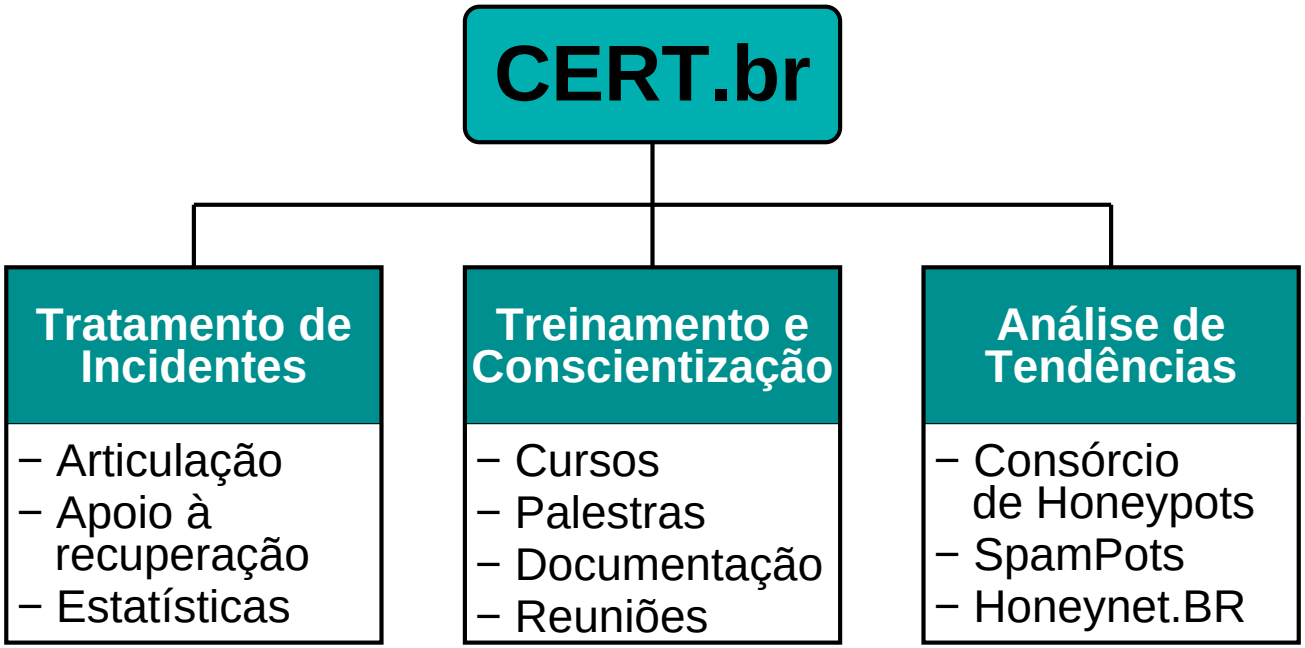
Gerência de Porta 25/TCP em Conexões Residenciais: Controle de *Direct Delivery* e Adoção de *Message Submission*

Cristine Hoepers
cristine@cert.br
Klaus Steding-Jessen
jessen@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

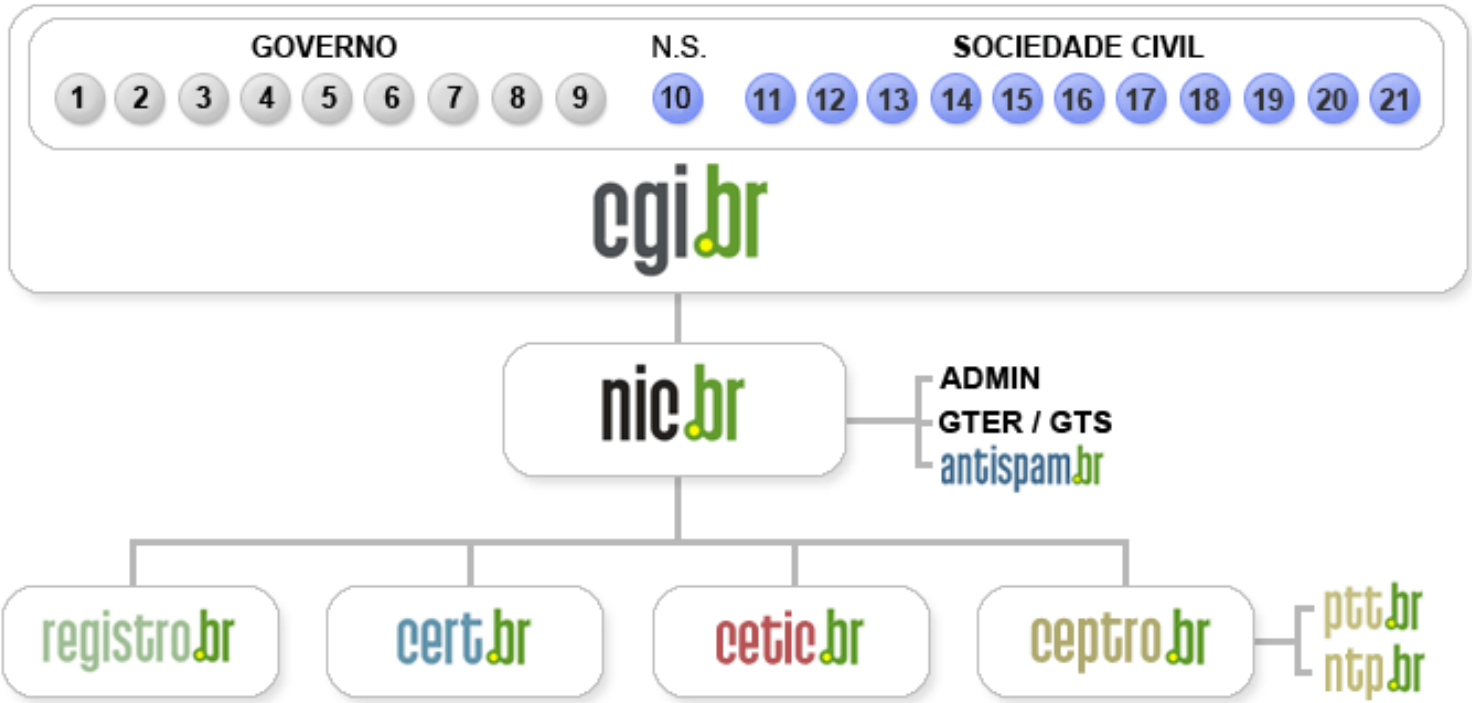
APWG

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

- Introdução
  - Motivação
- Porque Nossa Infra-Estrutura é Abusada
- Proposta de Novo Cenário
- Benefícios
- Impacto
- Dúvidas Comuns
- Referências

Evolução dos Padrões

SMTP definido como um protocolo de **transferência** de mensagens (mas também usado como protocolo de **submissão**)

- 1982 "RFC 821: Simple Mail Transfer Protocol" (Standards Track, obsoleto)
- 2001 "RFC 2821: Simple Mail Transfer Protocol" (Standards Track)

Diferenciação entre transporte/entrega e submissão

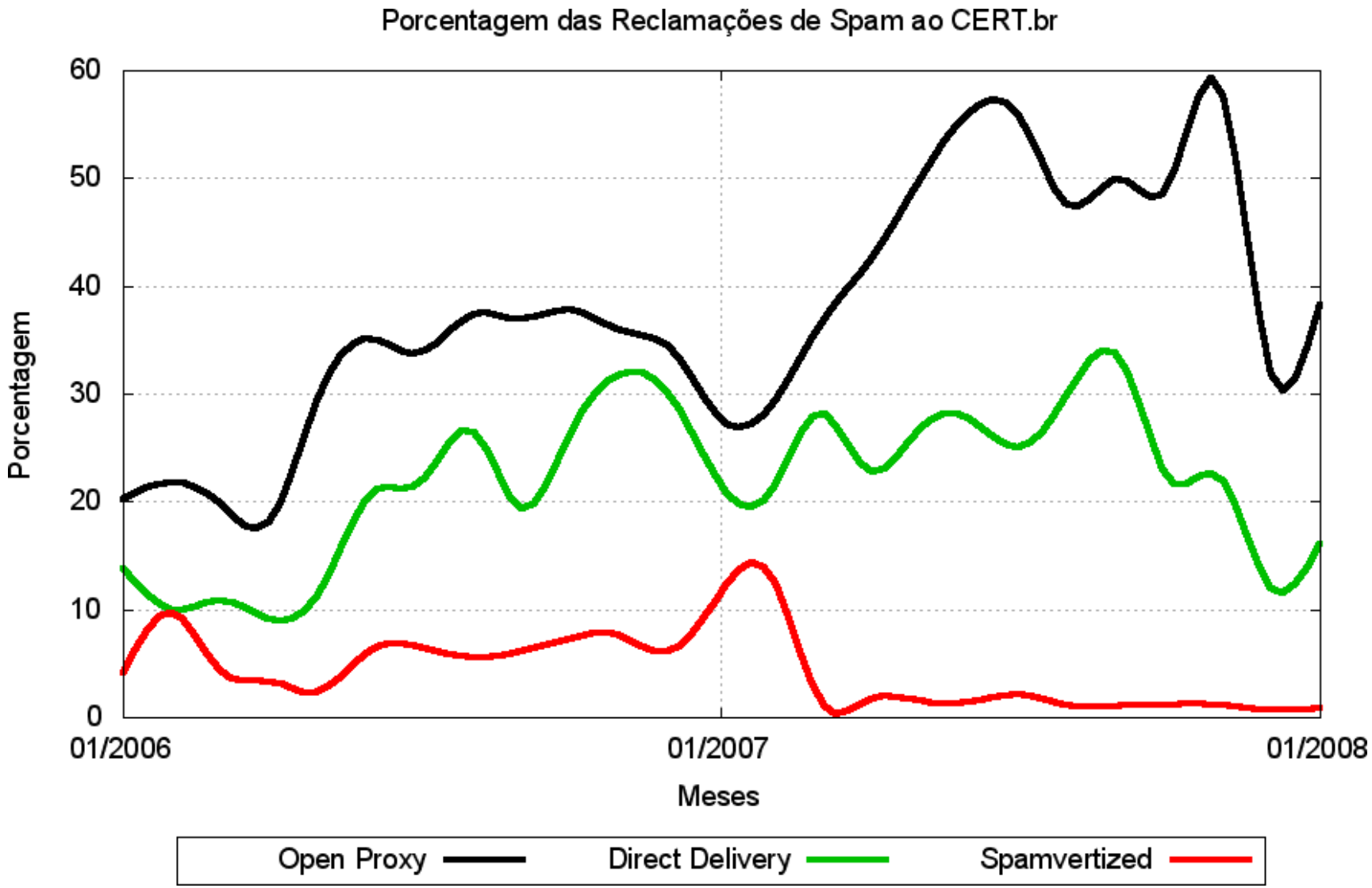
- 1998 "RFC 2476: Message Submission" (Standards Track, obsoleto)
- 2006 "RFC 4409: Message Submission for Mail" (Standards Track)
- 2007 "RFC 5068: Email Submission Operations: Access and Accountability Requirements" (BCP: 134)

Fóruns Discutindo Gerência de Porta 25

- *Messaging Anti-Abuse Working Group* – MAAWG
  http://www.maawg.org/port25/
- London Action Plan – LAP
- EU's Contact Network of Spam Authorities – CNSA
- Comissão de Trabalho Anti-Spam – CT-Spam
  - 21/06/2005: seminário com teles e provedores para discutir o documento "Tecnologias e políticas para Combate ao *Spam*"
  - 15/12/2005: Participação na 5ª reunião ordinária do CBC-1 da Anatel, para discussão deste documento

Motivação

Reclamações de *Spam* ao CERT.br



Brasil na CBL (1/2)

O Brasil é o segundo país com maior número de IPs listados na CBL

- 485.679 IPs listados (8.87%)
- China é o primeiro com 560.055 IPs (10.23%)

"*The CBL takes its source data from very large spamtraps/mail infrastructures, and only lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, wingate etc) which have been abused to send spam, worms/viruses that do their own direct mail transmission (. . .)*"

http://cbl.abuseat.org/ – dados de 18/02/2008

Brasil na CBL (2/2)

Posição no Ranking	Domínio	Número de IPs Listados	Porcentagem do Total
4	telesp.com.br	158.734	2.91
6	brasiltelecom.net.br	137.275	2.51
10	telebahia.net.br	107.594	1.97
66	ctbctelecom.net.br	13.702	0.25
74	netservicos.com.br	11.902	0.22
83	ig.com.br	10.732	0.20
84	gvt.net.br	10.670	0.20
134	embratel.net.br	5.879	0.11
150	canbrasnet.com.br	5.099	0.09
189	uol.com.br	3.420	0.06

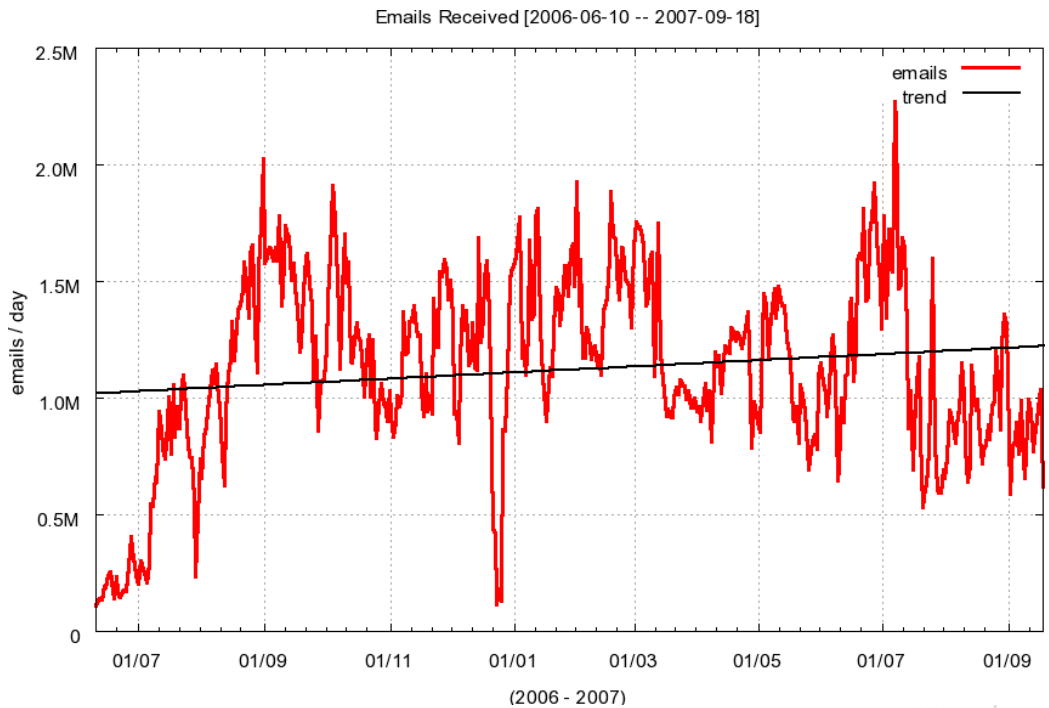
Total de IPs na CBL: 5.458.565 – dados de 18/02/2008

Resultados do Projeto SpamPots

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

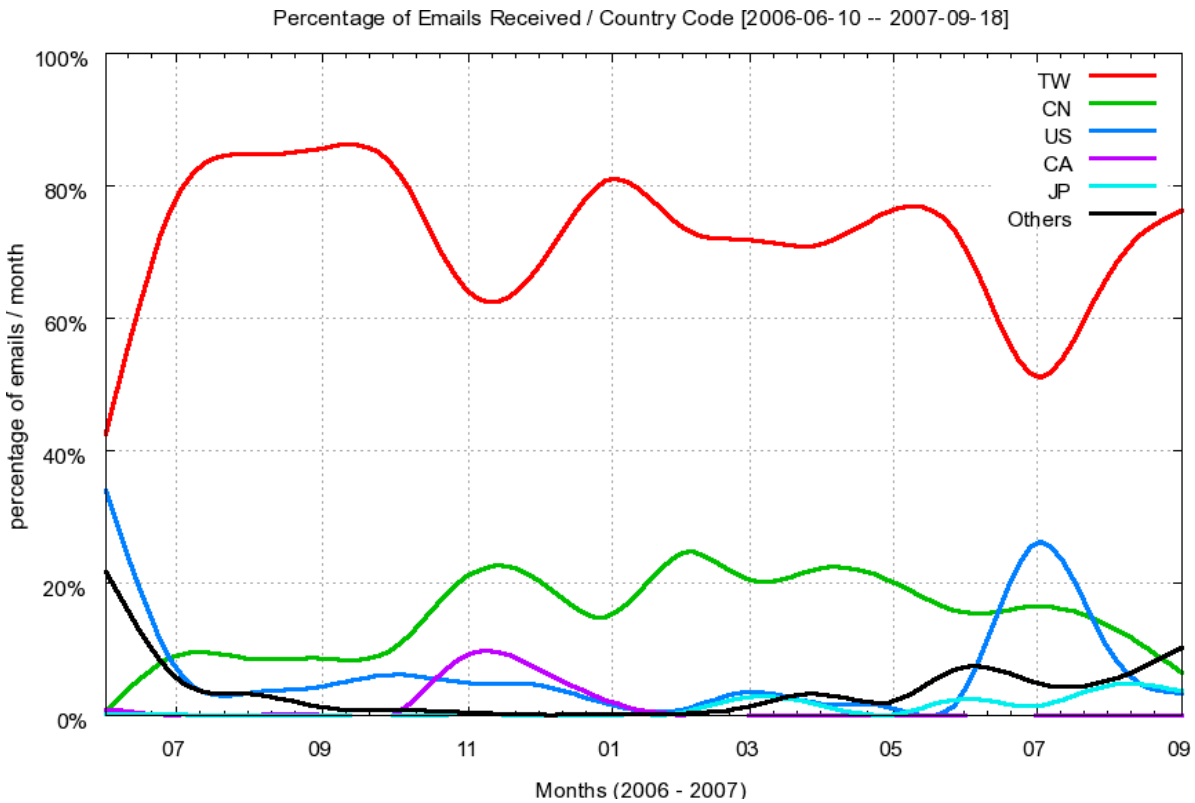
- Mantido pelo CGI.br/NIC.br, como parte da CT-Spam
- 10 *honeypots* de baixa interatividade
  - 5 operadoras diferentes de cabo e DSL
  - em conexões residenciais e comerciais

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**



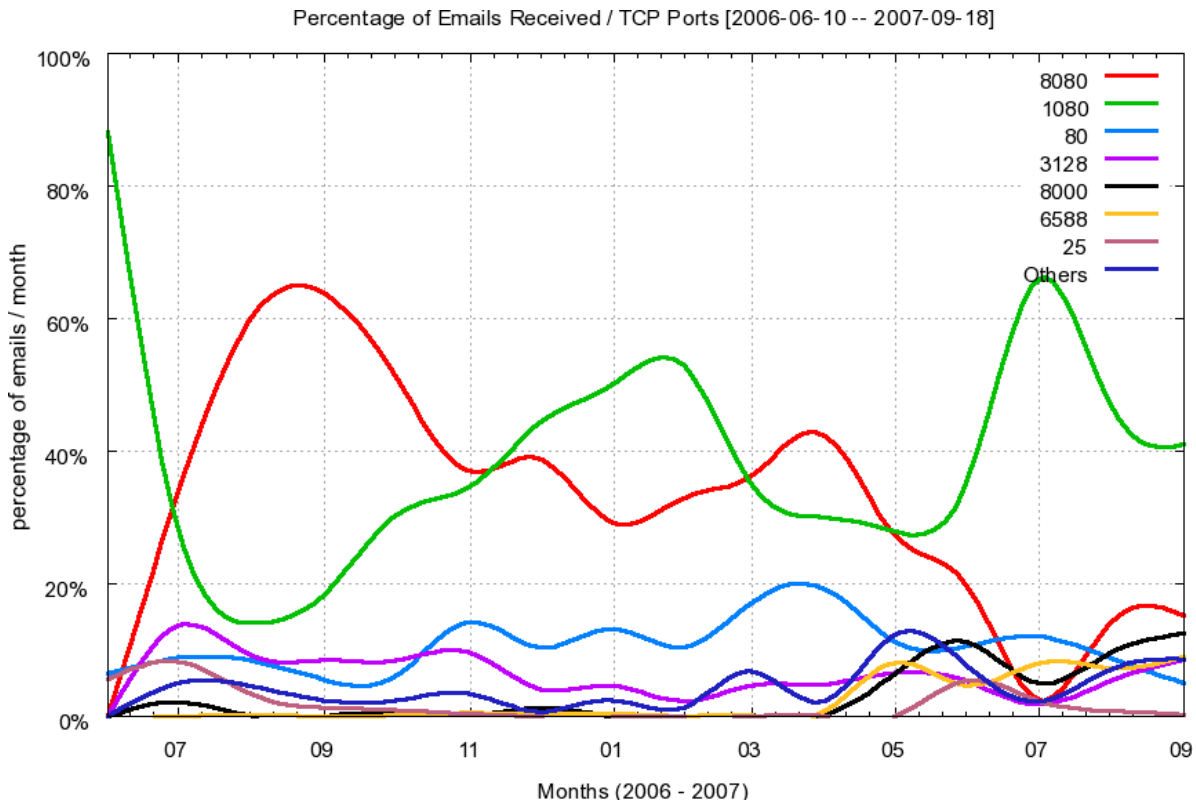
Country Codes (CCs)

#	CC	Emails	%
01	TW	385.189.756	73,43
02	CN	82.884.642	15,80
03	US	29.764.293	5,67
04	CA	6.684.667	1,27
05	JP	5.381.192	1,03
06	HK	4.383.999	0,84
07	KR	4.093.365	0,78
08	UA	1.806.210	0,34
09	DE	934.417	0,18
10	BR	863.657	0,16



Portas Abusadas

Porta	Protocolo	Serviço	%
1080	SOCKS	socks	37,31
8080	HTTP	http	34,79
80	HTTP	http	10,92
3128	HTTP	Squid	6,17
8000	HTTP	http	2,76
6588	HTTP	AnalogX	2,29
25	SMTP	smtp	1,46
4480	HTTP	Proxy+	1.38
3127	SOCKS	MyDoom	1,00
3382	HTTP	Sobig.f	0,96
81	HTTP	http	0,96



Tentativas de Saída de Tráfego

HTTP

Tipo	Requisições	%
Saída para 25/TCP	**89.496.969**	**97.62**
Saída para outras	**106.615**	**0.12**
`get` **(geralmente web)**	**225.802**	**0.25**
Erros	**1.847.869**	**2.01**
Total	**91.677.255**	**100.00**

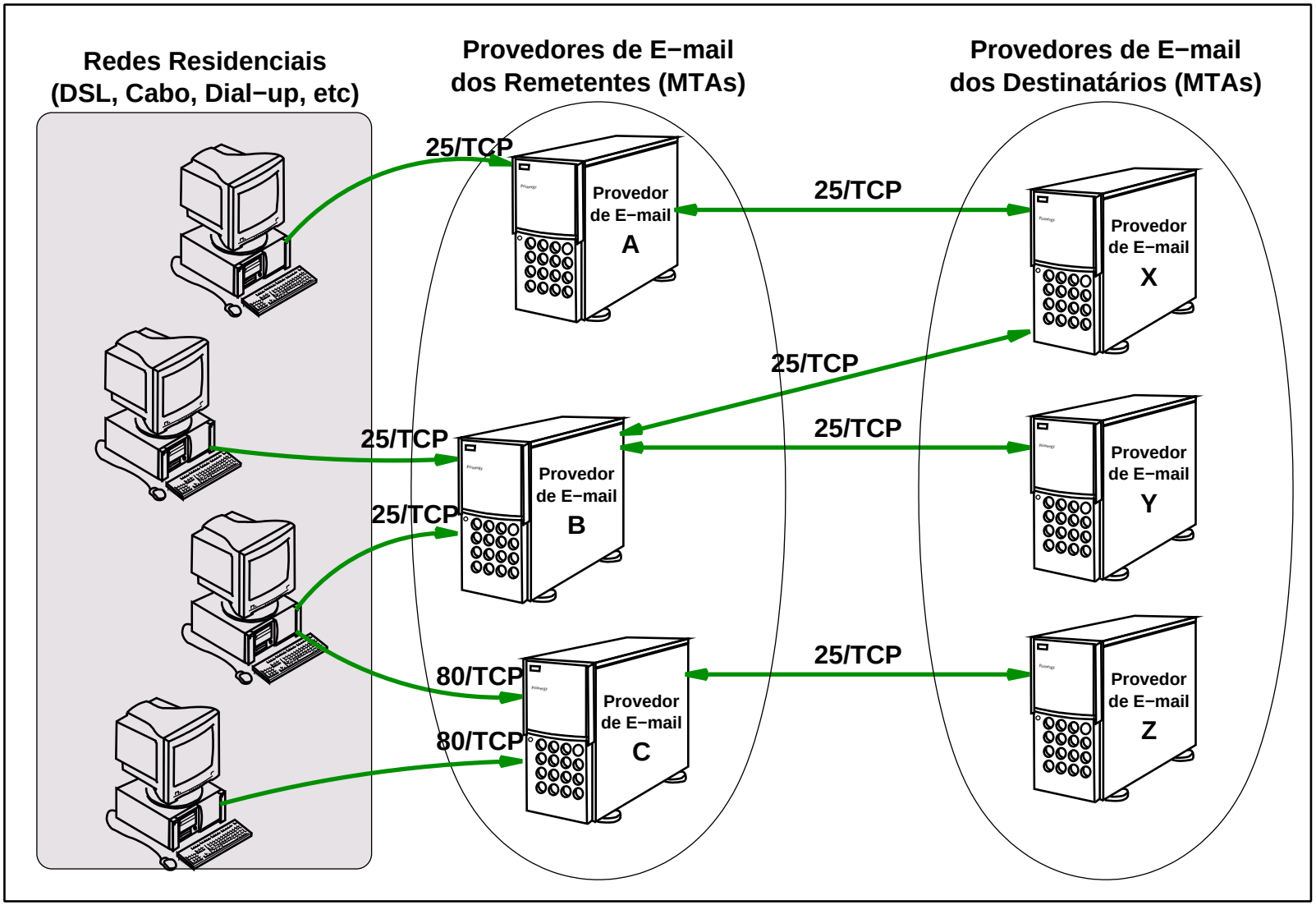
SOCKS

Tipo	Requisições	%
Saída para 25/TCP	**46.776.884**	**87.31**
Saída para outras	**1.055.081**	**1.97**
Erros	**5.741.908**	**10.72**
Total	**53.573.873**	**100.00**

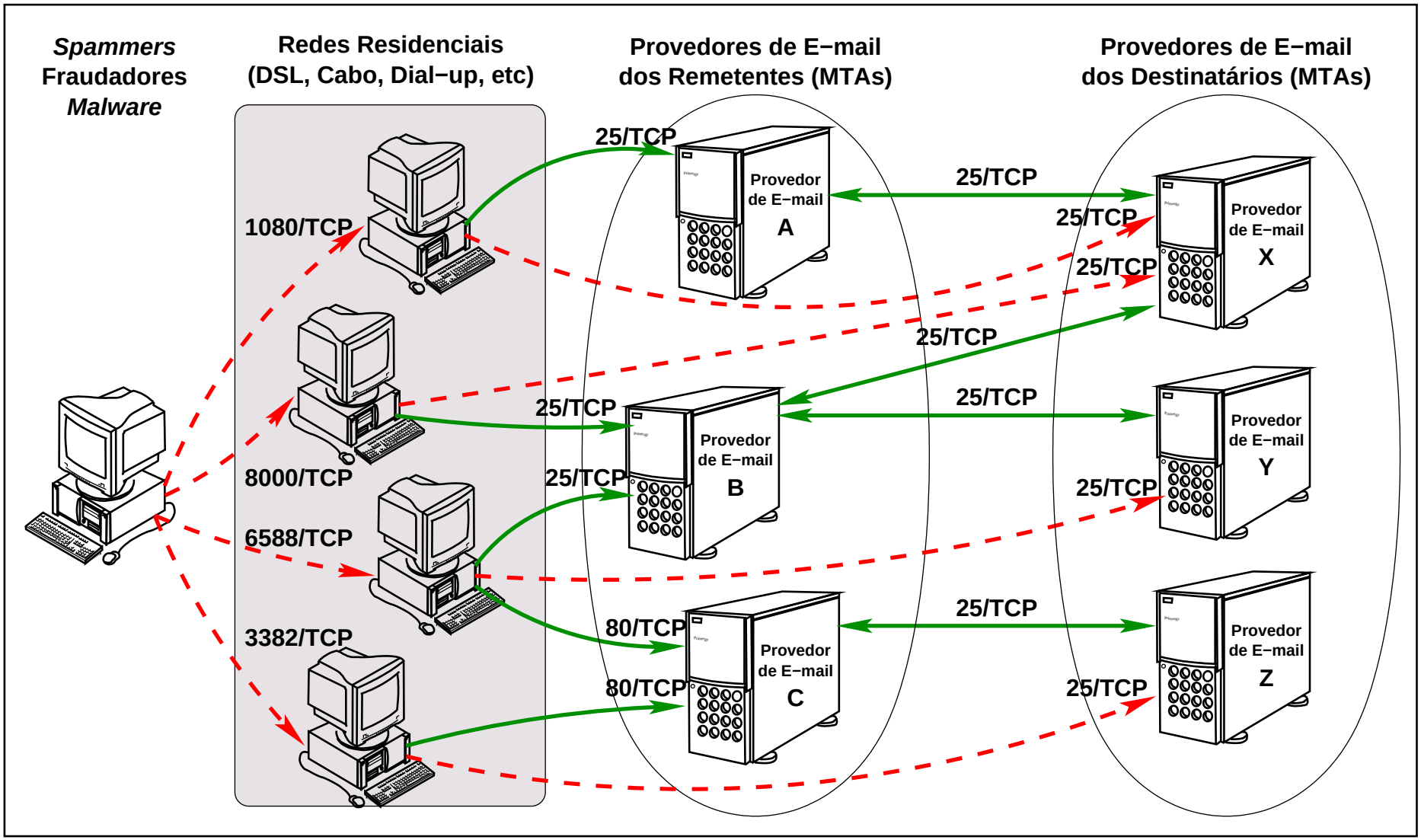
Obs.: Para este cálculo considerou-se apenas a primeira tentativa de cada endereço IP.

Porque Nossa Infra-Estrutura é Abusada

Uso Legítimo – Cenário Atual



Abuso – Cenário Atual

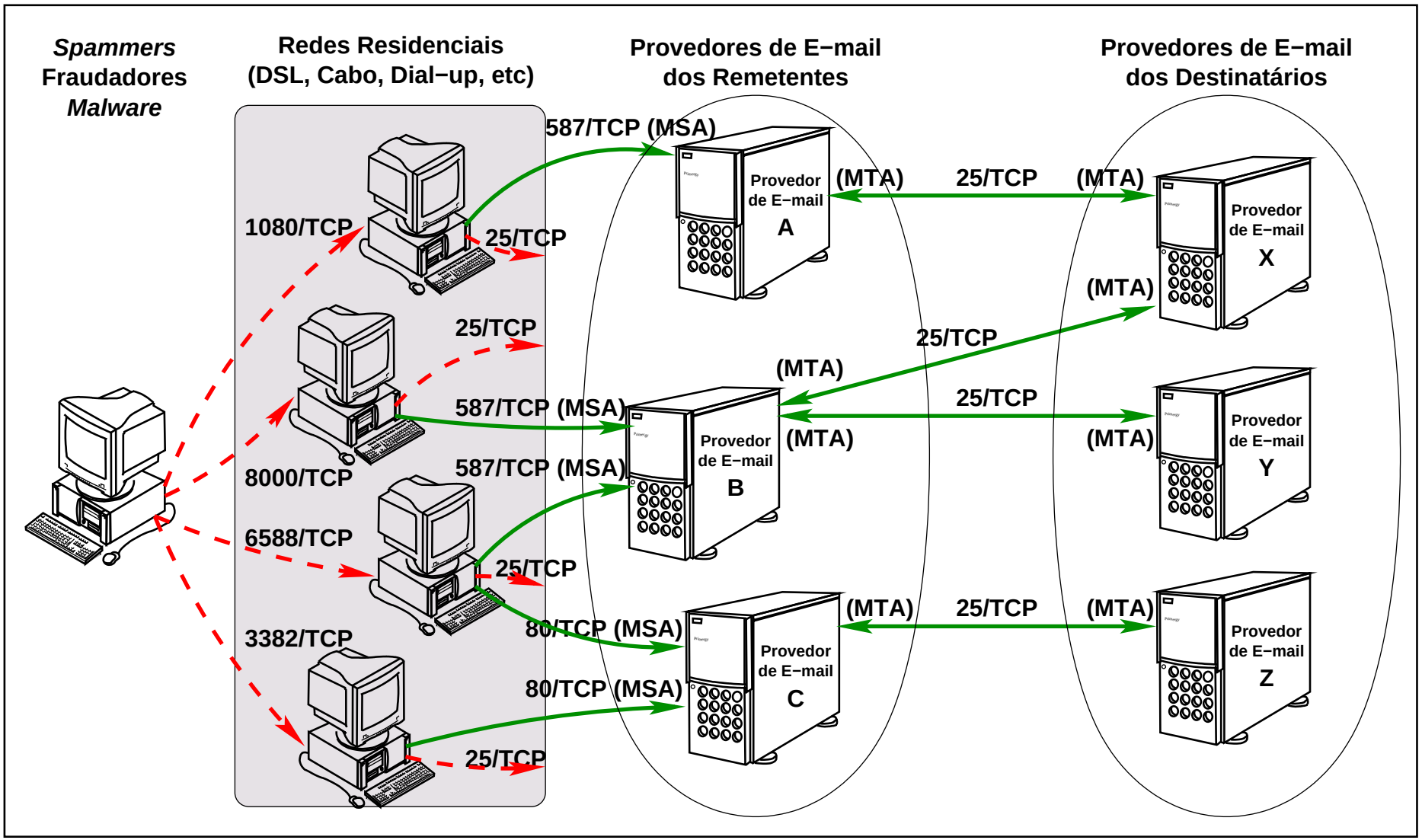


Proposta de Novo Cenário

Gerência de Porta 25

- Tecnologias e Políticas para Combate ao *Spam*
  http://www.cert.br/docs/ct-spam/
  - Primeira versão: 13/05/2005
  - Última revisão: 21/02/2008
- Recomendação às Operadoras de Banda Larga:
  - Impedir envio direto de mensagens eletrônicas (seção 3.2)
  - deve ser implementado em conjunto com a recomendação abaixo
- Recomendação para Provedores de Correio Eletrônico
  - Implementar SMTP autenticado em porta diferente da 25 (seção 4.1)
  - preferencialmente usar o padrão de *Message Submission* (RFC 4409)

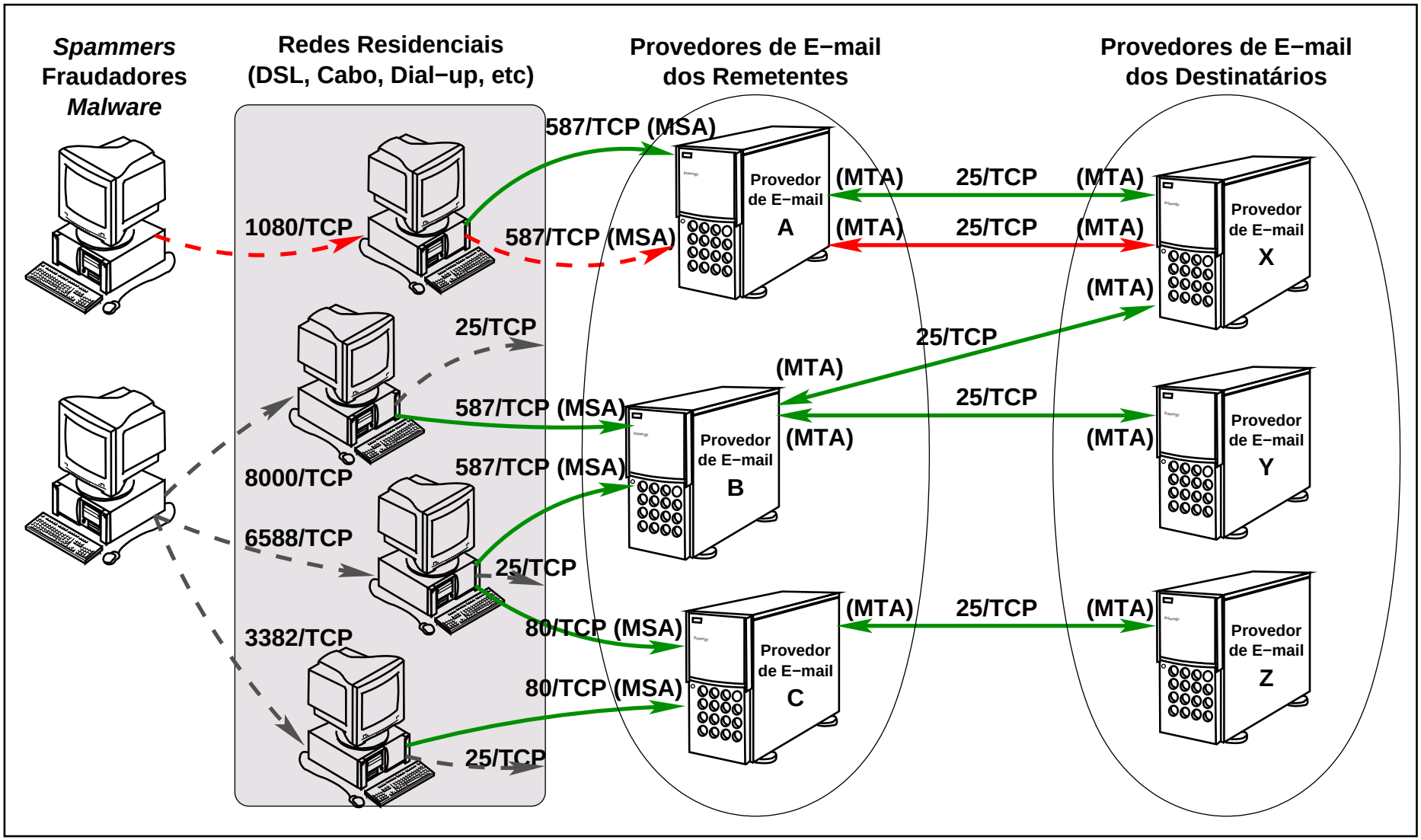
Impacto do Novo Cenário



Quem Adota Gerência de Porta 25

- Segundo a diretoria do MAAWG, todos os seus membros, que incluem: AT&T, Comcast, Earthlink, France Telecom, Verizon, Sprint, Time Warner Cable, Telefonica SA (EUA) e Bell Canada
- Referências *on-line* sobre quem adota:
  - *Earthlink blocks port 25 outgoing!, Oct 2000*
    http://www.broadbandreports.com/shownews/492
  - *Blocking Port 25 Traffic – 'MyDoom' virus reheats the discussion, Jan 2004*
    http://www.broadbandreports.com/shownews/38004
  - *Comcast takes hard line against spam, Jun 2004*
    http://news.zdnet.com/2100-3513_22-5230615.html
  - *Providers That Block Port 25*
    http://kb.earthlink.net/case.asp?article=resid9226

Possível Abuso do Novo Cenário



Benefícios (1/2)

- Saída dos blocos da operadora de listas de bloqueio
- Diminuição de reclamações de usuários
- Dificultar o uso da infra-estrutura da operadora para atividades ilícitas
  - *emails* de fraude são geralmente enviados via entrega direta
  - assim como os dados capturados das vítimas
- Aumento de rastreabilidade

Benefícios (2/2)

- Diminuição de vírus propagados por *email* (*email-borne viruses*)
- Proatividade
  - atuar na submissão, antes da mensagem entrar na infra-estrutura de *email*
- Percepção positiva pelos clientes e pela comunidade
- Possibilidade de comercializar conexões diferenciadas

Impacto

- Carga no suporte dos provedores: precisam contactar o usuário final
- Necessidade de segregar conexões residenciais de conexões comerciais
- Questões contratuais com clientes antigos

Dúvidas Comuns

- Todos os provedores de *email* precisam implementar *Message Submission*?
- Meus clientes vão migrar para a concorrente, que permite entrega direta de *email*?
- Vou ter que diferenciar conexão residencial de conexão comercial?
- Vai funcionar se não tiver uma lei obrigando?

Referências (1/2)

- RFC 3207: SMTP Service Extension for Secure SMTP over Transport Layer Security
  http://www.ietf.org/rfc/rfc3207.txt
- RFC 4409: Message Submission for Mail
  http://www.ietf.org/rfc/rfc4409.txt
- RFC 4954: SMTP Service Extension for Authentication
  http://www.ietf.org/rfc/rfc4954.txt
- RFC 5068: Email Submission Operations: Access and Accountability Requirements
  http://www.ietf.org/rfc/rfc5068.txt

Referências (2/2)

- Managing Port 25 for Residential or Dynamic IP Space: Benefits of Adoption and Risks of Inaction
  http://www.maawg.org/port25/
- Tecnologias e Políticas para Combate ao *Spam*
  http://www.cert.br/docs/ct-spam/
- Resultados Preliminares do Projeto SpamPots
  http://www.cert.br/docs/whitepapers/spampots/
- CERT.br
  http://www.cert.br/
- NIC.br
  http://www.nic.br/
- CGI.br
  http://www.cgi.br/