SPAM

Questões técnicas e "netizenship"

Hermann Wecke
hermann@abuse.net

O histórico do SPAM

- A primeira RFC a tratar do SPAM foi em Nov 1975 – RFC 706 “On the Junk Mail Problem”, escrita por Jon Postel
- Ago/93 – Pesquisa acadêmica (William Milheim – Penn State University)
- Abr/94 – Green Card Lottery, postada por dois advogados em mais de 6 mil grupos de discussão
- Jul/95 – Jeff “Spam King” Slaton, vendedor das páginas amarelas no Novo México oferecendo os segredos da Bomba Atômica e serviço de SPAM. Pioneiro nas técnicas ainda usada pelos spammers atuais
- Outono/96 – Spamford Wallace/CyberPromotions. Após uma longa batalha judicial, anunciou sua “aposentadoria” em 13/abr/98

O SPAM é uma forma perversa de propaganda, pois

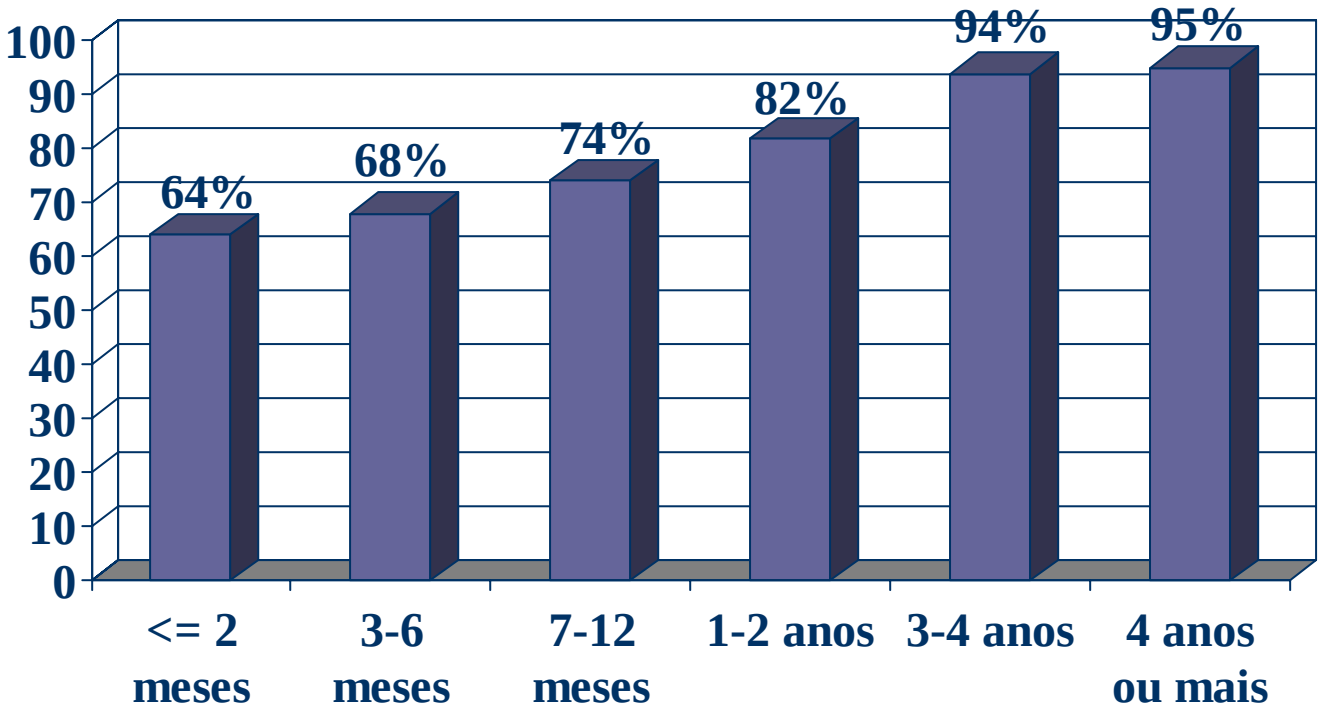
transfere todos os custos para quem o recebe.

Questões legais envolvendo o SPAM

- SPAM geralmente é crime (artigo 299 do CPB - falsidade ideológica)
- Princípio constitucional
- Prática comercial abusiva (artigo 39 do CDC)
- Transmissão onerosa ou gratuita das mailing lists só mediante autorização ou prévia comunicação (artigo 43 e §§1º e 2º do CDC)
- Decisão recente de uma juíza (Rosângela Lieko Kato), de Campo Grande/MS
- Projeto de Lei 6210/02 do deputado Ivan Paixão (PPS-SE)

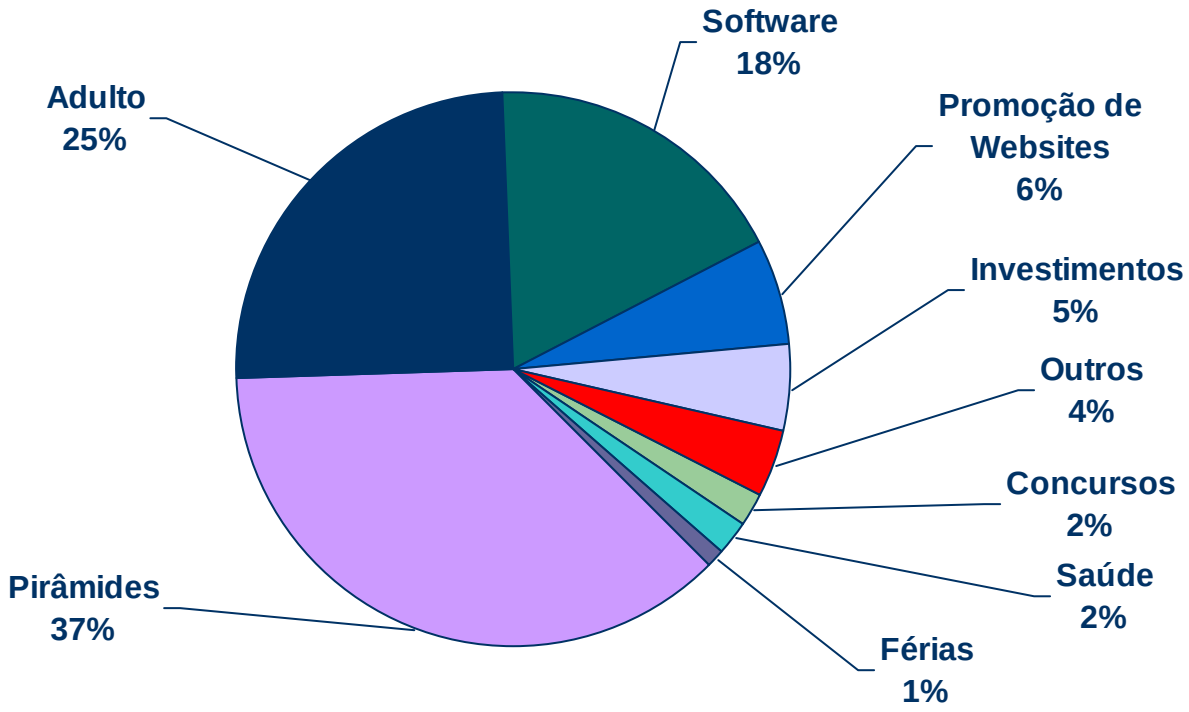
Tempo como cliente X SPAM

95% dos clientes antigos de um ISP são alvo de SPAM



Fonte: Gartner Group

Divisão por tipo de SPAM



Fonte: Gartner Group

Média de SPAMs Recebidos por Semana

Número médio de SPAMs	Respostas – em %
Nenhum	9
1-5	40
6-10	20
11-20	17
21-35	9
36-50	3
51-100	1
100 ou mais	1

Fonte: Gartner Group

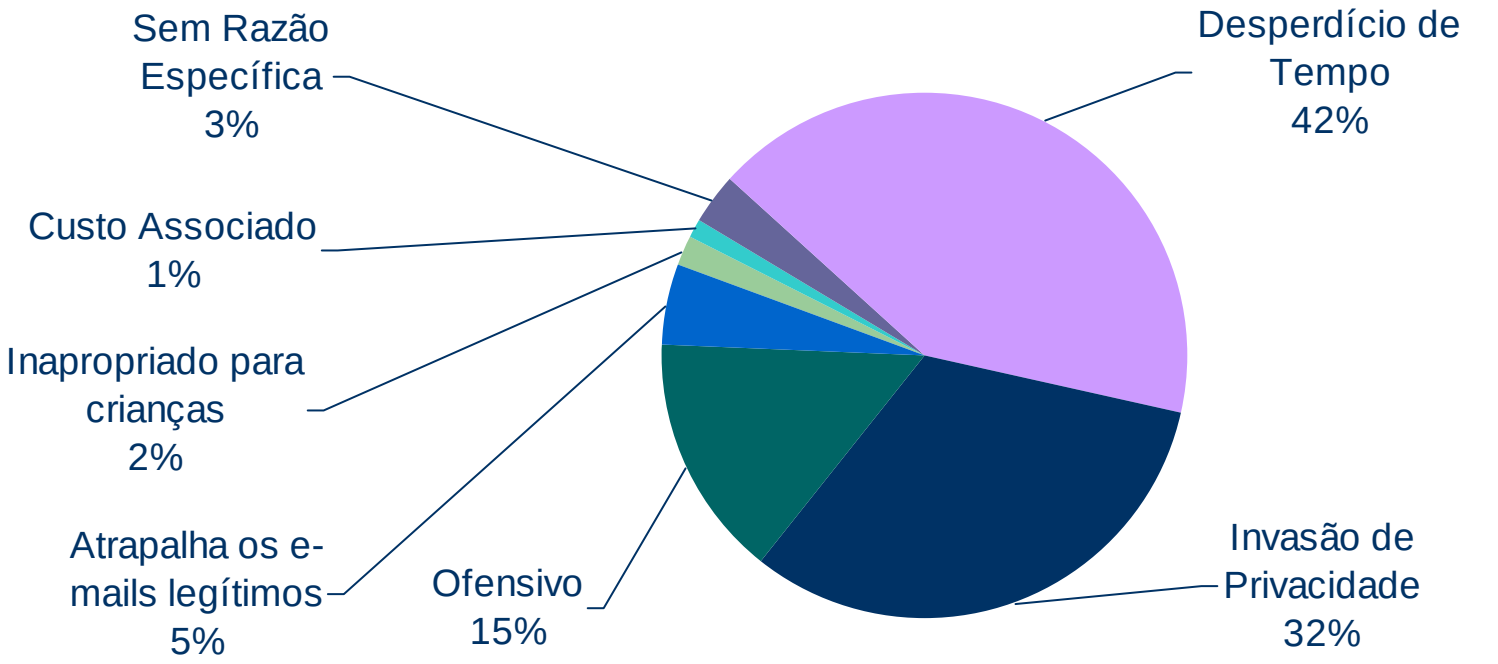
Sentimento dos Clientes em Relação ao SPAM

Sentimento em relação ao SPAM	% das Respostas
Gosta Bastante	1
Gosta um pouco	2
Neutro (nem gosta nem odeia)	14
Não gosta um pouco	20
Odeia	63

Fonte: Gartner Group

A tolerância ao SPAM é inversamente proporcional à quantidade de mensagens recebidas.

Motivos Alegados pelo cliente para não gostar do SPAM



Fonte: Gartner Group

20 Maiores "Contos do Vigário" na Net

- Web cramming
- Roubo de Identidade
- Fraudes relacionadas ao dia 11 de Setembro
- Trabalhe em Casa
- Fraude no Cartão de Crédito
- Tratamentos Médicos e Perda de Peso
- Correntes/Pirâmides
- MMP (Multilevel Marketing Plans – comprar produtos para depois tentar revender)
- Amostras Grátis
- Produtos contra o Bioterrorismo
- Empréstimo Pessoal
- Registro de Domínios
- Recuperação de Crédito
- Promoção de Pacotes de Férias
- Sobra de Caixa do Governo (CFR 4-1-9) – Esquema da Nigéria
- Loteria Internacional
- Oportunidade de Negócios (seja seu próprio patrão)
- Bulk E-Mail (faça seu próprio SPAM)
- Fraudes em Leilões Online
- Ligação Internacional via modem

Fonte: Yahoo!Internet Life, março/2002

Métodos de Entrega

- DIRECT DELIVERY
- RELAY AUTORIZADO
- OPEN RELAY
- OPEN PROXY

Métodos de Filtragem

- IP
- REVERSO
- REMETENTE
- DOMÍNIO
- CIDR
- ANÁLISE DE CONTEÚDO

Métodos de Filtragem

IP

IP individual, baseado em investigação/denúncias/spamtraps

Reverso

Alguns provedores solicitam explicitamente que seu reverso seja bloqueado.
Como exemplo disso temos:
brdterra.com.br
dial-up.vento.com.br
p001.terra.com.br

Outros alocam o reverso de forma a "facilitar" a vida de quem quer bloquear, mesmo que inconscientemente:
in-addr.arpa.ig.com.br
xdsl-dinamico.ctbcnetsuper.com.br

Lista completa em:
http://www.spambr.org/bloqueio.php3

Métodos de Filtragem

Remetente

Bloqueio individual, baseado em incidentes anteriores

brdivulgacao_1@hotmail.com	brdivulgacao1@hotmail.com	brdivulgaco_1@hotmail.com
brdivulgacao_2@hotmail.com	brdivulgacao2@hotmail.com	brdivulgaco_2@hotmail.com
brdivulgacao_3@hotmail.com	brdivulgacao3@hotmail.com	brdivulgaco_3@hotmail.com
ina_training_01@hotmail.com	ina_training_1@hotmail.com	inna_trainning1@hotmail.com
ina_training_02@hotmail.com	ina_training_2@hotmail.com	inna_trainning2@hotmail.com
ina_training_03@hotmail.com	ina_training_3@hotmail.com	inna_trainning3@hotmail.com

Domínio

Aplicado somente contra spammers insistentes

CIDR

Bloqueio específico contra faixas de dial-up ou origens não aceitas

Ex. 200.151/16 200.227/16

Métodos de Filtragem

Conteúdo

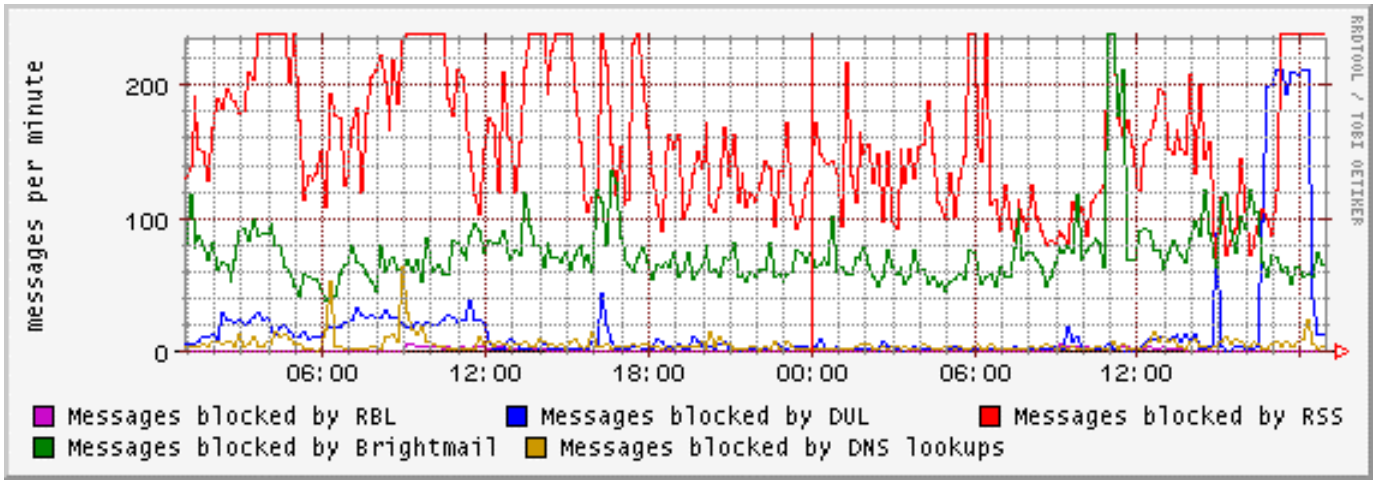
- DCC – Distributed Checksum Clearinghouse (MAPS)
- Vipul's Razor
- Baseado em padrões conhecidos

Esta mensagem é enviada em concordância com a legislação internacional sobre o Correio Eletrônico, Seção 301, Parágrafo (a) (3) (c) Decreto S 1618, Título Terceiro aprovado pelo 105º Congresso Base das Normativas Internacionais sobre o SPAM. Um e-mail não poderá ser considerado SPAM quando incluir uma forma de ser removido. Para evitar futuras mensagens deste "site", simplesmente responda este e-mail colocando na linha de assunto: REMOVER.

Para maiores informações sobre o "Decreto do Congresso Mundial dos Spammers Brasileiros", visite http://www.antispam.org.br/congresso.html

Listas de bloqueio existentes

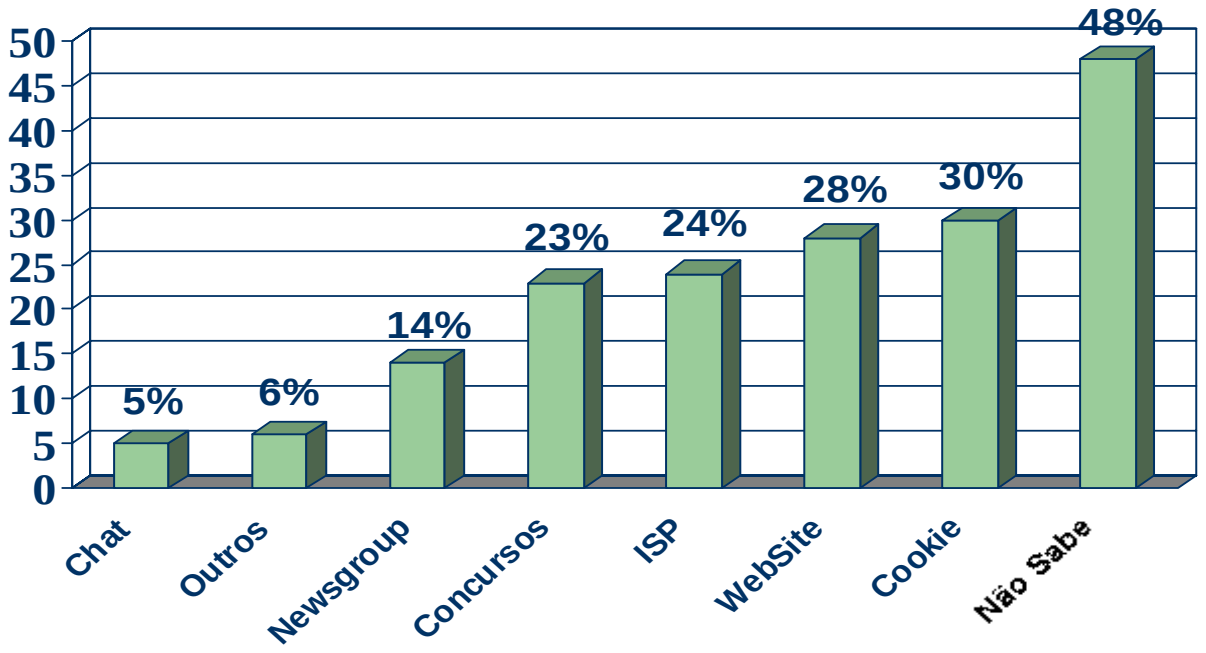
- Open relay (RSS, ORDB, Visi)
- Open proxy (Monkeys)
- Dial-ups (SPAMBR, DUL)
- SPAM Source (SpamCOP)
- Lista de discussão com inscrição insegura (NML)
- Lista da incompetência (RBL)
- Análise múltipla (BrightMail, MessageLabs)



Problemas causados pelo SPAM para o provedor e para o usuário final

- Provedor
- Usuário Final

Como os spammers conseguem os e-mails, na opinião dos usuários (múltipla escolha)



Fonte: Gartner Group

Como não gerar mais spam involuntariamente (open relays, controle de dispatchers SMTP)

- Limitar a quantidade de e-mails que seus clientes podem mandar por um determinado período de tempo
- Fazer com que os seus clientes (hospedagem/dial-up/broadband) utilizem um servidor de SMTP que não seja o mesmo definido como MX do domínio
- Forçar a autenticação do usuário para o uso do SMTP (POP antes do SMTP ou SMTP-AUTH)
- Forçar, nas conexões dial-up e broadband sob o seu controle, o uso do SMTP no provedor (bloqueio da porta 25 além dos limites do provedor)

ABUSE.net

ABUSE.NET

Proporciona uma ferramenta de cadastramento do e-mail do abuse desk para o domínio

Quem deve usar:

- Provedores
- Webhosting

Ferramenta de pesquisa WHOIS:

whois.abuse.net

whois -h whois.abuse.net dominio.tld

ou via WEB em

http://www.abuse.net/lookup.phtml

Instruções para cadastramento e atualização em

http://www.abuse.net/contact.html

Links Úteis

Network Abuse Clearinghouse - http://www.abuse.net/
MAPS - Mail Abuse and Prevention System - http://www.mail-abuse.org/
BrightMail - http://www.brightmail.com/
MessageLabs - http://www.messagelabs.com/

SpamCOP - http://www.spamcop.net/
SPAMBR - http://www.spambr.org/
Movimento AntiSPAM Brasileiro - http://www.antispam.org.br/
NIC-BR - mail-abuse@nic.br

ip4r (DNSBL-style) DNS lookups - Declude
http://www.declude.com/JunkMail/Support/ip4r.htm
Blacklists Compared - http://www.sdsc.edu/~jeff/spam/cbc.html

Como configurar o MTA para usar uma zona DNSBL:

http://www.mail-abuse.org/dul/examples.htm

Sugestões de ações

- Criar caixas postais "armadilha", com nomes comuns/fáceis (antonio, carlos, jose, marcos, maria...)
- Utilizar listas de bloqueio para proteger seus clientes
- Configurar o reverso da rede ("dial.exemplo.tld" ou "dsl.provedor.tld")
- Separar claramente os blocos dial-up de servidores
- Agrupar os IPs correspondentes ao pool de dial-up em blocos CIDR PREFERENCIALMENTE maiores que /26

Sugestões de leitura

Stopping Spam, Schwartz, Alan & Garfinkel, Simson, 1998, O'Reilly & Associates, Inc, ISBN 1-56592-388-X

RFC 2142

Mailbox Names for Common Services, Roles and Functions

http://RFC.net/rfc2142.html

http://www.cg.org.br/grupo/rfc2142.htm

abuse@ security@ postmaster@

SPAM
Questões técnicas e “netizenship”

Esta apresentação está disponível em
http://www.abuse.net/slides/gter14.html

Hermann Wecke

hermann@abuse.net