



spam

História,
Histórico e
Futuro do spam

Hermann Wecke
hermann@abuse.net

SSI 2003
Novembro/2003

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 Stat University)
 - Abr/94 – Green Card Lottery, postada por dois advogados em mais de 6 mil grupos de discussão
-

O histórico do SPAM

- 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
- spam representa 32% do total de mensagens em 2003 contra 24% em 2002 ^[1]

Como o Brasil é visto lá fora (e aqui dentro também)

- Brazil Becomes a Cybercrime Lab (New York Times, 27/Oct/2003) [2]
- Top 10 Open Proxies (telesp.net.br tem 6,9% de todos os open-proxies do mundo) [3]
- Telefônica: 1º Lugar em origem dos ataques [4]

[2] <http://www.nytimes.com/2003/10/27/technology/27hack.html>

[3] <http://darkwing.uoregon.edu/~joe/open-proxies-used-to-send-spam.html>

[4] <http://www.nbso.nic.br/stats/2003-abr-jun/top-atacantes.html>

Brazil Becomes a Cybercrime Lab

- the world's 10 most active groups of Internet vandals and criminals were Brazilian
 - this year [2003], nearly 96,000 overt Internet attacks - ones that are reported, validated or witnessed - have been traced to Brazil
 - the electronic crime division of the São Paulo police catch about 40 cybercrooks a month
 - [We] don't have the specific legislation for these crimes like they do in America and Europe
-

Top Autonomous Systems with Open Proxies

- 1° AS10429 (TELESP - Telecomunicacoes de Sao Paulo S.A., Brasil) 32.252
- 2° AS7738 (Telecomunicacoes da Bahia S.A., Bahia Brasil) 29.797 *Telemar*
- 8° AS8167 (TELESC - Telecomunicacoes de Santa Catarina SA, Santa Catarina Brasil) 19.379 *Brasil Telecom*
- 28° AS4230 (Embratel, Rio de Janeiro, Brasil) 6.712

The Top 39 Domains with Open Proxies

- 1° telesp.net.br (6.9% = 21.609 listed open proxies)
- 2° veloxzone.com.br (3.6%)
- 14° brasiltelecom.net.br (0.9%)
- 29° speedyterra.com.br (0.4%)
- 37° virtua.com.br (0.3%)
- 39° telepar.net.br (0.3% == 1.002 listed open proxies)

Picaretas do spam

- Eddy Marin – condenado por tráfico de drogas e lavagem de dinheiro – envia sozinho 50 milhões de e-mails por dia – ou 250 milhões se usar toda sua “spam gang”;
- Alan Ralsky – 9 pedidos de falência desde 1993 e perda da licença de corretor de seguros;
- Juan Garavaglia – Argentino, o representante latino-americano. Usou um servidor da BBC para enviar spam de “noivas russas”.

Fonte: WORLD'S TOP TEN SPAMMERS – MSNBC

http://www.msnbc.com/news/wld/tech/brill/Top10Spammers_dw.htm

Amigos do spam no Brasil

- Jean 'Cretinian' – vende desde kits “quero ser hacker em 1/2 hora” até a própria mãe (cliente fiel da Telefônica – adsl/dial-up)
 - Econoshop / Diar (Telefônica)
 - CD CONCURSO - CD JURIDICO (velox via open-relay/proxy – hospedado na GVT – mensagem com imagens na kit.net)
-

Jean 'Cretinian'

Date: Wed, 1 Aug 2001 01:19:11 -0300

From: mala2001w1@zipmail.com.br

Subject: Delegado tenta impedir curso de Hackerismo!?

Delegado de São Paulo, especialista por crimes praticados na Internet, disse que curso de Hackerismo ministrado no site www.cursognome.com incentiva crimes cibernéticos. De acordo com a justiça, a partir do dia 13 de agosto de 2001, o site não poderá aceitar novas matrículas para o curso "Hackerismo e Segurança". Portanto, se você ainda estiver interessado em fazer este curso, matricule-se até o dia 12 de agosto de 2001.

José dos Santos

CPF: 125.432.456-93

- [ative.pro.br](#)
- [freequote.pro.br](#)
- [getpaid.pro.br](#)
- [hollywoodshottest.pro.br](#)
- [lowermortgagepayments.pro.br](#)
- [mylarti.pro.br](#)
- [onestopshop.pro.br](#)
- [rapidwords1.pro.br](#)
- [sdjukk.pro.br](#)
- [weho.pro.br](#)



Receita Federal

Secretaria da Receita Federal

Consulta Pública ao Cadastro de Pessoas Físicas - CPF

CPF: 125.432.456-93

CPF não existe em nossa base de dados. Compareça a uma [unidade da Receita Federal](#) para regularização.

TMD Internet

CNPJ 54.258.741/0001-04

- 15minmiracle.com.br
- bizland.com.br
- enhanceyourlife.com.br
- fasteffect.com.br
- financebiz.com.br
- financeland.com.br
- finances.com.br
- financetotal.com.br
- getithard.com.br
- greatsensation.com.br
- landofbiz.com.br
- quickresults.com.br
- tfinan.com.br
- totalfreedom.com.br
- yourchoice.com.br
- yourfinances.com.br

Contribuinte,

Número do CNPJ: 54258741000104

Não existe no Cadastro de Pessoas Jurídicas o número de CNPJ informado. Verifique se o mesmo foi digitado corretamente.

Consulta realizada em 03/11/2003 às 01:03:34

spam é crime?

O spam não é, em si, um crime. O que o transforma em conduta criminosa é o envio de mensagens com o uso de falsificação e roubo de identidade.

Eliot Spitzer
promotor-geral do Estado de Nova York

Futuro do spam - I

- Fuga do padrão (evitar filtros)

,Expa""nd y*ou*r MA-"NH-O'OD^‘

-':.B,O0'S,T "D:I'CK` _S-I^ZE"" _^,

-,^B^O^0`ST" ^D`IC;K` _S_I`Z-E`*`

;. *P:R`0;VEN` -T0: :E*N_HAN'CE P;EN_I,S":;^

easy-to-use solution - V:AGRA rocks

Ge.ne.ri.c V1A.GRA

V\$ Viagra for Less

Vi@agra for Less

V|rg|n sch00lg|rls get their very f|rst d|(ks ever

Futuro do spam - 2

- Eric Allman, da Sendmail, diz que o “Spam provocará a morte do e-mail”
(WebWorld 28/Jun/2002) [6]
- Mail From Brazil Isn't Welcome Here
(Internet.com – 18/Out/2002) [7]
- Uma grande BBS chamada Internet Brasil
(brazil.blackholes.us)

[6] <http://idgnow.terra.com.br/webworld/namidia/2002/06/0134>

[7] http://www.isp-planet.com/technology/2002/brazil_bol.html

Futuro do spam - 3

- Intensificação do uso de open-proxies
- Spam e Instant Messaging ameaçam utilidade do e-mail. IDC estima que em 2006, 20 bilhões de spam/dia para 500 milhões de usuários [8]
- Brasil fortalecerá sua posição de “nova China”

O que está por trás do spam

Interesses Econômicos

- spammer contrata conexão e paga (interesse econômico por parte do provedor – “pink contract”)
 - Companhia telefônica não desconecta para inflar relatórios de desempenho para a matriz / controladora no exterior
 - Provedor garante faturamento e consumo de banda (interconexão / peering?)
-

O que está por trás do spam

As contas do spammer

- Spammer não quer retorno (de e-mails – usa remetente falso = *crime*)

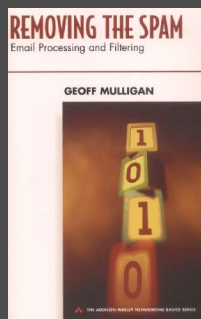
Um dia na vida do spammer:

- 50 milhões de e-mails/dia gera um retorno aproximado de 0,5% - ou 250 mil consultas/visitas/compras
 - Custo para o spammer: R\$ 267 pelo link de 2 Mb/s (R\$ 8 mil por mês)
 - Custo do produto = zero → lucro máximo (teorema de Dilbert)
-

Sugestão de Leitura



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



- Removing the Spam: Email Processing and Filtering, Geoff Mulligan, 1999, Addison Wesley Longman, Inc, ISBN 0-201-37957-0



- Internet Legal - O Direito na Tecnologia da Informação, Omar Kaminski, Juruá Editora.



spam

História,
Histórico e
Futuro do spam

Hermann Wecke
hermann@abuse.net