Gerência de Porta 25: Motivação, Vantagens e Desafios

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

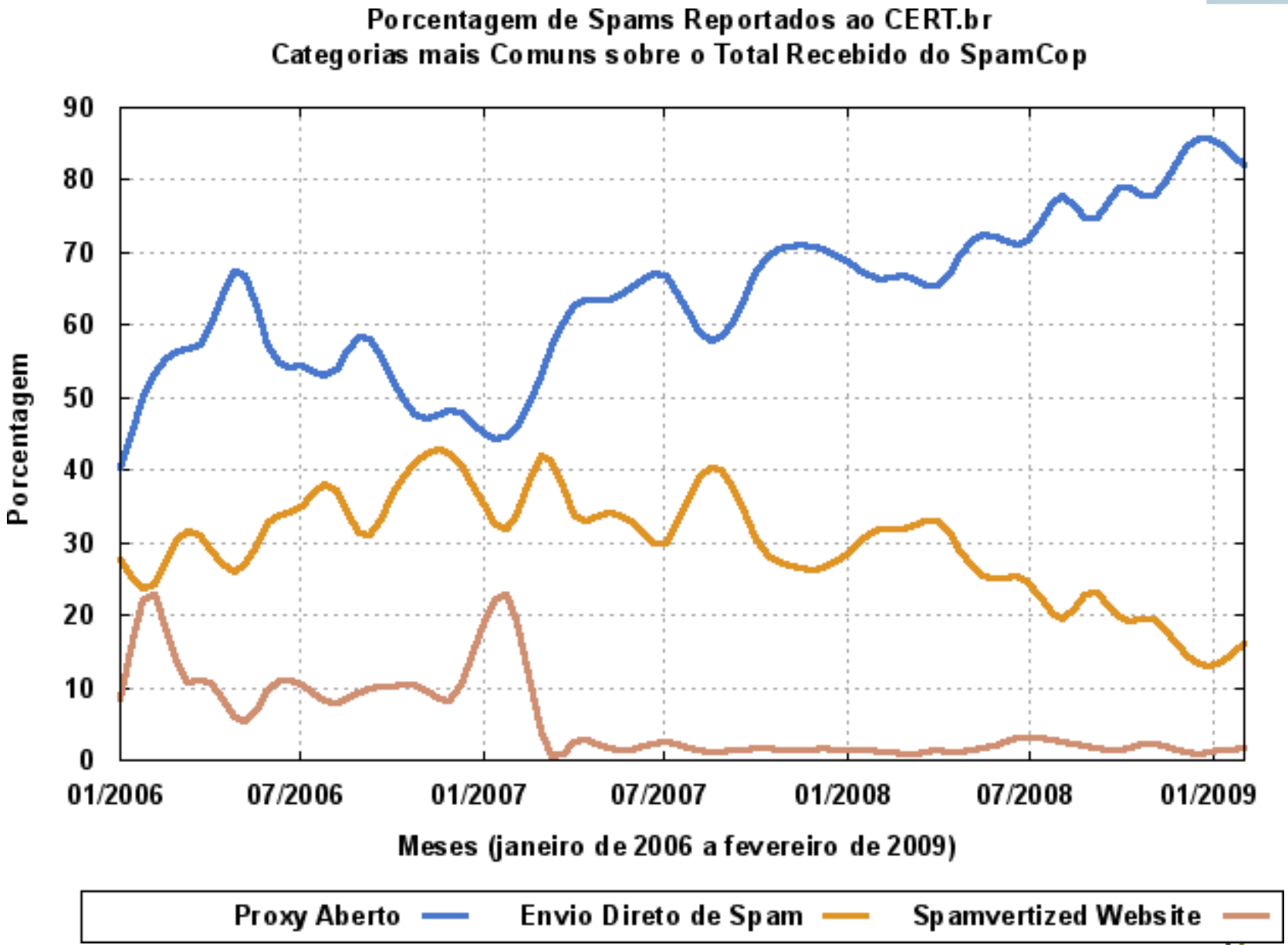
Agenda

Motivação

Gerência de Porta 25
- Benefícios
- Quem adota
- Possíveis desafios do processo de implantação
- Evolução das discussões no Brasil

Referências

http://www.cert.br/stats/spam/porcentagens/



Brasil na CBL (1/2)

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

- 815.630 IPs listados (14,53%)
- Outros países com mais de 5%: RU (10,45%), IN (8,00%), TR (6,74%) e CN (5,89%)

"*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 26/01/2009

Brasil na CBL (2/2)

Domínio (reverso)	Posição no Ranking	Número de IPs Listados	% dos IPs do Brasil	% do Total de IPs da CBL
telebahia.net.br **(Oi)**	2	255.129	31,28	4,55
telesp.com.br	4	184.519	22,62	3,29
brasiltelecom.net.br	6	154.289	18,92	2,75
telet.com.br **(Claro)**	18	54.521	6,68	0,97
netservicos.com.br	35	32.357	3,97	0,58
gvt.net.br	38	26.124	3,20	0,47
ig.com.br	44	23.822	2,92	0,42
ctbctelecom.net.br	52	18.928	2,32	0,34
timbrasil.com.br	55	17.956	2,20	0,32
embratel.net.br	77	12.336	1,51	0,22
canbrasnet.com.br	112	8.109	0,99	0,14
ig.com	141	6.240	0,77	0,11

Dados de 26/01/2009

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**

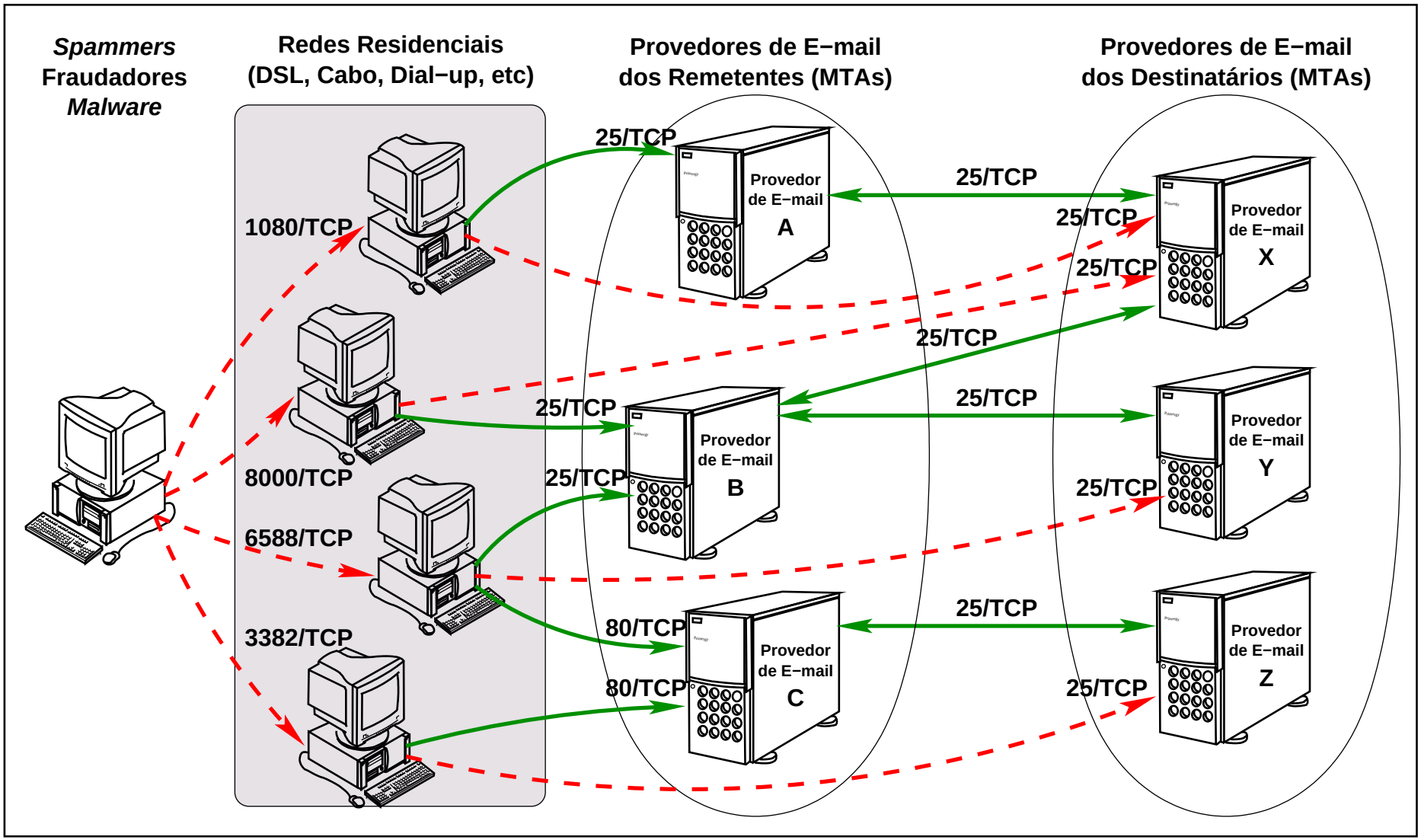
Principais Resultados:

- 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



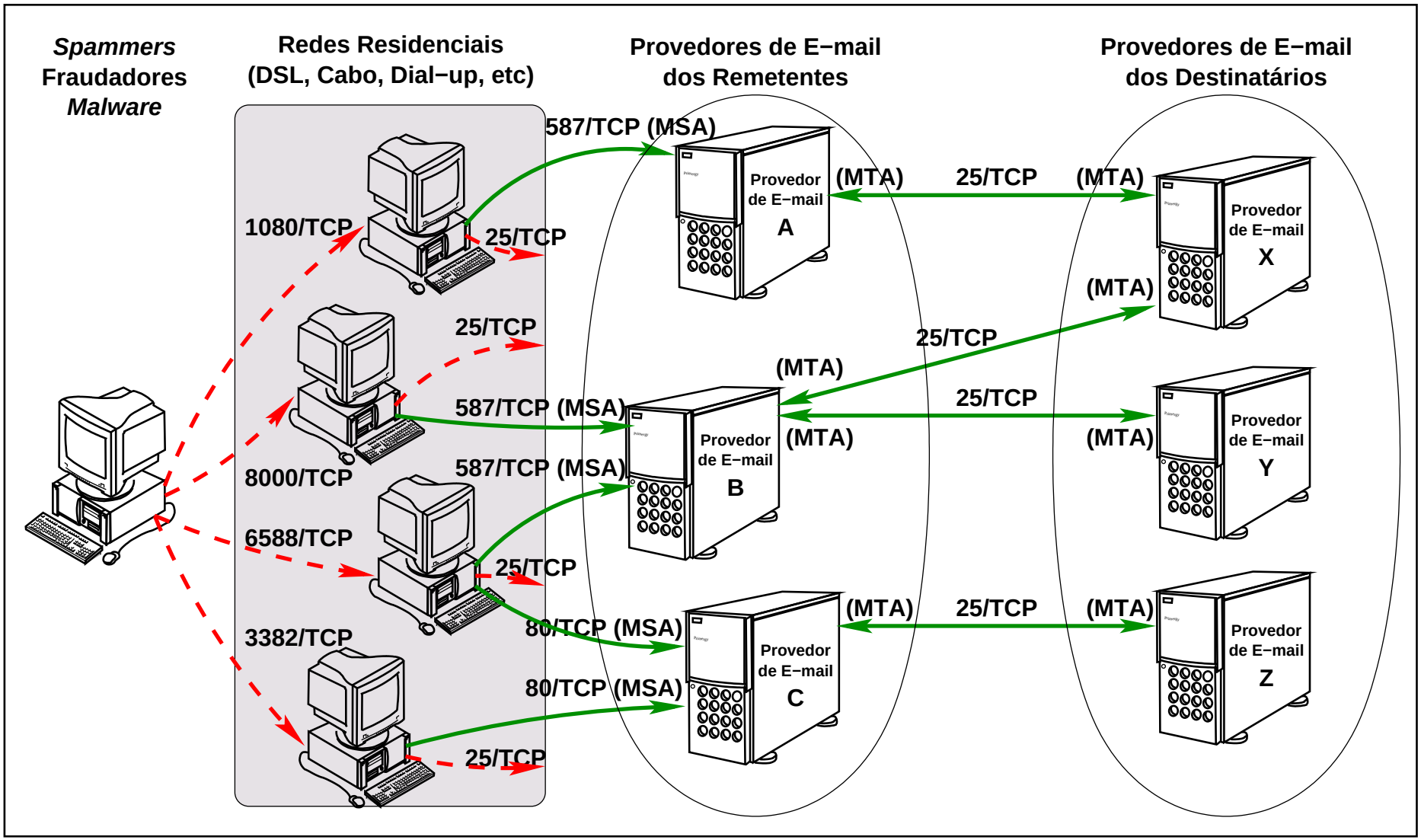
Gerência de Porta 25

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)

Gerência de Porta 25 e Seu Impacto



Benefícios

- Saída dos blocos das operadoras de listas de bloqueio
- Diminuição de reclamações de usuários
- Dificulta o abuso da infra-estrutura da Internet para atividades ilícitas (fraudes, furto de dados, etc)
- Aumento de rastreabilidade em caso de abuso
- Atua na submissão, antes da mensagem entrar na infra-estrutura de *e-mail*
- Diminuição do consumo de banda internacional por *spammers*
- Diminuição de custos operacionais
  - spam foi o mais apontado como responsável pela demanda de recursos operacionais no "*2008 Worldwide Infrastructure Security Report*"

    http://www.arbornetworks.com/report

Quem Adota Gerência de Porta 25 (1/2)

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 nos EUA:

- *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: NetZero, Mindspring, MSN, Earthlink, Flashnet, MediaOne, AT&T, Verizon, BellSympatico*
  http://kb.earthlink.net/case.asp?article=resid9226

Quem Adota Gerência de Porta 25 (2/2)

- Sercomtel, no Brasil (Londrina/PR)
  - ftp://ftp.registro.br/pub/gter/gter23/videos/mp4/gts-06-mail-submission.mp4
- Europa
  - Segundo a ENISA, 50% dos ISPs Europeus consultados http://www.enisa.europa.eu/pages/spam/doc/enisa_spam_study_2007.pdf
  - S.I.A.S. (Swiss ISPs Against Spam): Bluewin, cablecom e green.ch http://www.stopspam.ch/engl/infos.htm
- Japão
  - Recomendação do JEAG (Japan Email Anti-Abuse Group) http://jeag.jp/

Possíveis Desafios do Processo de Implantação

- Efetividade depende da ação conjunta de provedores e operadoras
- Carga no suporte dos provedores: precisam contactar o usuário final para alterar configurações
- Necessidade de diferenciar, nas operadoras, conexões de perfil residencial daquelas de perfil empresarial
- Questões contratuais com clientes antigos
- Lidar com exceções
  - *softwares* desatualizados/antigos, sem suporte para *Message Submission*
  - serviços de e-mail sem suporte para *Message Submission*

Evolução das Discussões no Brasil (1/3)

21/06/2005: seminário com operadoras e provedores para discutir o documento "Tecnologias e políticas para Combate ao *Spam*".

15/12/2005: discussão do documento na 5ª reunião ordinária do CBC-1 da Anatel.

12/07/2007 e 13/09/2007: reuniões entre operadoras, CERT.br e setor financeiro sobre o abuso das redes de banda larga para atividades maliciosas; como resultado destas discussões foi consenso que gerência de porta 25 deveria ser o primeiro tema a ser tratado, evidenciando a importância de envolver os provedores nas discussões.

Evolução das Discussões no Brasil (2/3)

08/11/2007: reunião entre operadoras, CERT.br, setor financeiro e provedores, sobre gerência de porta 25.

22/02/2008: discussão sobre gerência de porta 25 na 13ª reunião ordinária do CBC-1 da Anatel; nesta reunião o representante da Anatel solicitou às operadoras o estudo da viabilidade técnica de implantação e prazo necessário.

19/12/2008: primeira reunião entre associações e representantes de operadoras de banda larga e de provedores de acesso e a CT-Spam do CGI.br, para discussão e definição do cronograma de adoção.

Evolução das Discussões no Brasil (3/3)

12/02/2009: segunda reunião entre associações e representantes de operadoras de banda larga e de provedores de acesso e a CT-Spam do CGI.br.

19/03/2009: terceira reunião entre associações e representantes de operadoras de banda larga e de provedores de acesso e a CT-Spam do CGI.br.

16/04/2009: reunião entre operadoras móveis, CERT.br e Anatel, para discutir peculiaridades técnicas relativas à adoção no serviço móvel.

14/05/2009: próxima reunião.

Referências

- Antispam.br – Administradores de Redes
  Gerência de Porta 25
  http://www.antispam.br/admin/porta25/
- Documentos e Palestras do CERT.br no Escopo do seu Trabalho na CT-Spam
  http://www.cert.br/docs/ct-spam/
- Managing Port 25 for Residential or Dynamic IP Space: Benefits of Adoption and Risks of Inaction
  http://www.maawg.org/port25/
- RFC 4409: Message Submission for Mail
  http://www.ietf.org/rfc/rfc4409.txt
- RFC 5068: Email Submission Operations: Access and Accountability Requirements
  http://www.ietf.org/rfc/rfc5068.txt