Políticas e Padrões para a Redução do Abuso de *Proxies* Abertos para o Envio de *Spam*

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

Agenda

O Problema do Abuso de Proxies Abertos
- Reclamações de Spam ao CERT.br
- Resultados do Projeto SpamPots

Como Este Abuso Acontece

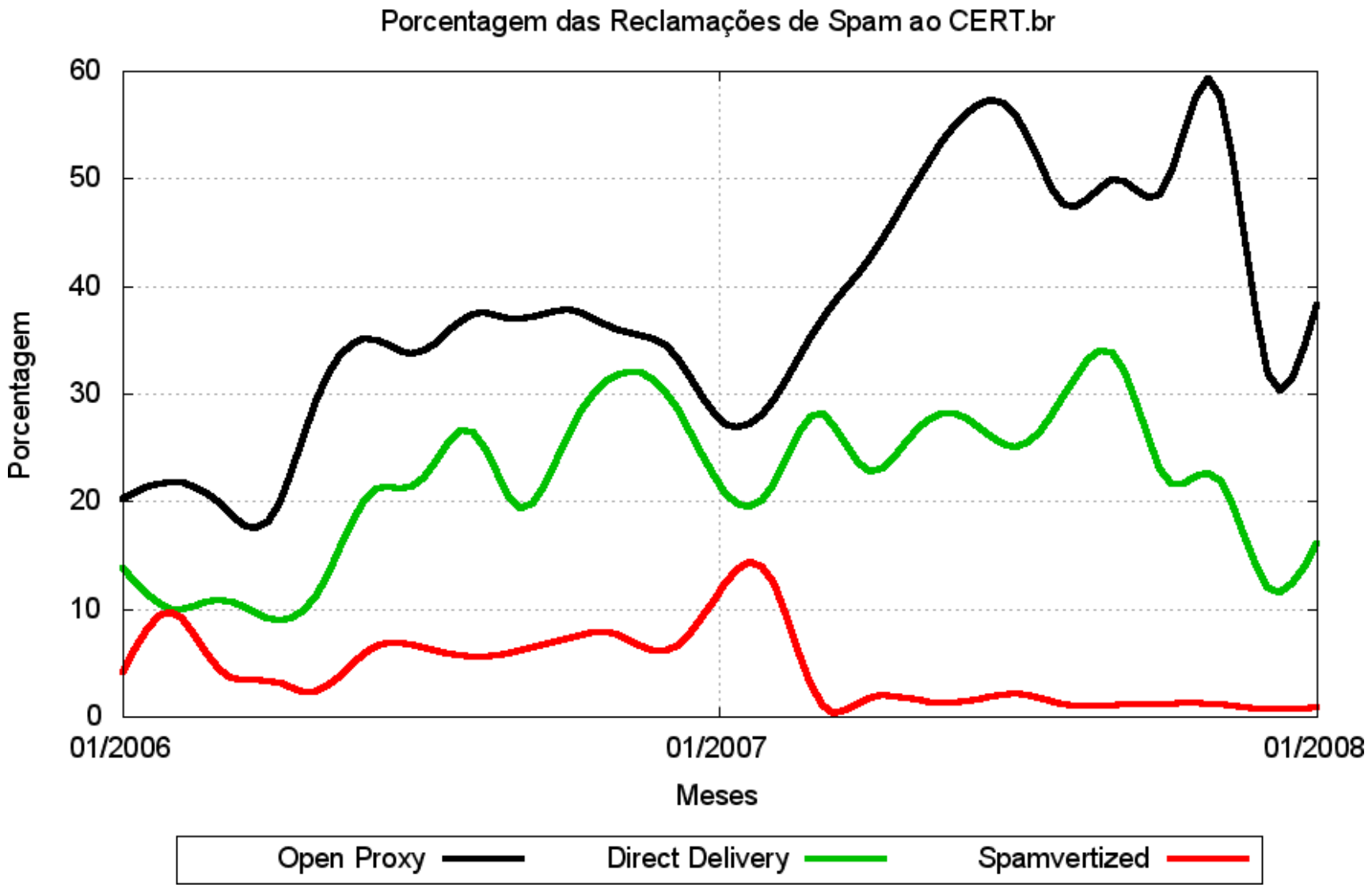
Padrões e Políticas Disponíveis para Mitigar o Problema
- Evolução dos Padrões
- Impacto

Benefícios

Referências

O Problema do Abuso de *Proxies* Abertos

Reclamações de *Spam* ao CERT.br

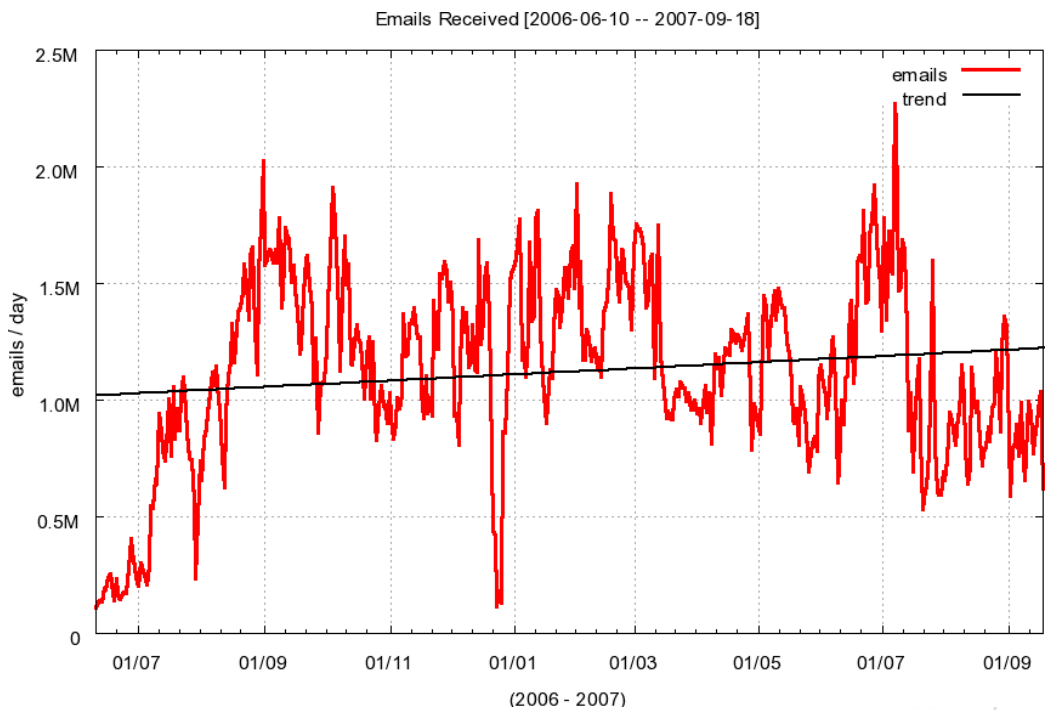


Resultados do Projeto SpamPots

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

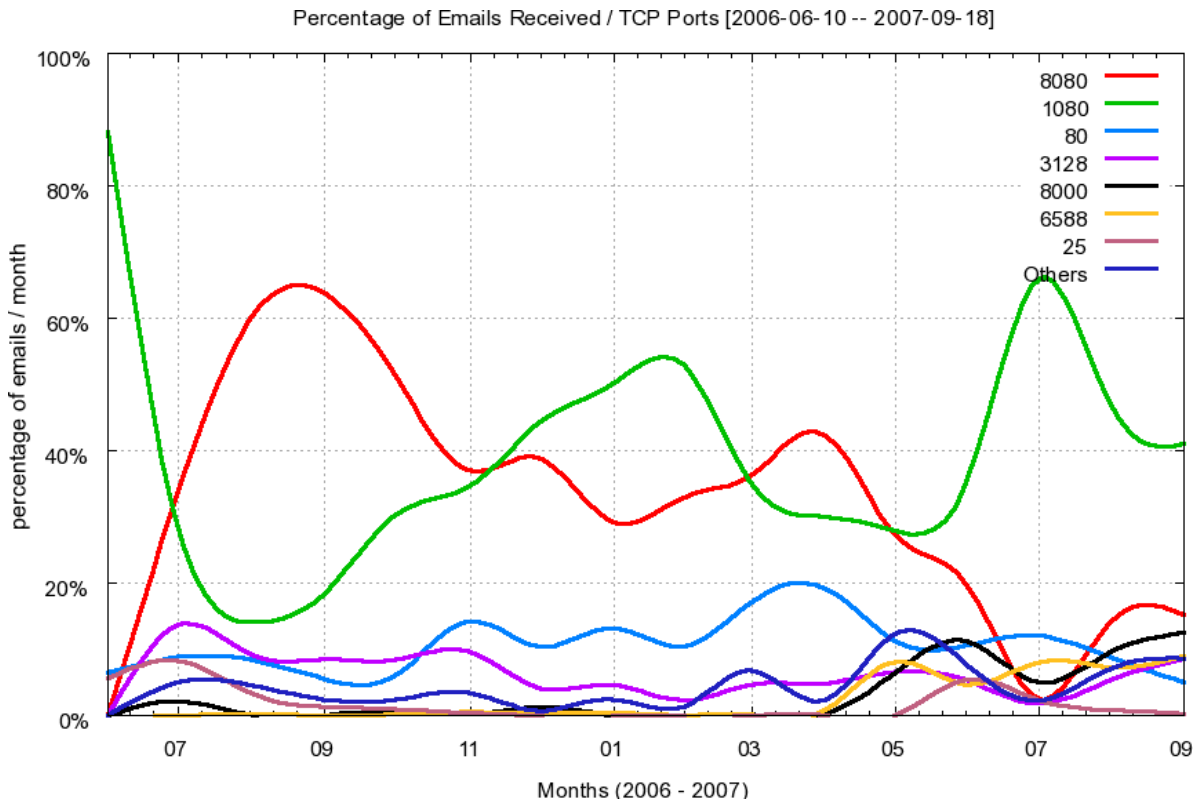
- Mantido pelo CGI.br/NIC.br, como parte da CT-Spam
- 10 *honeypots* de baixa interatividade
  - 5 operadoras diferentes de cabo e DSL
  - em conexões residenciais e comerciais

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**



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**

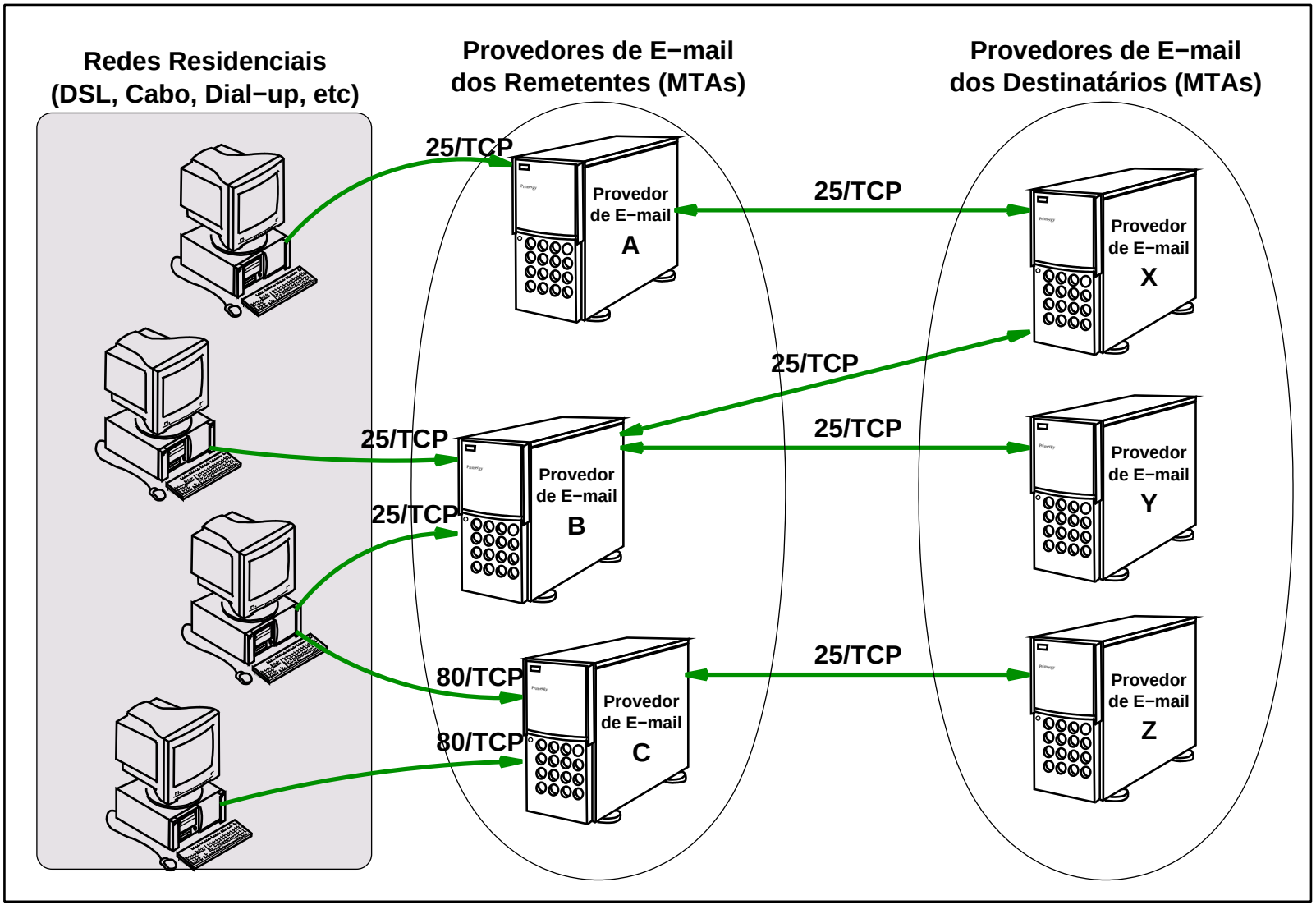
SOCKS

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**

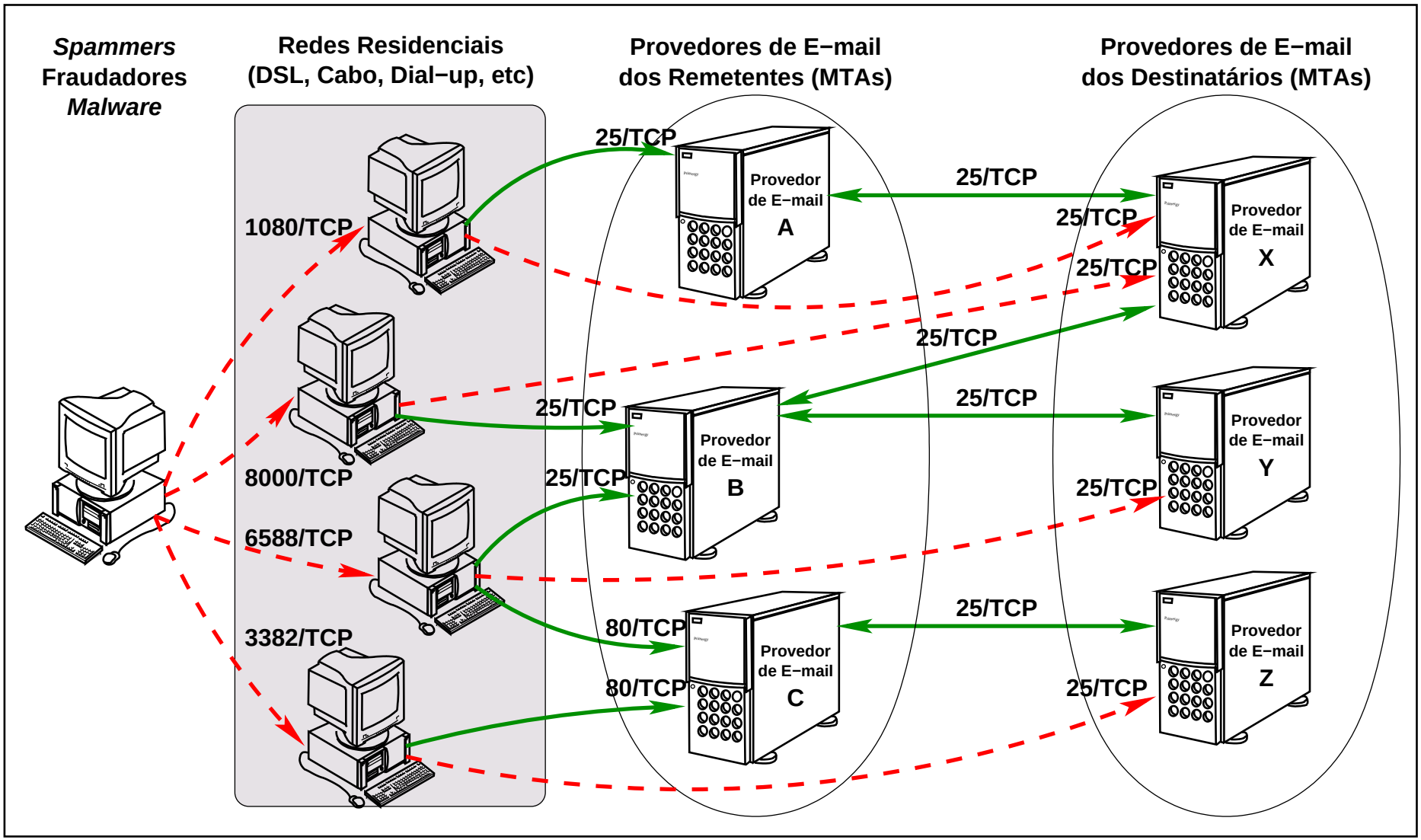
Obs.: Para este cálculo considerou-se apenas a primeira tentativa de cada endereço IP.

Como Este Abuso Acontece

Uso Legítimo – Cenário Atual



Abuso – Cenário Atual



Padrões e Políticas Disponíveis para Mitigar o Problema

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)

Gerência de Porta 25

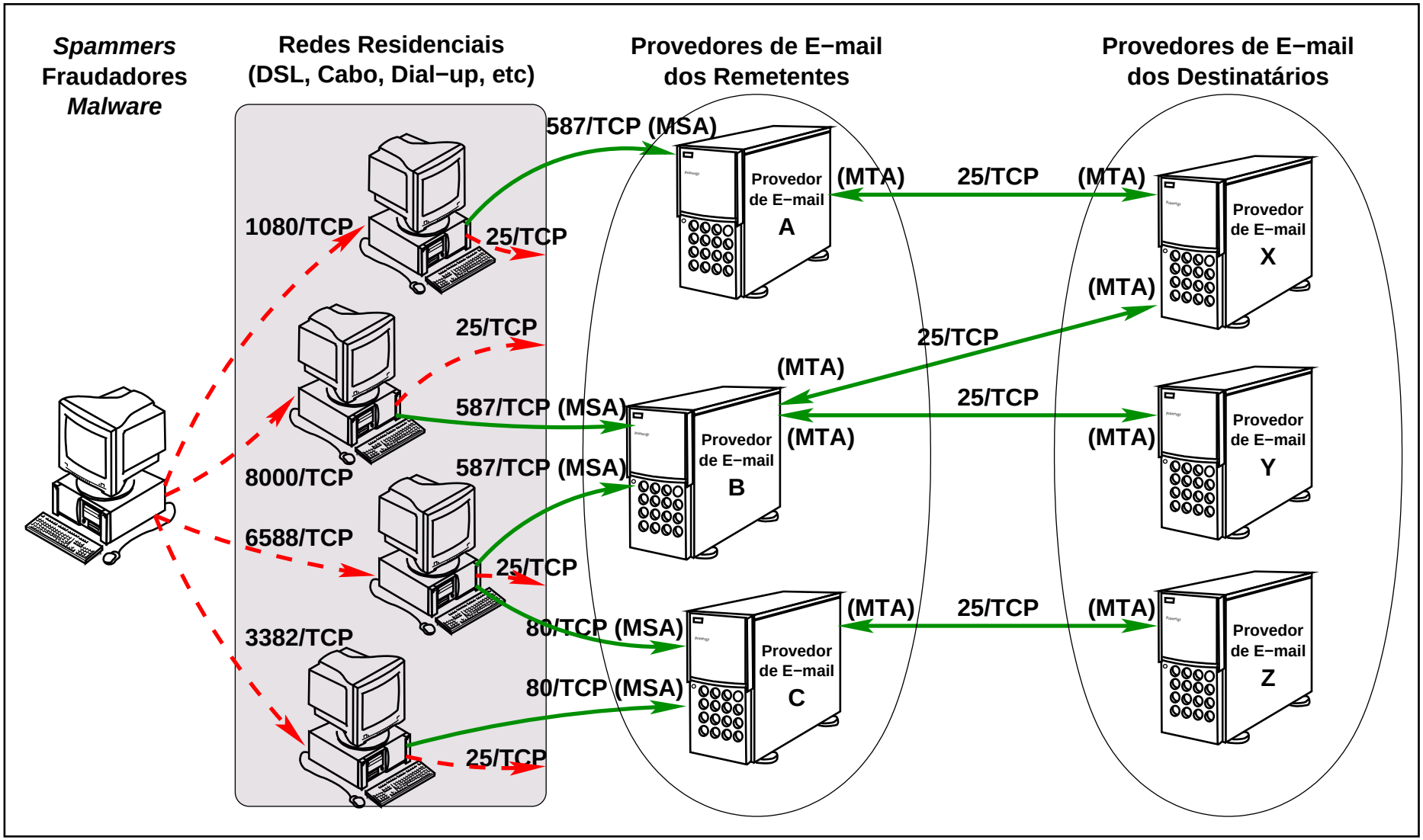
- requerer autenticação para a submissão de mensagens, como recomendado na RFC 4954;
- não interferir no tráfego para a porta 587/TCP;
- configurar o *software* cliente de *email* para usar porta 587/TCP e autenticação;
- bloquear acesso de saída para porta 25/TCP a partir de todas as máquinas que não sejam MTAs ou explicitamente autorizadas.

Fonte: *Managing Port 25 for Residential or Dynamic IP Space – Benefits of Adoption and Risks of Inaction* – http://www.maawg.org/port25/

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
  - 15/12/2005: discussão na Anatel (Agência Nacional de Telecomunicações) com teles;
  - 22/02/2008: nova discussão com Anatel e teles

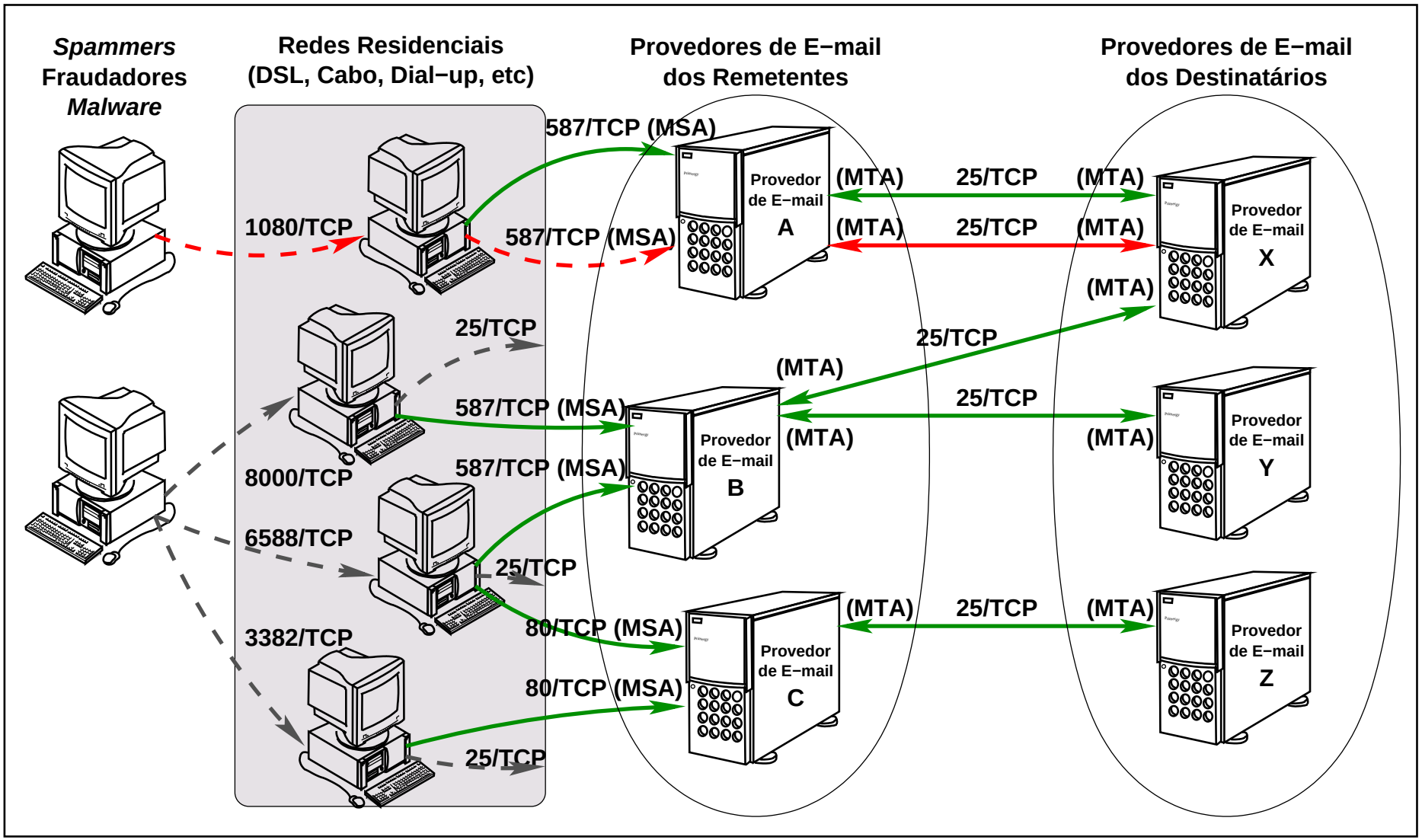
Impacto


Spammers
Fraudadores
Malware
Redes Residenciais
(DSL, Cabo, Dial−up, etc)
Provedores de E−mail
dos Remetentes
Provedores de E−mail
dos Destinatários
587/TCP (MSA)
1080/TCP
25/TCP
25/TCP
587/TCP (MSA)
8000/TCP
587/TCP (MSA)
6588/TCP
25/TCP
80/TCP (MSA)
3382/TCP
80/TCP (MSA)
25/TCP
Provedor de E−mail A
Provedor de E−mail B
Provedor de E−mail C
Provedor de E−mail X
Provedor de E−mail Y
Provedor de E−mail Z
(MTA)
25/TCP
(MTA)
(MTA)
25/TCP
(MTA)
(MTA)
25/TCP
(MTA)
(MTA)
25/TCP
(MTA)

Quem Adota Gerência de Porta 25

- Membros do MAAWG, incluindo: AOL, Comcast e Earthlink
- Referências *on-line* sobre quem adota:
  - *The Only Good Spam Comes from Hormel. ;login: Magazine, February 2005*
    http://www.usenix.org/publications/login/2005-02/openpdfs/motd.pdf
  - *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

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/