Aspectos de Segurança Relacionados ao Spam

Cristine Hoepers
cristine@nic.br

Klaus Steding-Jessen
jessen@nic.br

NIC BR Security Office

Brazilian Computer Emergency Response Team

Comitê Gestor da Internet no Brasil

http://www.nbso.nic.br/

Roteiro

- cenário do spam no Brasil
- spam como vetor de fraudes
- trabalho do NBSO com relação ao spam
- fatores técnicos que facilitam o spam
  - proxies abertos
  - bots
- “gangues de spam”
- formas de combate ao spam
- mitos do combate ao spam

Cenário do Spam no Brasil

Estatísticas do NBSO

Objetivos

- acompanhar o perfil do spam no Brasil
  - tipo de abuso mais cometido
  - origens dos problemas
- ajudar as redes brasileiras a direcionar os esforços
- acompanhar as mudanças (melhoras ou pioras do quadro)
- não usar os dados para blacklist

Estatísticas do NBSO (cont.)

Origem dos dados

- emails recebidos em `mail-abuse@nic.br`

Tipos de Abuso

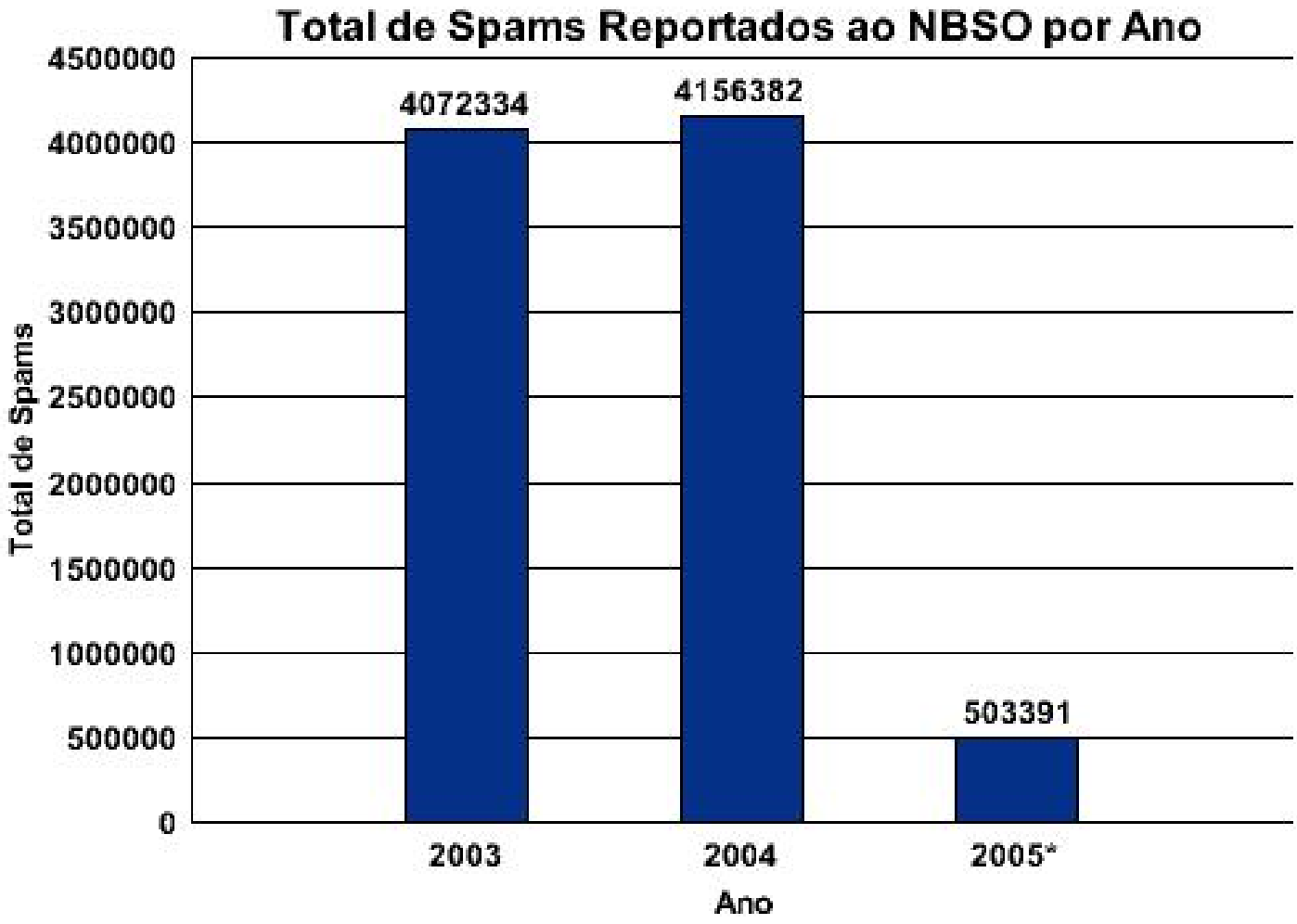
- Spamvertised Website: páginas com informações de produtos e serviços sendo oferecidos no spam
- Proxy Aberto: máquinas com serviço de proxy mal configurado, sendo abusadas
- Relay Aberto: máquinas com serviço de email mal configurado, sendo abusadas

Estatísticas do NBSO (cont.)

Tipo de Reclamação		Notificações	(%)
SpamCop	Spamvertised	57.532	28,54
	Proxy	71.116	35,28
	Relay	10	0,00
	Outras	43.196	21,43
Outras Fontes		29.747	14,76
Total		201.601	100,00

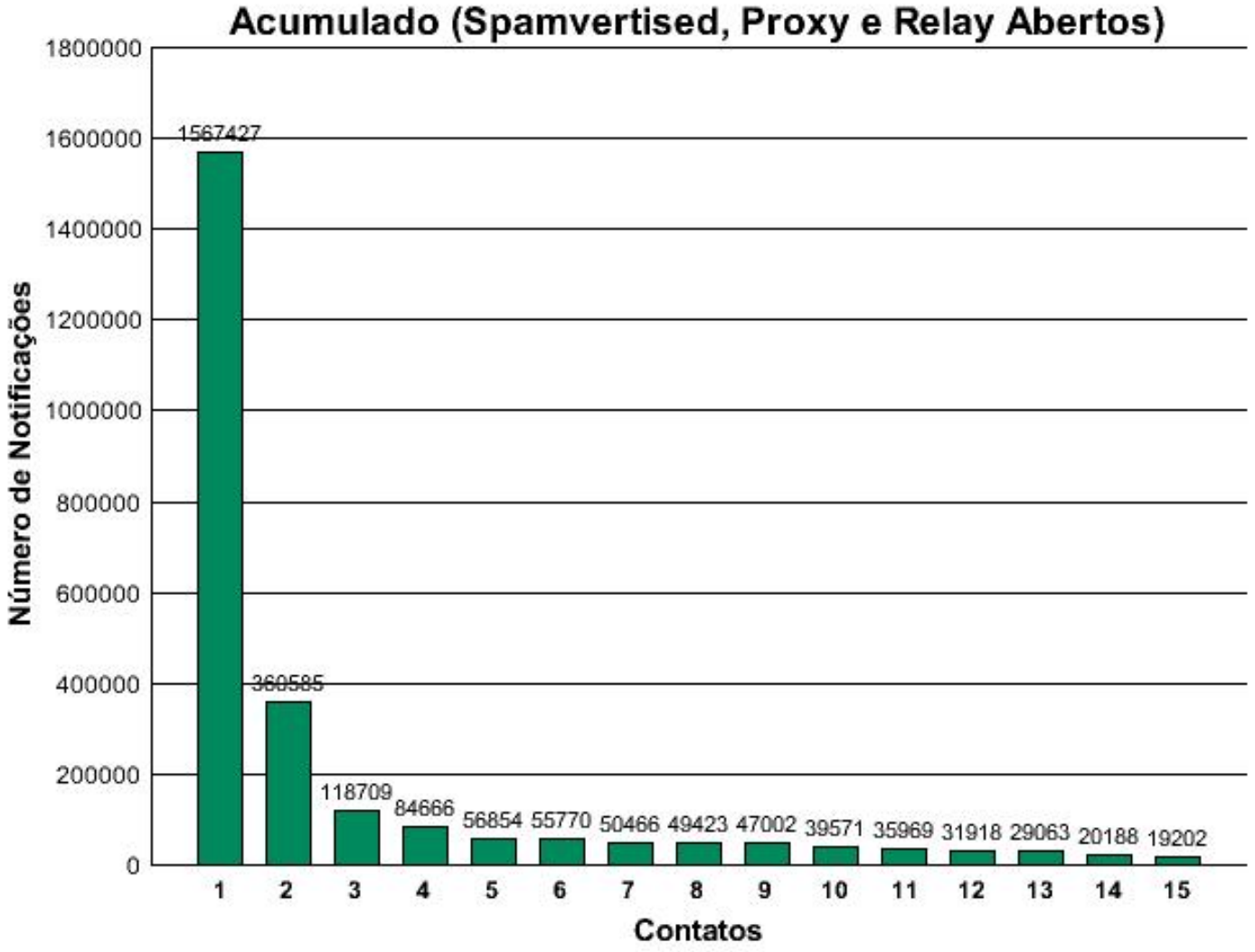
* Dados referentes a fevereiro de 2005

Estatísticas do NBSO (cont.)



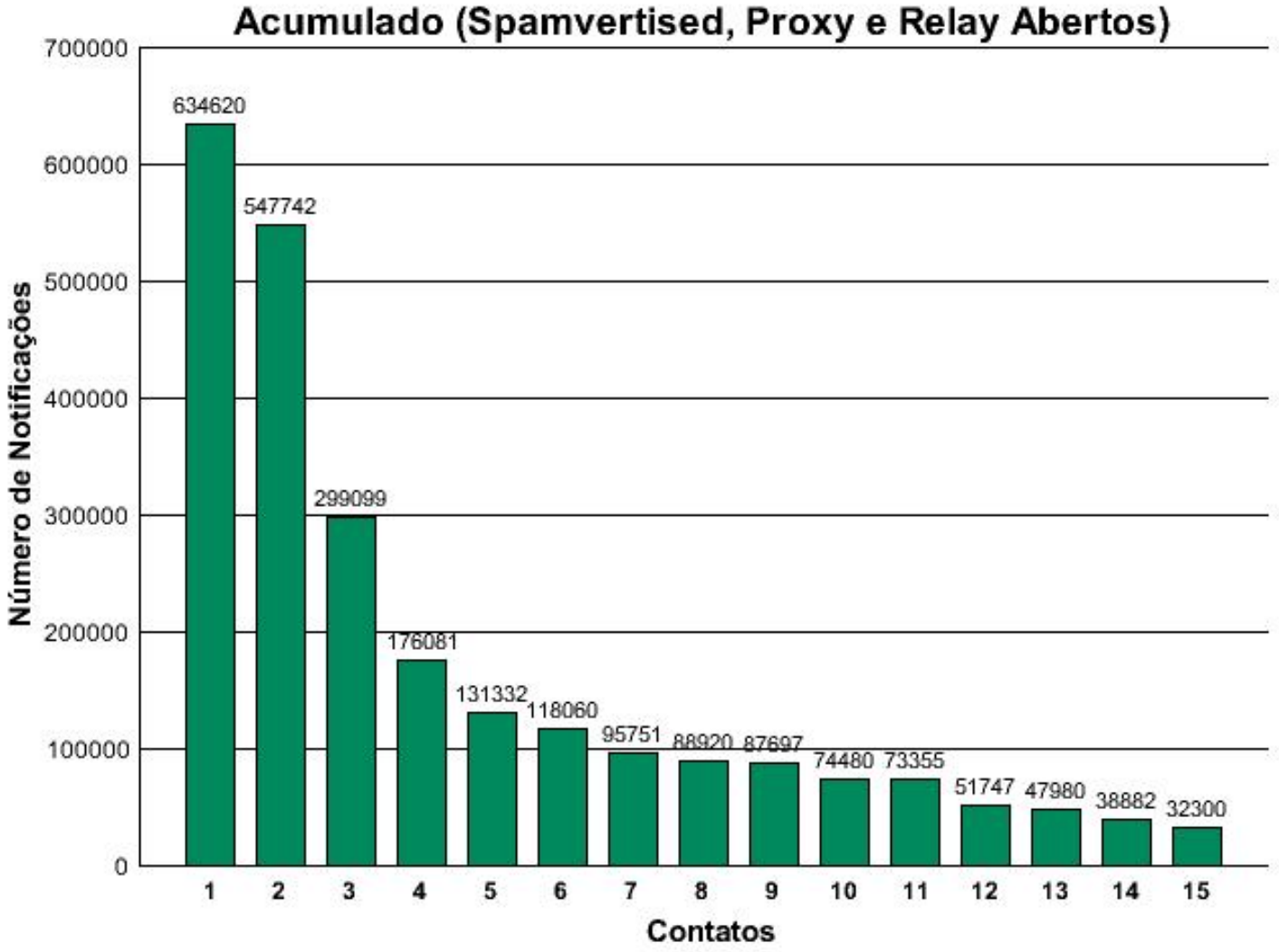
* Até fevereiro de 2005

Valores Acumulados 2003



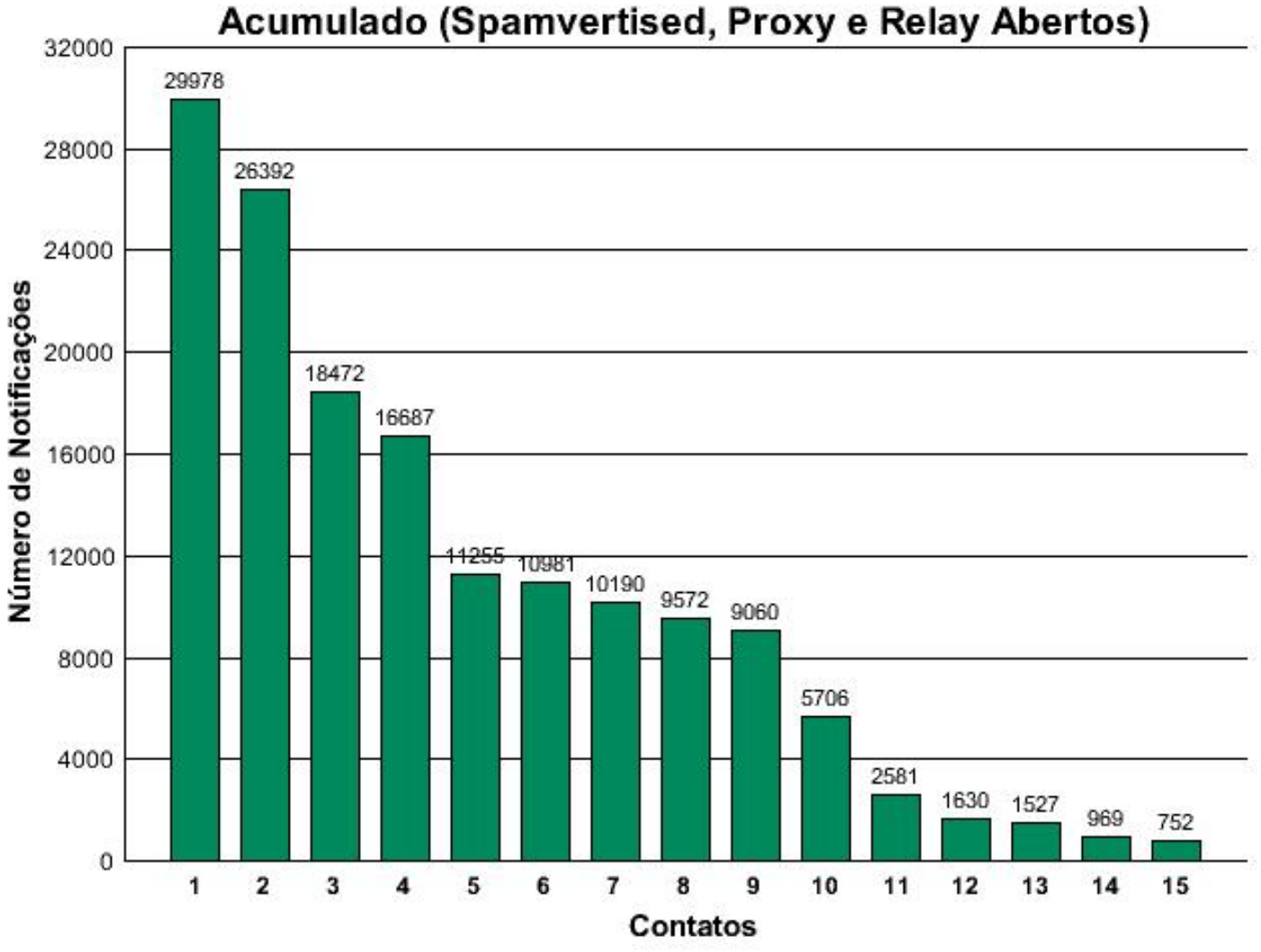
1	telefonica
2	telemar
3	brasiltelecom
4	embratel
5	ajato
6	impsat
7	tbline
8	diveo
9	tiger
10	ctbctelecom
11	comdominio
12	e-hosting
13	terra
14	globocabo
15	globo

Valores Acumulados 2004



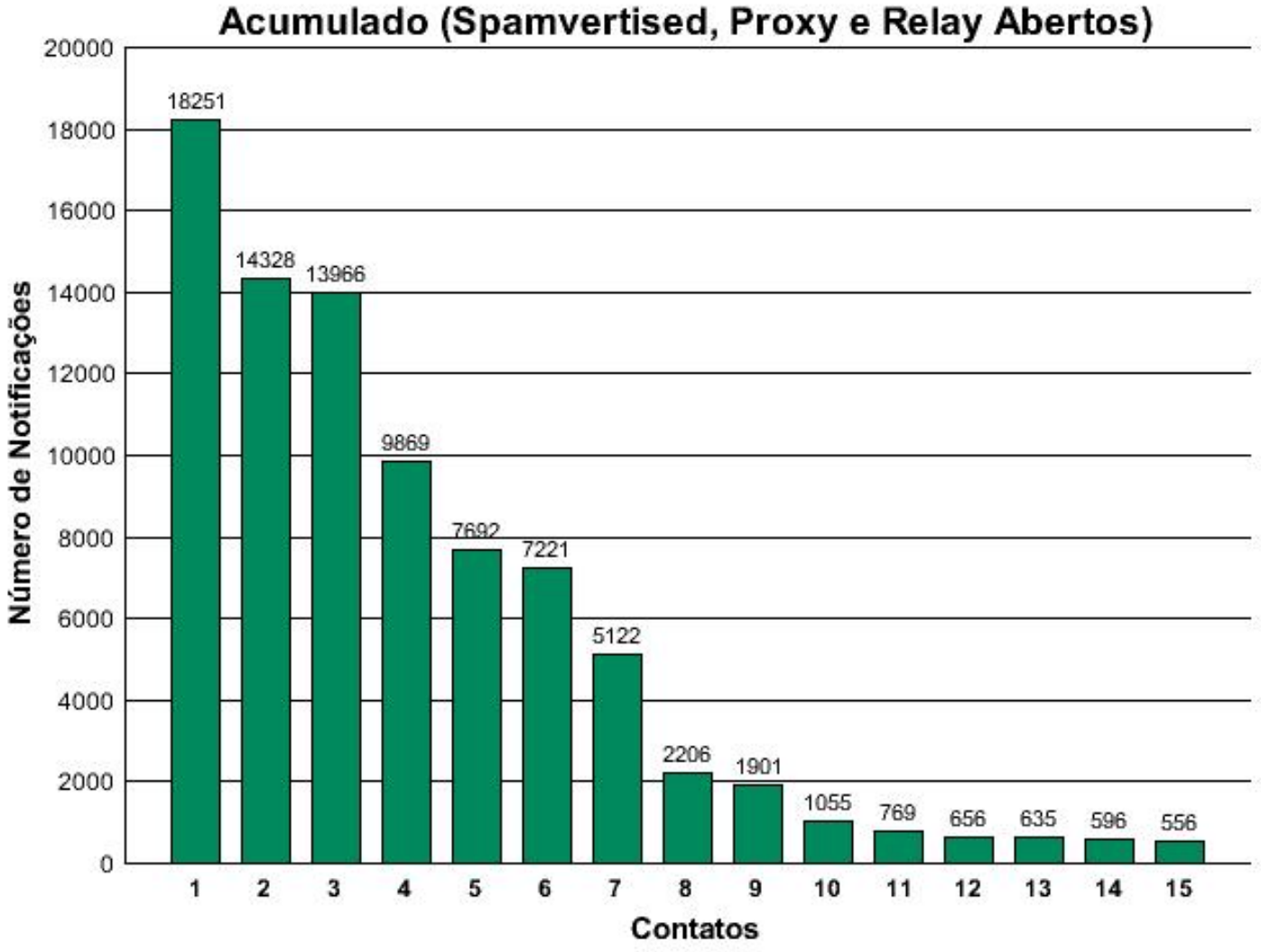
1	telefonica
2	brasiltelecom
3	telemar
4	via-rs
5	globocabo
6	rotasdealagoas
7	gvt
8	rafaelvitor
9	intelignet
10	britconsulting
11	econocell
12	acessiva
13	embratel
14	virtua
15	ajato

Valores Acumulados Jan/2005



1	gvt
2	britconsulting
3	econocell
4	telefonica
5	virtua
6	refaelvitor
7	brasiltelecom
8	telemar
9	globocabo
10	ajato
11	embratel
12	terra
13	sac-on-line
14	horizon
15	ctbctelecom

Valores Acumulados Fev/2005



1	globocabo
2	telefonica
3	virtua
4	gvt
5	brasiltelecom
6	telemar
7	web2go
8	embratel
9	ajato
10	vivax
11	econocell
12	ctbctelecom
13	gvi
14	waybrasil
15	terra

Spam como Vetor de Fraudes

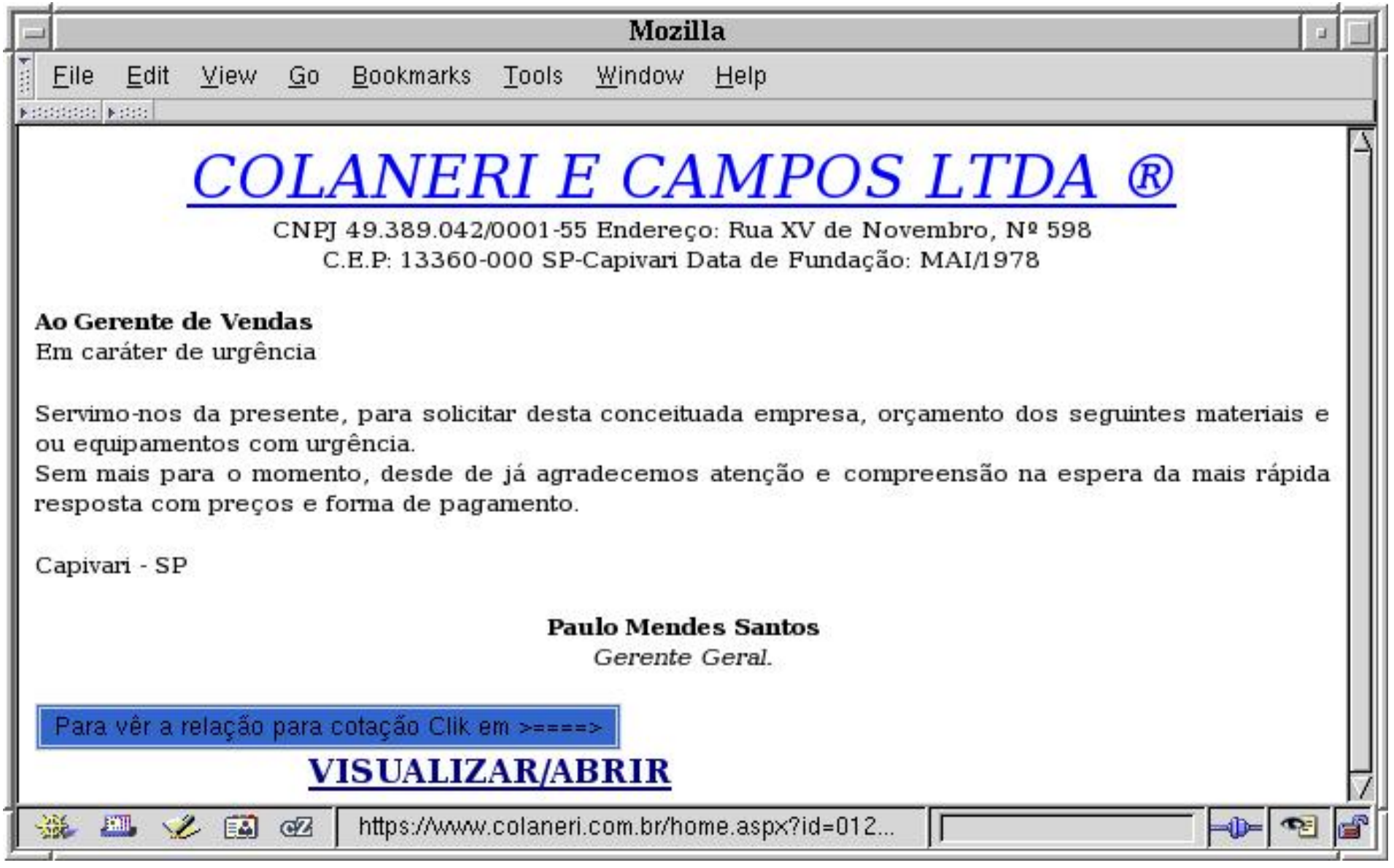
Histórico de Fraudes no Brasil

- 2001: ataques de força bruta em senhas fracas de netbanking
- 2002/2003: cavalos de tróia via email e diversos tipos de ataques a servidores DNS
- 2003/2004: “phishing” – páginas clonadas, muito similares às originais.

Histórico de Fraudes no Brasil

- 2004/2005: concentração no envio de cavalos de tróia via spam
  - BBB5, Serasa, Receita (IRPF), Eleições, Censo do IBGE, Cartões Virtuais, irregularidades de CPF, “Você está sendo traído”, “Recorra das Multas de Trânsito”, atualizações de antivirus, extrato TIM, extrato Embratel, cartilha da Febraban, etc.

Email visto em um navegador



Cabeçalho do email

```
From colaneriecampos@oi.com.br  Thu Mar 24 20:07:16 2005
Return-Path: <colaneriecampos@oi.com.br>
Received: by mx.dominio.br (Postfix)
        id 504645C0C0; Thu, 24 Mar 2005 20:07:15 -0300 (BRT)
Delivered-To: vitima@dominio.br
Received: from velox.com.br (200164175049.user.veloxzone.com.br
        [200.164.175.49])
        by mx.dominio.br (Postfix) with SMTP id B6C175C1C6
        for <vitima@dominio.br>; Thu, 24 Mar 2005 20:07:12 -0300 (BRT)
From: "Colaneri e Campos ltda." <colaneriecampos@oi.com.br>
To: colaneriecampos@oi.com.br
Subject: Departamento de Compras.
MIME-Version: 1.0
Content-Type: text/html
Message-Id: <20050324230712.B6C175C1C6@mx.dominio.br>
Date: Thu, 24 Mar 2005 20:07:12 -0300 (BRT)
```

HTML do email

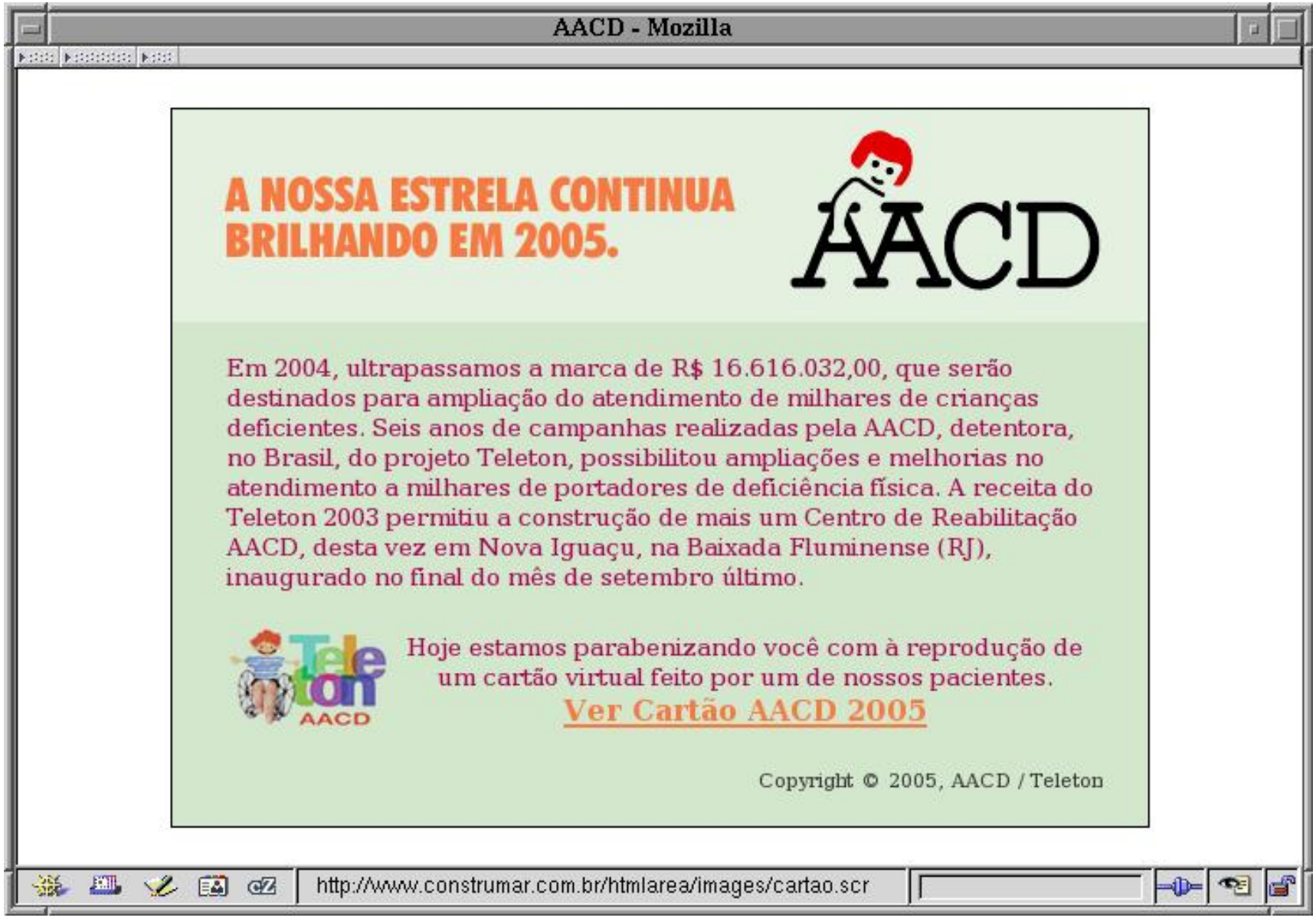
```
<html> <meta http-equiv="refresh" content="10;
url=http://mywebpage.netscape.com/Licitaemp/cotacaoabril.scr"> </head> <p
align="center"><u><font color="#0000ff"><i> <font style="FONT-SIZE: 19pt"
face="Arial Black">COLANERI E CAMPOS LTDA &reg;<br> </font></i></font></u> <font
face="Arial" size="2">CNPJ 49.389.042/0001-55 Endereço: Rua XV de Novembro, Nº
598<br> C.E.P: 13360-000 SP-Capivari Data de Fundação: MAI/1978</font></p> <p
align="left"><font face="Arial" size="2"><b>Ao Gerente de Vendas</b><br> Em
caráter de urgência</font></p><BODY><p align="justify"><font face="Arial"
size="2">Servimo-nos da presente, para solicitar desta conceituada empresa,
orçamento dos seguintes materiais e ou equipamentos com urgência.<br></BODY> Sem
mais para o momento, desde de já agradecemos atenção e compreensão na espera da
mais rápida resposta com preços e forma de pagamento.</font></p> <p
align="left"><font face="Arial" size="2">Capivari - SP</font></p> <p
align="center"><font face="Arial" size="2"><b>Paulo Mendes Santos<br>
</b><i>Gerente Geral.</i></font></p> <input type = "submit" value = "Para vêr a
relação para cotação Clik em >====>" size="20" style="border-style: double;
border-width: 3; padding-left: 4; padding-right: 4; padding-top: 1;
padding-bottom: 1; background-color: #3366CC"> <font face="Arial"> <span
style="text-transform: uppercase"> <strong> <a target="_new"
href="http://mywebpage.netscape.com/Licitaemp/cotacaoabril.scr"><font
color="#000080"><marquee behavior = slide width=40%>
Visualizar/Abrir</marquee></font></a>
```

Resultado do AV Kaspersky

```
Scanned file:   cotacaoabril.scr
cotacaoabril.scr - packed with UPX
cotacaoabril.scr - archived by RAR
cotacaoabril.scr/archive comment - OK
cotacaoabril.scr/MSWINSCK.OCX - OK
cotacaoabril.scr/RICHTX32.OCX - OK
cotacaoabril.scr/Vaiurl.txt - OK
cotacaoabril.scr/Pimballog.exe - infected by
Trojan-Spy.Win32.Bancos.bg
```

http://www.kaspersky.com/scanforvirus

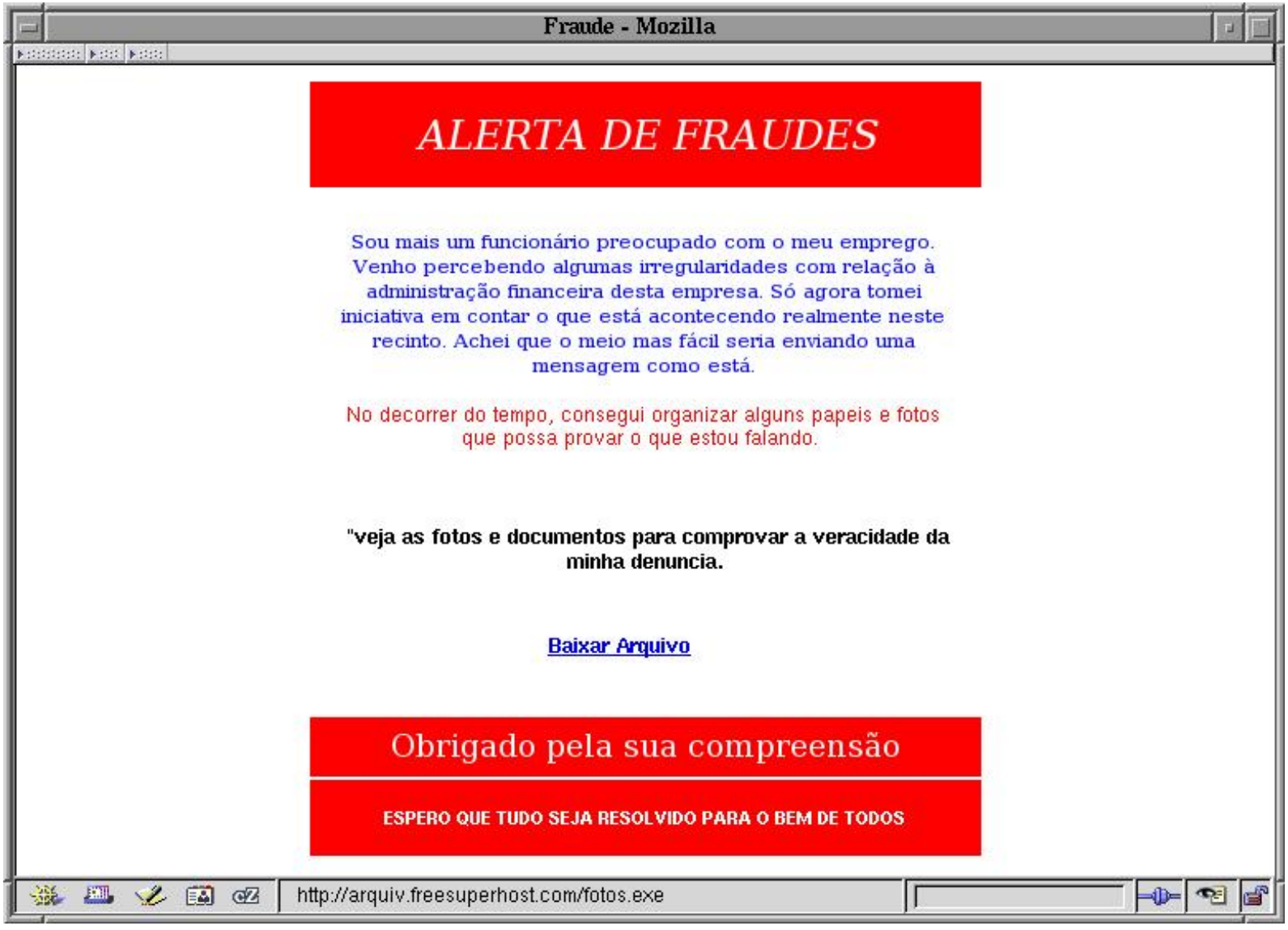
Email 2 visto em um navegador



Resultado do AV Kaspersky

```
Scanned file:   cartao.scr
cartao.scr - packed with PE_Patch.PECompact
cartao.scr - packed with PecBundle
cartao.scr - packed with PECompact
cartao.scr - infected by Trojan-Spy.Win32.Banker.ju
```

Email 3 visto em um navegador



Resultado do AV Kaspersky

```
Scanned file:   fotos.exe
fotos.exe - packed with UPX
fotos.exe - infected by Trojan-Spy.Win32.Bancos.cr
```

Email 4 visto em um navegador

Resultado do AV Kaspersky

```
Scanned file:   escuteradioterra.exe
escuteradioterra.exe - packed with PECompact
escuteradioterra.exe - infected by
                       Trojan-Spy.Win32.Banbra.q
```

Números relacionados com trojans

1233 URLs diferentes entre 21/02 a 22/03.

URLs mais referenciadas:

```
1400 http://paginas.aol.com.br/fastcard0003/Cartao_Gratuito_AACD.exe
1229 http://hometown.aol.co.uk/fotos0001/fotos.exe
1209 http://hometown.aol.co.uk/fastcard0003/Meu+amor.exe
1094 http://hometown.aol.co.uk/fastcard0003/Pendencias.exe
 966 http://paginas.aol.com.br/faetcard0002/cardfestas.exe
 959 http://hometown.aol.co.uk/cardvirtual001/card_file.exe
 957 http://hometown.aol.co.uk/fastcard0003/Meu+amor.exe
 762 http://mywebpage.netscape.com/shellbr02/Cartao.exe
 655 http://www.meumundo.americaonline.com.br/JHanemann7/kisss.exe
 520 http://paginas.aol.com.br/brazil0123/fotos.exe
 467 http://hometown.aol.co.uk/saudades2005/fotos.scr
 447 http://paginas.terra.com.br/informatica/swcrew/92839048940_223.exe
 386 http://www.kerberos.nu/voxcards.scr
 376 http://hometown.aol.com.au/atualizacao000/antivirus.exe
 331 http://209.40.169.162/svchost.scr
 324 http://meumundo.aol.com.br/cartaodoamor2005/Fotos.ExE
 281 http://paginas.terra.com.br/informatica/programa2005/IRPF2005v1.2.scr
```

Trabalho do NBSO com Relação ao Spam

Estatísticas e Notificações

- estatísticas sobre o spam no Brasil
  - Spamcop: já notifica as redes
- Projeto Honeypots Distribuídos: são notificadas redes que possuem máquinas
  - procurando proxies abertos
  - enviando spam e/ou pop-up spam
- notificação de todos os sites que hospedam cavalos de tróia relacionados a fraudes
  - envio de novos exemplares para os mantenedores de assinaturas de antivírus

http://www.spamcop.net/
http://www.honeypots-alliance.org.br/

Fatores técnicos que facilitam o spam

Proxies Abertos

- máquinas com serviço de proxy mal configurado, podendo ser abusadas para:
  - envio de spam
  - realização de ataques
- garantem anonimato
- podem ser encadeados
- podem ser instalados por malware (MyDoom)
- geralmente são máquinas de usuários finais com banda-larga (adsl, cabo, etc)

Bots

- se propagam automaticamente através da exploração de vulnerabilidades (como os worms)
- permitem controle remoto por parte do invasor
- garantem anonimato
- uma rede de bots (botnet – ou “rede de zumbis”) pode ser usada para:
  - atividades de negação de serviço, esquemas de fraude, envio de spam, etc.

softwares de “bulk email”

- extremamente fáceis de obter e usar
- permitem uso de proxies e relays abertos, ou envio direto
- muitos “vendors” oferecem serviços como envio diário de listas de proxies abertos
- são alimentados por listas de e-mails obtidas de páginas Web, newsgroups, etc.
- tentam evitar emails que pareçam ser “spam traps”, .mil, .gov, abuse, etc.

“Gangues de Spam”

Atuação das “Gangues”

- contratam seus próprios links e servidores para envio de spam ou hospedagem de sites
- grande rotatividade entre Teles/ISPs
- oferecem serviços para spammers internacionais
- difíceis de combater
  - são bons pagadores
  - contratam muita banda
- **Tendência:** obter seus próprios ASs e/ou blocos de IP

Tendências

- spammers migrarão para a utilização de redes/países onde encontrem “melhores recursos”:
  - proxies abertos
  - teles/provedores sem políticas ou contratos que prevejam spam
  - aluguel de redes para spam
- esquemas de fraude devem aumentar cada vez mais com a união entre criminosos, spammers e invasores

Formas de Combate ao Spam

Formas de Combate

- bloquear envio direto de emails (porta 25/TCP) a partir de máquinas de usuários finais, forçando o uso do SMTP do provedor (ex. Comcast)
- estimular o uso do verdadeiro opt-in, com confirmação, para uso de email com fins comerciais
- combater proxies abertos
- aumentar a segurança das máquinas de usuários, evitando que sejam comprometidas por malwares e bots

Formas de Combate (cont.)

- incentivar as operadoras e provedores a definirem contratos que prevejam desligamento de clientes cuja atividade principal seja hospedar sites citados em spams (Spamvertised Website) ou enviar spams
- considerar a tendência das gangues de spam de solicitar seus próprios ASs e blocos de endereço

Mitos do combate ao spam

Mitos

- “É só deletar o email”
  - perda de produtividade
  - perda de emails importantes classificados como spam
- “Mas tem uma opção para ser removido”
  - em geral apenas inclui o email na lista de emails ativos dos spammers
- “Os antivirus já pegam os trojans de banco”
  - existe um tempo entre a descoberta do novo trojan e a criação da assinatura
  - assume que todos os usuários atualizam constantemente seus antivirus

Mitos (cont.)

- “RBLs, SPF, greylisting, filtros de email resolvem o problema”
  - efeitos colaterais
  - atuam nos efeitos do problema, após ter consumido banda, tempo de processamento, tempo de profissionais configurando ACLs e filtros, etc.

Mitos (cont.)

- “Uma lei ou código de ética resolvem o problema”
  - é necessário levar em conta os aspectos técnicos e a facilidade de anonimato que os spammers têm
  - os spammers têm meios de enviar infinitos emails de acordo com regras como “ser o primeiro email”, “ter opções de remoção”, “ter [XXX] no subject”, etc

Referências

- Estatísticas de Spam
  http://www.nbso.nic.br/stats/spam/
- Projeto e Desenvolvimento de um Sistema de Controle e Acompanhamento de Notificações de Spam, artigo apresentado pelo NBSO no SSI de 2003
  http://www.nbso.nic.br/docs/papers/spamctl-ssi2003.pdf
- Faça uma campanha de marketing por email livre de spam
  http://www.1to1.com.br/spam/