Spam: Cenário atual e ações para redução do problema

Klaus Steding-Jessen
jessen@cert.br

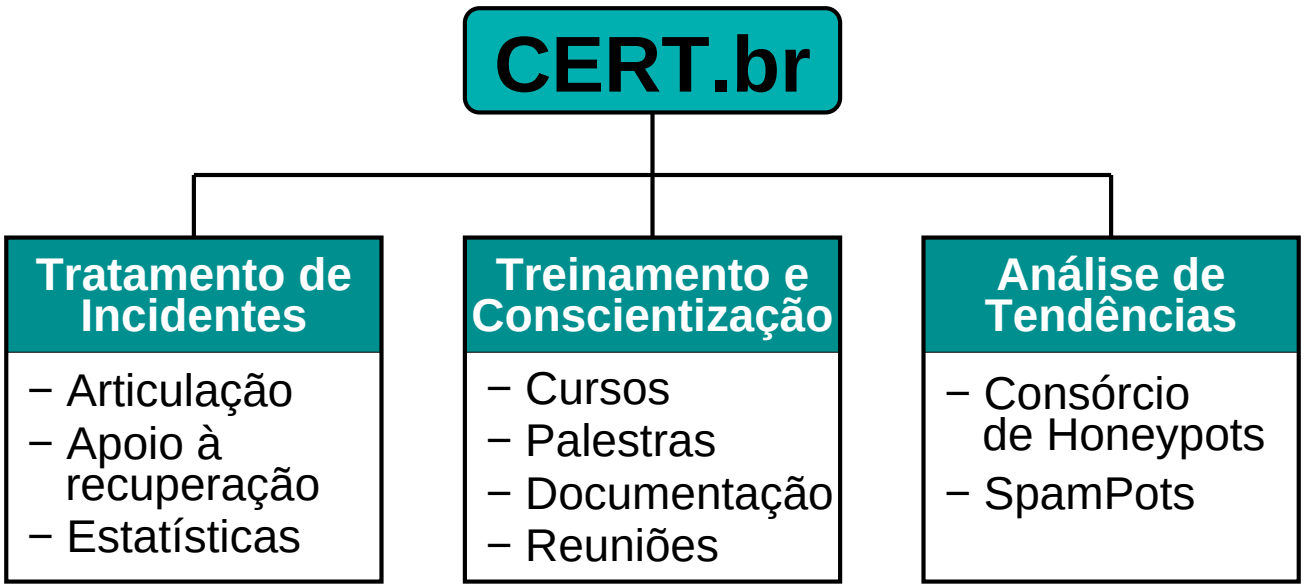
Esta apresentação:

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

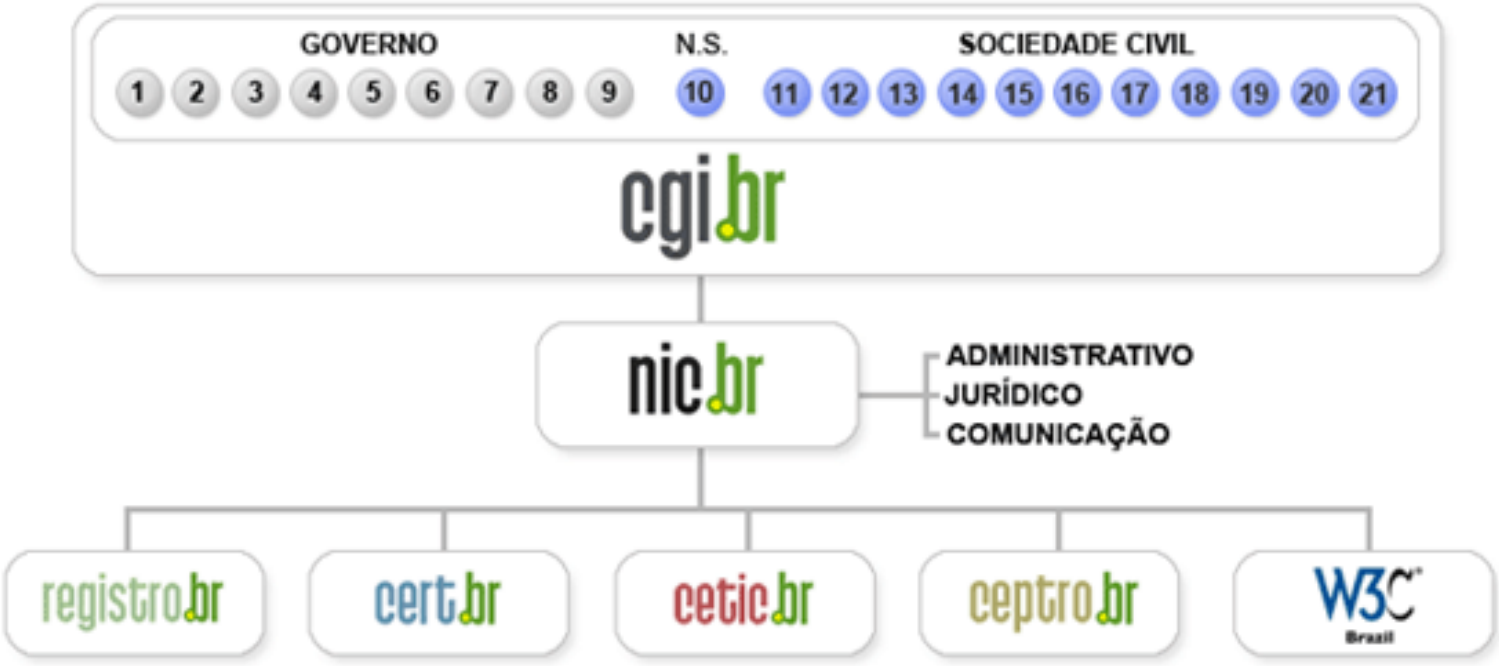
Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



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

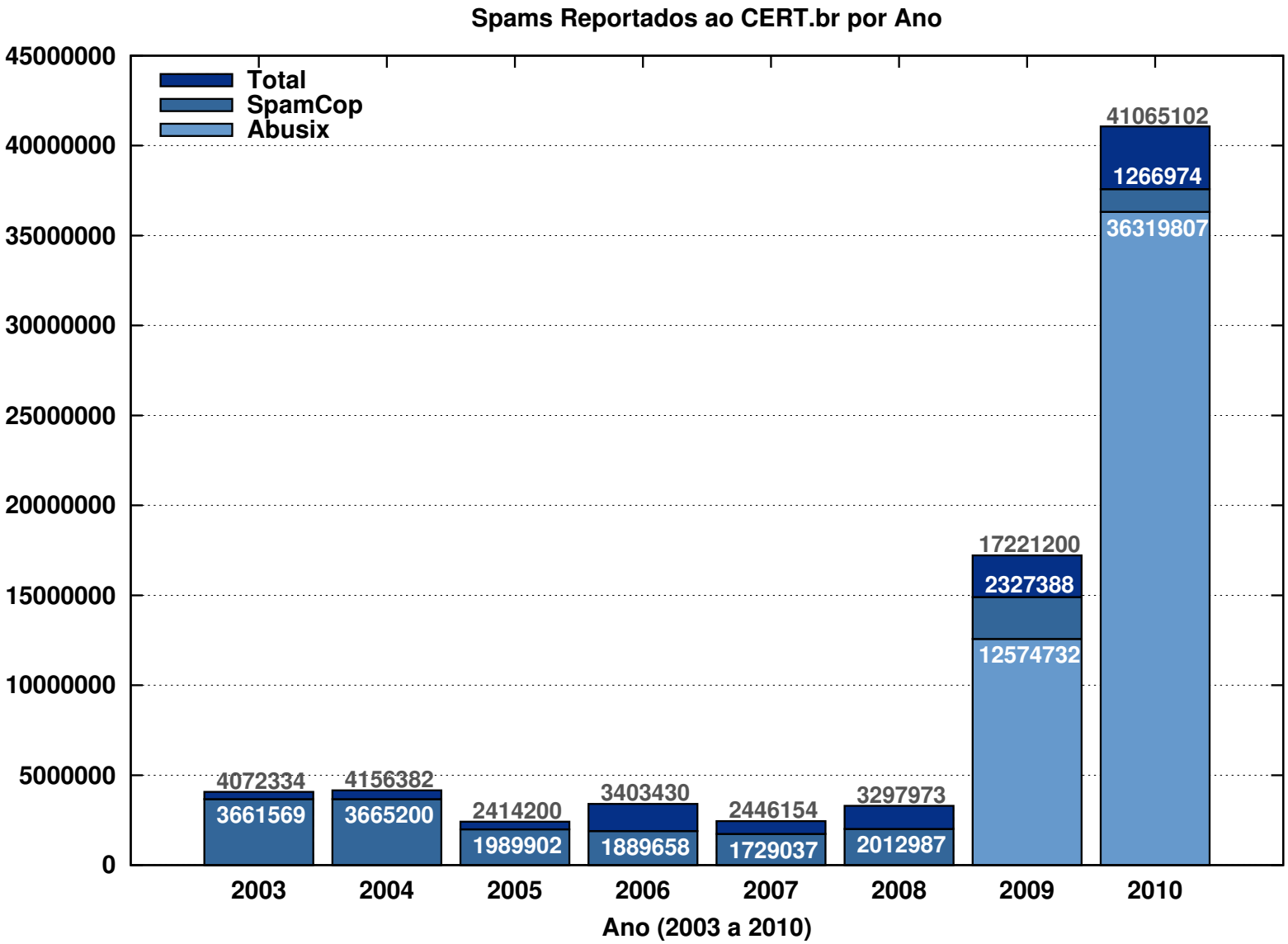
Cenário do Spam no Brasil
- Reclamações ao CERT.br em 2010
- Brasil na CBL

Ações para Redução do Problema

Referências

Cenário do *Spam* no Brasil

Reclamações ao CERT.br em 2010



Brasil na CBL

	País	Endereços IP	% do Total	Taxa de Infecção (%)
1	Índia (IN)	1.129.747	17,06	4,881
2	Brasil (BR)	630.446	9,52	1,234
3	Rússia (RU)	585.637	8,84	1,672
4	Vietnã (VN)	319.472	4,82	2,840
5	Ucrânia (UA)	313.528	4,73	3,415
6	Indonésia (ID)	213.132	3,22	2,390
7	China (CN)	198.271	2,99	0,071
8	Tailândia (TH)	171.941	2,60	1,712
9	Paquistão (PK)	164.467	2,48	4,667
10	Itália (IT)	154.803	2,34	0,355

Fonte: CBL, uma lista de endereços IP de computadores que comprovadamente enviaram *spams* nas últimas 24 horas e estavam infectados.

Dados gerados em: `Mon Jan 17 11:37:41 2011 UTC/GMT`

`Composite Blocking List` http://cbl.abuseat.org/

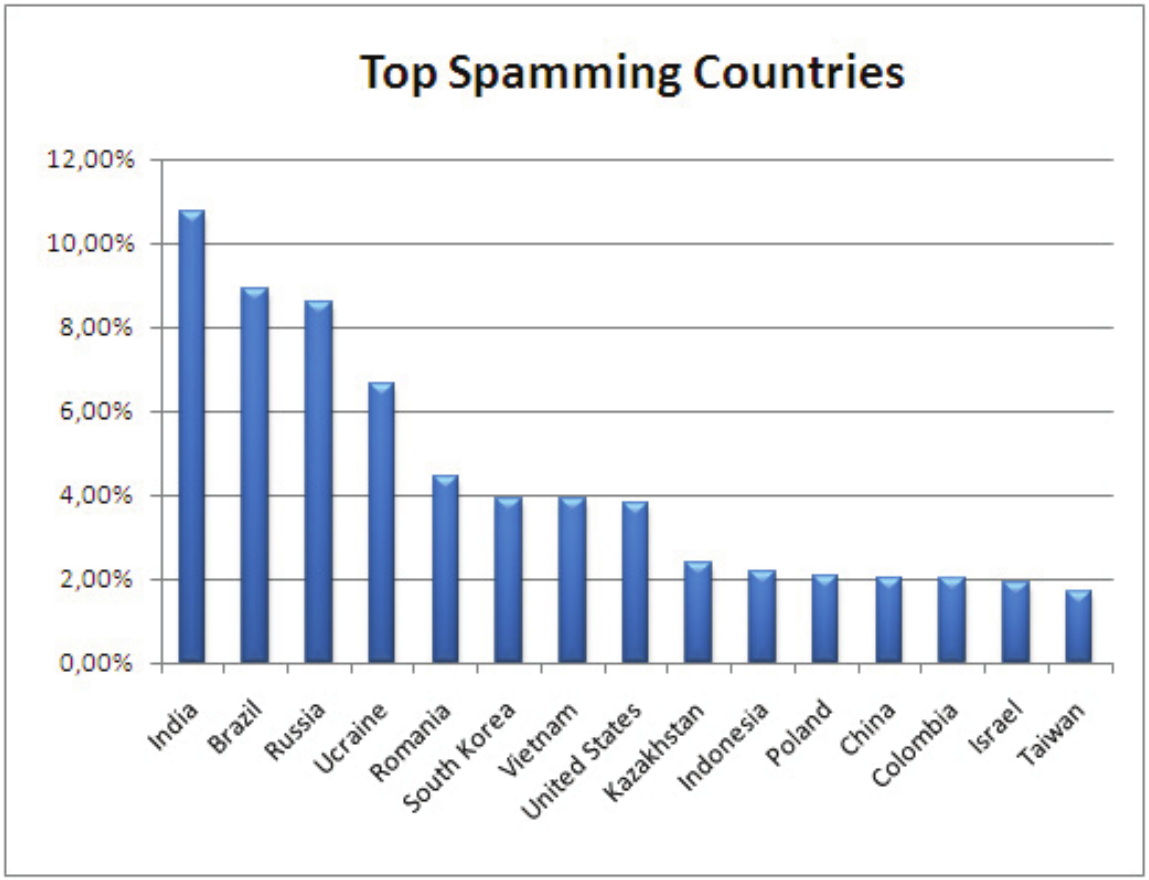
Cisco 2009 Annual Security Report

Brazil experienced the largest year-over-year increase of countries examined by Cisco researchers: ***Brazil's spam output tripled between 2008 and 2009****. In fact, the world's* ***emerging economies*** *(as defined by membership in the G-20 developing nations group)* ***are responsible for output of 55 percent of the world's total global spam.***

http://www.cisco.com/go/securityreport

Fonte da matéria *"Brazil: The New Spam King"*
www.forbes.com/2009/12/08/spam-china-cisco-technology-cio-network-brazil.html

Quarterly Report PandaLabs (Jul-Sep 2010)



http://prensa.pandasecurity.com/wp-content/uploads/2010/09/Quarterly-Report-PandaLabs-3-Q-2010.pdf

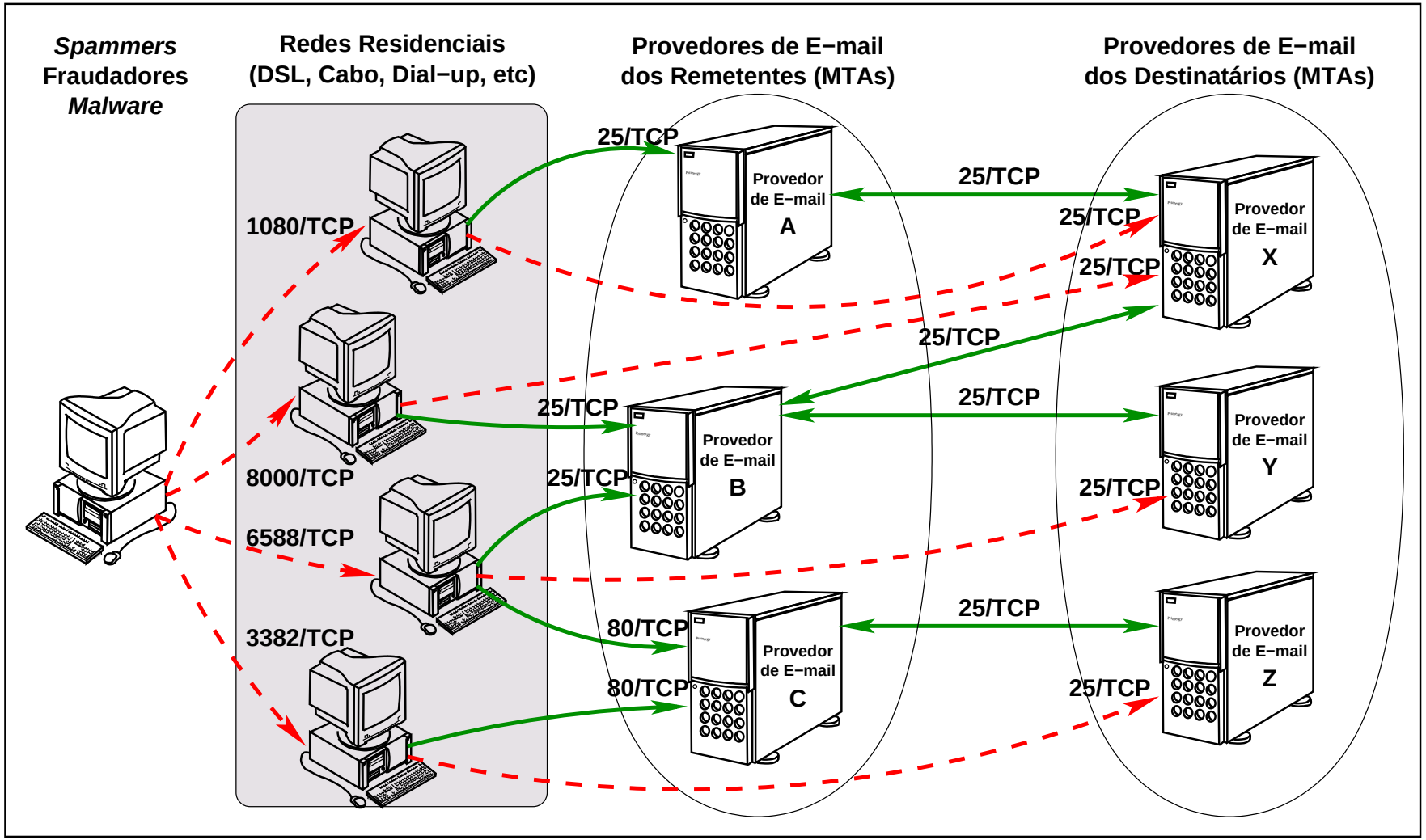
Sophos Dirty Dozen

Dados do último relatório (Outubro a Dezembro de 2010)

1. USA	18.83%
2. India	6.88%
3. Brazil	5.04%
4. Russia	4.64%
5. UK	4.54%
6. France	3.45%
7. Italy	3.17%
8. S Korea	3.01%
9. Germany	2.99%
10. Vietnam	2.79%
11. Romania	2.25%
12. Spain	2.24%
Other	40.17%

http://www.sophos.com/pressoffice/news/articles/2011/01/dirty-dozen-q42010.html

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

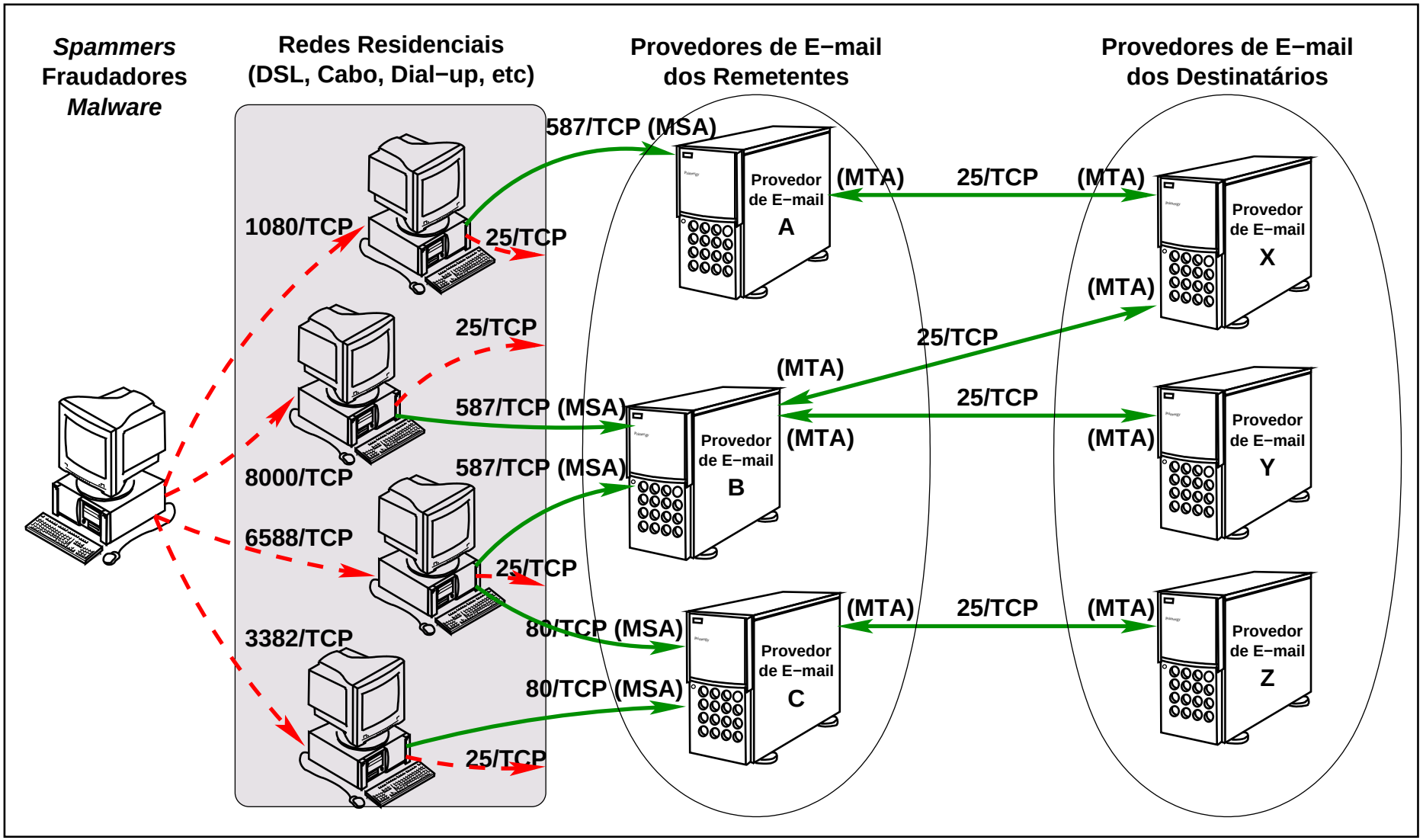
Diferenciar a submissão de *e-mails* do cliente para o servidor, da transmissão de *e-mails* entre servidores.

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