Spam: Cenário atual e ações para redução do problema

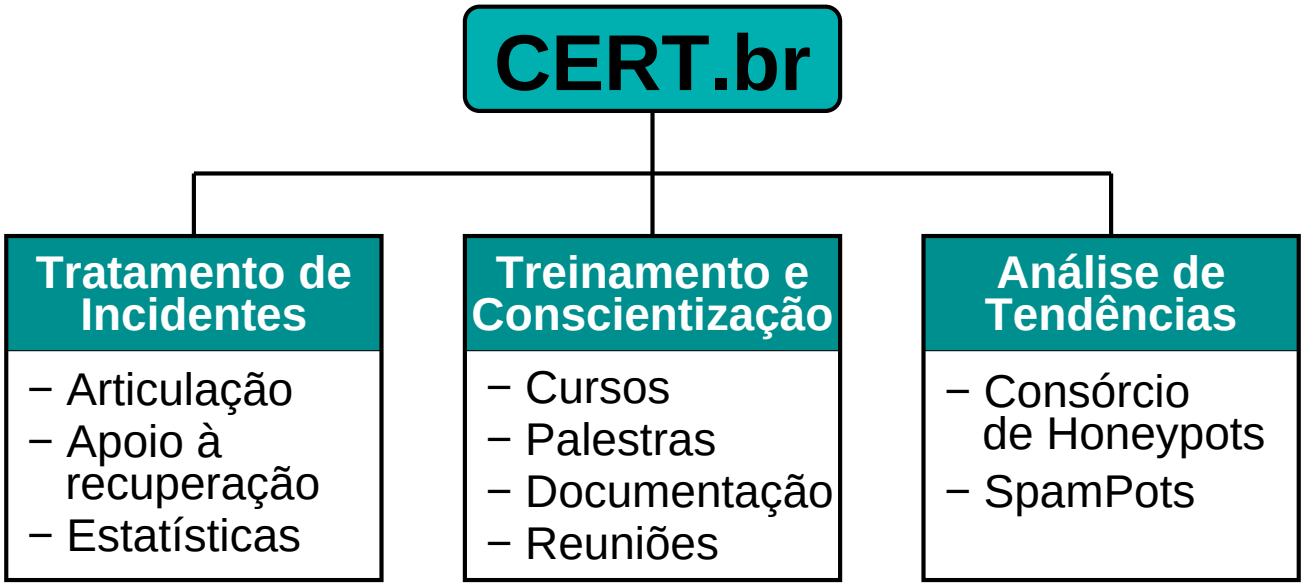
Aritana Pinheiro Falconi
falconi@cert.br
Klaus Steding-Jessen
jessen@cert.br
Marcelo H. P. C. Chaves
mhp@cert.br

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

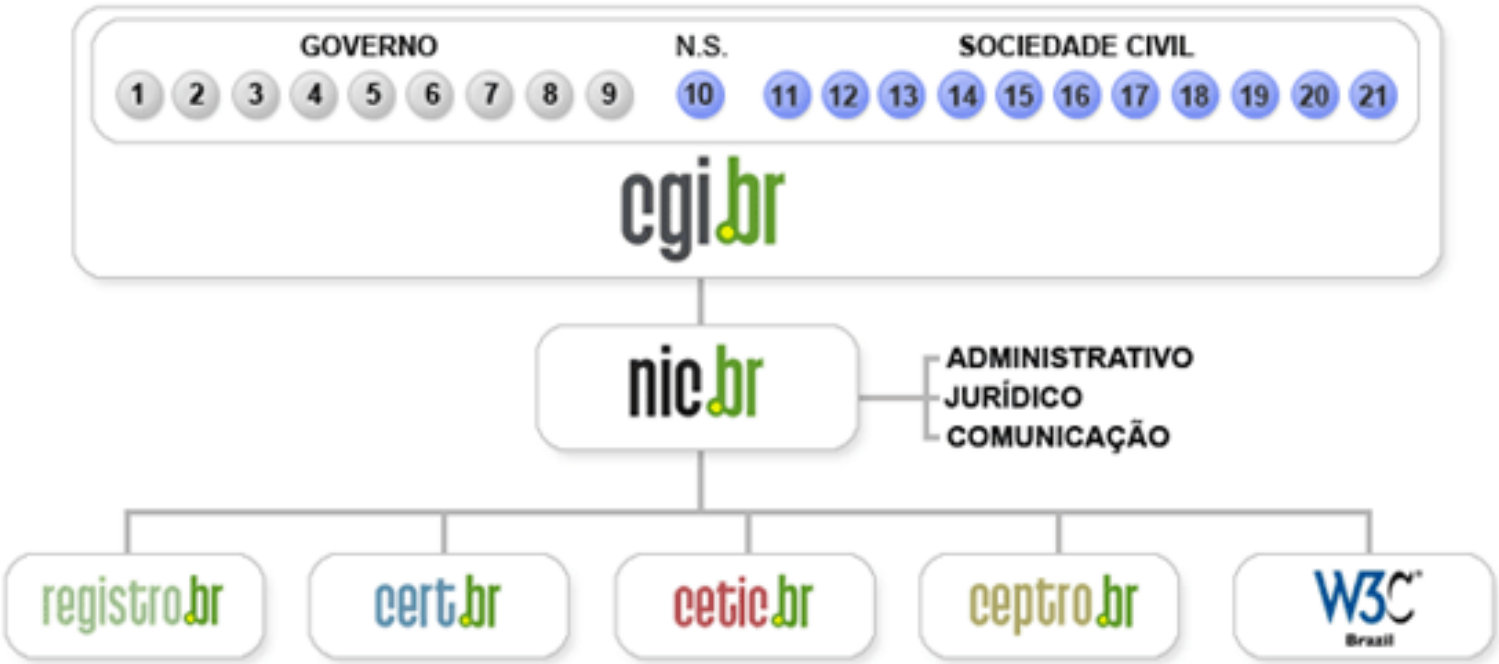
APWG

SEIPartner 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 da Defesa
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério do Planejamento, Orçamento e Gestão
07- Agência Nacional de Telecomunicações (Anatel)
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- 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

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

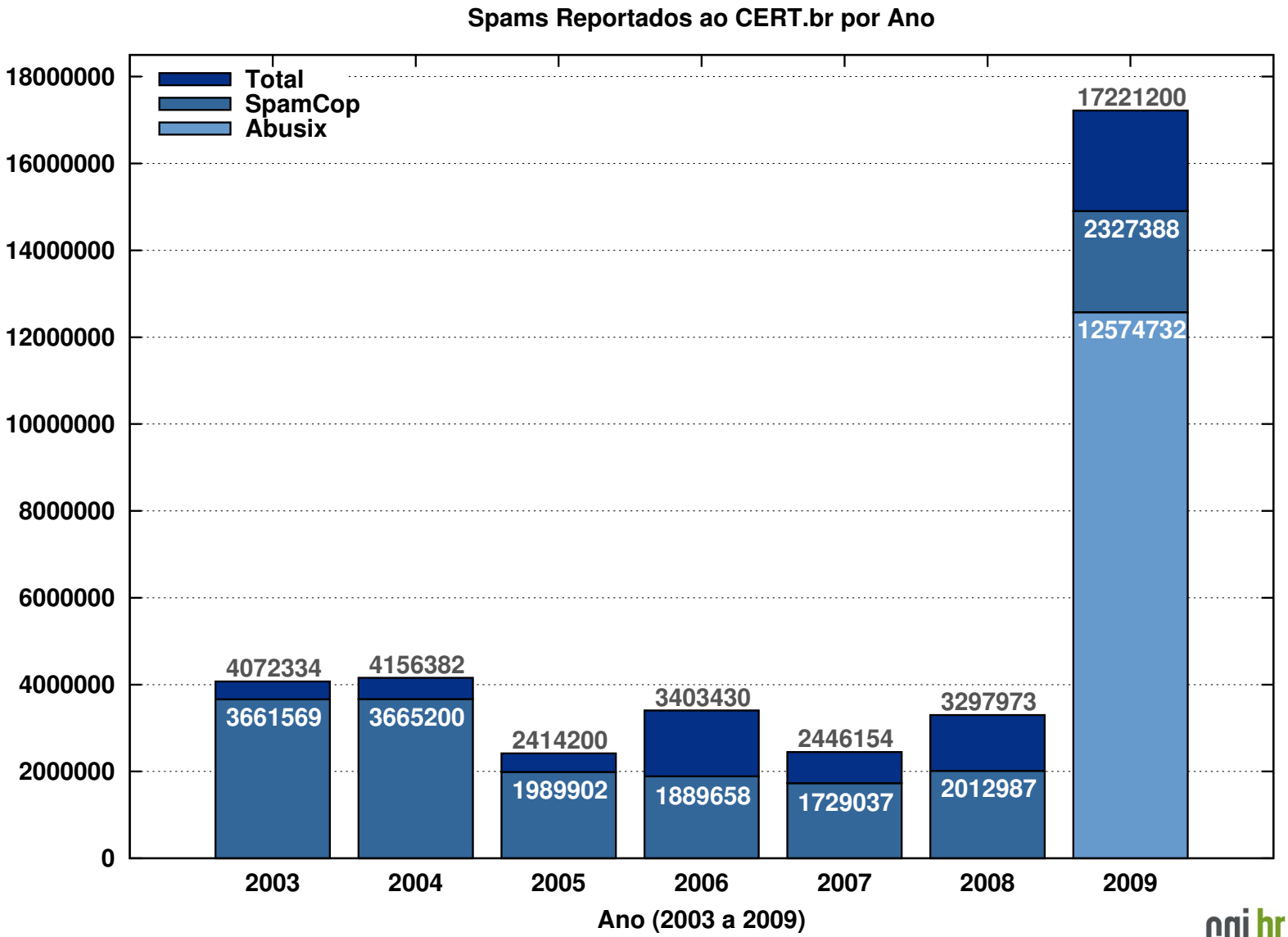
Cenário do Spam no Brasil
- Reclamações ao CERT.br em 2009
- Abuso de Proxies em PCs Infectados
- Brasil na CBL

Ações para Redução do Problema

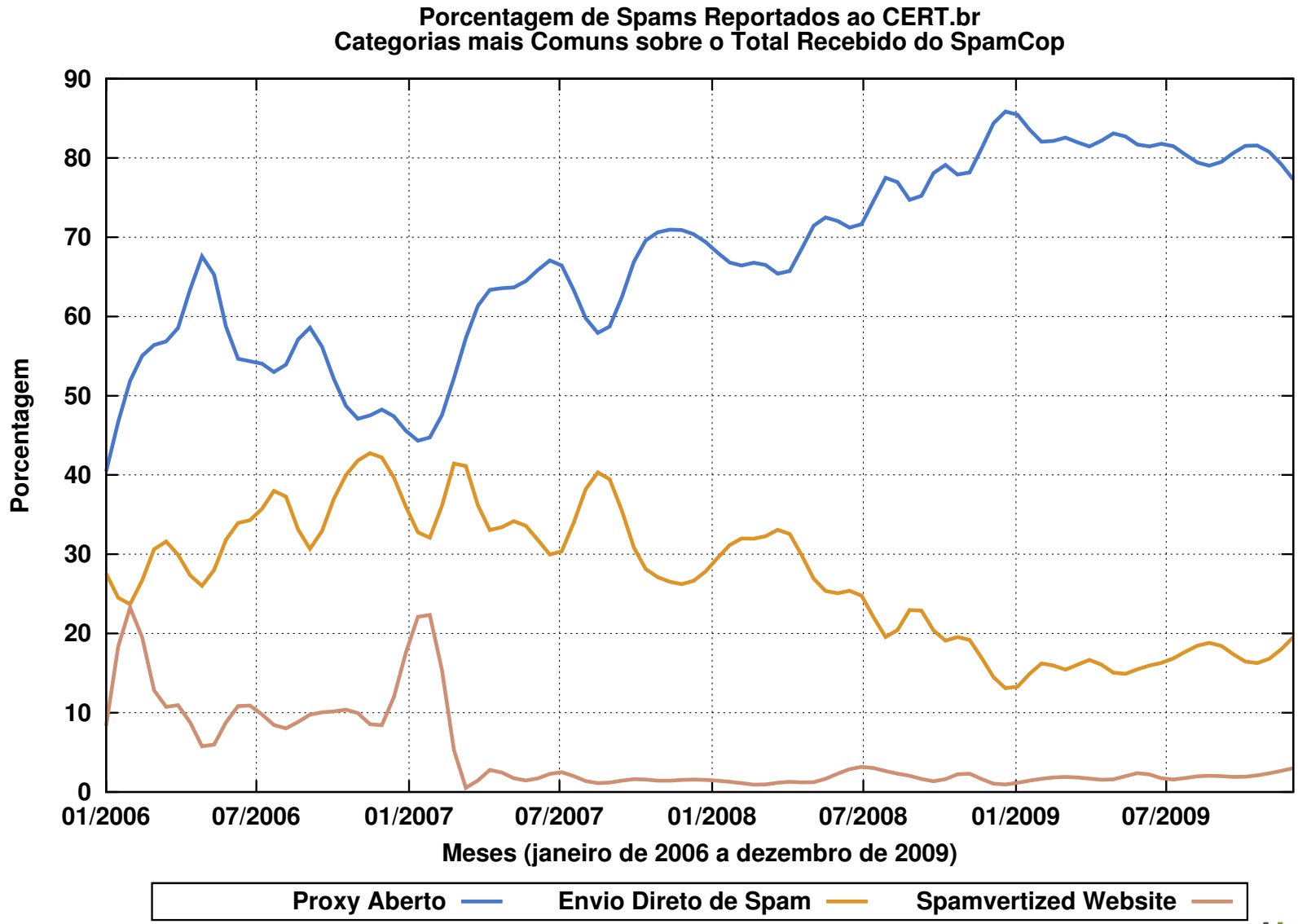
Referências

Cenário do *Spam* no Brasil

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**

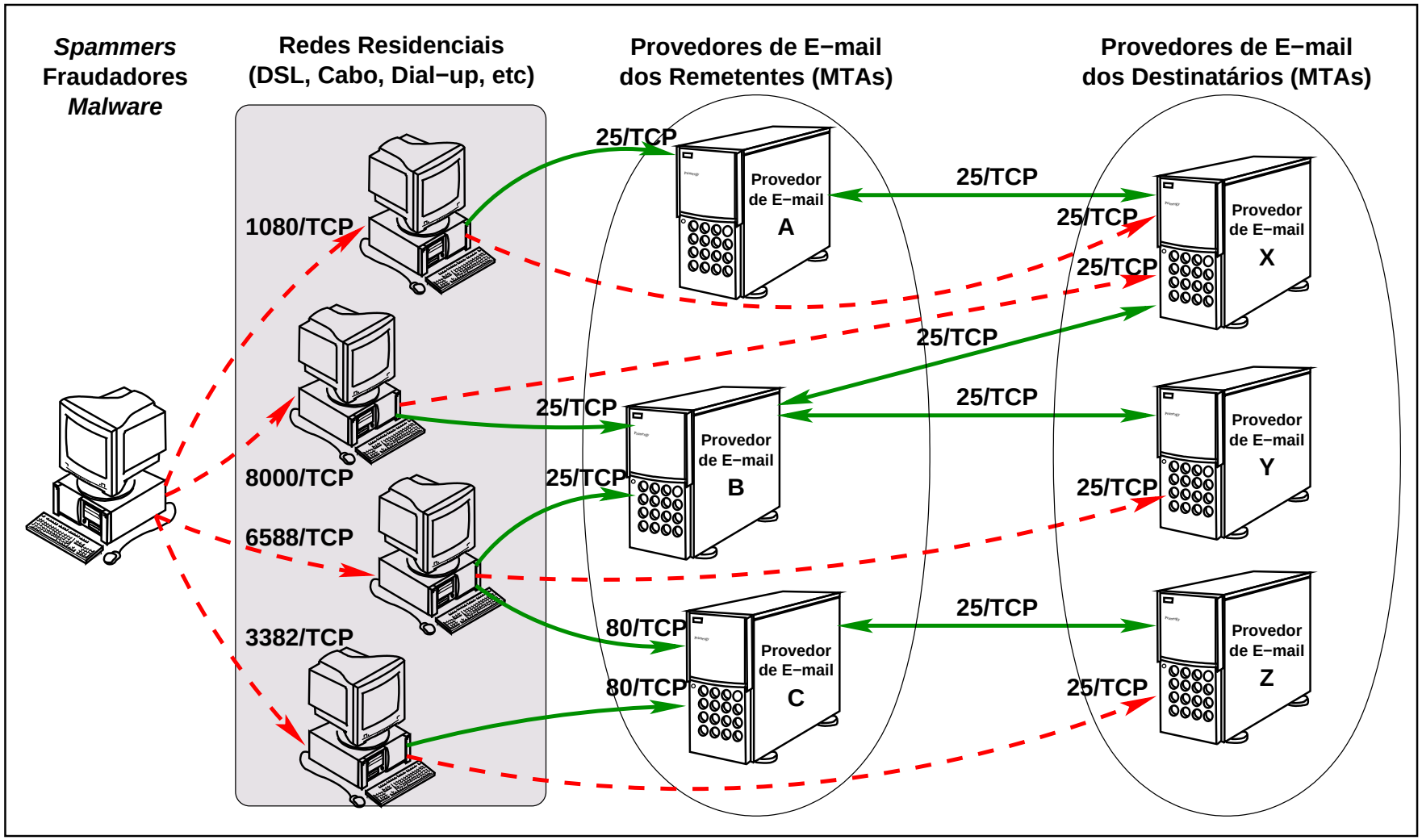
Principais Resultados:

- 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

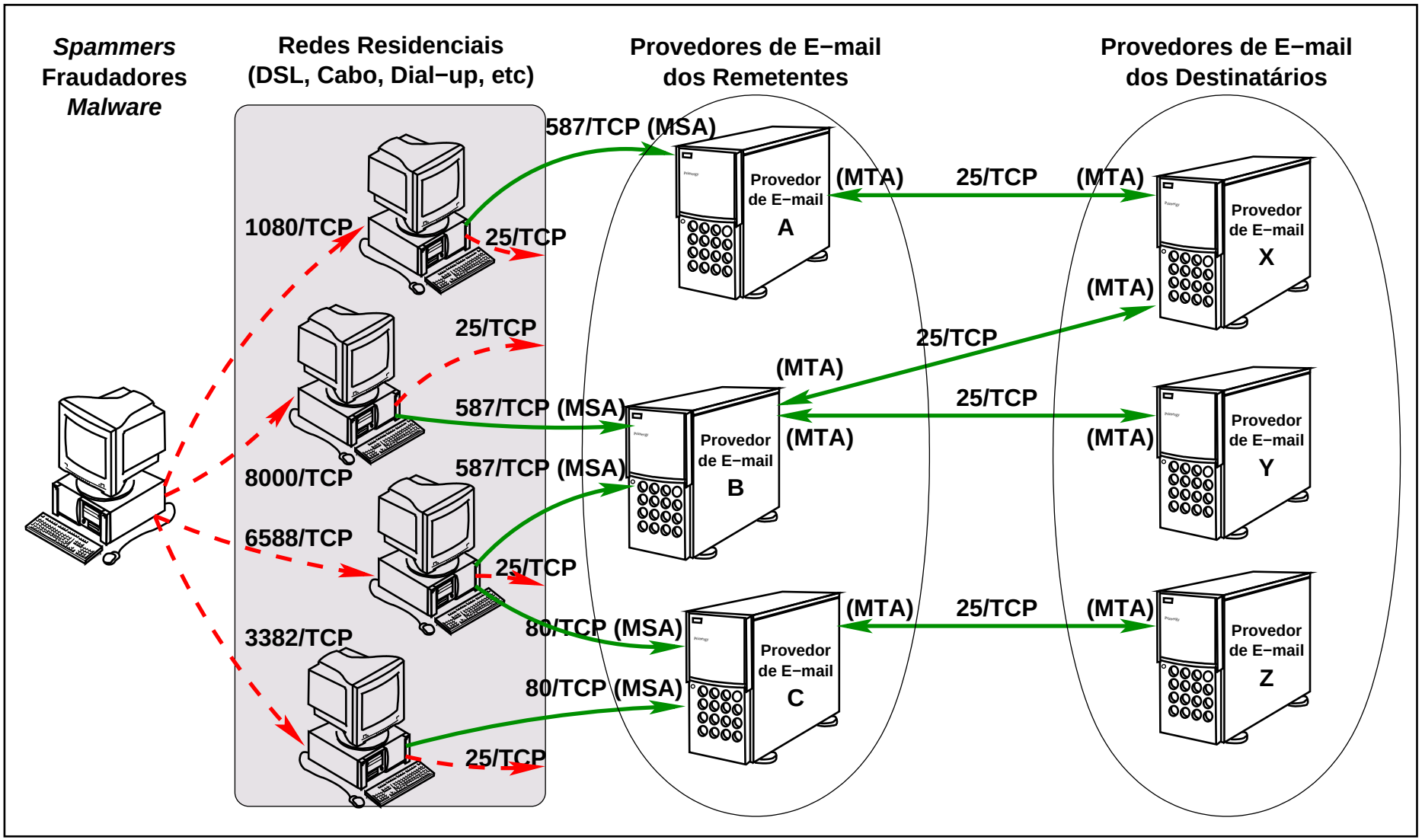
Diferenciar a submissão de *e-mails* do cliente para o servidor, da transmissão de *e-mails* entre servidores.

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
- Documentos e Palestras do CERT.br no Escopo do seu Trabalho na CT-Spam
  http://www.cert.br/docs/ct-spam/ct-spam-gerencia-porta-25.pdf
- Resultados Preliminares do Projeto SpamPots
  http://www.cert.br/docs/whitepapers/spampots/