Cenário das Fraudes e do *Spam* no Brasil

Klaus Steding-Jessen
jessen@cert.br

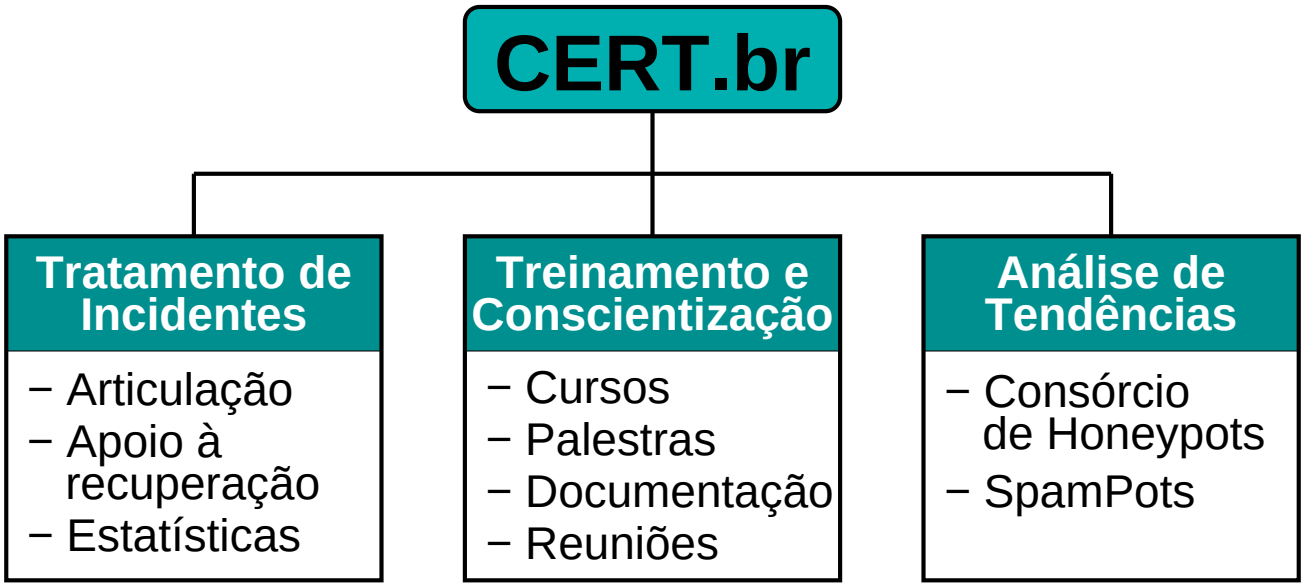
Marcelo H. P. C. Chaves
mhp@cert.br

Esta apresentação:
http://www.cert.br/docs/palestras/

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto br
Comitê Gestor da Internet no Brasil

Sobre o CERT.br

Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



FIRST Improving Security Together MEMBER

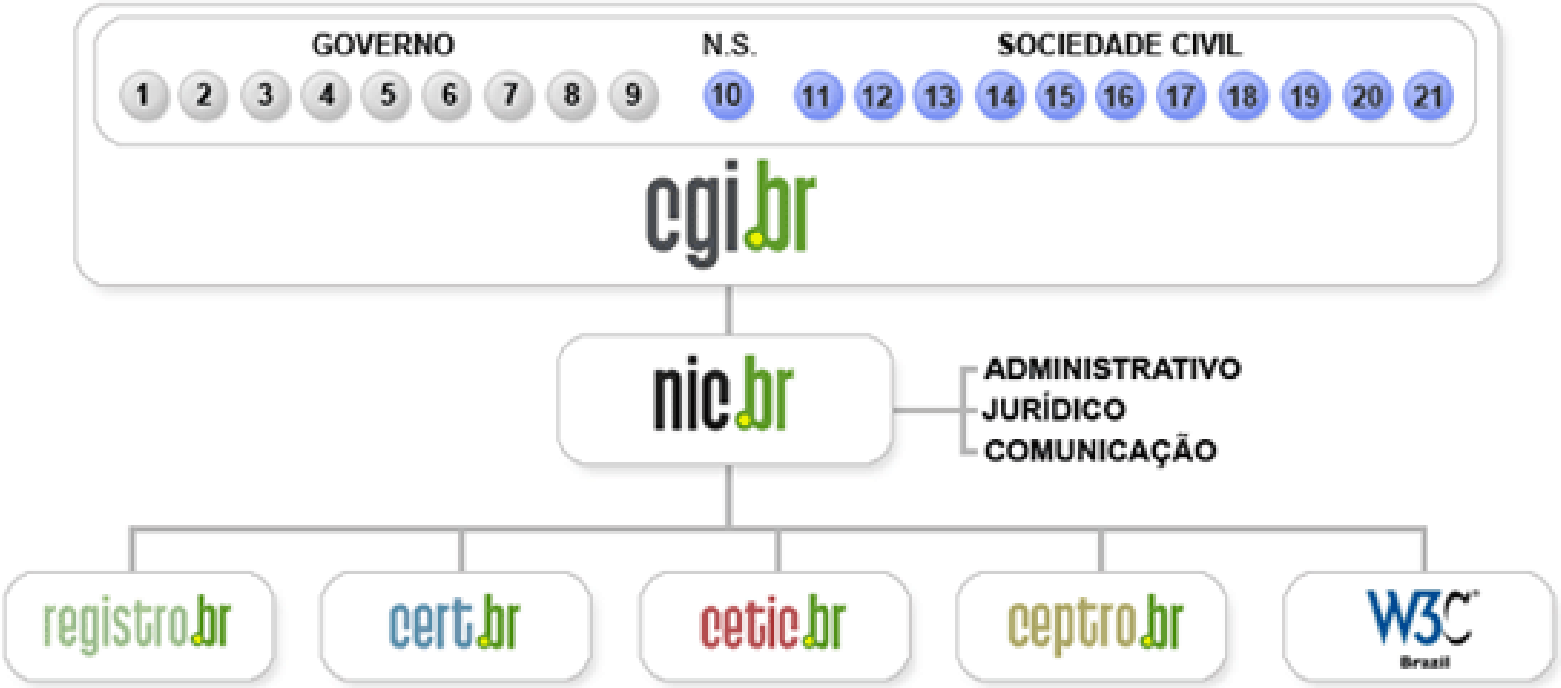
APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner CERT Courses

The Honeynet PROJECT®

http://www.cert.br/missao.html

Estrutura do CGI.br



01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério do Planejamento, Orçamento e Gestão
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério da Defesa
07- Agência Nacional de Telecomunicações
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades 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**

Agenda

- Fraudes
  - Histórico e cenário atual
  - *Malware*
  - *Phishing*
- *Spam*
  - Reclamações ao CERT.br em 2009
  - Abuso de Proxies em PCs Infectados
  - Brasil na CBL
  - Gerência de Porta 25
- Referências

Fraudes

Histórico e cenário atual (1/2)

2001 *Keyloggers* enviados por *e-mail*, ataques de força bruta

2002–2003 *Phishing* e uso disseminado de DNSs comprometidos

2003–2004 Aumento dos casos de *phishing* mais sofisticados
- *Sites* coletores: processamento/envio de dados p/ contas de *e-mail*

2005–2006 *Spams* em nome de diversas entidades/temas variados
- *Links* para cavalos de tróia hospedados em diversos *sites*
- Vítima raramente associa o *spam* com a fraude financeira

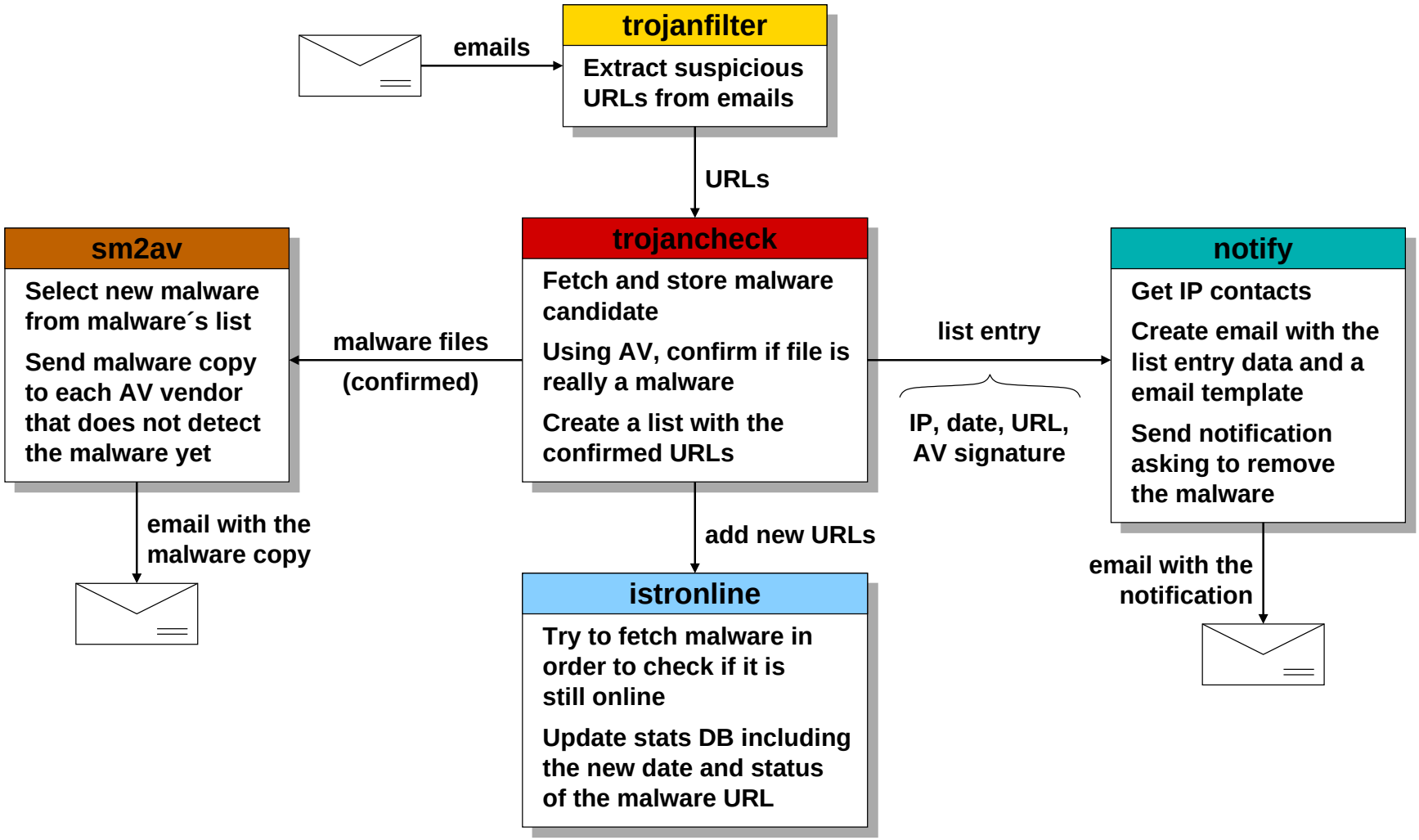
2007 *downloads* involuntários (via JavaScript, ActiveX, etc) - Continuidade das tendências de 2005–2006

Histórico e cenário atual (2/2)

2008–hoje

- Continuidade das tendências de 2005–2007
- *downloads* involuntários mais freqüentes, inclusive em grandes sites
  - casos publicados na mídia nos últimos meses incluem: sites principais da Vivo, da Oi e da Ambev
- *links* patrocinados do Google usando a palavra “banco” e nomes de instituições como “AdWords”
- *Malware* modificando arquivo *hosts* – antigo, mas ainda efetivo
- *Malware* modificando configuração de *proxy* em navegadores (arquivos PAC)
- *Malware* se registrando como Browser Helper Objects (BHO) em navegadores
- *Malware* validando, no site real, os dados capturados

Sistema de Monitoramento de *Malware*



Estatísticas de *Malware* (1/3)

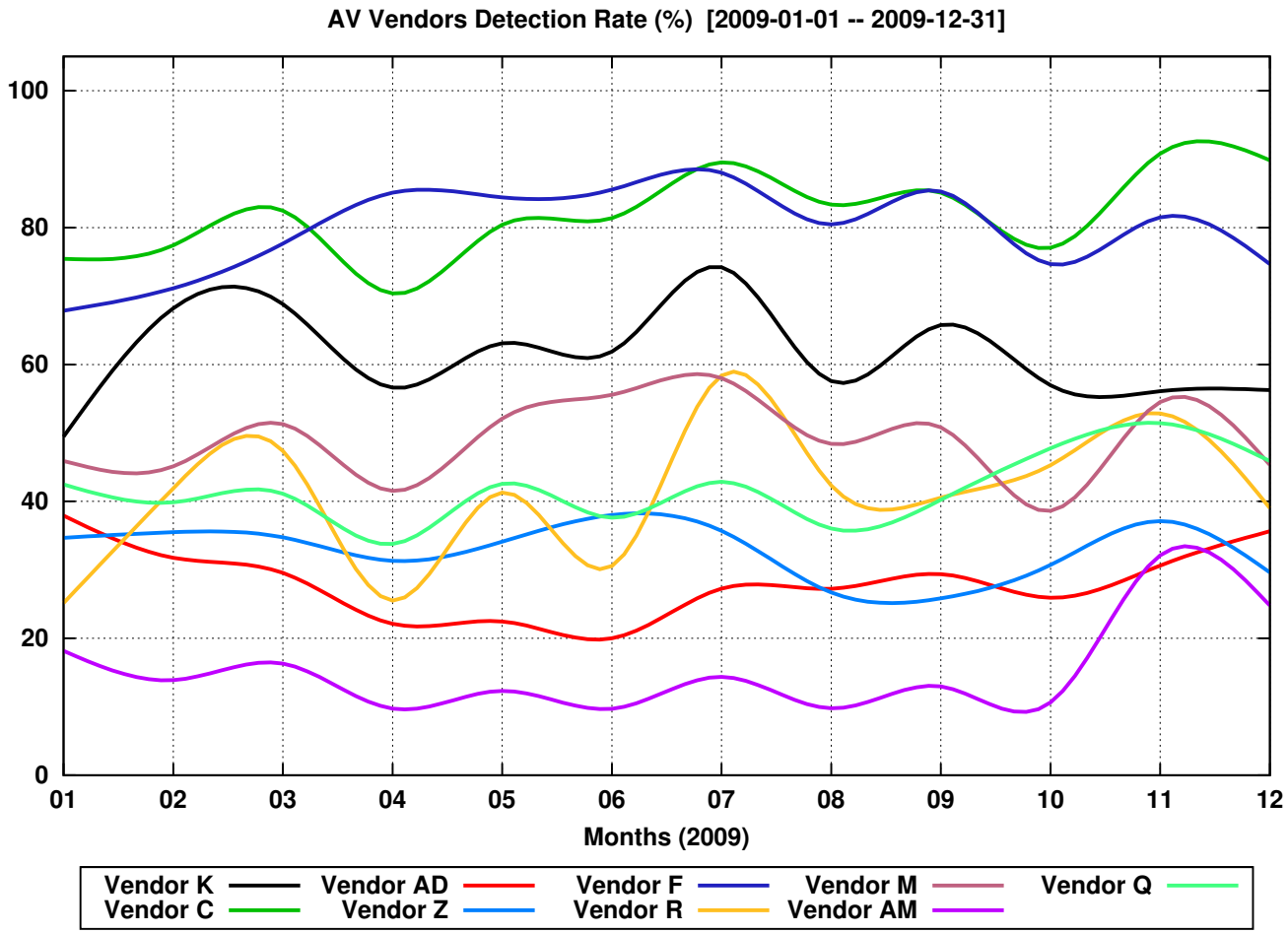
Tentativas de fraude tratadas envolvendo *malware**:

Categoria	2006	2007	2008	2009
URLs únicas	**25.087**	**19.981**	**17.376**	**10.864**
Códigos maliciosos únicos (*hashes* únicos)	**19.148**	**16.946**	**14.256**	**8.151**
Assinaturas de Antivírus (únicas)	**1.988**	**3.032**	**6.085**	**4.101**
Assinaturas de Antivírus ("família")	**140**	**109**	**63**	**93**
Extensões de arquivos usadas	**73**	**112**	**112**	**100**
Domínios	**5.587**	**7.795**	**5.916**	**4.447**
Endereços IP únicos	**3.859**	**4.415**	**3.921**	**3.233**
Países de origem	**75**	**83**	**78**	**76**
Emails de notificação enviados pelo CERT.br	**18.839**	**17.483**	**15.499**	**9.935**

(*) Incluem *keyloggers*, *screen loggers*, *trojan downloaders* – não incluem *bots*/*botnets*, *worms*

Estatísticas de *Malware* (2/3)

Taxas de Detecção dos Antivírus em 2009:

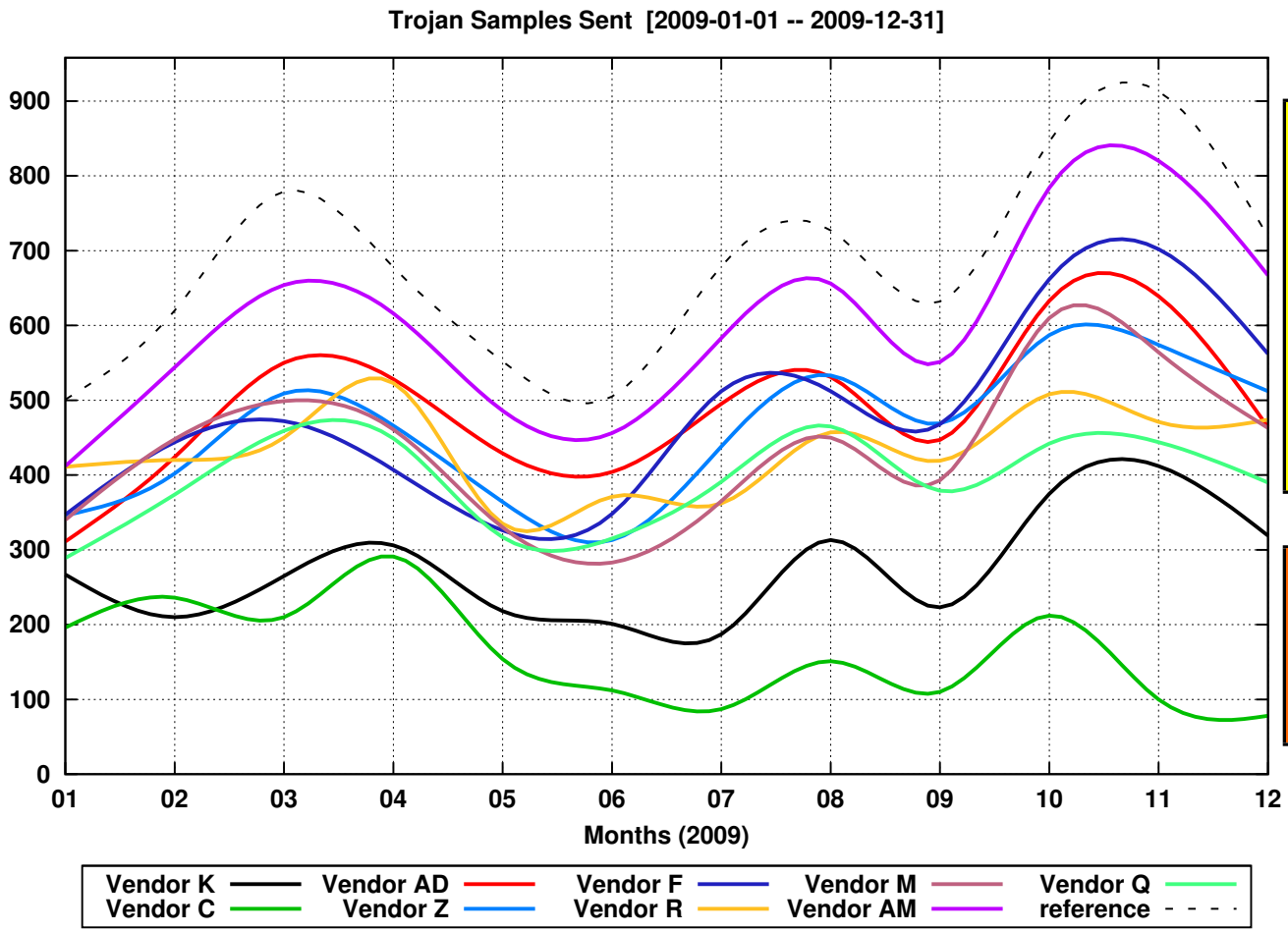


21% dos antivírus detectaram mais de 70% dos exemplares

72% dos antivírus detectaram menos de 50% dos exemplares

Estatísticas de *Malware* (3/3)

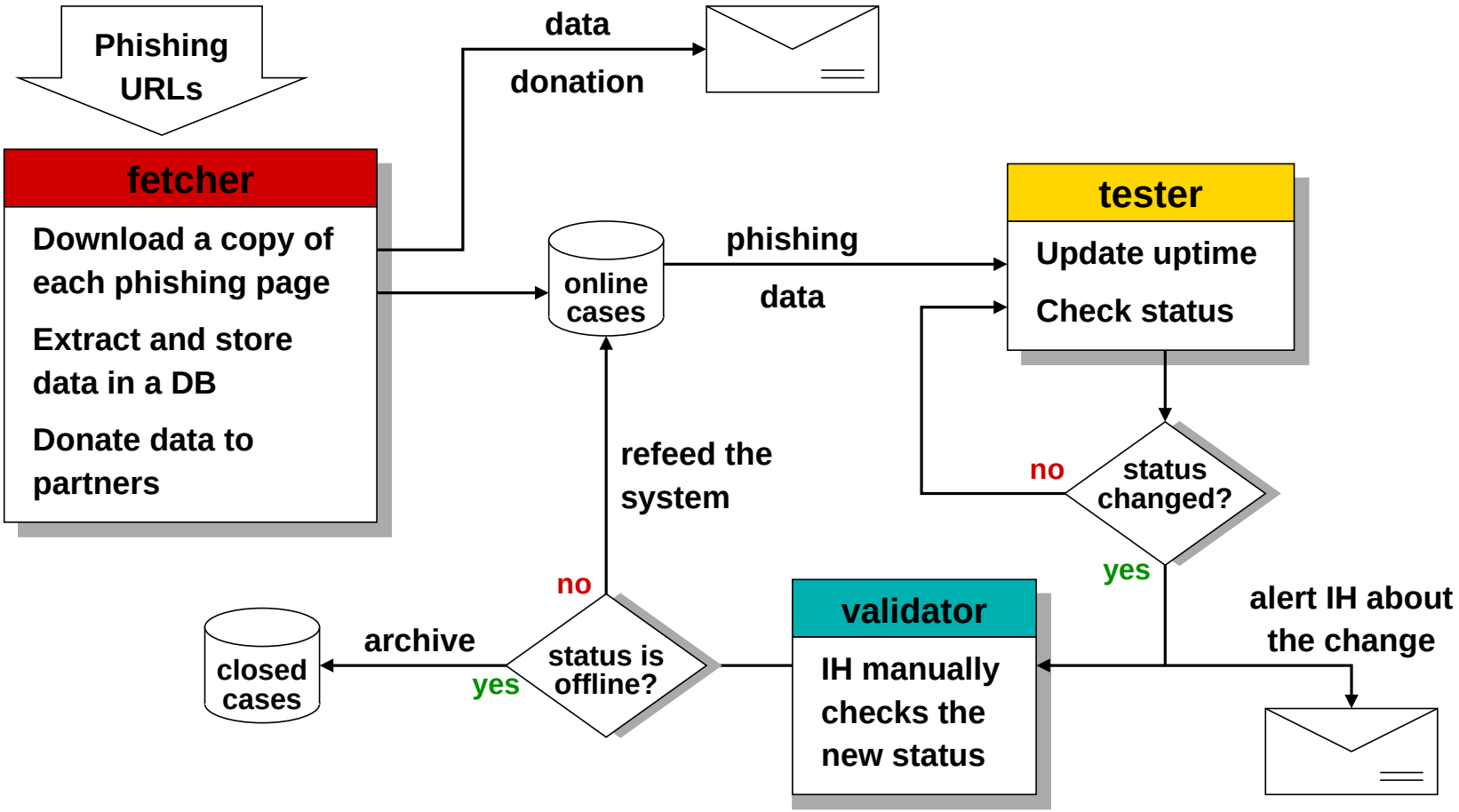
Malwares enviados para 25+ Antivírus em 2009:



Casos de fraude relacionados a *malware* reduziram 23% do ano de 2008 para 2009, mas aumentaram 14% do terceiro para o quarto trimestre de 2009

Casos de páginas de *phishing* aumentaram 112% do ano de 2008 para 2009

Sistema de Monitoramento de *Phishing*



Estatísticas de *Phishing* (1/2)

Tentativas de fraude tratadas envolvendo *phishing* em 2009

Casos	**total**	**3332**
	online	**51**
	off-line	**3281**
	bancos (BR)	**1916**
Alvos	**total**	**177**
	bancos (BR)	**32**

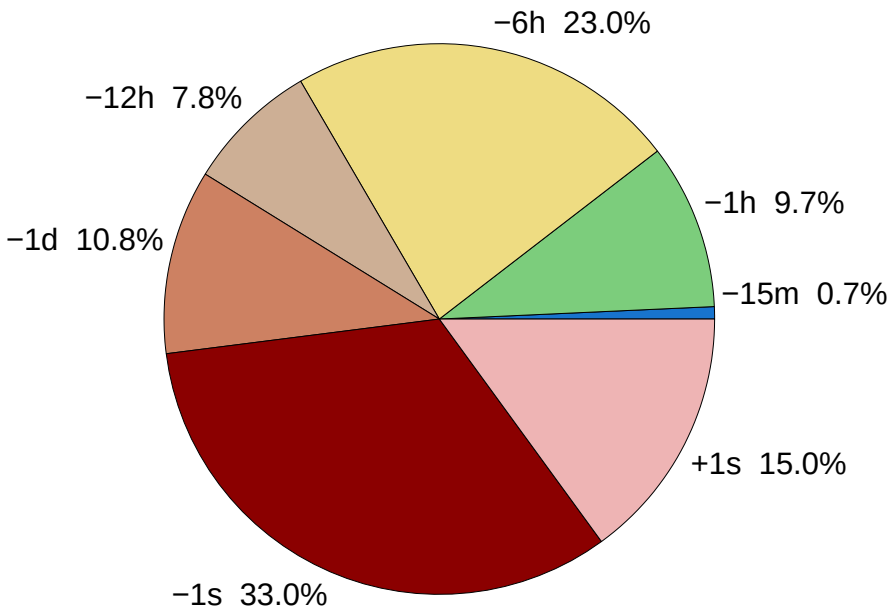
URLs únicas	**3215**
***Hashes* únicos**	**1671**
Domínios	**1619**
Endereços IP	**1344**
CIDRs	**452**
Países (CCs)	**49**

tempo de vida

Máximo	**218d 05h 26m**
Mínimo	**0d 00h 00m**
Média	**4d 07h 12m**
Desvio padrão	**11d 01h 25m**

casos por tempo de vida

<=	**15 minutos**	**(-15m)**	**24**
<=	**1 hora**	**(-1h)**	**324**
<=	**6 horas**	**(-6h)**	**765**
<=	**12 horas**	**(-12h)**	**259**
<=	**1 dia**	**(-1d)**	**361**
<=	**1 semana**	**(-1s)**	**1100**
>	**1 semana**	**(+1s)**	**499**



Estatísticas de *Phishing* (2/2)

Tentativas de fraude tratadas envolvendo *phishing* em 2009

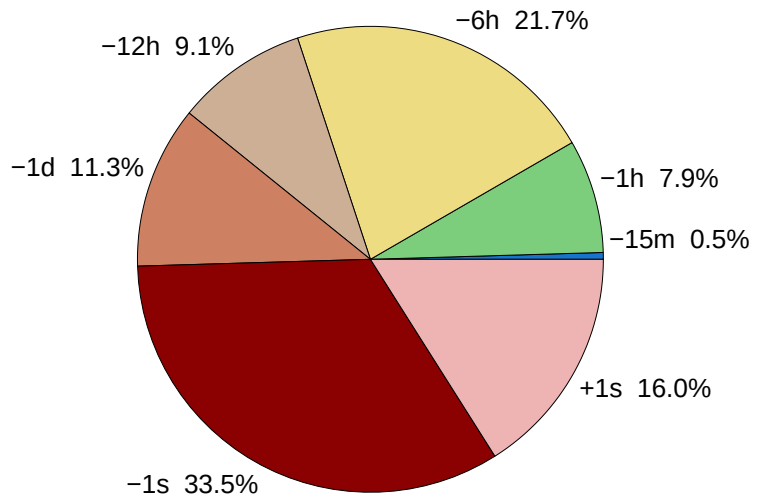
Bancos Brasileiros

tempo de vida

Máx.	**149d 22h 06m**
Mín.	**0d 00h 00m**
Média	**4d 13h 54m**
D. P.	**10d 13h 08m**

casos por tempo de vida

<=	**15 minutos**	**(-15m)**	**9**
<=	**1 hora**	**(-1h)**	**151**
<=	**6 horas**	**(-6h)**	**416**
<=	**12 horas**	**(-12h)**	**175**
<=	**1 dia**	**(-1d)**	**216**
<=	**1 semana**	**(-1s)**	**642**
>	**1 semana**	**(+1s)**	**307**



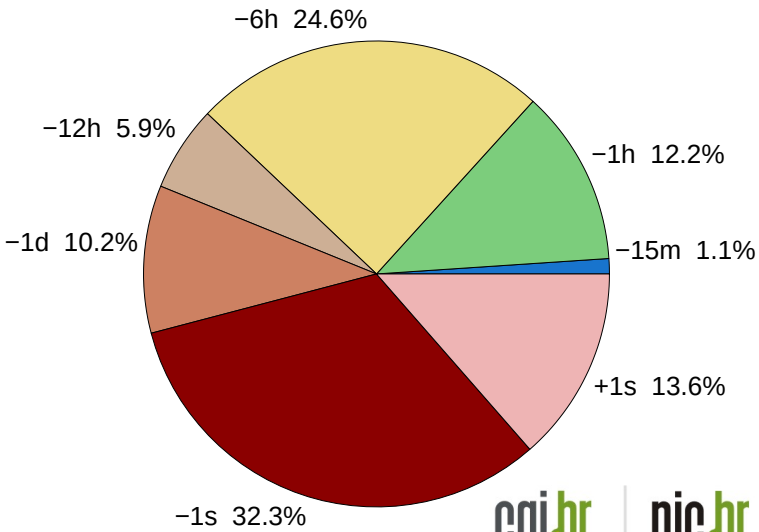
Outras Entidades

tempo de vida

Máx	**218d 05h 26m**
Mín.	**0d 00h 00m**
Média	**3d 22h 09m**
D. P.	**11d 17h 46m**

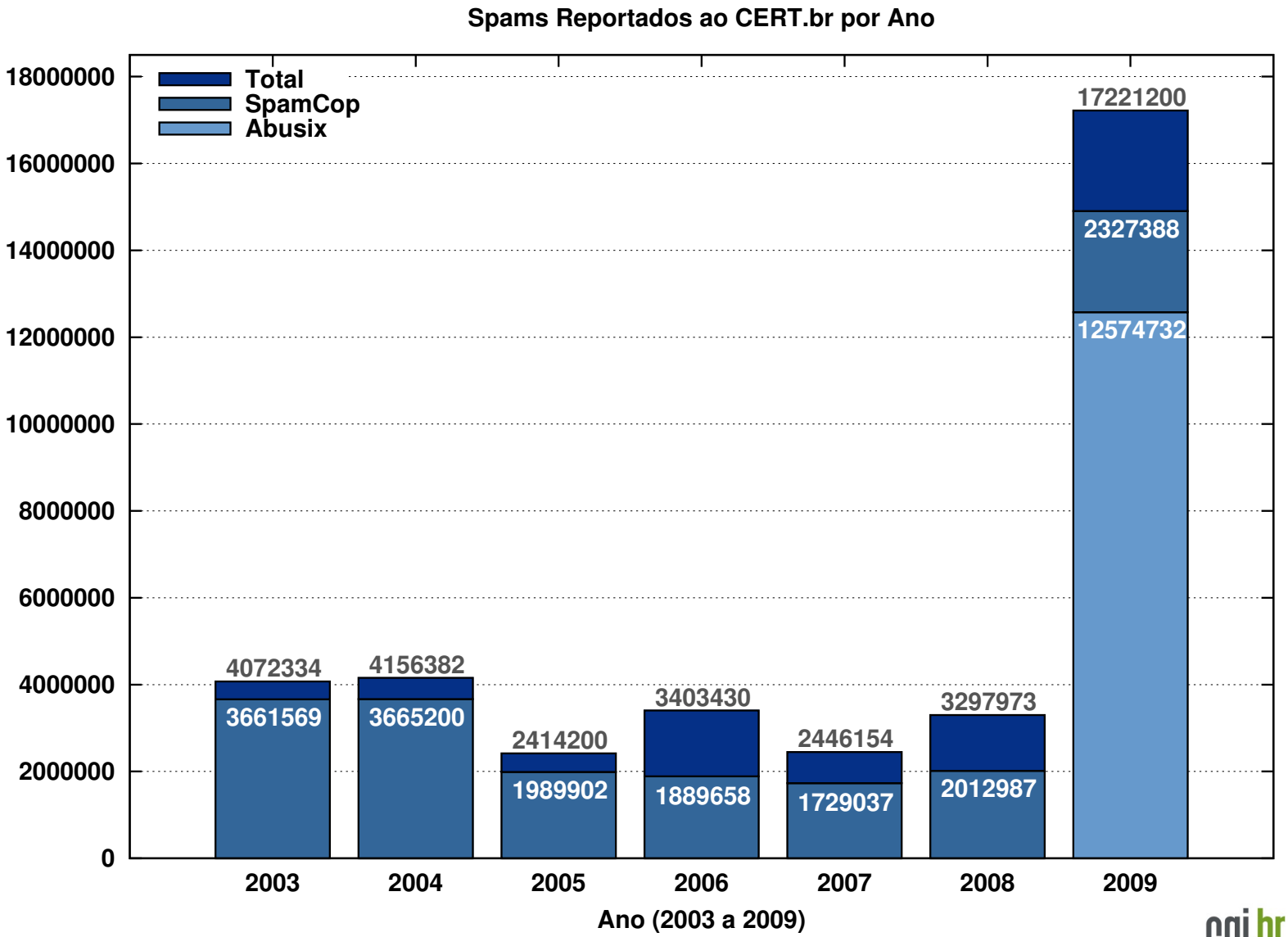
casos por tempo de vida

<=	**15 minutos**	**(-15m)**	**15**
<=	**1 hora**	**(-1h)**	**173**
<=	**6 horas**	**(-6h)**	**349**
<=	**12 horas**	**(-12h)**	**84**
<=	**1 dia**	**(-1d)**	**145**
<=	**1 semana**	**(-1s)**	**458**
>	**1 semana**	**(+1s)**	**192**

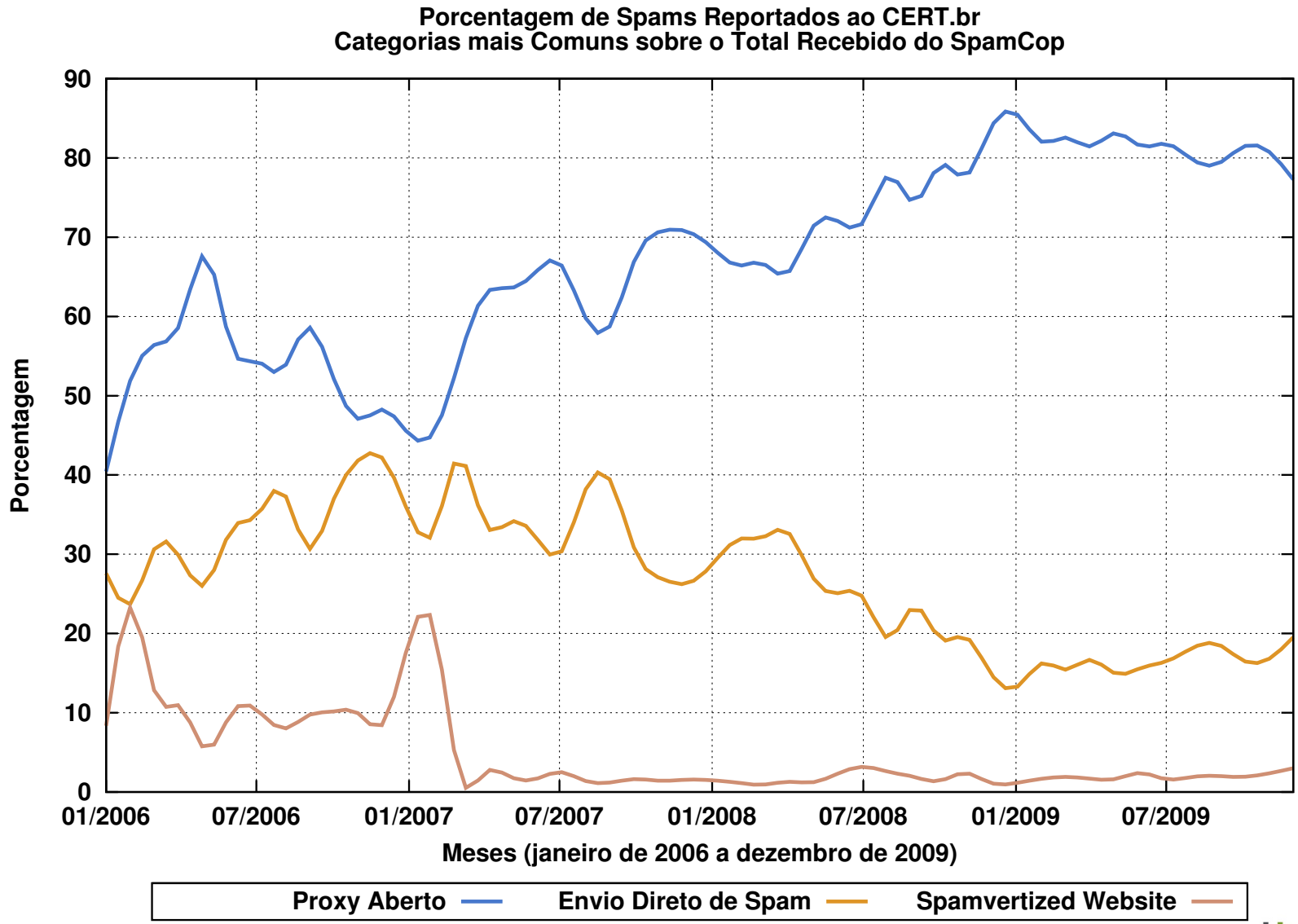


Spam

Reclamações ao CERT.br em 2009



Abuso de *Proxies* em PCs Infectados



Brasil na CBL

***Country Codes* com maior número de IPs listados**

CC	Total	%	Rank
BR	970.983	13,47	01
IN	907.018	12,58	02
VN	435.601	6,04	03
RU	380.800	5,28	04
DE	361.723	5,02	05
UA	256.546	3,56	06
CN	212.269	2,94	07
TH	208.814	2,90	08
US	183.377	2,54	09
RO	158.354	2,20	10

Domínios (DNS reverso) com maior número de IPs listados

Domínio	Total	%	Rank
telebahia.net.br	316.532	4,39	02
brasiltelecom.net.br	192.706	2,67	05
telesp.com.br	170.867	2,37	06
netservicos.com.br	60.069	0,83	24
telet.com.br (claro)	50.892	0,71	29
gvt.net.br	49.566	0,69	30
ig.com.br	48.795	0,68	32
ctbctelecom.com.br	18.431	0,26	73
timbrasil.net.br	13.556	0,19	91
canbrasnet.com.br	10.110	0,14	121

Dados gerados em: `Fri Jan 22 11:58:37 2010 UTC/GMT`

Composite Blocking List http://cbl.abuseat.org/

Resultados do Projeto SpamPots

Métricas sobre o Abuso de Redes de Banda Larga para o Envio de *Spam*

Período de coleta	**10/06/2006 a 18/09/2007**
Dias coletados	**466**
Total de *emails*	**524.585.779**
***Emails*/dia**	**1,2 milhões**
Destinatários	**4.805.521.964**
Destinatários/*spam*	**9,16**
IPs únicos	**216.888**
ASNs únicos	**3.006**
Country Codes	**165**

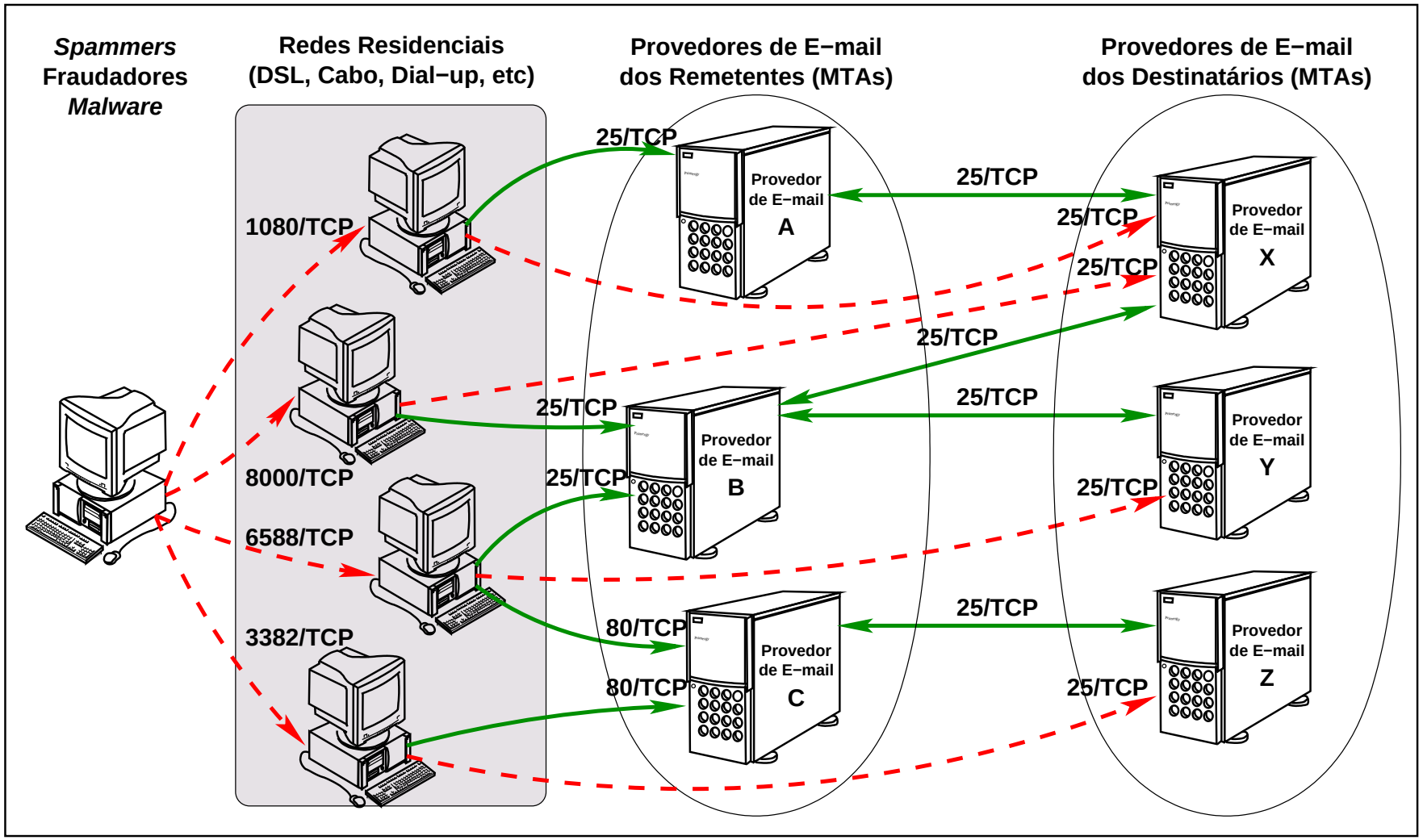
Principais Resultados:

- 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.

- Projeto mantido pelo CGI.br/NIC.br, como parte da CT-Spam
- 10 sensores (*honeypots* de baixa interatividade)
  - 5 operadoras diferentes de cabo e DSL
  - em conexões residenciais e comerciais

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

Abuso - Cenário Atual



Ações para Redução do Problema

Ações para Redução do Problema

Ações por parte das Operadoras de Telecomunicações e Provedores de Acesso à Internet

- Implementar, em ação coordenada, a **Gerência de Porta 25**

Ações por parte dos Usuários de Serviços de *E-mail*

- Alterar suas configurações de *e-mail*, conforme instruções de seu provedor de *e-mail*
- Seguir as recomendações de segurança para evitar a infecção de seus computadores

Gerência de Porta 25

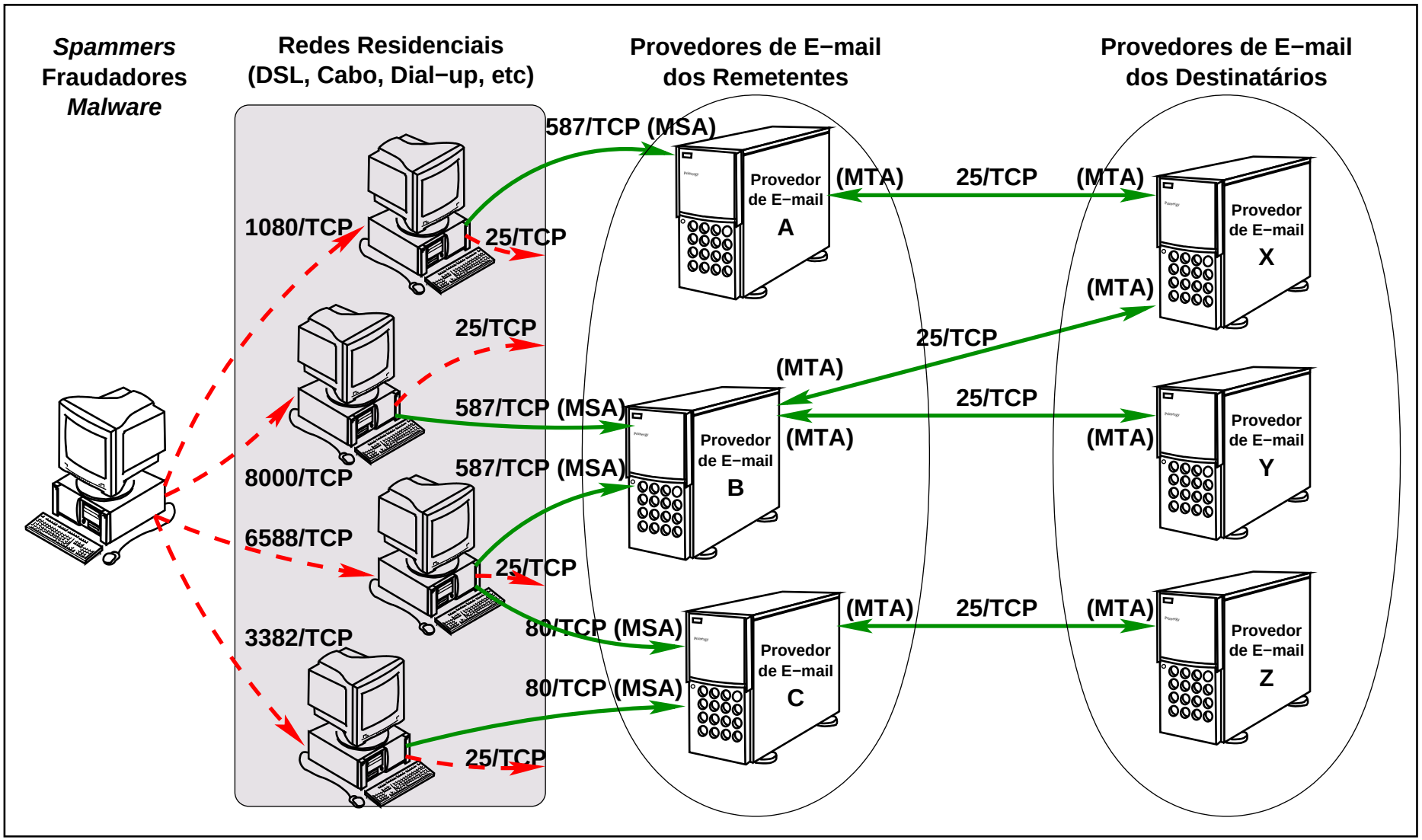
Diferenciar a submissão de *e-mails* do cliente para o servidor, da transmissão de *e-mails* entre servidores.

Implementação depende da aplicação de medidas por provedores e operadoras:

- Provedores de serviços de correio eletrônico:
  - Implementar o padrão de *Message Submission*, tipicamente na porta 587/TCP (RFC 4409), e implementar SMTP autenticado
- Operadoras de banda larga/*dial up* de perfil residencial (usuário final):
  - Impedir envio direto de mensagens eletrônicas (através da filtragem da saída de tráfego com destino à porta 25/TCP)

Detalhes em: http://www.antispam.br/admin/porta25/

Gerência de Porta 25 e seu Impacto



Benefícios da Gerência de Porta 25

- Melhores condições de utilização da rede
  - há melhores condições de utilização da rede com a redução do desperdício de banda para o envio de spam
  - sobram mais recursos computacionais para o usuário legítimo pelo fato do computador ser menos abusado
- Melhor qualidade de serviço de *e-mail*
  - como atua na submissão, antes da mensagem entrar na infra-estrutura de *e-mail* dos provedores, tem o potencial de aliviar a carga e melhorar a qualidade de serviço para o usuário

Referências

- Esta Apresentação:
  http://www.cert.br/docs/palestras/
- Antispam.br: Gerência de Porta 25
  http://www.antispam.br/admin/porta25/
- Resolução CGI.br/RES/2009/002/P: Recomendação para adoção de gerência de Porta 25 em redes de caráter residencial
  http://www.cgi.br/regulamentacao/resolucao2009-02.htm
- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- Núcleo de Informação e Coordenação do Ponto br – NIC.br
  http://www.nic.br/
- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br
  http://www.cert.br/