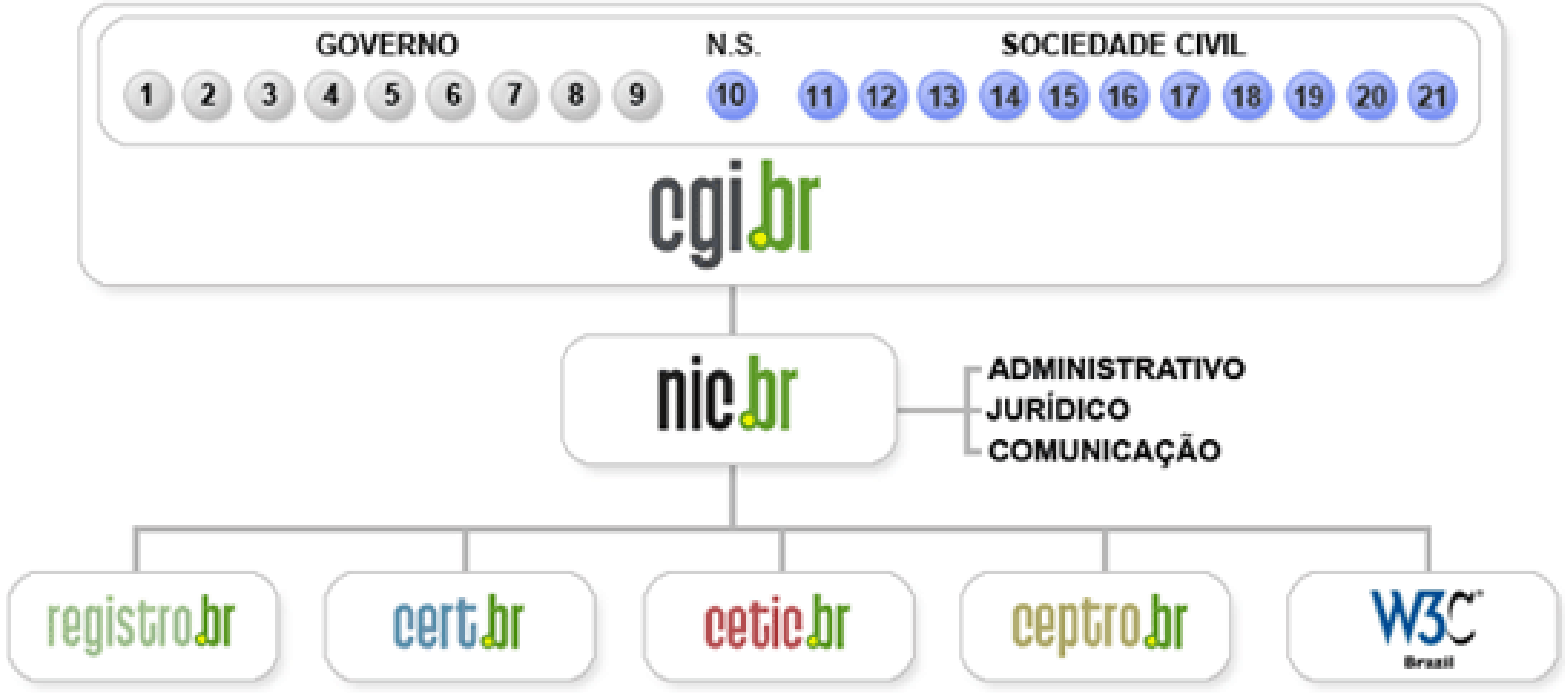
Reflexões Sobre o Brasil e o Cenário Mundial de *Spam*

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

Estrutura do CGI.br



01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério do Planejamento, Orçamento e Gestão
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério da Defesa
07- Agência Nacional de Telecomunicações
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

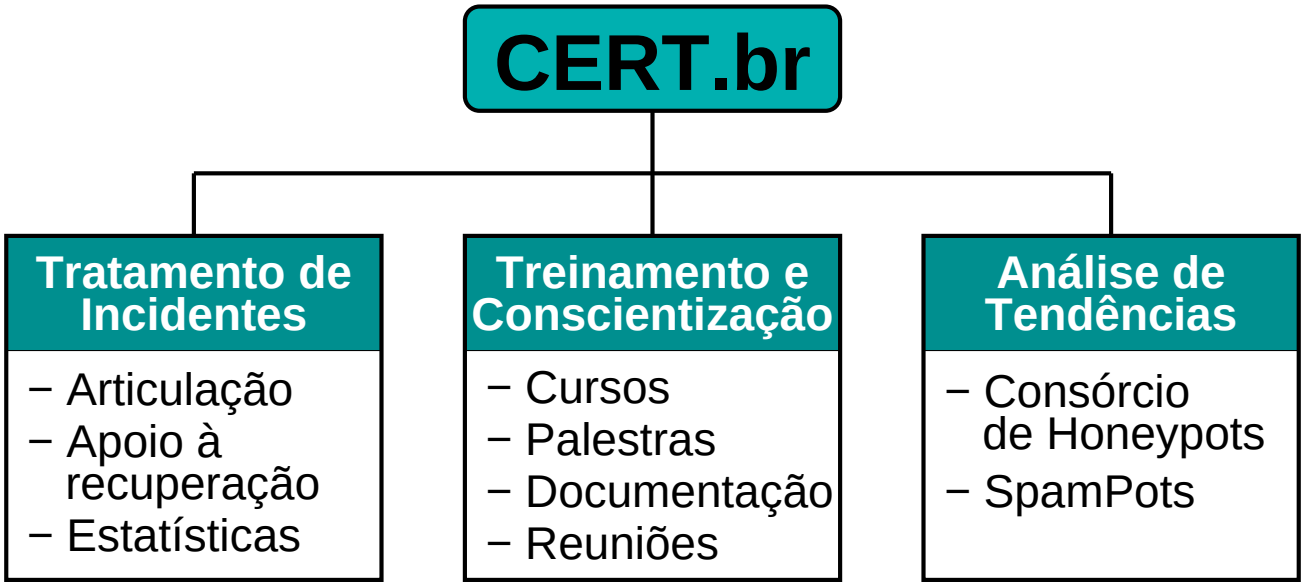
Atribuições do CGI.br

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**

Sobre o CERT.br

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



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEIPartner CERT Courses

The Honeynet PROJECT®

http://www.cert.br/missao.html

Agenda

Cenário do Spam no Brasil

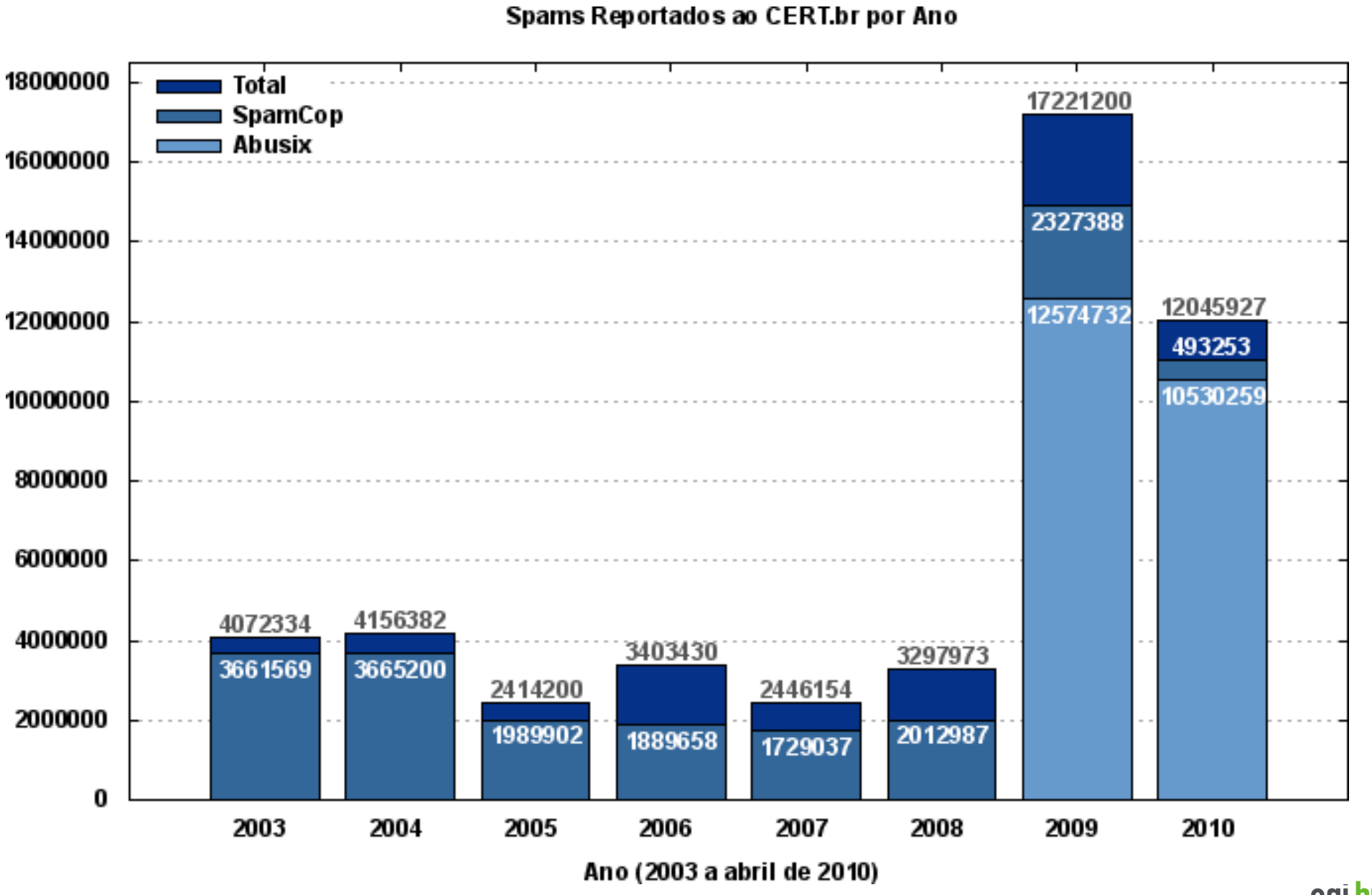
Percepção por Parte de outros Países

Ações para Redução do Problema

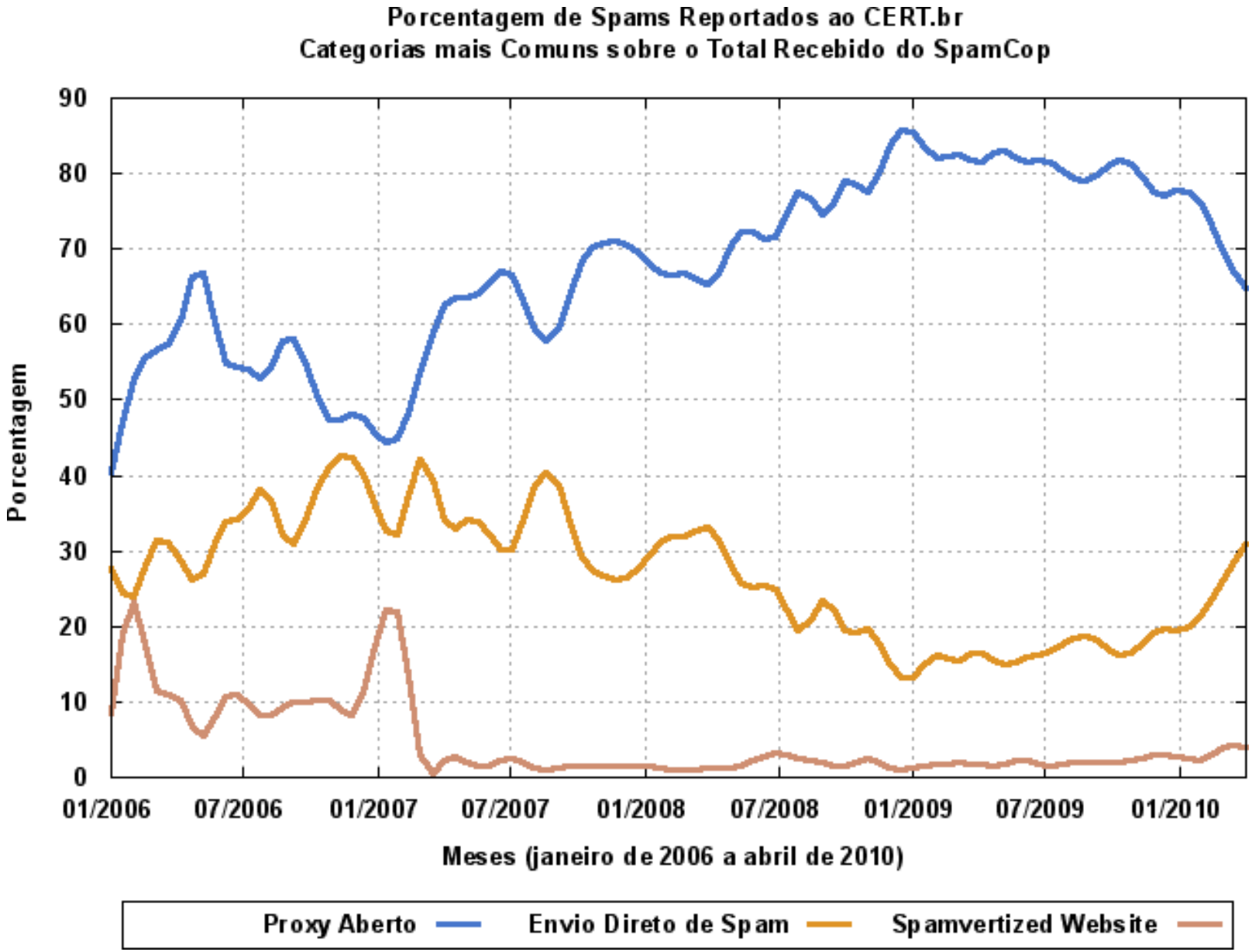
Referências

Cenário do *Spam* no Brasil

Reclamações ao CERT.br 2003–2010



Abuso de *Proxies* e Envio por PCs Infectados



Resultados da 1ª Fase 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/

Percepção por Parte de outros Países

Brasil na CBL

Country Codes com maior número de IPs listados

CC	Total	%	Rank
IN	1.235.078	15.53	1
BR	711.040	8.94	2
VN	422.260	5.31	3
DE	363.145	4.57	4
RU	332.186	4.18	5
US	269.585	3.39	6
UA	255.967	3.22	7
IT	248.211	3.12	8
SA	227.599	2.86	9
CO	193.187	2.43	10

Domínios (reverso) com maior número de IPs listados

Domínio	Total	%	Rank
telebahia.net.br	220.910	2.78	4
brasiltelecom.net.br	123.168	1.55	8
telesp.com.br	115.159	1.45	10
netservicos.com.br	51.419	0.65	33
ig.com.br	50.297	0.63	34
telet.com.br	44.034	0.55	39
gvt.net.br	41.413	0.52	43
ctbctelecom.net.br	12.541	0.16	110
timbrasil.com.br	11.573	0.15	122
canbrasnet.com.br	10.562	0.13	133

Dados gerados em: `Wed May 12 16:53:14 2010 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.***

"It's clear that Internet service providers in ***developed nations are making great strides in combating spam,****" said Russell Smoak, director of technical support for Cisco. "****That knowledge needs to be shared*** *with their counterparts in emerging economies,* ***so that these growing countries can avoid the problems associated with high levels of botnets and their related spam*** *– including reduced productivity and increased threats of crime."*

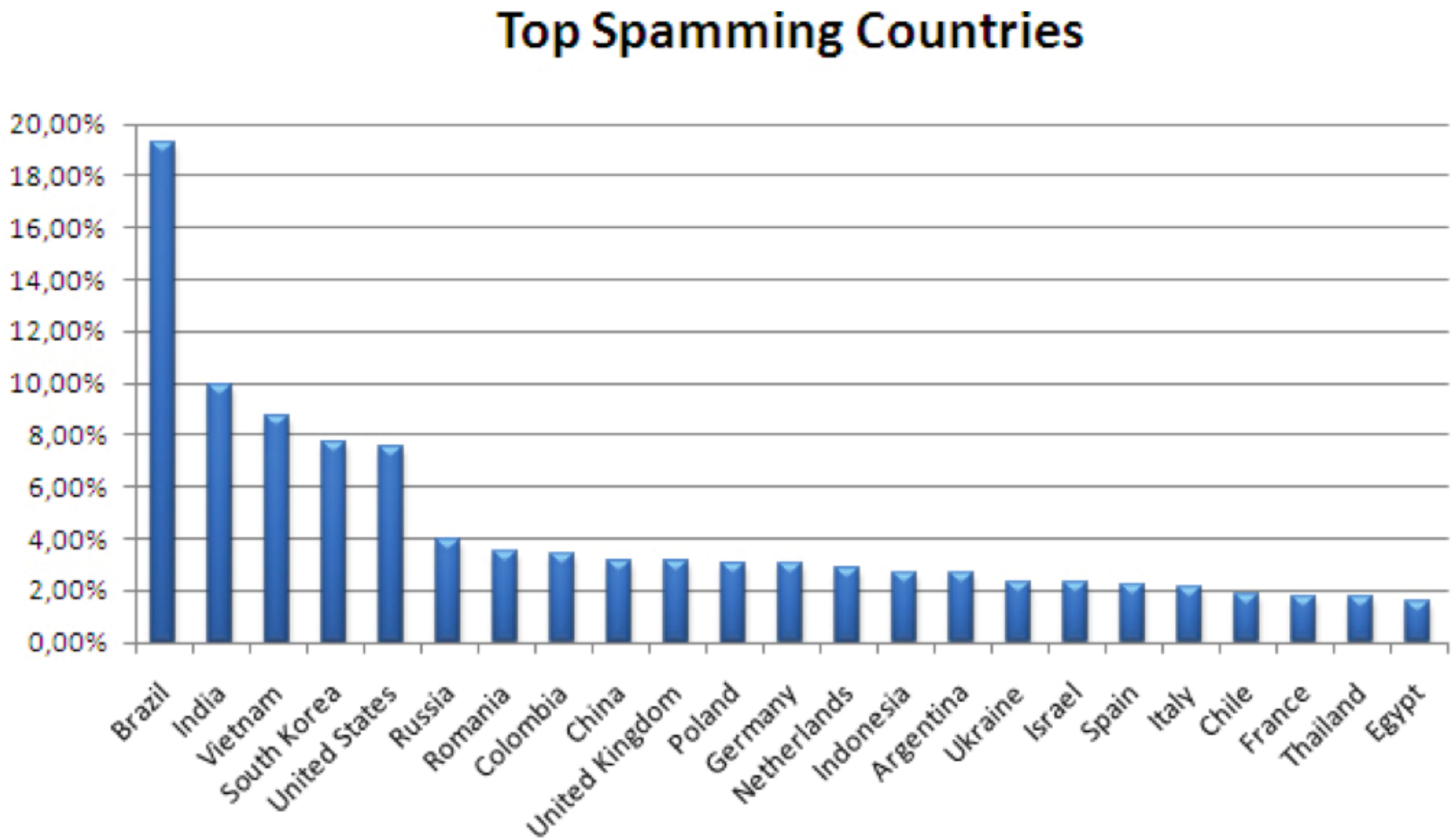
http://www.cisco.com/go/securityreport

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 (Jan-Mar 2010)

Brazil is by far the most important source of spam, accounting for some 20% of the total.



http://pandalabs.pandasecurity.com/pandalabs-quarterly-report-q1-2010/

Sophos Dirty Dozen

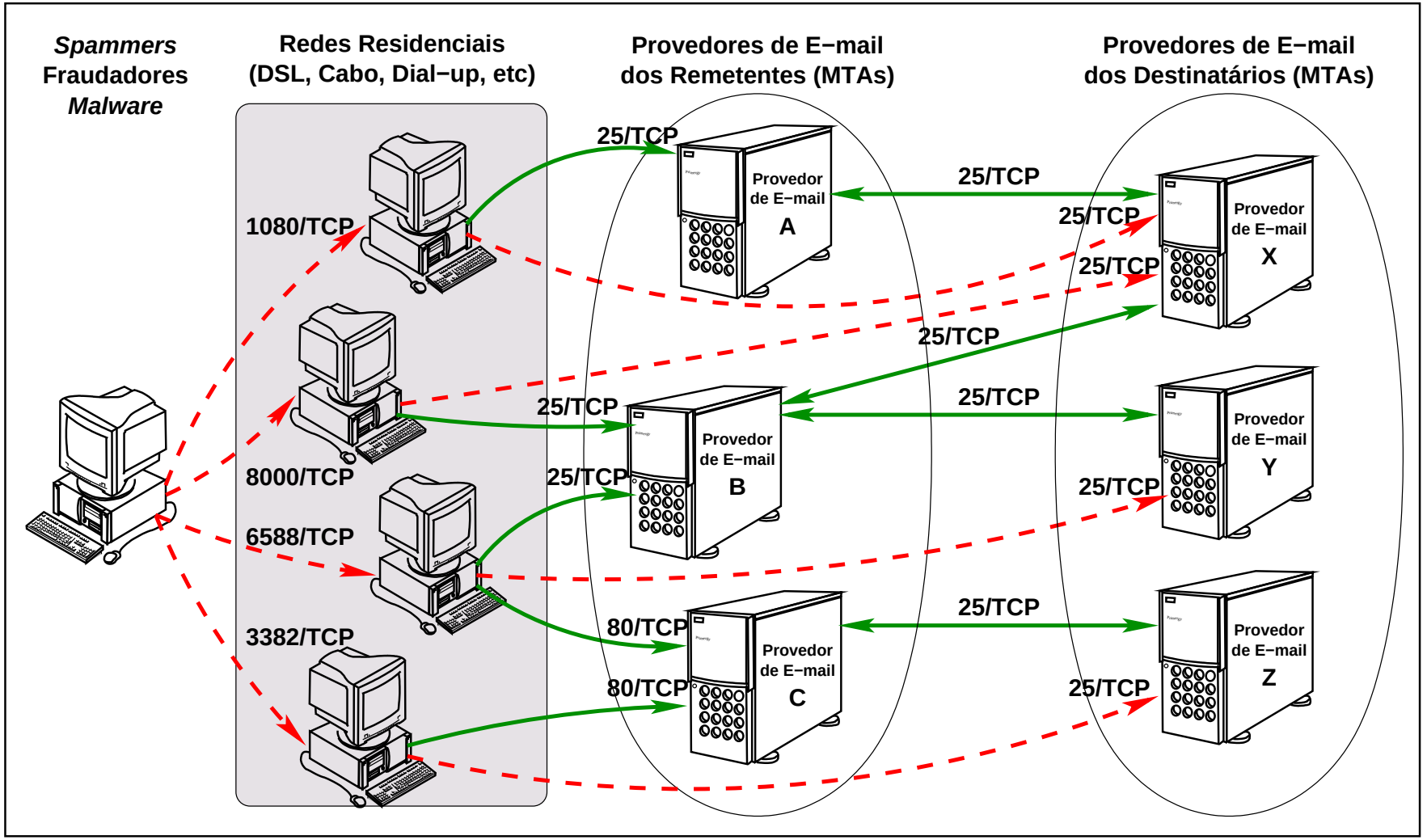
"A new dirty 'gang of four' - South Korea, Brazil, India and their ringleader USA - account for over 30% of all the spam relayed by hacked computers around the globe."

The top twelve spam relaying countries for January to March 2010

1.	USA	13.1%
2.	India	7.3%
3.	Brazil	6.8%
4.	S Korea	4.8%
5.	Vietnam	3.4%
6.	Germany	3.2%
=9.	United Kingdom	3.1%
=9.	Russia	3.1%
=9.	Italy	3.1%
10.	France	3.0%
11.	Romania	2.5%
12.	Poland	2.4%
Others		47.3%

http://www.sophos.com/pressoffice/news/articles/2010/04/dirty-dozen.html

Qual o Problema que nos Coloca Nessa Posição



Ações para Redução do Problema

Possíveis Cursos de Ação

Legislação e autorregulamentação

- delimitam o que é aceitável ou não

Filtros, blacklists, DKIM, reputação de e-mails em geral

- ajudam o destinatário a separar o *spam* dos *e-mails* legítimos
- problemas: o e-mail legítimo compete com o *spam*, banda já foi consumida, demanda custos com hardware, software, pessoal e tempo de profissionais e usuários

Técnicas para impedir que o spam deixe as redes de origem

- principal técnica: Gerência de Porta 25

Gerência de Porta 25

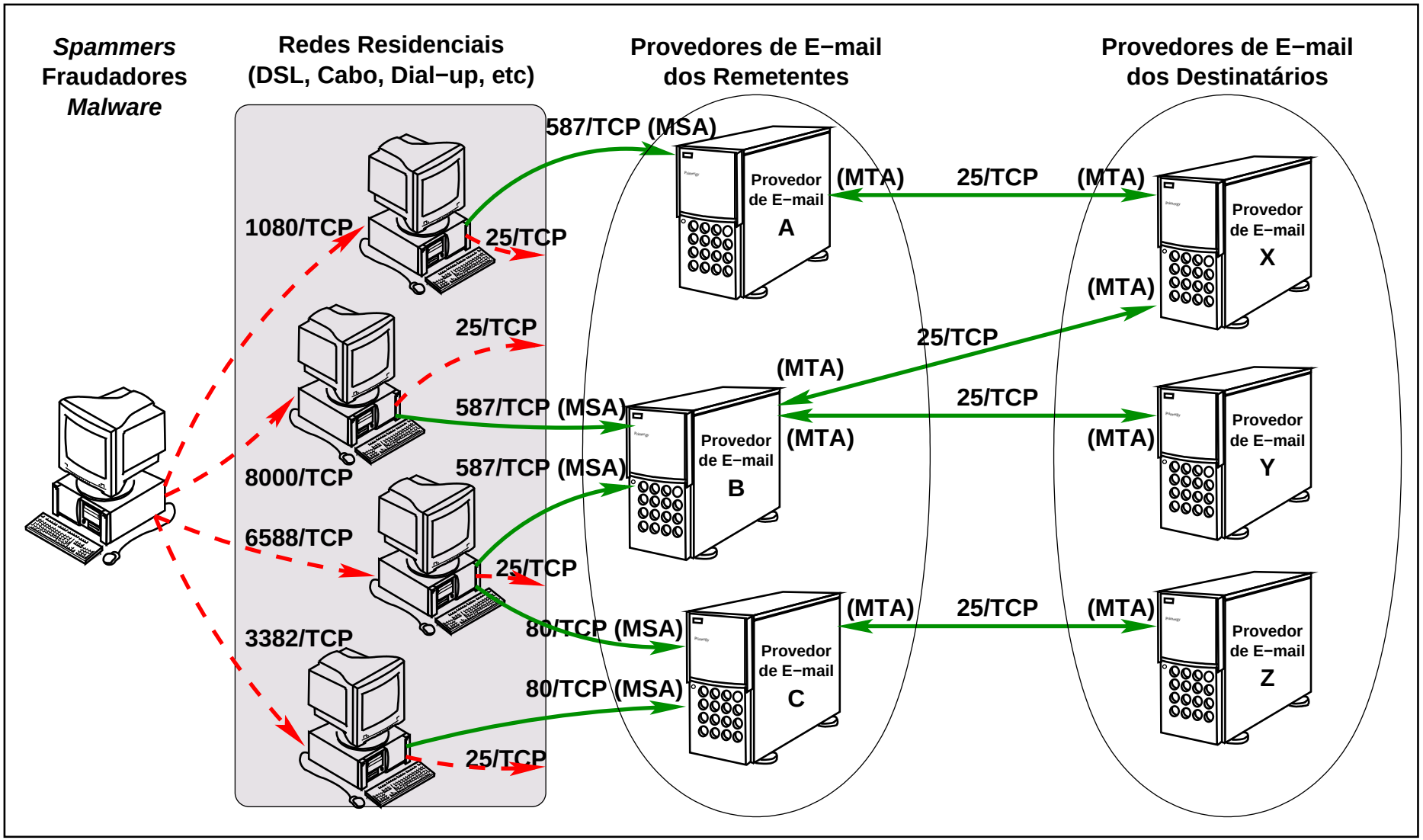
Diferenciar a submissão de *e-mails* do cliente para o servidor, da transmissão de *e-mails* entre servidores.

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

Estado da Implementação no Brasil e no Mundo

Algumas Ações Internacionais

- 2000: Earthlink (EUA)

  http://www.broadbandreports.com/shownews/492

- 2004: Comcast (EUA) – à época com com 5.7 milhões de usuários, passou a barrar 700 milhões de spams por dia
  The Only Good Spam Comes from Hormel

  http://www.usenix.org/publications/login/2005-02/openpdfs/motd.pdf

- 2006: Japão – ação colaborativa levou à implementação por todos os grandes provedores de banda larga residencial
  - isto levou à saída do Japão da lista dos "*Dirty dozen*"

    http://jeag.jp/

- Lista completa em:

  http://antispam.br/admin/porta25/adocao/

Algumas Ações no Brasil

- 2005: Tecnologias e Políticas para Combate ao Spam.
  http://www.cert.br/docs/ct-spam/ct-spam-tecnologias-politicas.pdf
- 2006: Sercomtel – implementação, seguindo as recomendações da CT-Spam do CGI.br
  http://gter.nic.br/reunioes/gter-23/programa/
- 2008: Início das reuniões mensais do Grupo de Gerência de Porta 25 da CT-Spam
- 2009: CGI.br/RES/2009/001/P – Recomendação para a Adoção de Gerência de Porta 25 em Redes de Caráter Residencial
  http://www.cgi.br/regulamentacao/resolucao2009-001.htm
- 2009: InternetSul – definiu outubro como a data para migração dos usuários de seus associados e criou um selo
  http://www.internetsul.org.br/portal/porta25.php
- 2010: UOL iniciou uma grande campanha e a migração dos usuários de e-mail

Algumas Ações no Brasil (cont.)

- 2010: Ofício da Presidência da Anatel apoiando a recomendação do CGI.br

ANATEL Agência Nacional de Telecomunicações
SAUS Quadra 6 – Bloco H – Brasília/DF – CEP: 70.070-940
Te.: (61) 2312-2004 e Fax: (61) 2312-2202
http://www.anatel.gov.br

Ofício nº 195/2010-PR-ANATEL

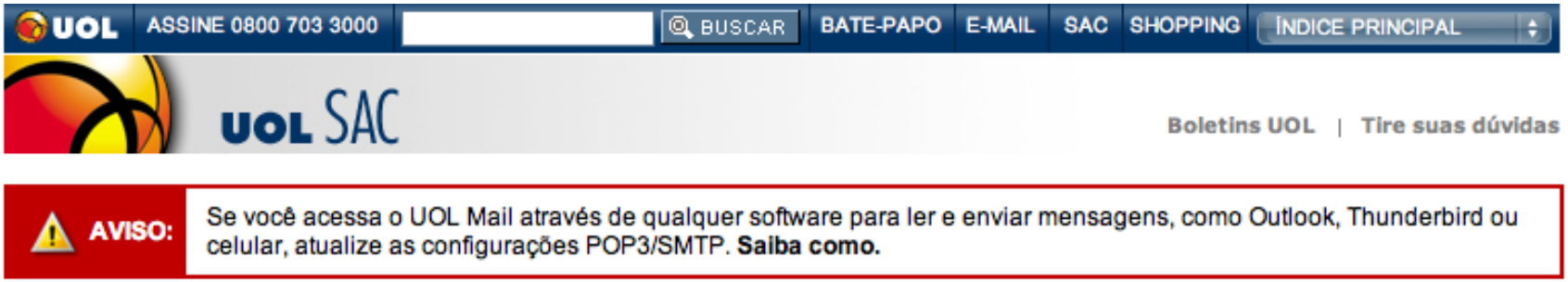
Brasília, 4 de março de 2010.

Assunto: **Combate ao *Spam* na Internet brasileira – Gerência de Porta 25/TCP**

1. A Anatel, com o objetivo de cooperar com as atividades desenvolvidas por essa instituição, vem reforçar seu apoio às iniciativas conduzidas pelo Comitê Gestor da Internet no Brasil (CGI.Br) no combate ao *spam*, em especial com o projeto que visa à implantação da Gerência de Porta 25/TCP em redes de caráter residencial.

Estudo de Caso: UOL

- Campanha realizada e migração da maioria dos usuários de e-mail em 11 de janeiro de 2010
- Releases na mídia, mudanças estimuladas via help-desk
- Chamada na primeira página do SAC



- E-mail enviado a todos os usuários legados que ainda conectam na Porta 25/TCP
  - no momento de cada autenticação, a mensagem é disparada para usuário

E-mail Recebido se Submeter via Porta 25 no UOL

De: Equipe UOL [mailto:equipeuol@uol.com.br]
Assunto: UOL Mail: Atualize suas configurações de POP3/SMTP.

Atenção para as novas configurações de softwares gerenciadores de e-mail

Este comunicado foi gerado automaticamente. O UOL detectou que seu programa gerenciador de e-mails está configurado de forma inadequada.

Por favor, atualize seu software com as informações a seguir para garantir que suas mensagens cheguem corretamente aos destinatários.
Caso tenha dúvidas, consulte os tutoriais para POP3 e IMAP clicando em "Configurações" na página de ajuda do e-mail (http://email.uol.com.br) ou entre em contato com UOL SAC pelos telefones 4003-2002 ou 0800-7717774.

Servidor de SMTP: smtps.uol.com.br
Porta de SMTP: 587
Requer conexão segura: sim
Meu servidor requer autenticação: sim

Servidor de POP3: pop3.uol.com.br
Porta de POP3: 995
Requer conexão segura: sim

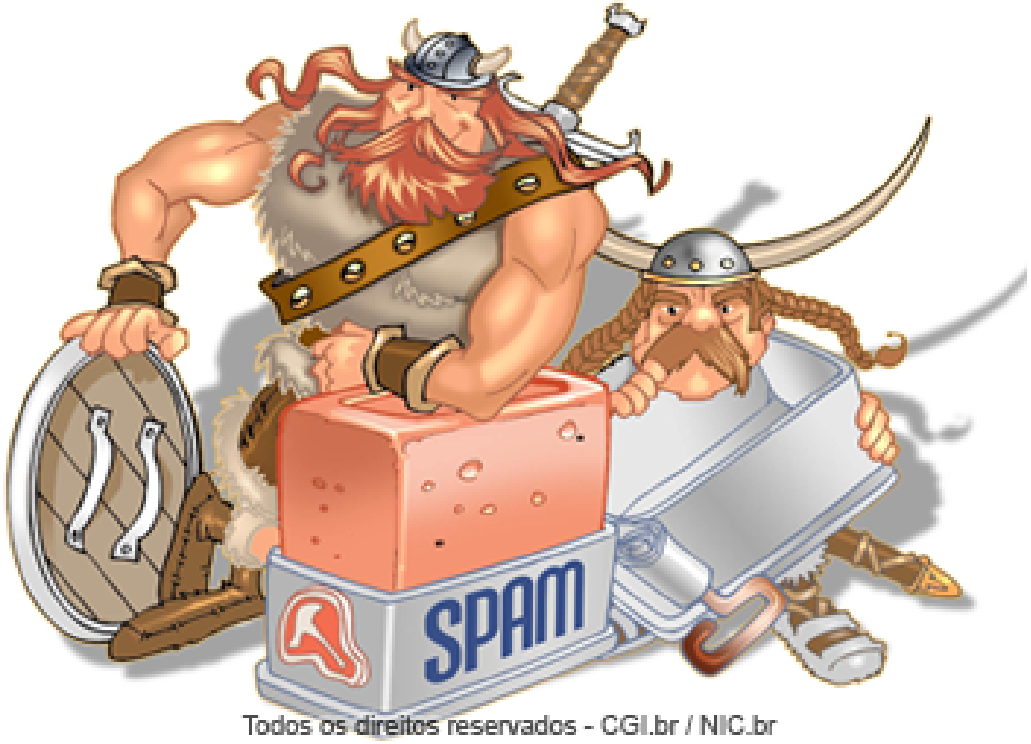
O objetivo da mudança é aprimorar o combate a spams e evitar a propagação de vírus por e-mails, conforme acordo com o Comitê Gestor da Internet e práticas internacionais de segurança.
Assinantes que enviam e recebem mensagens pelo webmail do UOL (recomendado) não precisam alterar nenhuma configuração no computador.

Equipe UOL

Referências

- Gerência de Porta 25
  http://antispam.br/admin/porta25/
- Resultados Preliminares da Primeira Fase do Projeto SpamPots
  http://www.cert.br/docs/whitepapers/spampots/
- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- Núcleo de Informação e Coordenação do Ponto br – NIC.br
  http://www.cgi.br/
- Centro de Estudo, Resposta e Tratamento de Incidentes no Brasil – CERT.br
  http://www.cert.br/

Perguntas?



"*The Only Good Spam Comes from Hormel*"
– Rob Kolstad