

Software Livre, Segurança e Legislação



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

Palestrante

Humberto Sartini

- Analista de Segurança do Provedor Onda S/A
- 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)

Tópicos

- O que é Software Livre
- Hacker x Cracker
- Tipos de Ameaças
- Legislação
- Casos e Exemplos

O que é software livre ?

O termo software livre se refere à liberdade dos usuários executarem, copiarem, distribuírem, estudarem, modificarem e aperfeiçoarem o software. Mais precisamente, ele considera quatro tipos de liberdade, para os usuários do software:

O que é software livre ?

- Executar o "software", para qualquer propósito;
- Estudar como o "software" funciona, e adaptá-lo para as suas necessidades;
- Redistribuir cópias, de modo que você possa ajudar ao seu próximo;
- Aperfeiçoar o programa, e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie.

Hacker x Cracker

HACKER - Definição

O termo hacker, no contexto da Informática, designa um técnico, especialista, geralmente associado aos tópicos de segurança das redes de computadores, o que pode induzir o leitor em erro sobre o seu significado, muitas vezes difundido pela mídia como "pirata eletrônico".

Fonte: Wikipedia

Hacker x Cracker

CRACKER - Definição

Tal como os Hackers, um Cracker é alguém que possui conhecimentos avançados de informática, mas, ao contrário dos primeiros, usam esses conhecimentos para destruir sistemas e arquivos alheios, sem se preocuparem com os resultados dos seus atos. São, geralmente, autodidatas. Também é conhecido como Cracker a pessoa que "quebra" senhas de sistemas ou jogos.

Hacker x Cracker

CRACKER – Modus Operandi

1. Crackers de sistemas
2. Crackers de programas
3. Phreakers
4. Desenvolvedores de vírus, worms e trojans
5. Piratas de programas
6. Distribuidores de warez

Fonte: Wikipedia

Hacker x Cracker

CRACKER - Motivações

1. Curiosos
2. Pichadores digitais
3. Revanchista
4. Vândalos
5. Espiões
6. Ciberterroristas
7. Ladrões
8. Estelionatários

Hacker x Cracker

Lammer

Um lammer é um pseudo-hacker ou pseudo-cracker. Sem conhecimentos informáticos de qualquer ordem para atacar a segurança informática de uma organização, sistema ou rede. No entanto, usa programas ou partes de programas disponíveis na Internet para efetuar os seus ataques.

Fonte: Wikipedia

Tipos de Ameaças

ADMINISTRADORES NÃO PREPARADOS

- Atualização de Softwares e SO's
- Configuração de Softwares e SO's
- Conhecimento de Novas Tecnologias
- Conhecimento Teórico
- Política de Utilização

Tipos de Ameaças

ENGENHARIA SOCIAL

É qualquer método usado para enganação ou exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes. Para isso, o enganador pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc.

Tipos de Ameaças

AMEAÇAS INTERNAS

Geralmente os responsáveis são (ex)-funcionários, visando alguma represália (moral, financeira, etc ...) à empresa ou funcionário. Também pode ocorrer por funcionários terceirizados.

- Alteração e danos lógicos à rede
- Alteração ou destruição de informações
- Danos físicos a hardware
- Roubo de informação

Tipos de Ameaças

SPAM

- Spamvertised: máquinas que hospedam páginas com produtos e serviços sendo oferecidos no spam
- Proxy: máquinas com serviço de proxy mal configurado, sendo abusadas
- Relay: máquinas com serviço de email mal configurado, sendo abusadas
- Outras fontes: reclamações que não se enquadram nos tipos anteriores

Tipos de Ameaças

SPAM

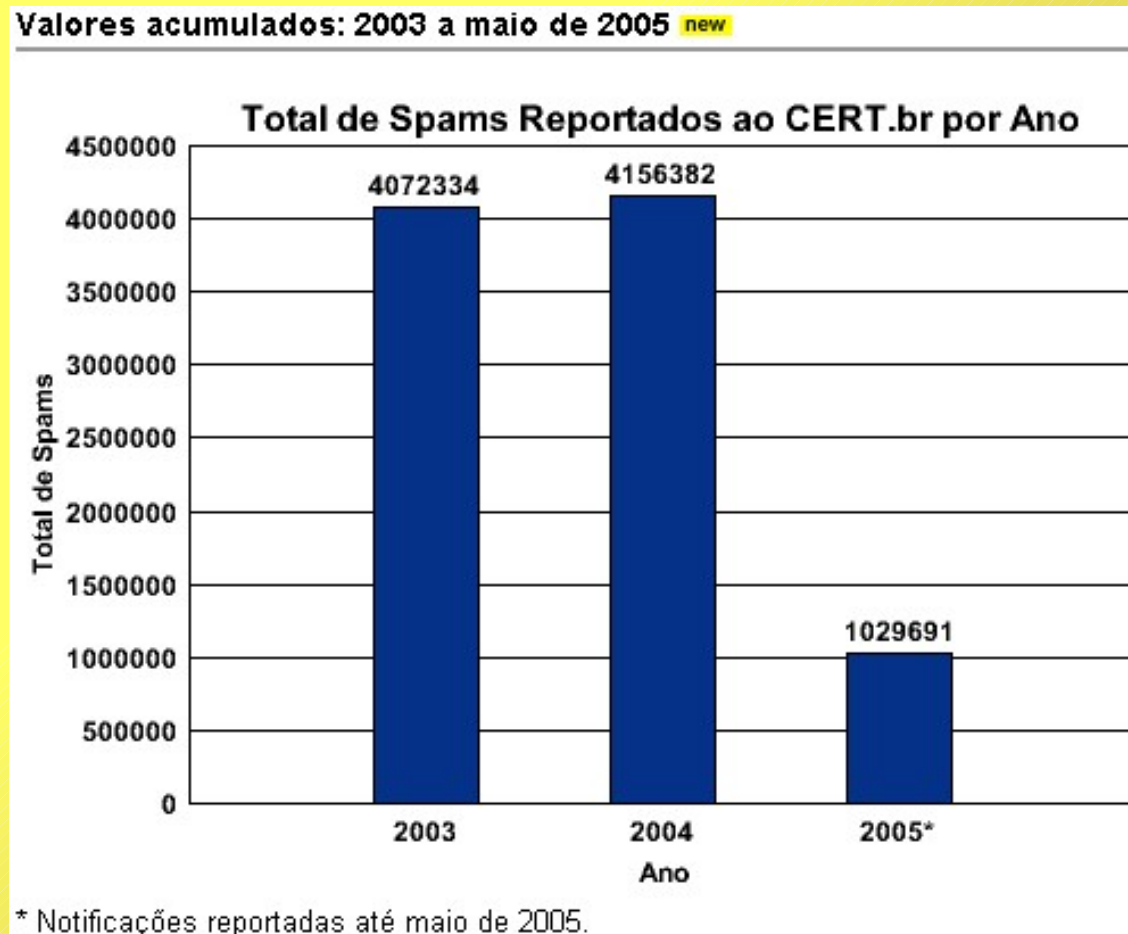
Spams Reportados ao CERT.br -- Maio de 2005

Tabela: Totais Classificados por Tipo de Reclamação.

Tipo de Reclamação		Notificações	(%)
SpamCop	Spamvertised	19.221	11,39
	Proxy	70.525	41,78
	Relay	36	0,02
	Outras	56.067	33,21
Outras Fontes		22.971	13,61
Total		168.820	100,00

Tipos de Ameaças

SPAM



Tipos de Ameaças

INCIDENTES

Existem vários tipos de incidentes, porém estatisticamente temos os seguintes:

- Ataque ao usuário final (af)
- Ataque a servidor Web (aw)
- Denial of Service (dos)
- Fraude
- Invasão
- Scan
- Worm

Tipos de Ameaças

INCIDENTES

Incidentes Reportados ao CERT.br -- Janeiro a Março de 2005

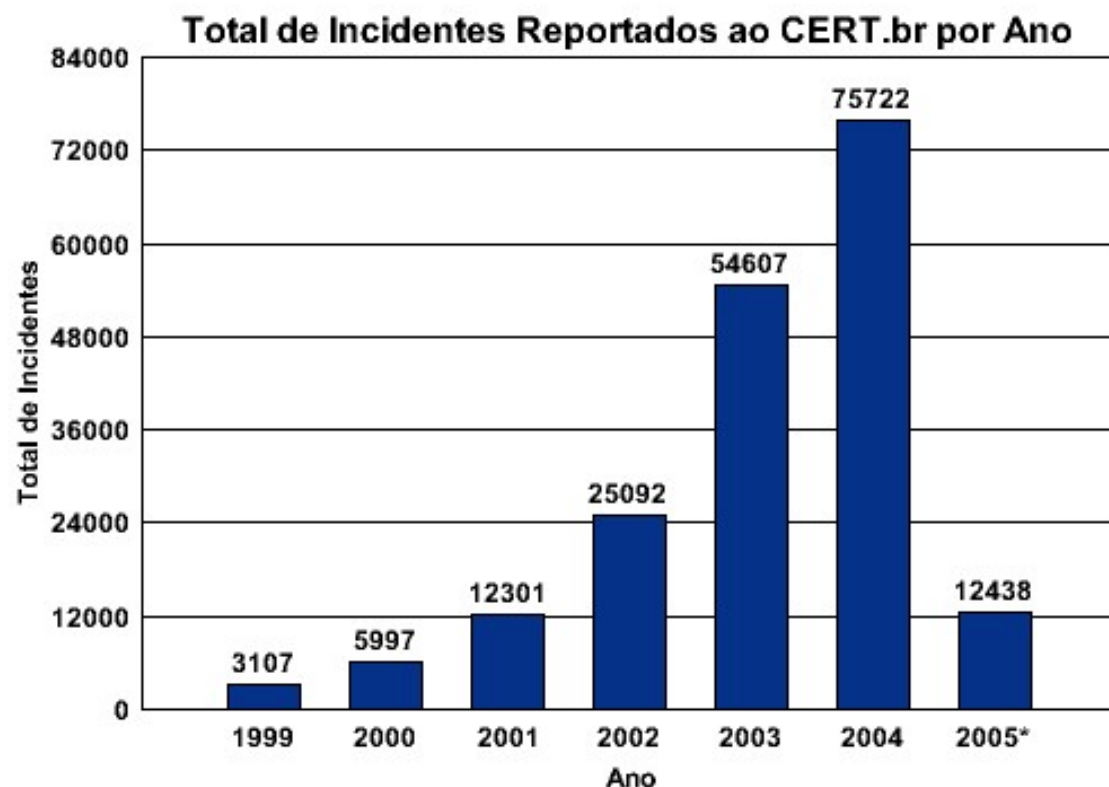
Tabela: Totais Mensais e Trimestral Classificados por Tipo de Ataque.

Mês	Total	worm (%)		af (%)		dos (%)		invasão (%)		aw (%)		scan (%)		fraude (%)	
jan	4448	1019	22	16	0	0	0	14	0	22	0	2694	60	683	15
fev	3142	1157	36	5	0	1	0	27	0	57	1	1433	45	462	14
mar	4848	1906	39	1	0	2	0	42	0	24	0	1805	37	1068	22
Total	12438	4082	32	22	0	3	0	83	0	103	0	5932	47	2213	17

Tipos de Ameaças

INCIDENTES

Valores acumulados: 1999 a março de 2005 new



* Notificações reportadas até março de 2005.

Legislação



Legislação

- Não temos Legislação Federal
- Vários Projetos de Leis
- Definições diferentes de SPAM

Legislação

Projeto de Lei (PL) 84/99

- Primeira legislação específica brasileira sobre crimes de informática
- Aprovada no Plenário da Câmara Federal, em novembro de 2003
- Parecer favorável, do senador Marcelo Crivella (PL-RJ) ao Projeto de Lei (PL) 84/99, que tramita atualmente pelo Senado Federal como PLC 89/2003

Legislação

Projeto de Lei (PL) 84/99

- Ementa: Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.
- Explicação da Ementa: Caracterizando como crime os ataques praticados por "hackers" e "crackers", em especial as alterações de "home pages" e a utilização indevida de senhas.

Legislação

Projeto de Lei (PL) 84/99

“Falsidade Informática”

Art. 154-C. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir no tratamento informático de dados, com o fim de obter, para si ou para outrem, vantagem indevida de qualquer natureza, induzindo a erro os usuários ou destinatários. Pena - detenção, de um a dois anos, e multa.

Parágrafo único. Nas mesmas incorre quem, com a mesma finalidade, cria, disponibiliza ou divulga comunicação eletrônica falsa.

Legislação

Projeto de Lei (PL) 84/99

“Sabotagem Informática”

Art. 154-D. Introduzir, modificar, apagar ou suprimir dado ou sistema informatizado, ou, de qualquer forma, interferir em sistema informatizado, com o fim de desorientar, embaraçar, dificultar ou obstar o funcionamento de um sistema informatizado ou de comunicação de dados à distância.

Pena - detenção, de um a dois anos, e multa.

Legislação

Grupo Brasil Anti Spam – Abranet, Abap, Abes, entre outras
<http://www.brasilantispam.org/>

Artigo 3º. – “Spam” - é a designação para a atividade de envio de Mensagens Eletrônicas e Mala Direta Digital que não possam ser consideradas nem Marketing Eletrônico, nem Newsletter, e nas quais se verifique a simultânea ocorrência de pelo menos 2 (duas) das seguintes situações:

- a) Inexistência de identificação ou falsa identificação do Remetente;
- b) Ausência de prévia autorização (opt-in) do Destinatário;
- c) Inexistência da opção “opt-out”;

Legislação

- d) Abordagem enganosa – tema do assunto da mensagem é distinto de seu conteúdo de modo a induzir o destinatário em erro de acionamento na mensagem;
- e) Ausência da sigla NS no campo Assunto, quando a mensagem não houver sido previamente solicitada;
- f) Impossibilidade de identificação de quem é de fato o Remetente;
- g) Alteração do Remetente ou do Assunto em mensagens de conteúdo semelhante e enviadas ao mesmo Destinatário com intervalos inferiores a 10 (dez) dias.

Legislação

Extorsão por e-mail deve ser julgada no PR

No caso de mensagens eletrônicas ameaçadoras, enviadas pela rede mundial de computadores (internet), o crime se consuma onde as vítimas as receberam, e não no local de onde foram enviadas. O entendimento é da Terceira Seção do Superior Tribunal de Justiça (STJ).

Legislação

“... pouco importa o local de onde foram enviadas as últimas mensagens eletrônicas, pois o crime de extorsão se consumou no lugar no qual os ofendidos receberam os e-mails e deles tomaram conhecimento, no caso, na cidade em que se situa a sede da empresa administrada pelas pessoas extorquidas.”

Fonte: Jornal O Estado do Paraná – 23/03/2004

Legislação

- Ministério da Defesa

PORTARIA NORMATIVA Nº 333/MD, DE 24
DE MARÇO DE 2004

Dispõe sobre a Política de Guerra Eletrônica
de Defesa.

Legislação

Art. 4º A definição dos objetivos e a determinação das diretrizes da Política de Guerra Eletrônica obedecem aos seguintes pressupostos básicos:

- I - as atividades de Guerra Eletrônica nas Forças Armadas são orientadas para atender às necessidades da defesa nacional;
- II - a capacitação tecnológica é buscada de maneira harmônica com a Política de Defesa para a área de Ciência e Tecnologia;
- III - as atividades de Guerra Eletrônica nas Forças Armadas são conduzidas de modo a assegurar o uso do espectro eletromagnético por nossas forças e impedir, reduzir ou prevenir seu uso contra os interesses do país; e
- IV - a eficácia das ações direcionadas à implementação da Guerra Eletrônica nas Forças Armadas depende diretamente do grau de conscientização alcançado junto às organizações e pessoas acerca do valor da informação que detêm ou processam.

Legislação

Art. 5º São objetivos da Política de Guerra Eletrônica de Defesa:

- I - interoperabilidade das atividades de Guerra Eletrônica desenvolvidas pelas Forças Armadas;
- II - ordenamento do intercâmbio entre as instituições de pesquisa das Forças Armadas no que se refere às atividades relacionadas com a Guerra Eletrônica;
- III - capacitação dos recursos humanos necessários à condução das atividades de Guerra Eletrônica;
- IV - capacitação das Forças Armadas para a utilização simultânea do espectro eletromagnético, com segurança e sem interferência mútua;
- V - implementação da mentalidade de Guerra Eletrônica desde o início da formação militar, em todos os níveis, nas Forças Armadas;
- VI - acompanhamento da evolução doutrinária e tecnológica da Guerra Eletrônica nos âmbitos nacional e internacional;
- VII - ordenamento do intercâmbio entre as instituições de ensino de Guerra Eletrônica das Forças Armadas; e
- VIII - redução do grau de dependência externa em relação a sistemas, equipamentos, dispositivos e serviços vinculados à Guerra Eletrônica, de interesse dos componentes da expressão militar do Poder Nacional.

Casos e Exemplos

**AJUDE UMA CRIANÇA
ENVIANDO SEU CARTUCHO
VAZIO**







Meu computador



Ambiente de rede



dream81.exe



Meus documentos



WINWORD



pemassv4.exe



EXCEL



Winamp



em2htm26.exe



Internet Explorer



Outlook Express



vma1281.exe



POWER

SYSTEM

SERIAL

SERIAL

OK

TX

RX

TELEPAR

COMUNICAÇÃO DE DADOS

USUÁRIO: Amélia Campos

- EM CASO DE DEFEITO CHAME: (041) 335-0088

- E INFORME ESTE NUMERO: 19001000

primante

Handwritten text on a cardboard box, possibly a shipping label or inventory note.

XEROX DIGITAL PA



... o seguinte endereço IP:

... endereço IP:

200 . 203 . 134 . 242

... máscara de sub-rede:

255 . 255 . 255 . 224

... gateway padrão:

200 . 203 . 134 . 41

... obter o endereço dos servidores DNS

... Usar os seguintes endereços de servidor DNS:

... servidor DNS preferencial:

200 . 192 . 100 . 11

... servidor DNS alternativo:

200 . 192 . 100 . 10

Avançado...

OK

Cancelar

Configurações IP podem ser atribuídas automaticamente se a rede oferecer suporte a esse recurso. Caso contrário, você precisa solicitar ao administrador de rede as configurações IP adequadas.

Obter um endereço IP automaticamente

Usar o seguinte endereço IP:

Endereço IP:

200 . 203 . 134 . 242

Máscara de sub-rede:

255 . 255 . 255 . 224

Gateway padrão:

200 . 203 . 134 . 241

Obter o endereço dos servidores DNS

Usar os seguintes endereços de servidor DNS:

Servidor DNS preferencial:

200 . 192 . 100 . 11

Servidor DNS alternativo:

200 . 192 . 100 . 10

Avançado











ACCESSORIES
CMB

GREE
ELECTRIC APPLIANCES
1.5匹 MOBILE AIR CONDITIONER
COOLER, FAN, DEHUMIDIFIER
REMOVABLE, SILENT OPERATION

Stack of papers and documents on a desk.

Office chair with a mesh backrest.



GREE
GREE MOTOR CORPORATION
1-800-828-8888
POWER STEERING PUMP
REPAIR KIT

NO GAS OIL

AH7 9467



Internet Explorer

RealShady.gz

NetMeeting

emassv4.e

ord_212s.exe

Email em Massa II - HTML (R26)

Arquivo Configurar Sobre o Emass II

Servidor Email (SMTP)

concoy.com.br

ex. mail.servidor.com

Porta

25



Qtd. Bloco

40



OK

Cancel

6.000
~~20000~~

Luiano Simão

CERTÃO CREDITO

WWW.HERALDO.HP.COM.BR
CRIANDO CONTAS FALSTS UOL

CREDIT WIZARD

CONVOY-

4128754132

BANCO
CITIBANK

4128 7541 3218 0366

4013

4271

4556



BM3

TO 600

Stack of various boxes, including one with "AAR" visible.

GREE
ELECTRIC APPLIANCES
1 IN 1 MOIST AIR CONDITIONER
WOODLICK FAN DEHUMIDIFIER
SERVABLE SILENT OPERATION

Stack of boxes with "S" and other markings.

Stack of cardboard boxes and a white container.

Stack of white boxes or materials on the right side of the image.

Casos e Exemplos

PHISING

Sua Conta

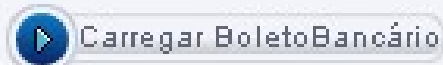
Prezado(a) Cliente.

Primeiramente gostaríamos de estar pedindo desculpas pelo inconveniente de estarmos enviando esta mensagem. Mais informamos que consta em nossos sistemas, faturas pendentes em nome de Vossa Senhoria.

Informamos que de acordo com o art. 55 na Lei nº 6.435/77 no prazo de 05 (cinco) dias úteis a partir da data de 05/03/2005 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 enviando uma cópia de boleto bancário para que Vossa Senhoria possa estar efetuando o pagamento até a data do vencimento em qualquer agencia bancária de sua preferência.

Clique no link abaixo para visualizar o boleto bancário.

 Carregar Boleto Bancário

**Certidão Negativa de Débitos de Tributos e Contribuições Federais.**

As informações disponíveis sobre o contribuinte não são suficientes para que se considere sua situação fiscal regular. Ressalvado o direito de a Fazenda Nacional cobrar quaisquer dívidas de responsabilidade do contribuinte que vierem a ser apuradas, é certificado que constam, até esta data, pendências em seu nome, relativas aos tributos e contribuições federais administrados pela Secretaria da Receita Federal. [Para visualizar pendências Clique aqui.](#)

Esta certidão refere-se exclusivamente à situação do contribuinte no âmbito desta Secretaria da Receita Federal, não constituindo, por conseguinte, prova de inexistência de débitos inscritos em Dívida Ativa da União, administrados pela Procuradoria Geral da Fazenda Nacional.

Solicitamos ao contribuinte que acesse o site: <http://www.receita.fazenda.gov.br/pendencias>. afim regularizar a(s) irregularidade(s) existente(s).

Brasília-DF 14 de Junho de 2005

A autenticidade desta certidão deverá ser confirmada na página da Secretaria da Receita Federal na Internet, no endereço <http://www.receita.fazenda.gov.br/confirmacao>.

Certidão gerada automaticamente, com base na IN/SRF no 93, de 10 de 06 de 2005.



Atualização de segurança para o Internet Explorer for Windows

Esta atualização elimina a vulnerabilidade discutida no Microsoft Security Bulletin MS06-019, e esta sendo disponibilizada para todos os usuários do Microsoft Internet Explorer de todas as versões.

Informações Rápidas

Nome do arquivo: Win-KB867282-x86-PTB.exe

Tamanho do Download: 23 KB

Data de Publicação: 11/06/2005

Versão: Todas as versões

 [Fazer download da atualização](#)

Visão Geral

Foi identificada uma questão de segurança que poderia permitir que um invasor comprometesse um computador que esteja executando o Internet Explorer e obtivesse controle total sobre ele. Você pode ajudar a proteger seu computador instalando esta atualização da Microsoft. Não será necessário reiniciar seu computador após instalar este item.

Estão disponíveis outras atualizações de segurança críticas:

Para localizar os lançamentos de segurança mais recentes, visite [Windows Update](#) e clique em "Procurar por atualizações disponíveis". E visite o site [Protect your PC](#) (em inglês) para saber como obter as atualizações de segurança mais recentes fornecidas diretamente para o seu computador.

Requisitos do Sistema

Saudades de vc...

Oi eu sou alguém que ha muito tempo te conheceu e logo após nós nos conhecermos eu tive que fazer uma viagem ao exterior e nós perdemos contato. Mas agora estou de volta e tenho muita vontade de te encontrar novamente, pois vc é uma pessoa muito especial pra mim, mas se por algum motivo vc não puder,eu vou entender, porque muita coisa deve ter mudado por aqui, mas mande pelo menos um e-mail assim vou ter certeza que vc recebeu minha mensagem.Eu procurei a maneira mais discreta para te localizar e acho que vc vai gostar da surpresa,elaborei um book com algumas fotos minhas e inclusive tenho uma foto sua que guardo com muito carinho!,o meu e-mail e fone está junto com as fotos.

Espero que goste das fotos...

[Ver fotos !](#)

Contato

- Através do site ou e-mail

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

humberto@onda.com.br

Créditos

- Figura Slide 1:
<http://ngc224.gerwinski.de/~anja/gnuart/a-gnu-head/small.png>
- Figura Slide 15:
<http://www.cert.br/stats/spam/2005-may/total.html>
- Figura Slide 16:
<http://www.nbso.nic.br/stats/spam/>
- Figura Slide 18:
<http://www.nbso.nic.br/stats/incidentes/2005-jan-mar/total.html>
- Figura Slide 19:
<http://www.nbso.nic.br/stats/incidentes/>
- Figura Slide 20:
<http://www.idc.org.br/justica.gif>
- Figura Slide 34 a 55: Arquivo Pessoal