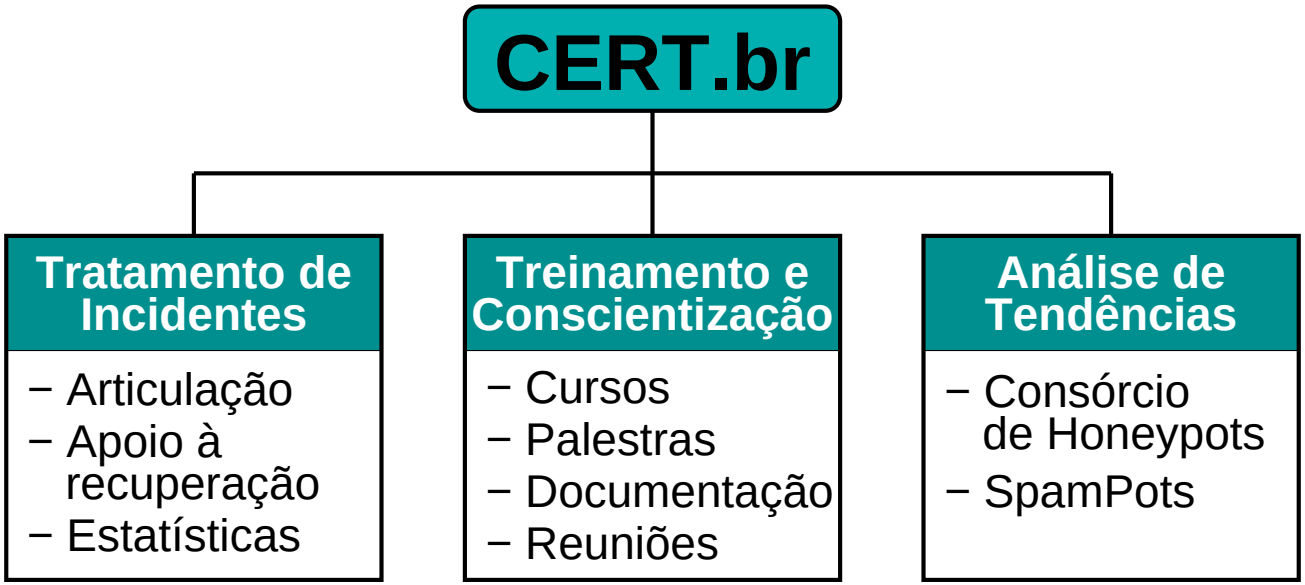
Cenário das Fraudes e do Spam no Brasil

Aritana Pinheiro Falconi
falconi@cert.br

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

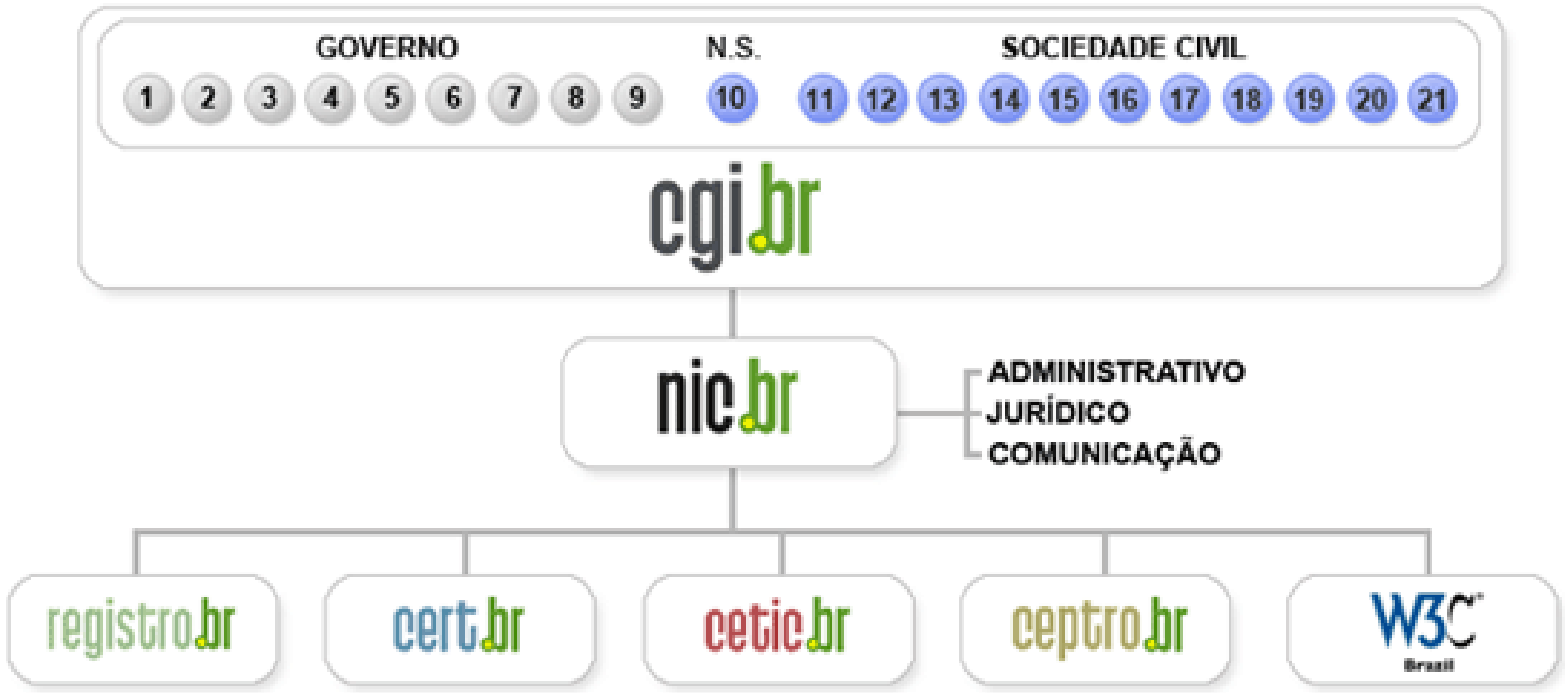
APWG RESEARCH PARTNER www.antiphishing.org

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 de spam enviadas ao CERT.br
  - Abuso de Proxies em PCs Infectados
  - Brasil na CBL
  - Gerência de Porta 25
- Prevenção
- 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

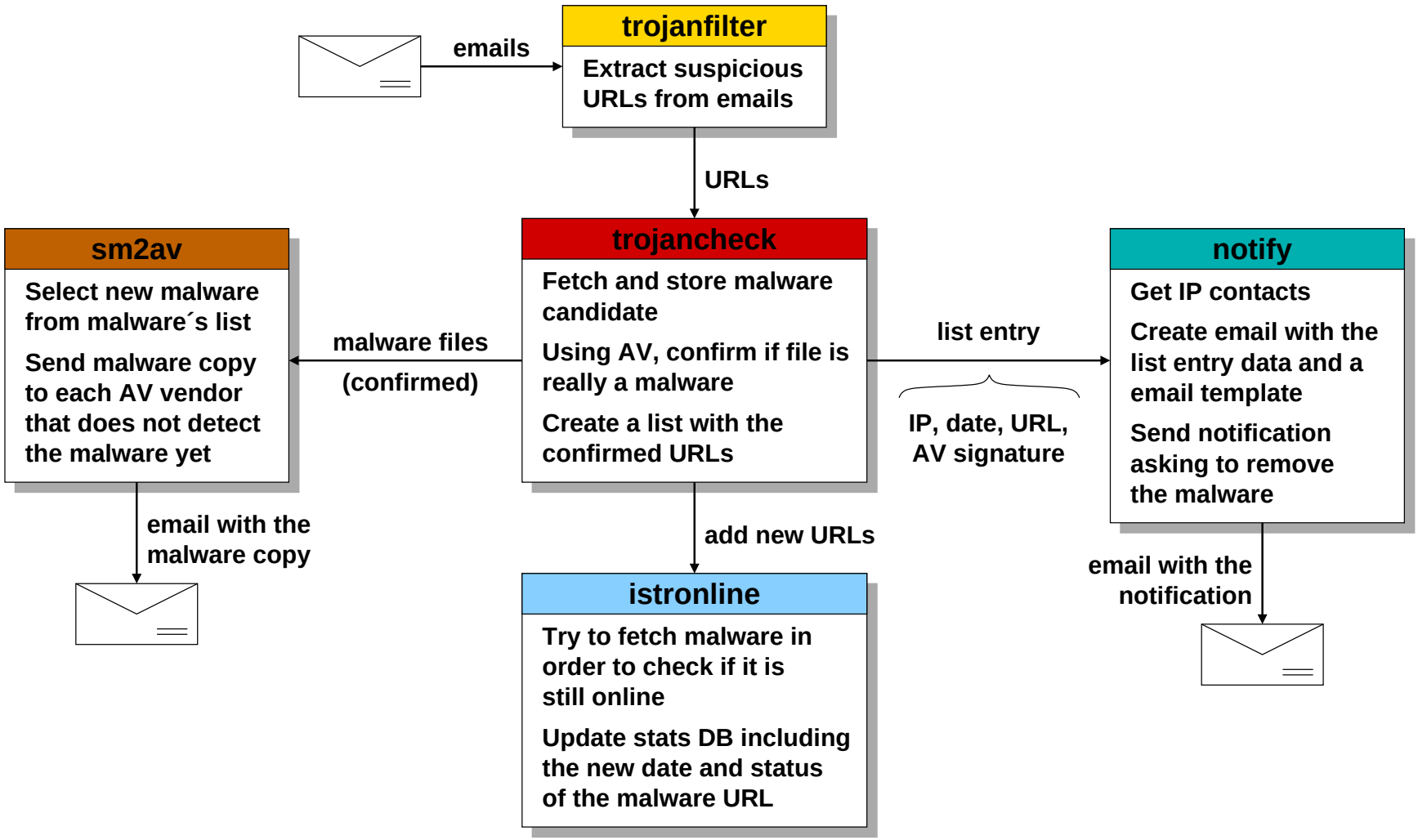
2007 *downloads* involuntários (via JavaScript, ActiveX, etc) - Continuidade das tendências de 2005–2006

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)

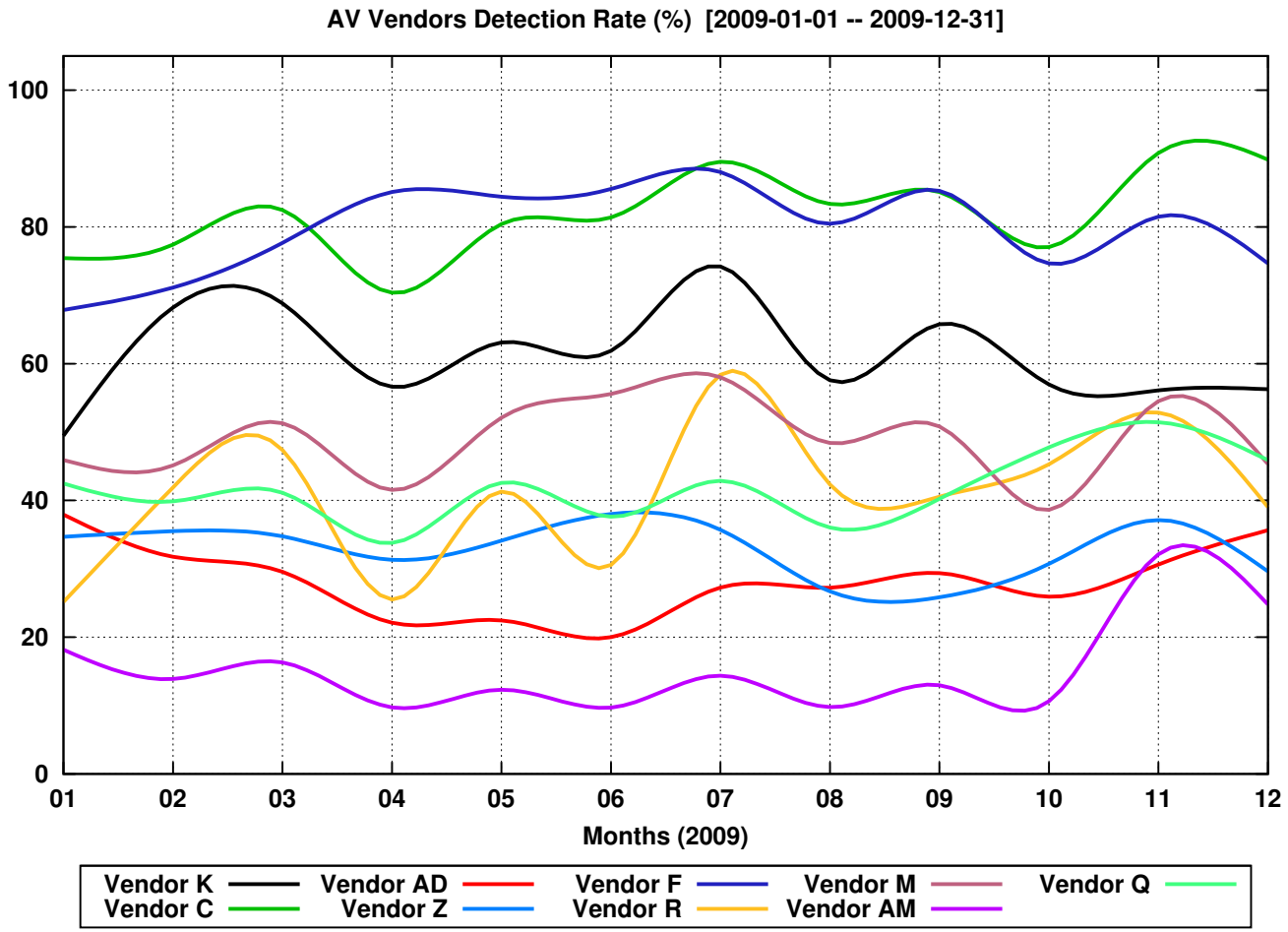
Tentativas de fraude tratadas envolvendo *malware**:

Categoria	2006	2007	2008	2009	2010-Q1
URLs únicas	25.087	19.981	17.376	10.864	2.798
Códigos maliciosos únicos (*hashes* únicos)	19.148	16.946	14.256	8.151	1.870
Assinaturas de Antivírus (únicas)	1.988	3.032	6.085	4.101	1.387
Assinaturas de Antivírus ("família")	140	109	63	93	51
Extensões de arquivos usadas	73	112	112	100	46
Domínios	5.587	7.795	5.916	4.447	1.311
Endereços IP únicos	3.859	4.415	3.921	3.233	996
Países de origem	75	83	78	76	53
Emails de notificação enviados pelo CERT.br	18.839	17.483	15.499	9.935	2.236

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

Estatísticas de *Malware* (2/3)

Taxas de Detecção dos Antivírus em 2009:

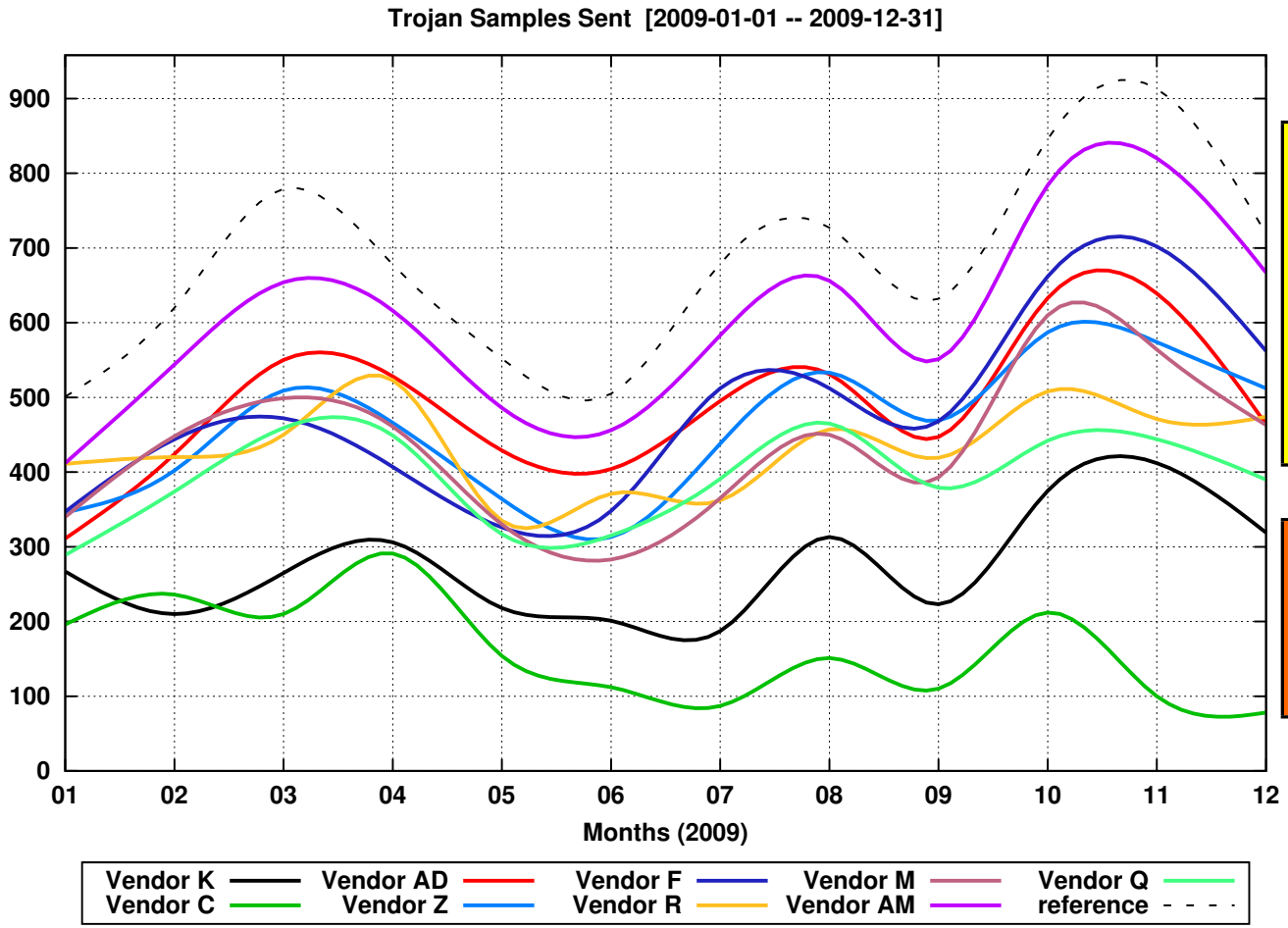


11% dos antivírus detectaram mais de 80% dos exemplares

75% dos antivírus detectaram menos de 50% dos exemplares

Estatísticas de *Malware* (3/3)

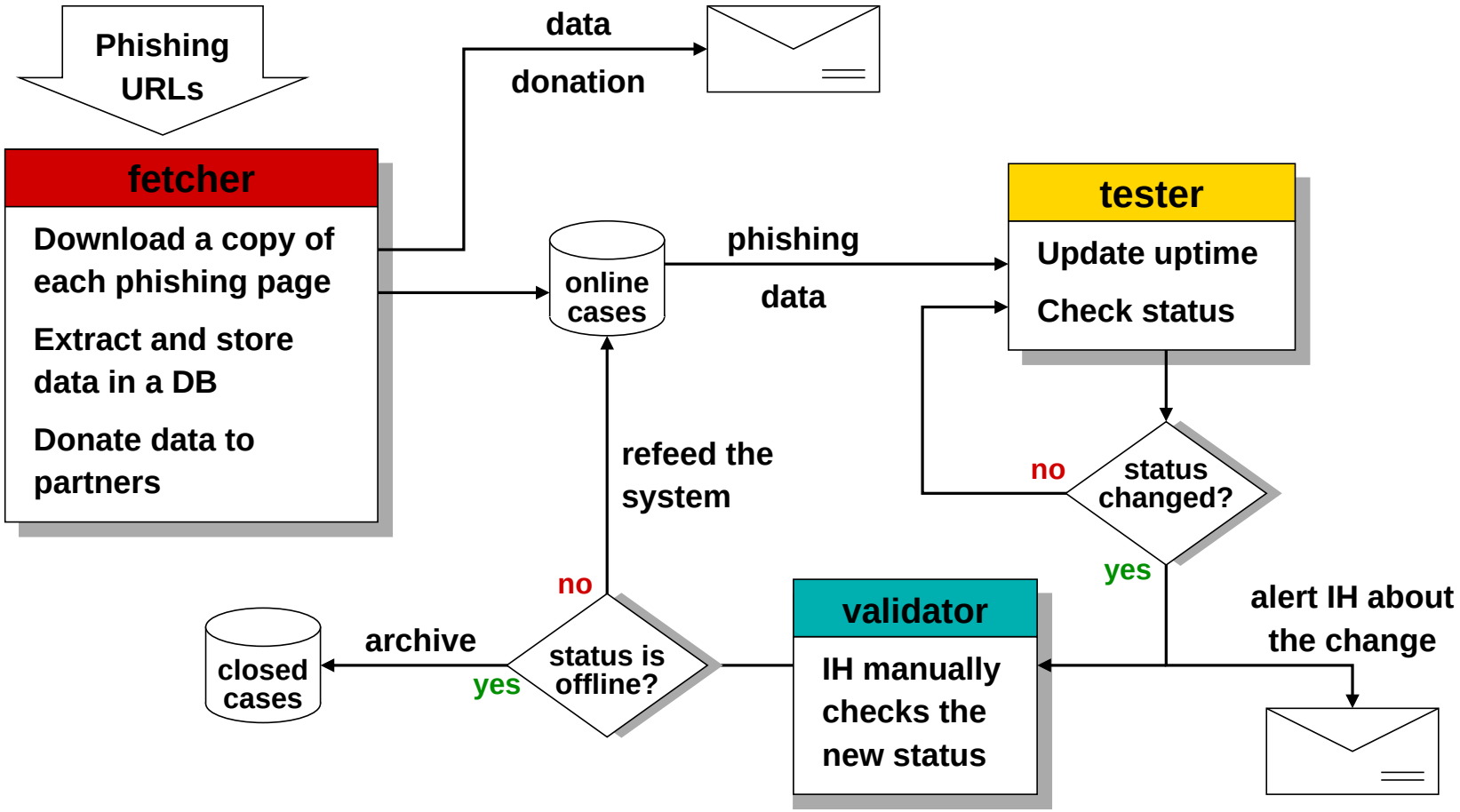
Malwares enviados para 25+ Antivírus em 2009:



Casos de fraude relacionados a *malware* reduziram 23% entre 2008 e 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

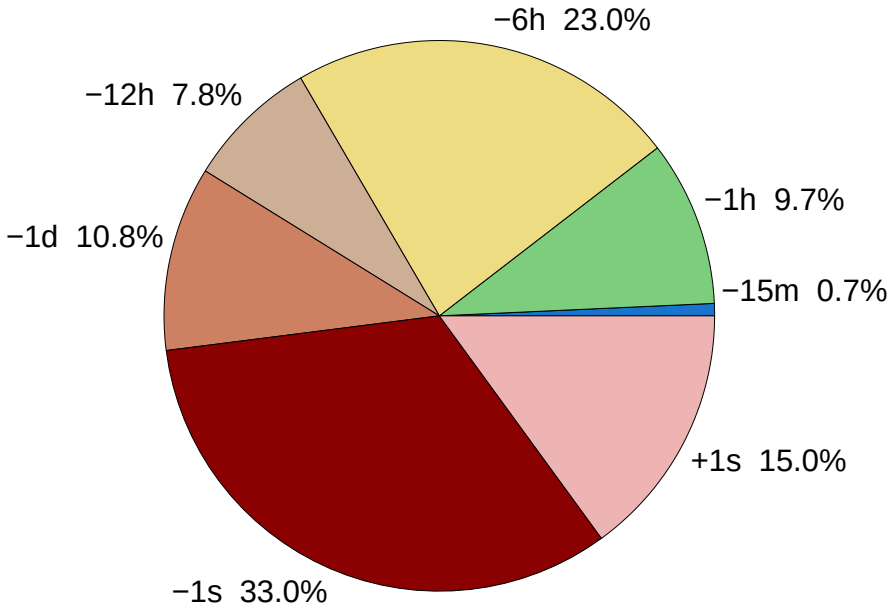
URLs únicas	3215
Hashes únicos	1671
Domínios	1619
Endereços IP	1344
CIDRs	452
Países (CCs)	49

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

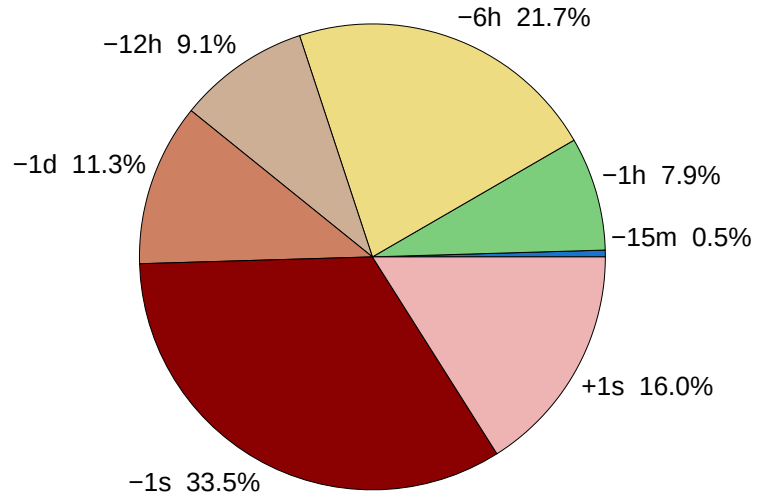
Bancos Brasileiros

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



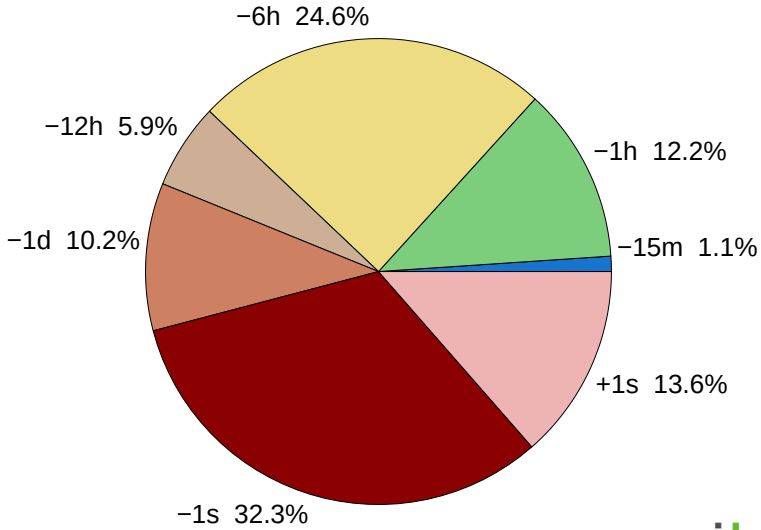
Outras Entidades

tempo de vida

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

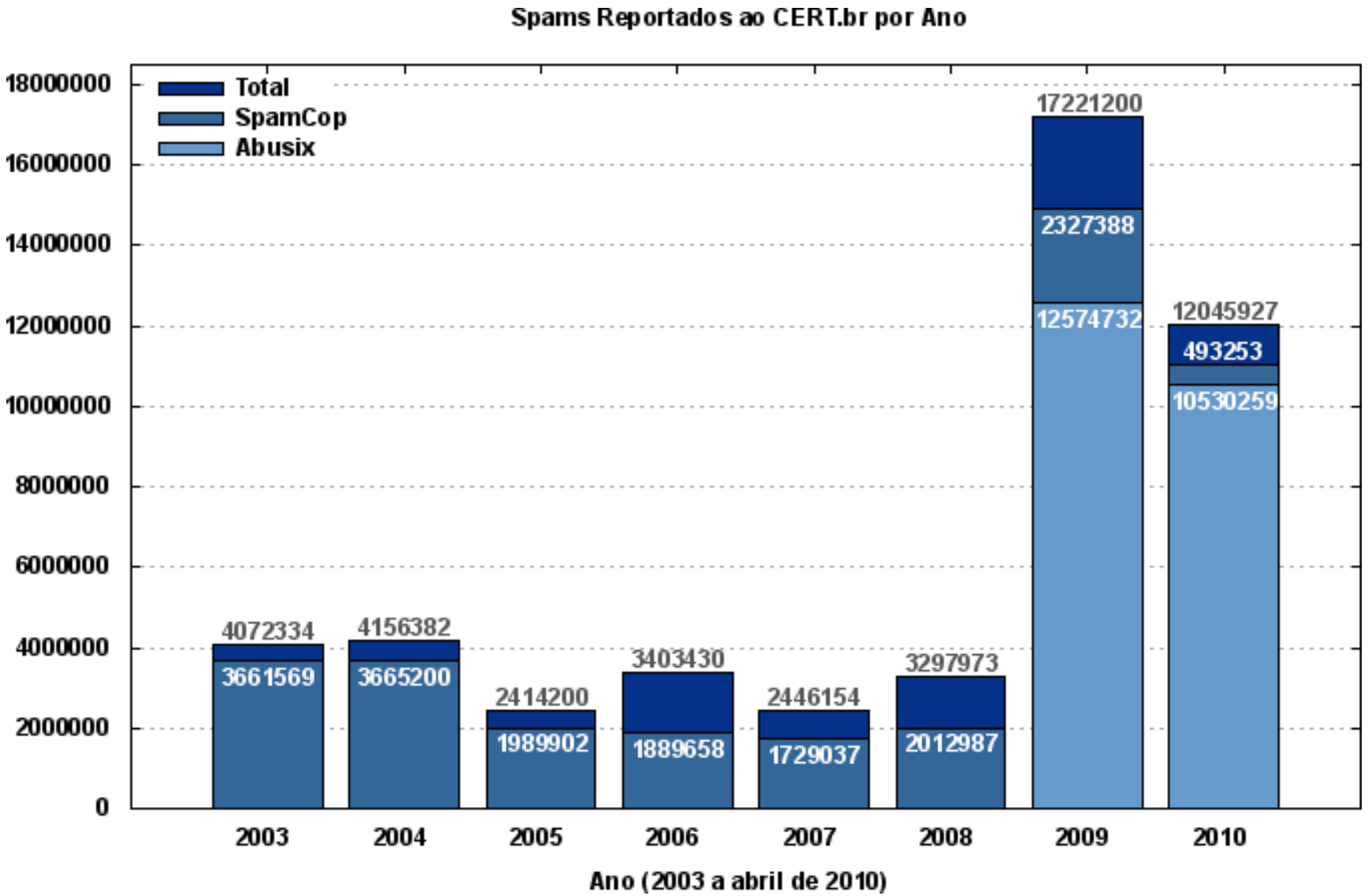
casos por tempo de vida

<=	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

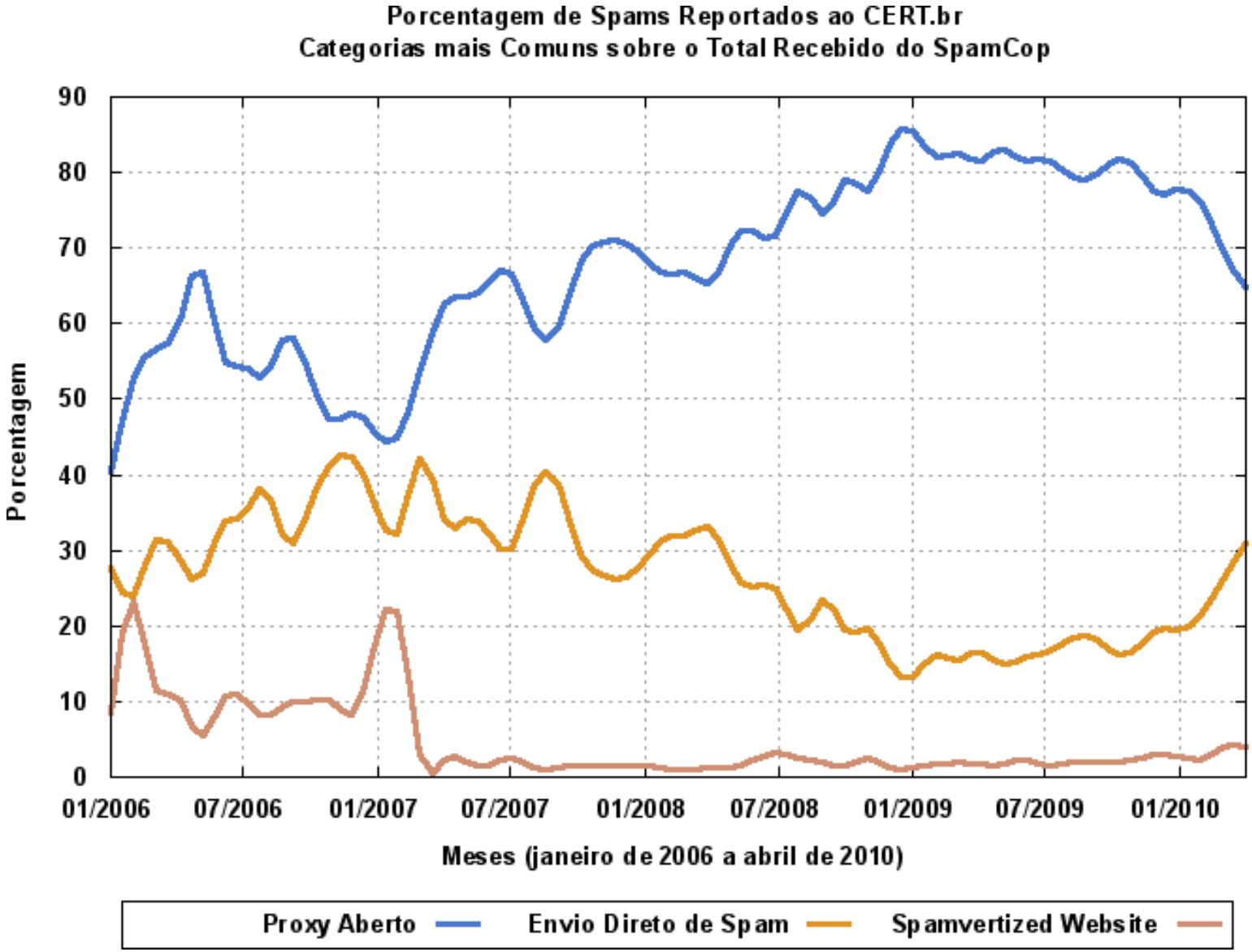


Spam

Reclamações de spam enviadas ao CERT.br



Abuso de *Proxies* em PCs Infectados



Brasil na CBL

Country Codes com maior número de IPs listados

CC	Total	%	Rank
IN	1.333.118	16.12	1
BR	719.101	8.69	2
VN	430.888	5.21	3
RU	396.295	4.79	4
DE	340.522	4.12	5
UA	271.198	3.28	6
US	265.782	3.21	7
IT	239.722	2.90	8
SA	232.668	2.81	9
CO	215.089	2.60	10

Domínios (reverso) com maior número de IPs listados

Domínio	Total	%	Rank
telebahia.net.br (OI)	226.924	2.74	4
brasiltelecom.net.br (OI)	120.981	1.46	9
telesp.com.br	115.771	1.40	10
ig.com.br	51.590	0.62	33
netservicos.com.br	51.385	0.62	34
telet.com.br (Claro)	45.154	0.55	37
gvt.net.br	41.323	0.50	43
ctbctelecom.net.br	12.800	0.15	114
timbrasil.com.br	11.654	0.14	124
canbrasnet.com.br	10.366	0.13	144

Dados gerados em: `Mon May 17 11:02:47 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**

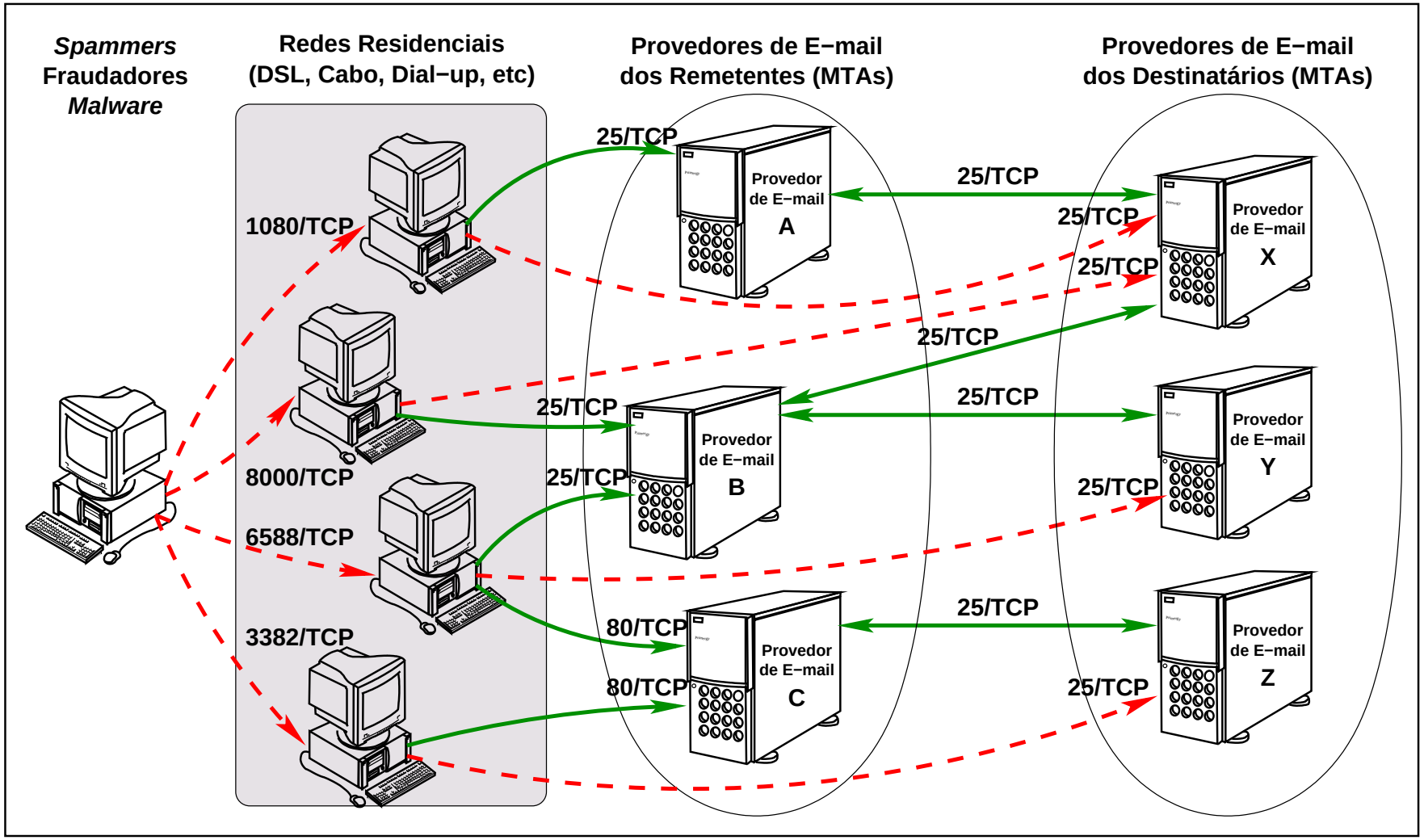
Principais Resultados:

- 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

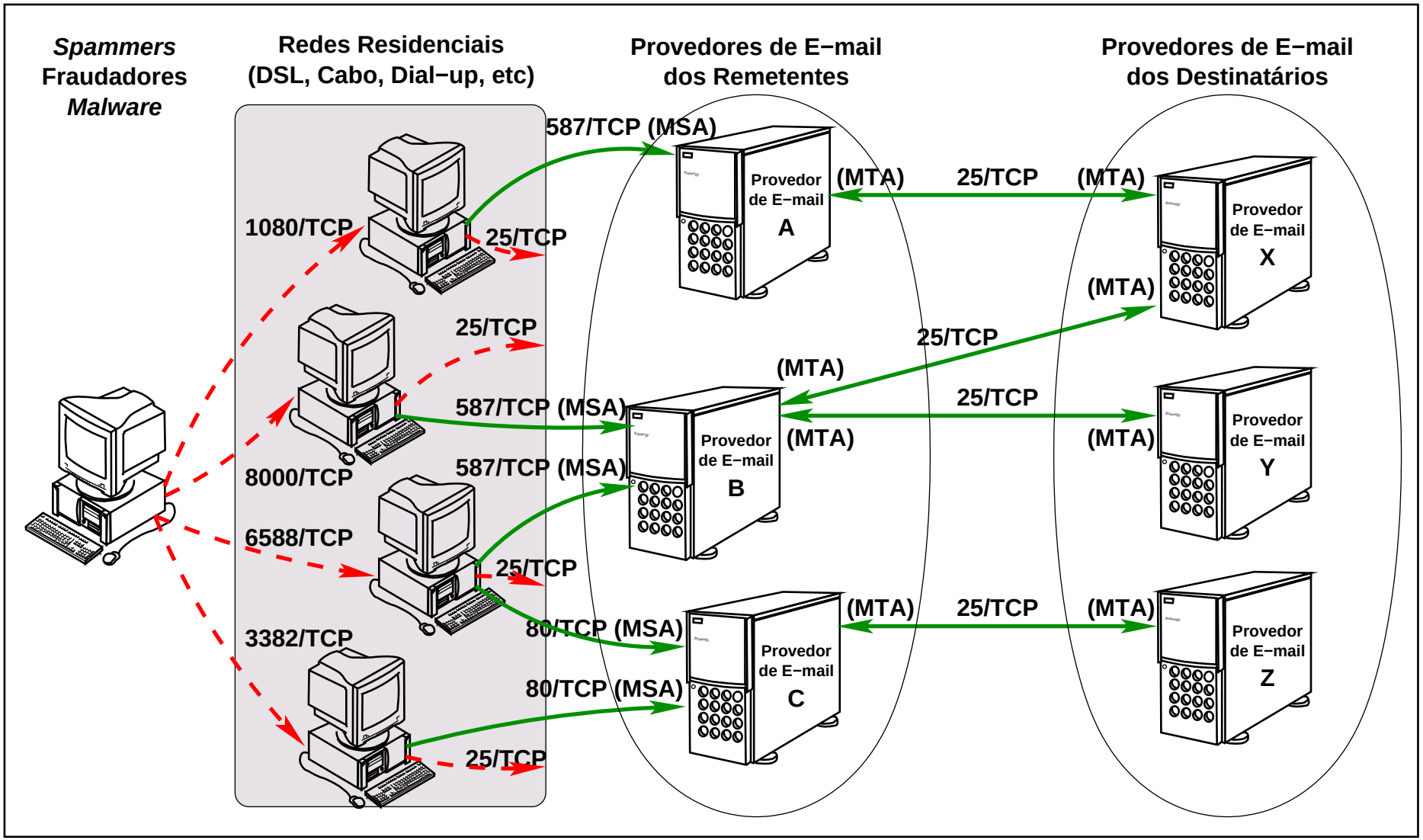
Diferenciar a submissão de *e-mails* do cliente para o servidor, da transmissão de *e-mails* entre servidores.

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

Prevenção

O Que Fazer para se Prevenir

Instalar a última versão e aplicar as correções de segurança (*patches*)

- sistema operacional (checar horário da atualização automática)
- aplicativos (navegador, proc. de textos, leitor de *e-mails*, visualizador de imagens, PDFs e vídeos, etc)
- *Hardware* (*firmware* de *switches*, bases *wireless*, etc)

Utilizar Programas de Segurança

- *firewall* pessoal
- antivírus (atualizar as assinaturas diariamente)
- anti-*spyware*
- anti-*spam*
- extensões e *plugins* em navegadores (gerência de JavaScript, *cookies*, etc)

Melhorar a Postura On-line (1/2)

Não acessar *sites* ou seguir *links*

- recebidos por *e-mail* ou por serviços de mensagem instantânea
- em páginas sobre as quais não se saiba a procedência

Receber um *link* ou arquivo de pessoa ou instituição conhecida não é garantia de confiabilidade

- códigos maliciosos se propagam a partir das contas de máquinas infectadas
- fraudadores se fazem passar por instituições confiáveis

Não fornecer em páginas *Web*, *blogs* e *sites* de redes de relacionamentos:

- seus dados pessoais ou de familiares e amigos (*e-mail*, telefone, endereço, data de aniversário, etc)
- dados sobre o computador ou sobre *softwares* que utiliza
- informações sobre o seu cotidiano
- informações sensíveis (senhas e números de cartão de crédito)

Melhorar a Postura On-line (2/2)

Precauções com contas e senhas

- utilizar uma senha diferente para cada serviço/*site*
- evitar senhas fáceis de adivinhar
  - nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras que façam parte de dicionários
- usar uma senha composta de letras, números e símbolos
- utilizar o usuário Administrador ou `root` somente quando for estritamente necessário
- criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador

Informar-se e Manter-se Atualizado (1/2)

Núcleo de Informação e Coordenação do Ponto br

Início Dicas Download Checklist Glossário Livro

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

cgi.br NIC.br Registro

Cartilha de Segurança para Internet 3.1

Livro Completo

A partir da versão 3.1 a Cartilha de Segurança para Internet passou a ser editada também como livro. Nesta página você encontra o prefácio do Livro e o arquivo para download.

Prefácio

A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças.

Produzido pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, com o apoio do Comitê Gestor da Internet no Brasil – CGI.br, o documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.

Livro Completo para download (886 KB)

Cartilha de Segurança para Internet, versão 3.1 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2006.

ISBN: 978-85-60062-06-5
ISBN: 85-60062-06-8

http://cartilha.cert.br/

Informar-se e Manter-se Atualizado (2/2)

http://www.antispam.br/videos/

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/