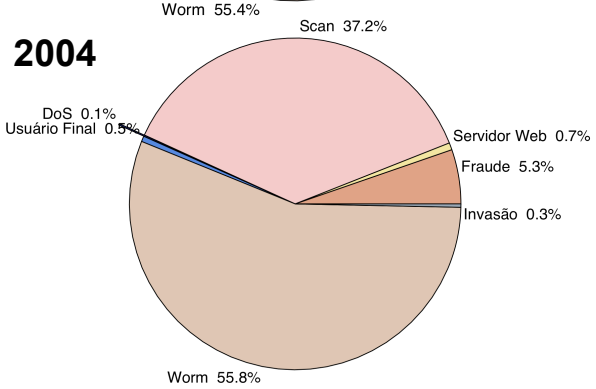
2006



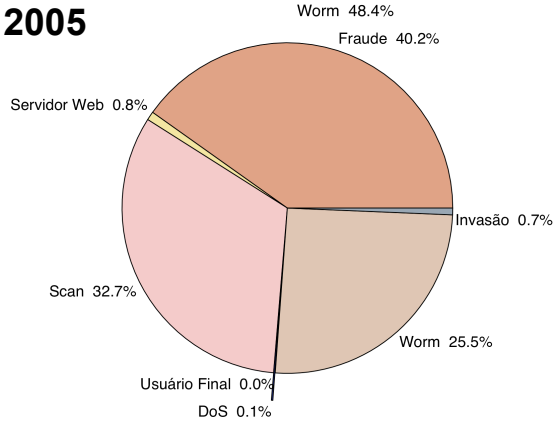
2007



2004



2005



Totais da categoria fraude:

2004	4.015 (05%)
2005	27.292 (40%)
2006	41.776 (21%)
2007	45.298 (28%)
2008	140.067 (62%)
2009/S1	239.022 (75%)

Totais da categoria *worm* (engloba *bots*):

2004	42.267 (55%)
2005	17.332 (25%)
2006	109.676 (55%)
2007	77.473 (48%)
2008	32.960 (14%)
2009/S1	38.852 (12%)

Resumo das Tendências

Mudança no enfoque dos atacantes:

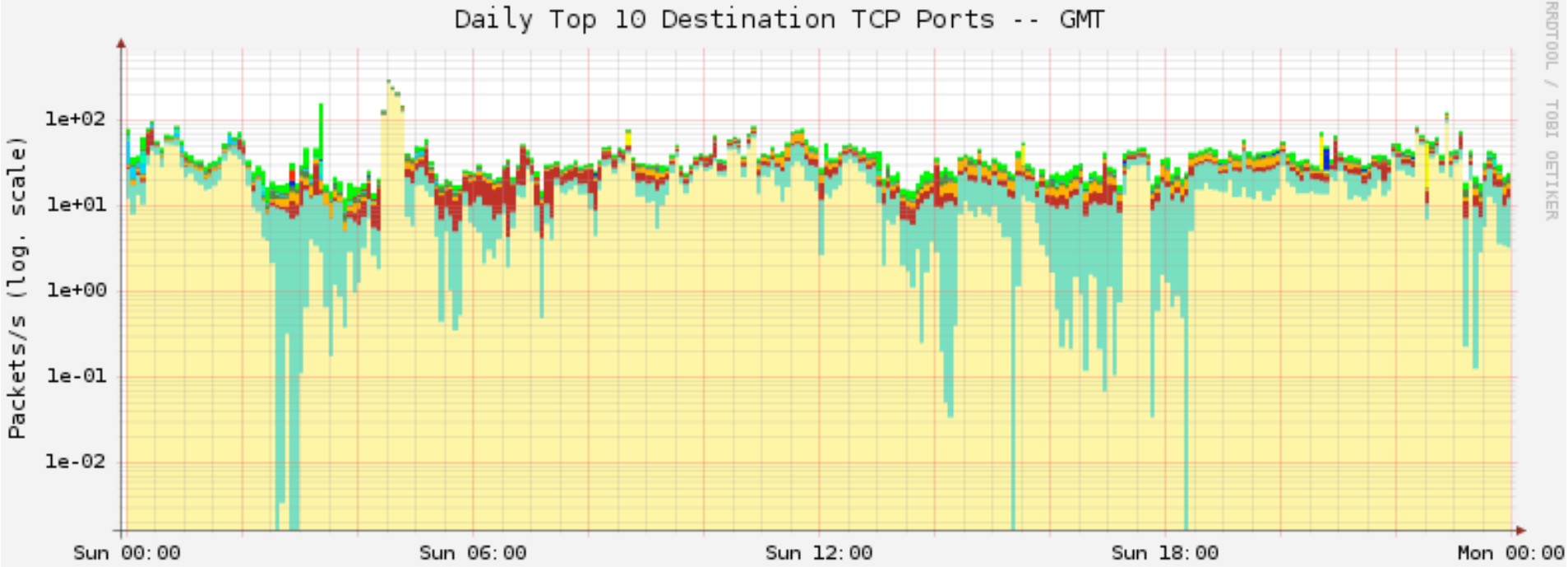
- **Ataques a usuários finais**
  - **fraudes, *bots*, *spyware*, etc**
- **Motivação financeira**

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 no último final de semana: *sites* principais da Vivo, da Oi e da Ambev**

Abuso da Infra-Estrutura de Redes

Varreduras mais freqüentes – *Honeypots* Distribuídos

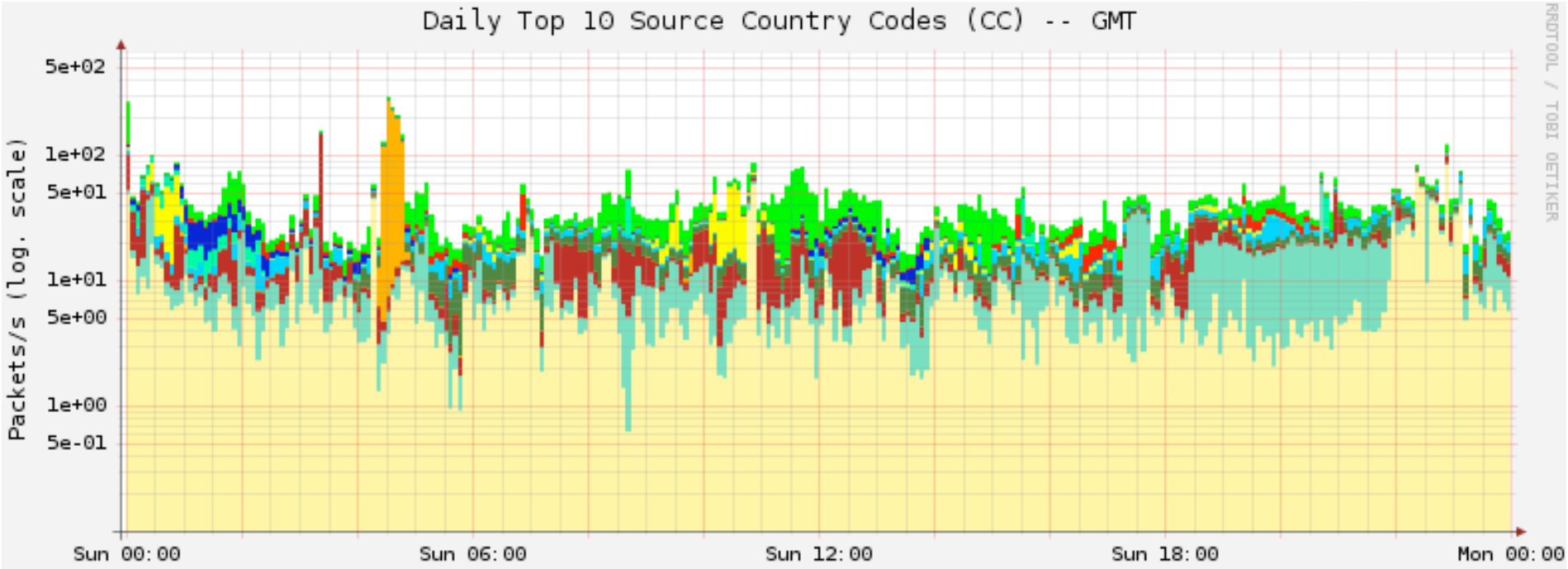


22 445 1433 139 135 1080 21 8080 5900 2967 Others

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

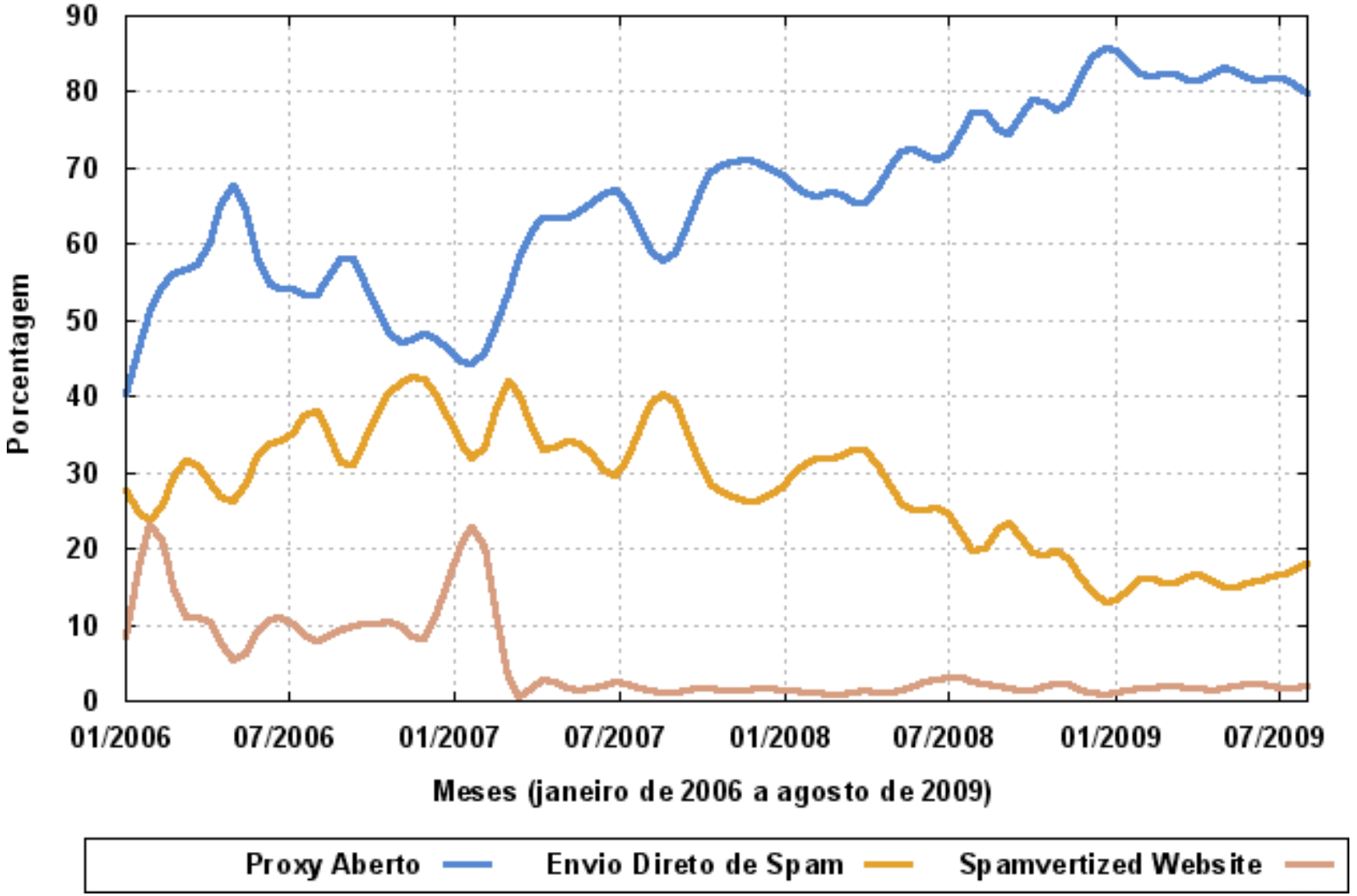


BR	Average:	8.15	pkts/s	Min:	0.62	pkts/s	Max:	83.74	pkts/s
CN	Average:	6.40	pkts/s	Min:	0.65	pkts/s	Max:	53.90	pkts/s
US	Average:	4.78	pkts/s	Min:	0.18	pkts/s	Max:	133.31	pkts/s
MX	Average:	3.20	pkts/s	Min:	0.00	pkts/s	Max:	262.98	pkts/s
VE	Average:	2.93	pkts/s	Min:	0.00	pkts/s	Max:	12.97	pkts/s
AR	Average:	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	1.537.377	17,37	01
IN	948.613	10,72	02
CN	548.955	6,20	03
RU	538.432	6,08	04
VN	494.946	5,59	05
PL	417.431	4,72	06
TH	233.900	2,64	07
IT	220.509	2,49	08
CO	216.495	2,45	09
UA	211.767	2,39	10

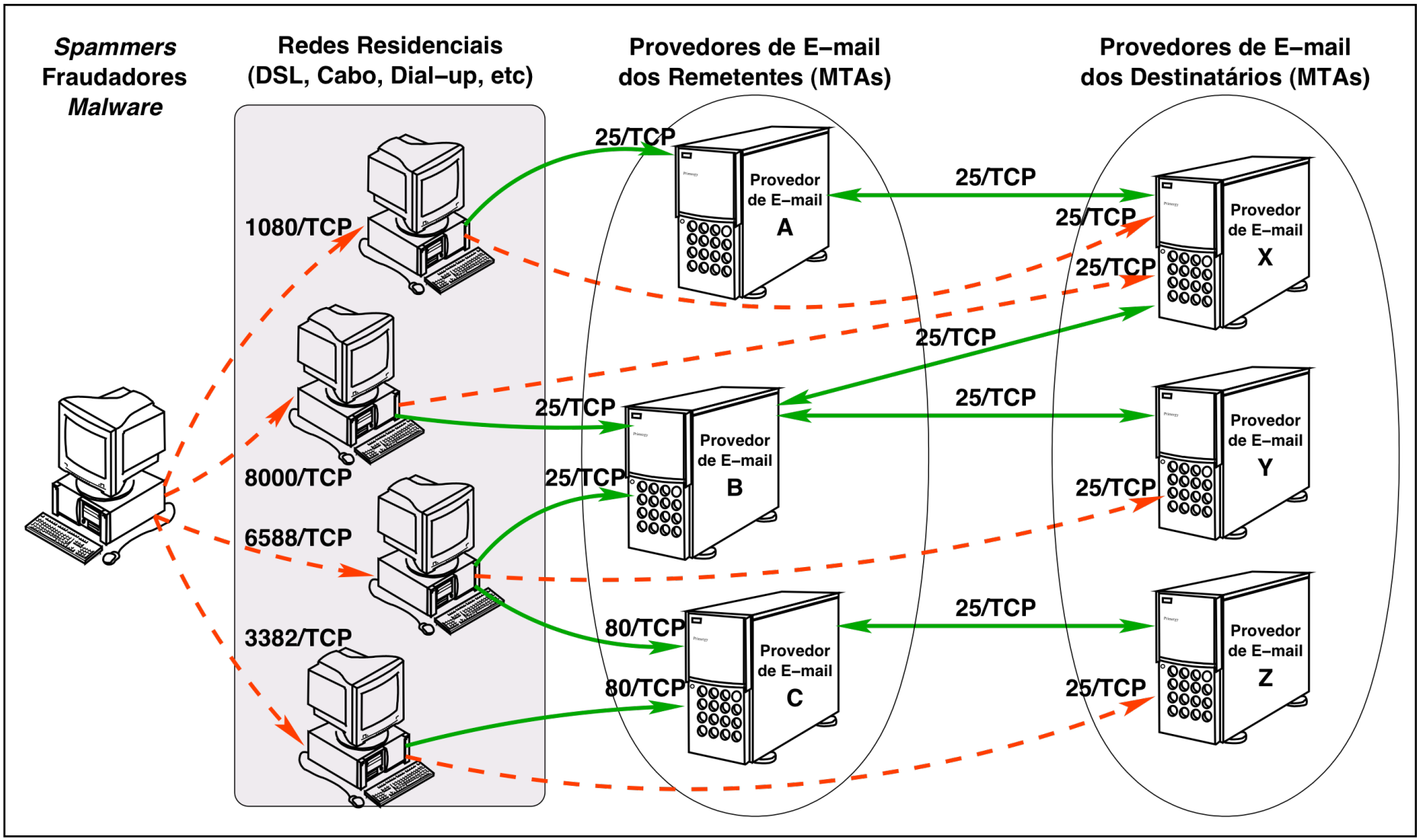
Domínios (DNS reverso) com maior número de IPs listados

Domínio	Total	%	Rank
telebahia.net.br	483.252	5.46	01
brasiltelecom.net.br	309138	3.49	05
telesp.com.br	268636	3.04	06
telet.com.br (claro)	99126	1.12	18
netservicos.com.br	90665	1.02	20
ig.com.br	71349	0.81	26
gvt.net.br	71140	0.80	27
timbrasil.com.br	35569	0.40	46
ctbctelecom.net.br	28053	0.32	56
embratel.net.br	17488	0.20	82

Dados gerados em: `Tue Sep 29 17:07:41 2009 UTC/GMT`
Composite Blocking List http://cbl.abuseat.org/

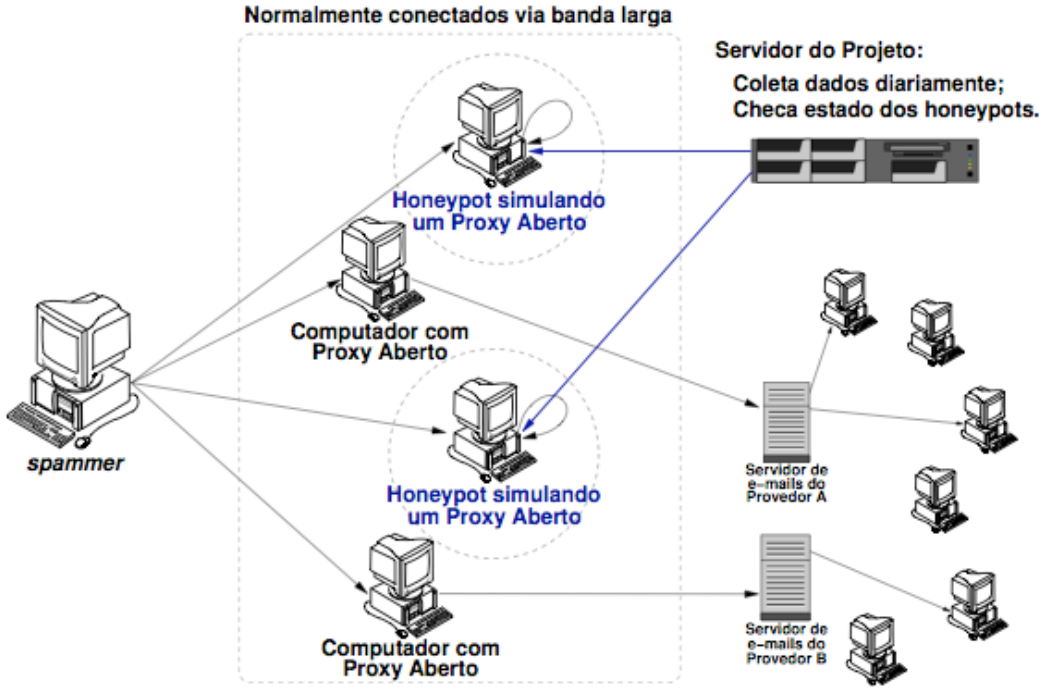
cgi.br | nic.br

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



Resultados do Projeto SpamPots: Métricas sobre o Abuso das Redes Brasileiras de Banda Larga

Dias de coleta:	**466**
***E-mails* capturados:**	**524.585.779**
Destinatários:	**4.805.521.964**
Destinatários/*e-mail*:	**≈ 9.1**
***E-mails*/dia:**	**≈ 1.2 Milhões**
IPs únicos:	**216.888**
ASNs únicos:	**3.006**
***Country Codes*:**	**165**



Principais Resultados:

- **99.84% das conexões eram originadas do exterior**
- **os *spammers* consumiam toda a banda de *upload* disponível**
- **mais de 90% dos *spams* eram destinados a redes de outros países**

http://www.cert.br/docs/whitepapers/spampots/

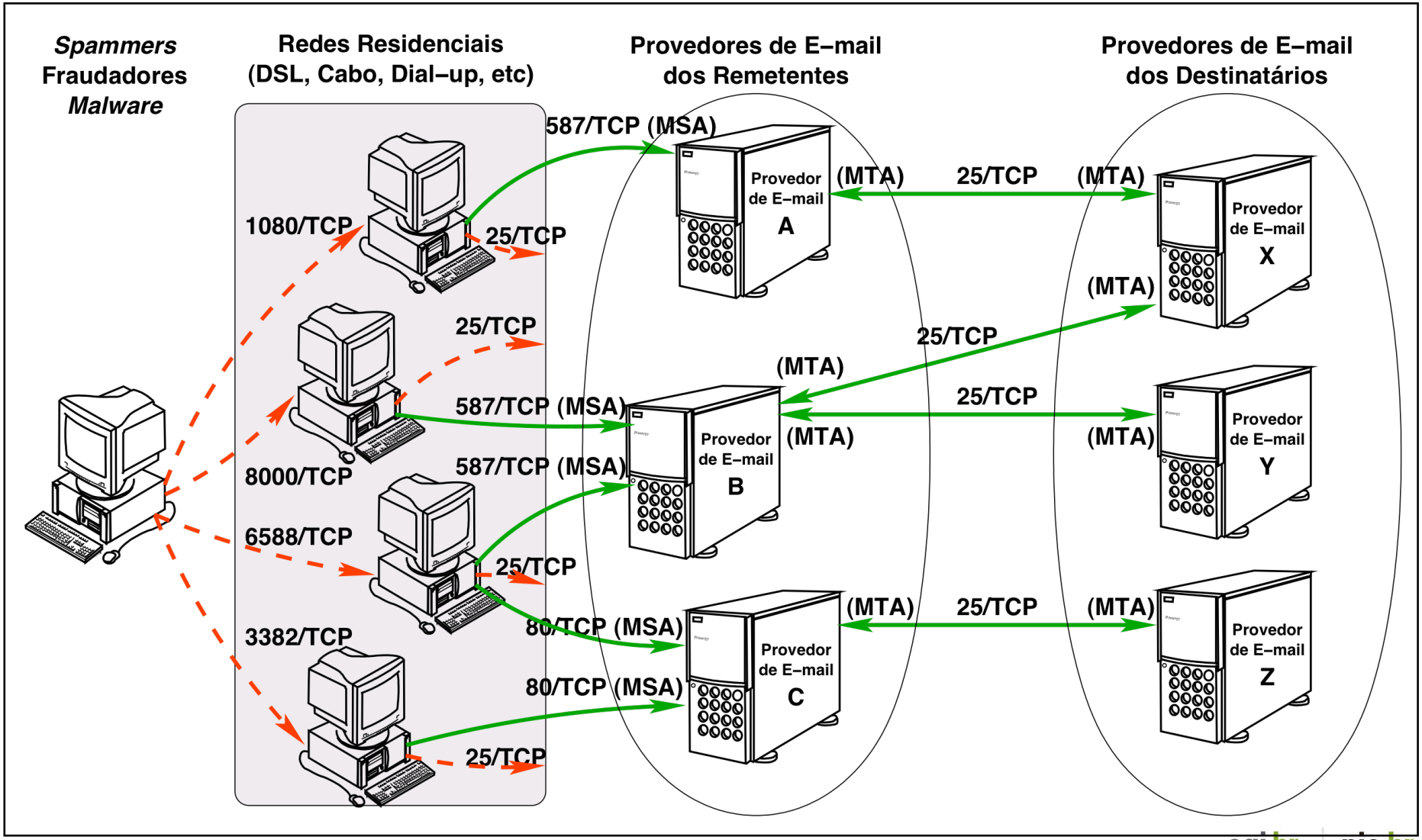
Características do Tráfego de Saída

Número de requisições recebidas pelos módulos, dividido de acordo com o tipo de conexão de saída solicitada:

Proxy HTTP		
Tipo	Requisições	%
conexão p/ 25/TCP	**89.496.969**	**97,62**
conexão p/ outras	106.615	0,12
`get`	225.802	0,25
erros	1.847.869	2,01
total	91.677.255	100,00

Proxy SOCKS		
Tipo	Requisições	%
conexão p/ 25/TCP	**46.776.884**	**87,31**
conexão p/ outras	1.055.081	1,97
erros	5.741.908	10,72
total	53.573.873	100,00

Método de Mitigação mais Efetivo: Gerência de Porta 25



Uso de *botnets* para DDoS

- **20 PCs domésticos abusando de Servidores DNS Recursivos Abertos podem gerar 1Gbps**
  - **No Brasil temos 15.000 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***

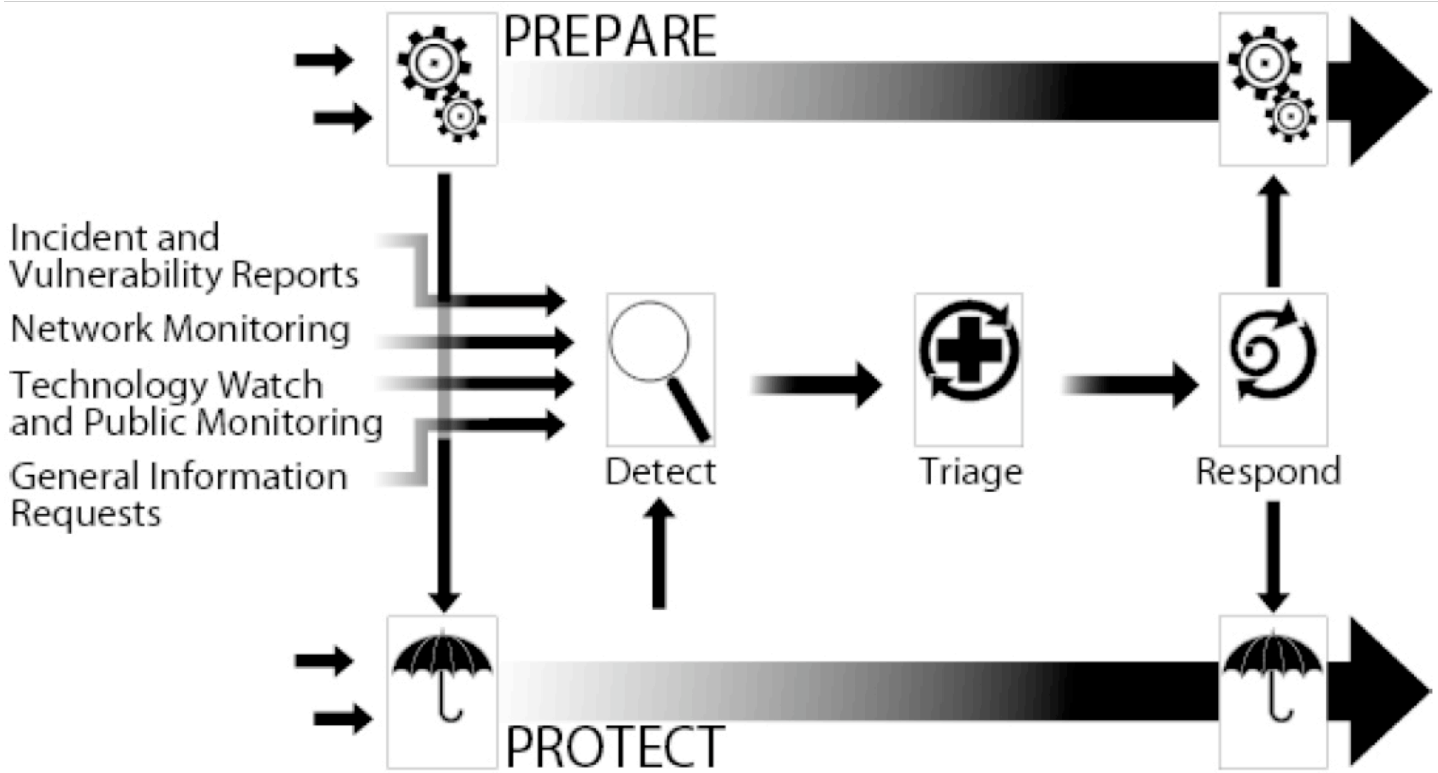
Fonte: ***Global Botnet Underground: DDoS and Botconomics*.**
***Jose Nazario, Ph.D., Head of Arbor* ASERT**
***Keynote* do Evento RioInfo 2009**

Papel dos CSIRTs

Definições: CSIRTs e 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 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

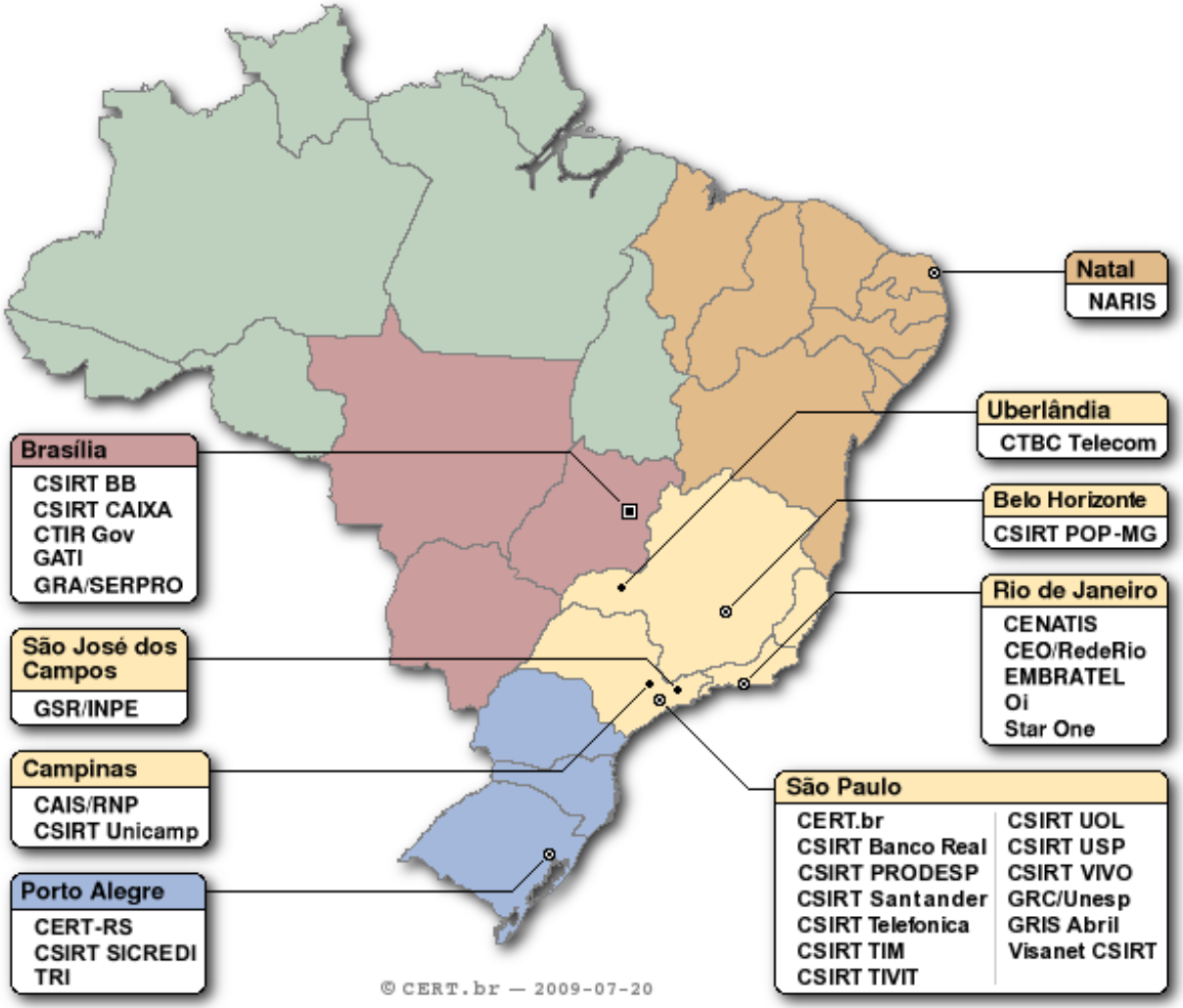
Evolução do Tratamento de Incidentes no Brasil (1/2)

- Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo CGI.br[1]
- Junho/1997: o CGI.br cria o CERT.br (naquele tempo chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]
- Agosto/1997: a RNP cria seu próprio CSIRT (CAIS)[3], seguida pela rede acadêmica do Rio grande do Sul (CERT-RS)[4]
- 1999: outras instituições, incluindo Universidades e Operadoras de Telecomunicações, iniciaram a formação de seus CSIRTs
- 2002–2004 : grupos de trabalho para definição da estrutura de um CSIRT para a Administração Pública Federal
- 2004: o CTIR-Gov foi criado, com a Administração Pública Federal como seu público alvo[5]

[1] http://www.nic.br/grupo/historico-gts.htm
[2] http://www.nic.br/grupo/gts.htm
[3] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[4] http://www.cert-rs.tche.br/cert-rs.html
[5] http://www.ctir.gov.br

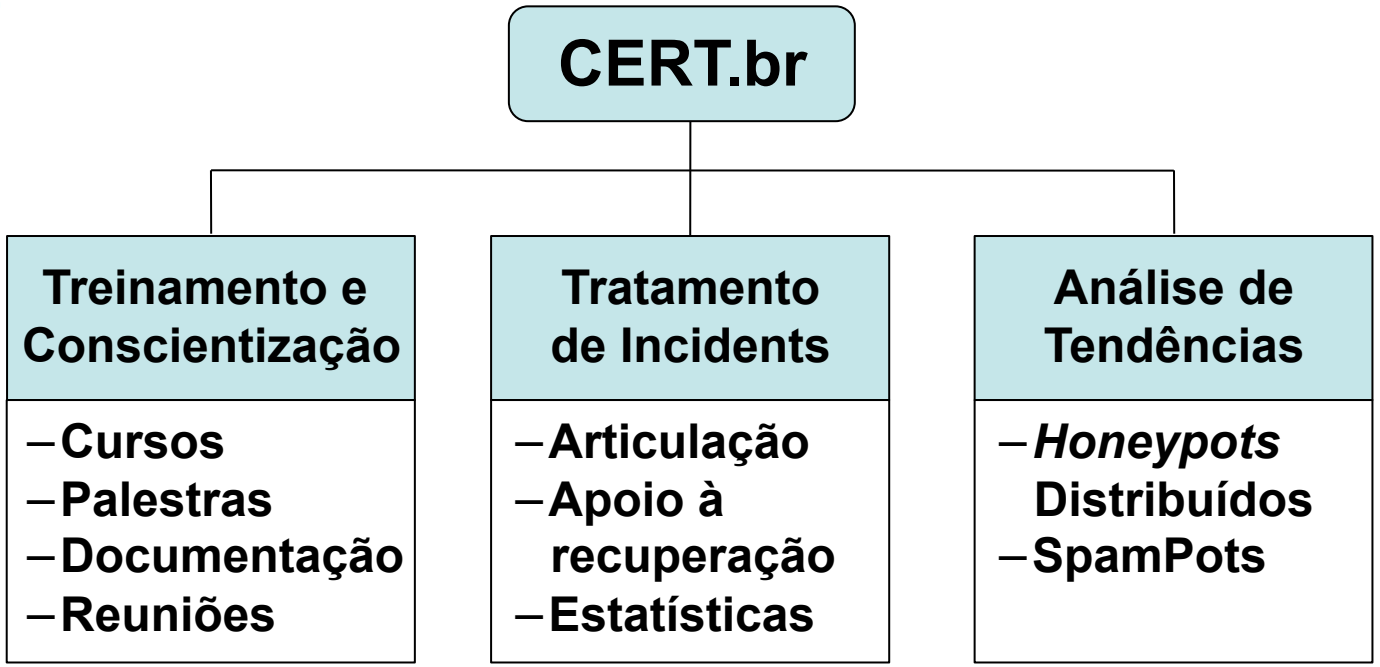
Evolução do Tratamento de Incidentes no Brasil (2/2)

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

Papel do CERT.br no Combate aos Crimes que Fazem Uso da Informática



SEIPartner
CERT Courses

FIRST
Improving Security Together
MEMBER

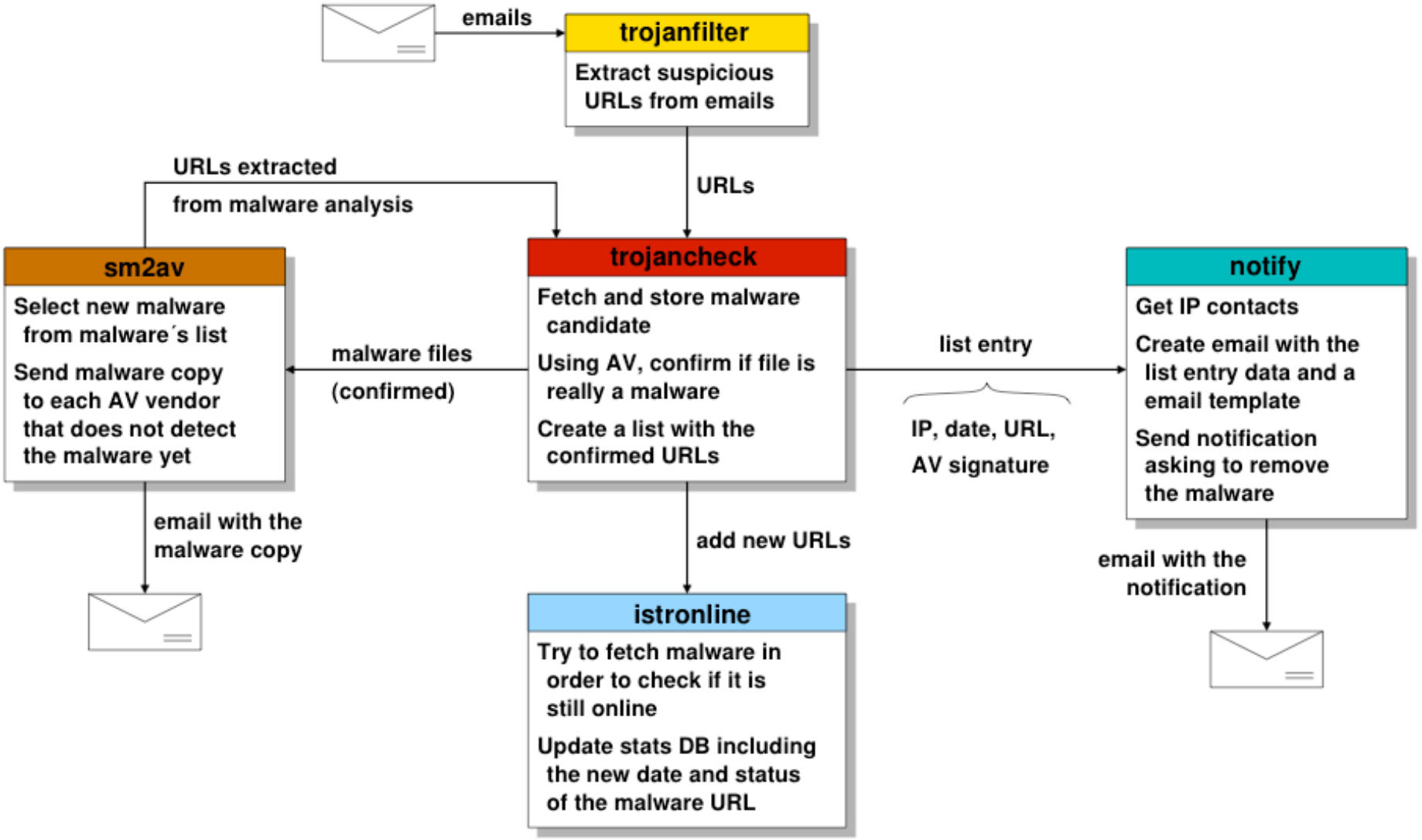
APWG
RESEARCH PARTNER
www.antiphishing.org

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

Identificação de *Trojans*, Solicitação de Remoção e Adição de Assinaturas em *Softwares* Antivírus



Malwares Relacionados com Fraudes: 2006–2009/1S

Category	2006	2007	2008	2009 1ºSem
URLs únicas	25.087	19.981	17.376	**4.973**
Exemplares de *Trojans* (*hashes* únicos)	19.148	16.946	14.256	**3.740**
Assinaturas de antivírus (únicas)	1.988	3.032	6.085	**1.564**
Assinaturas de antivírus (famílias)	41	125	447	**935**
Extensões de arquivos	73	112	112	**65**
Domínios	5.587	7.795	5.916	**2.048**
Endereços IP únicos	3.859	4.415	3.921	**1.595**
Países aos quais os IPs estão alocados	75	83	78	**64**
E-mails de notificação enviados pelo CERT.br	18.839	17.483	15.499	**4.354**

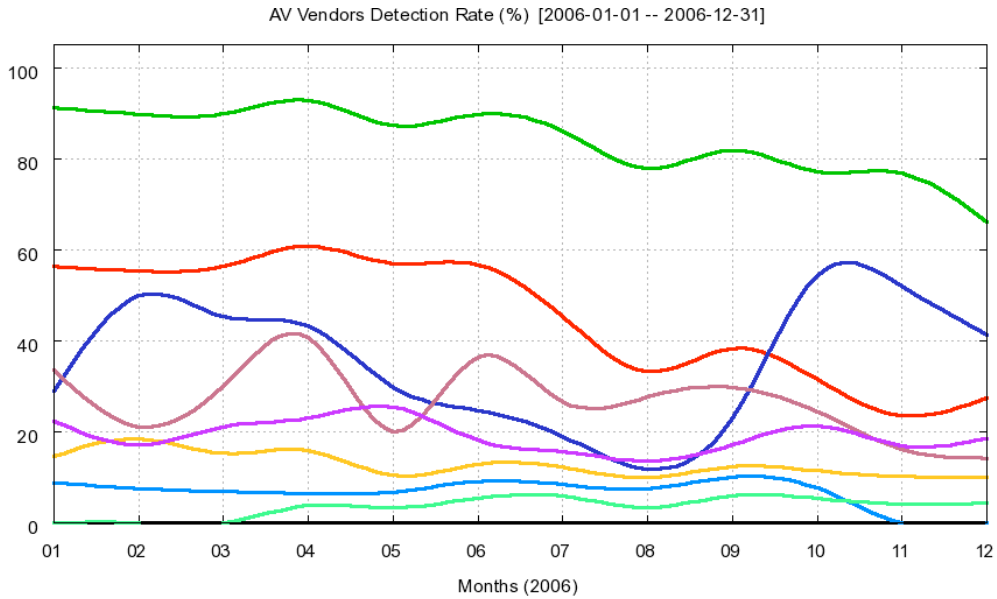
Inclui:

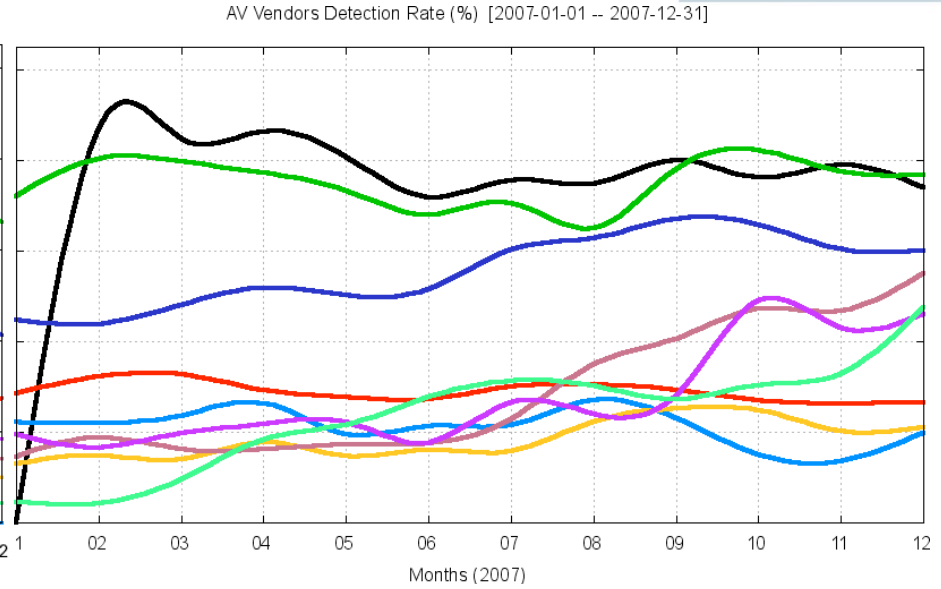
- *Keyloggers*
- *Screenloggers*
- *Trojan Downloaders*

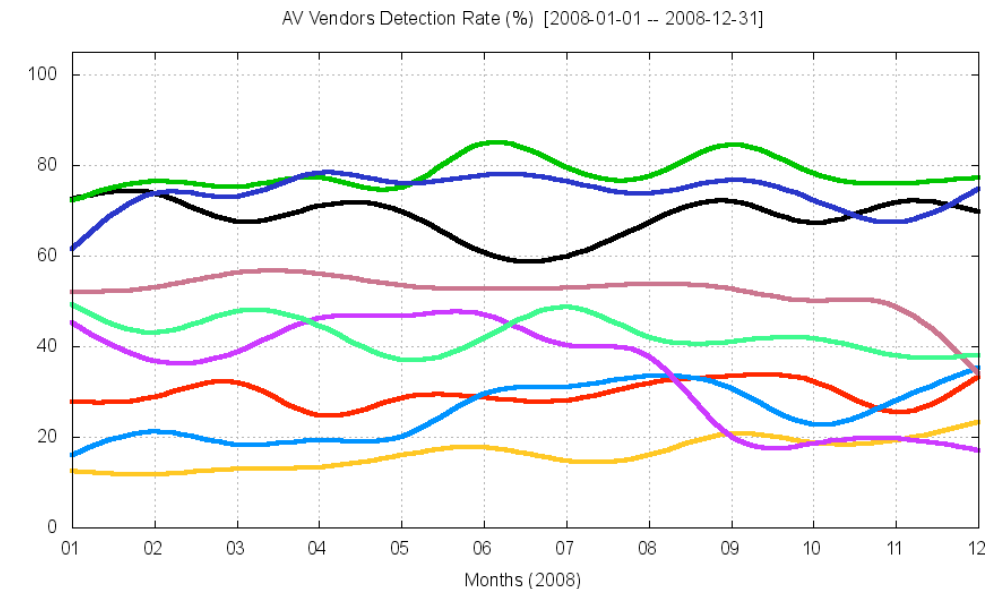
NÃO inclui:

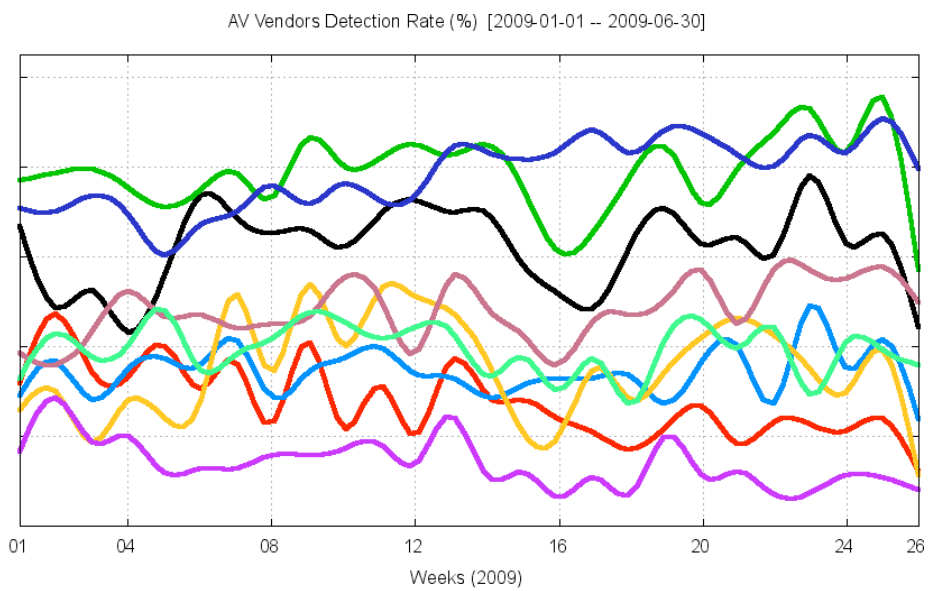
- *Bots/Botnets*
- *Worms*

Taxa de Detecção dos Antivírus - 2006–2009/1º Sem

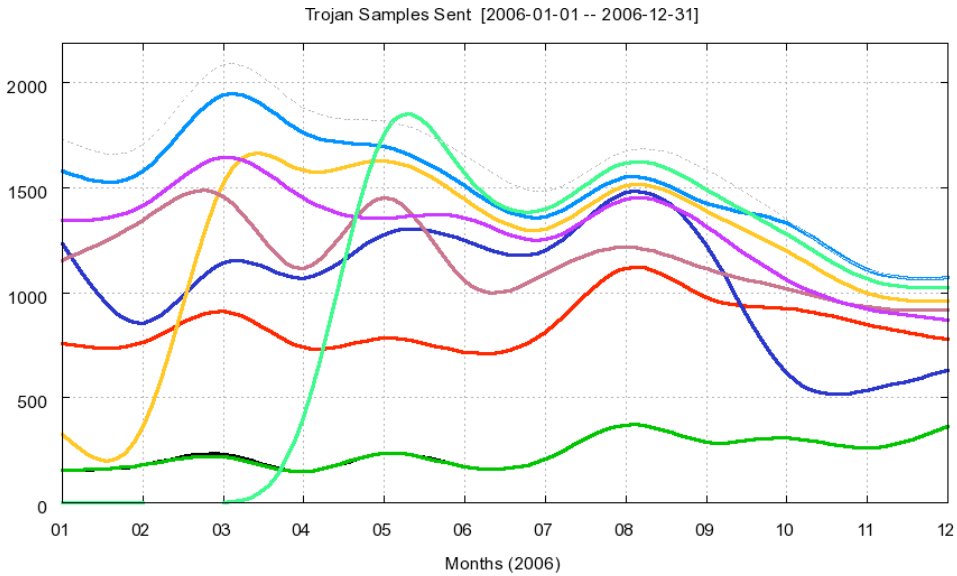


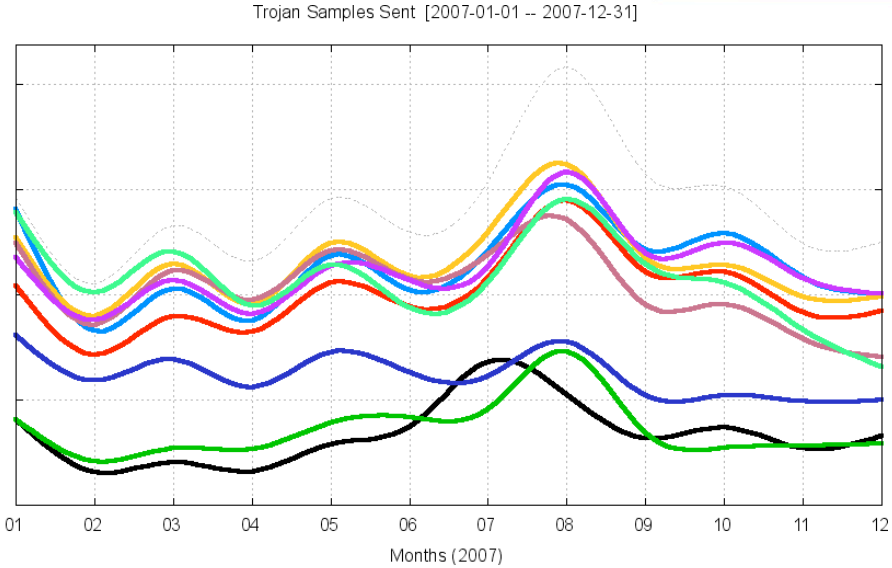


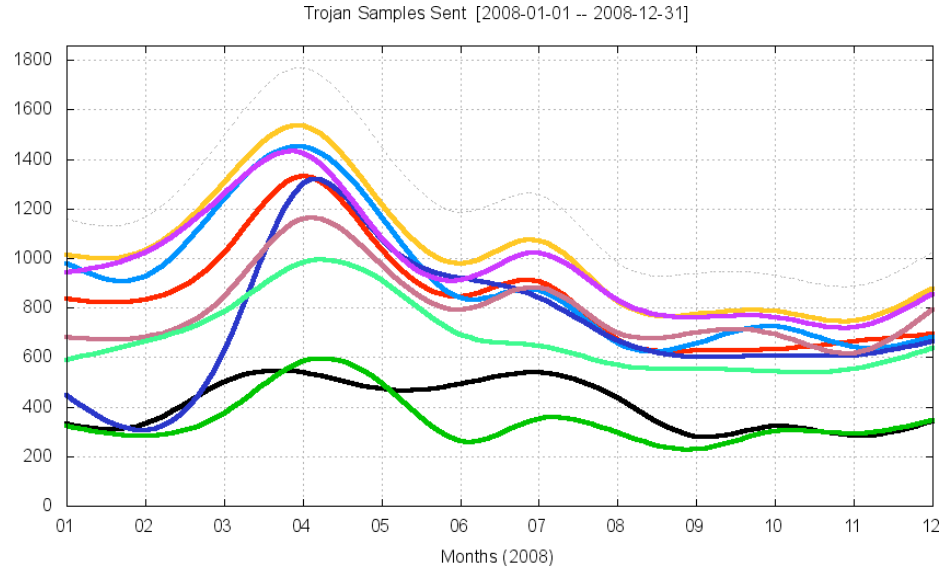


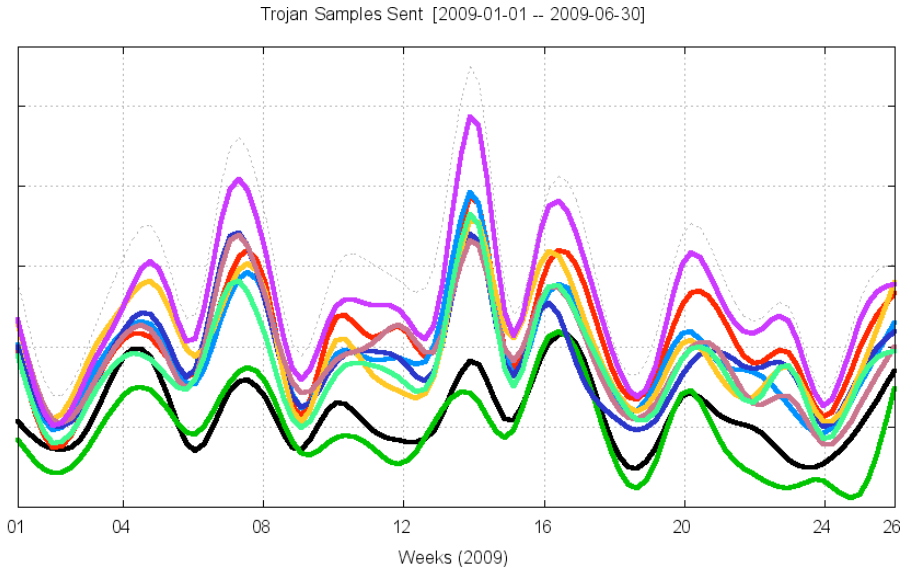


Exemplares enviados - 2006–2009/1º Sem









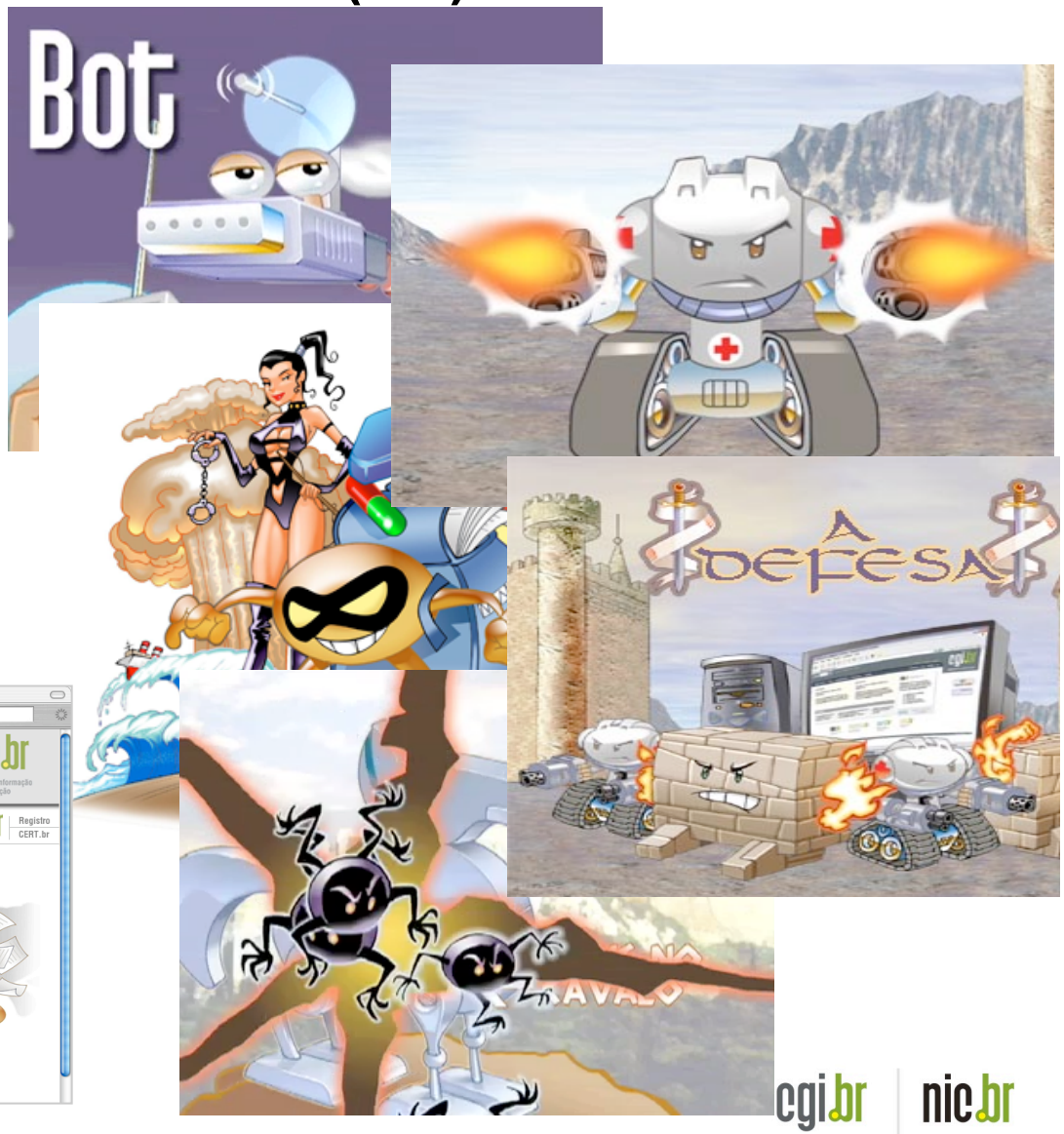
Material que reflete as causas dos Incidentes Mais Comuns e as Tendências Observadas (1/2)

- **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/

Material que reflete as causas dos Incidentes Mais Comuns e as Tendências Observadas (2/2)

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



Considerações Finais

- **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
- **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**

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/