Segurança com Software Livre

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

- Hacker x Cracker
- Tipos de Ameaças
- Mercado de Segurança
- Ferramentas Utilizadas
- Legislação
- Casos e Exemplos

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.

Fonte: Wikipedia

Hacker x Cracker

CRACKER - Motivações

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

Fonte: Wikipedia

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

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

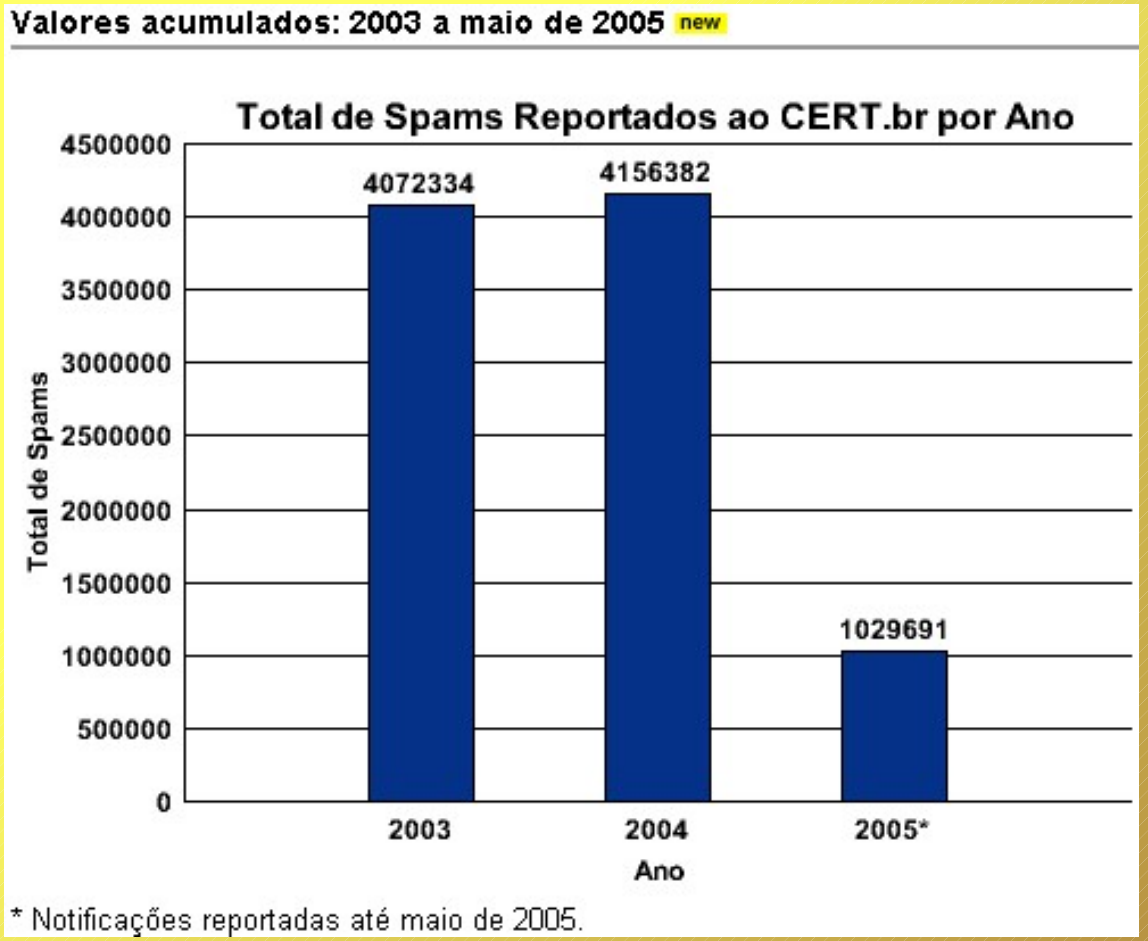
Spams Reportados ao CERT.br -- Maio de 2005

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 estatísticamente 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

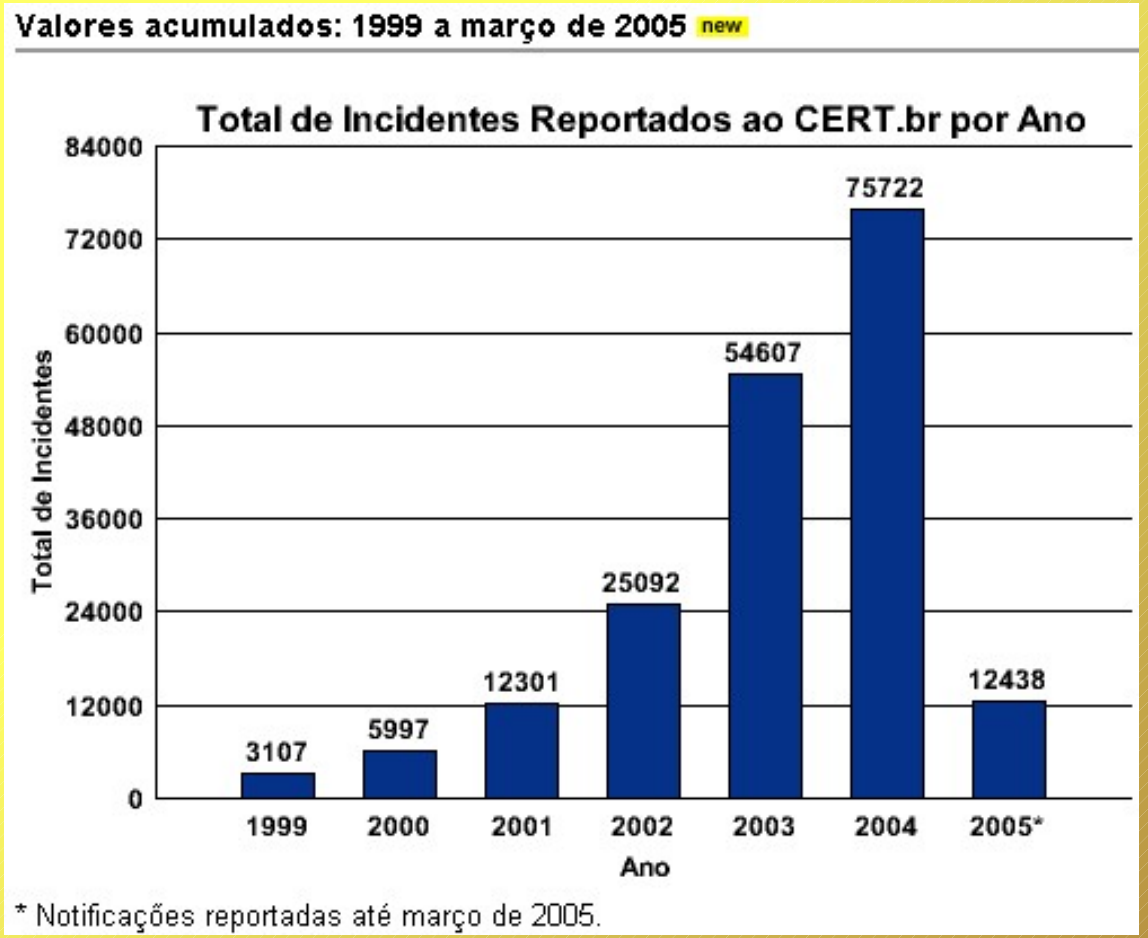
Incidentes Reportados ao CERT.br -- Janeiro a Março de 2005

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



Mercado de Segurança

- Crescimento estimado entre 15% a 20% para 2005

- Em 2004 foi movimentado 12 Bilhões de Reais, sendo que 1/3 foi movimentado por instituições financeiras

- Haverá uma grande “boom” no mercado de segurança e governança devido a três fatores:

Mercado de Segurança

1)Novo Acordo de Capital da Basiléia

Voltado ao mercado financeiro, e entrará em vigor a partir de 2007, criando condições para conhecer, mensurar e cobrir Riscos Operacionais, de Crédito e de Mercado

2) Sarbanes-Oxley

Promulgada em 2002, a Lei Sarbanes-Oxley determinou a certificação de uma série de controles internos, a fim de garantir que os resultados financeiros divulgados pelas empresas sejam obtidos de acordo com sólidos padrões de conduta

Mercado de Segurança

3)Novo Código Civil

Haverá maior responsabilidade do administrador, que, agora, ainda mais, deverá não só agir nas questões preventivas, mas também nas reparatórias

Os negócios eletrônicos também foram privilegiados com as disposições da recente Lei exaltando a boa-fé, finalidade social, usos e costumes.

Mercado de Segurança

- Equipamentos de Valor Agregado (“IN BOX”):
  - Analisador de SMTP
  - Firewall
  - Gateway/Proxy
  - VoIP
  - Etc ...
- Mercado de Wireless
- Perícia Forense

Ferramentas Utilizadas

- Existem diversas ferramentas desenvolvidas em Software Livre, e a relação a seguir não é, de forma alguma, uma relação “oficial”, serve como base para estudos futuros

- A utilização de qualquer dessas ferramentas deve ser analisada antes de ser aplicada, pois o uso indevido poderá acarretar problemas

Ferramentas Utilizadas

- Firewall
  - IpFW
    - http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-ipfw.html
  - NetFilter Iptables
    - http://www.netfilter.org/
  - PF
    - http://www.openbsd.org/faq/pf/index.html

Ferramentas Utilizadas

- “?”IDS
  - Prelude
    - http://www.prelude-ids.org/
  - Snort
    - http://www.snort.org/
  - Viper
    - http://www.coyotelinux.com/downloads/channel.php?ChannelID=7

Ferramentas Utilizadas

- Port Scanner / Vulnerabilidades
  - Nessus
    - http://www.nessus.org/
  - Nmap
    - http://www.insecure.org/nmap
  - XportScan2
    - http://www.freewebs.com/bh_x/xportscan.html

Ferramentas Utilizadas

- Sniffer
  - Dsniff
    - http://www.monkey.org/~dugsong/dsniff/
  - EtheReal
    - http://www.ethereal.com/
  - TcpDump
    - http://www.tcpdump.org/

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 onda foram enviadas. O entendimento é da Terceira Seção do Superior Tribunal de Justiça (STJ).

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

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:

III - as atividades de Guerra Eletrônica nas Forças Armadas são conduzidas de modo a assegurar o uso do espectro eletro-magnético 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:

III - capacitação dos recursos humanos necessários à condução das atividades de Guerra Eletrônica;

V - implementação da mentalidade de Guerra Eletrônica desde o início da formação militar, em todos os níveis, nas Forças Armadas;

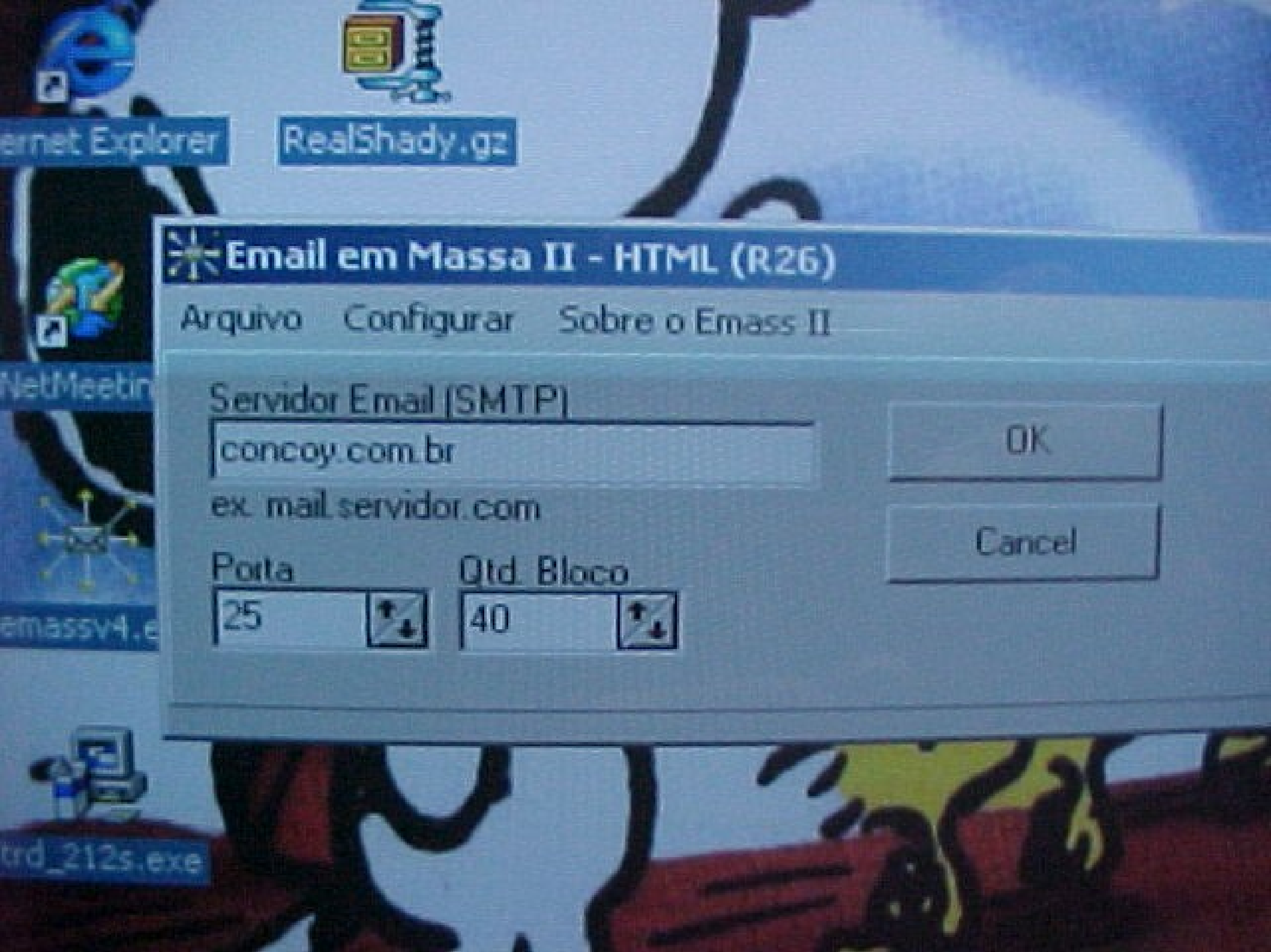
VI - acompanhamento da evolução doutrinária e tecnológica da Guerra Eletrônica nos âmbitos nacional e internacional;

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
dreame81.exe
Meus documentos
WINWORD
pemas5v4.exe
EXCEL
Winamp
em2htm26.exe
Internet Explorer
Outlook Express
vmail281.exe


ernet Explorer
RealShady.gz
NetMeetin
emassv4.e
trd_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

6002

Luciano Camilo

CARTÃO CREDITO

WWW.HERALDO.COM.BR/CJB.NET
CRIANDO CONTAS FALSAS UOL

CREDIT WIZARD

CONVOY -

4128 7541 32

BANCO CITIBANK

4128 7541 3218 0366

4013

4271

4556


Segurança
sem Fronteiras


GREE


ACCESSORIES
GREE


GREE

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 prefêrencia.

Clique no link abaixo para visualizar o boleto bancário.

Carregar BoletoBancário

Ministério da Fazenda

Receita Federal

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).

Brasilia-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.

File Edit View Go Message Enigmail Tools Help

Subject: Incidentes de segurança recentes **From:** seguranca 12-06-2005 13:55

Microsoft.com Brasil Home | Mapa do Site

Microsoft

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.

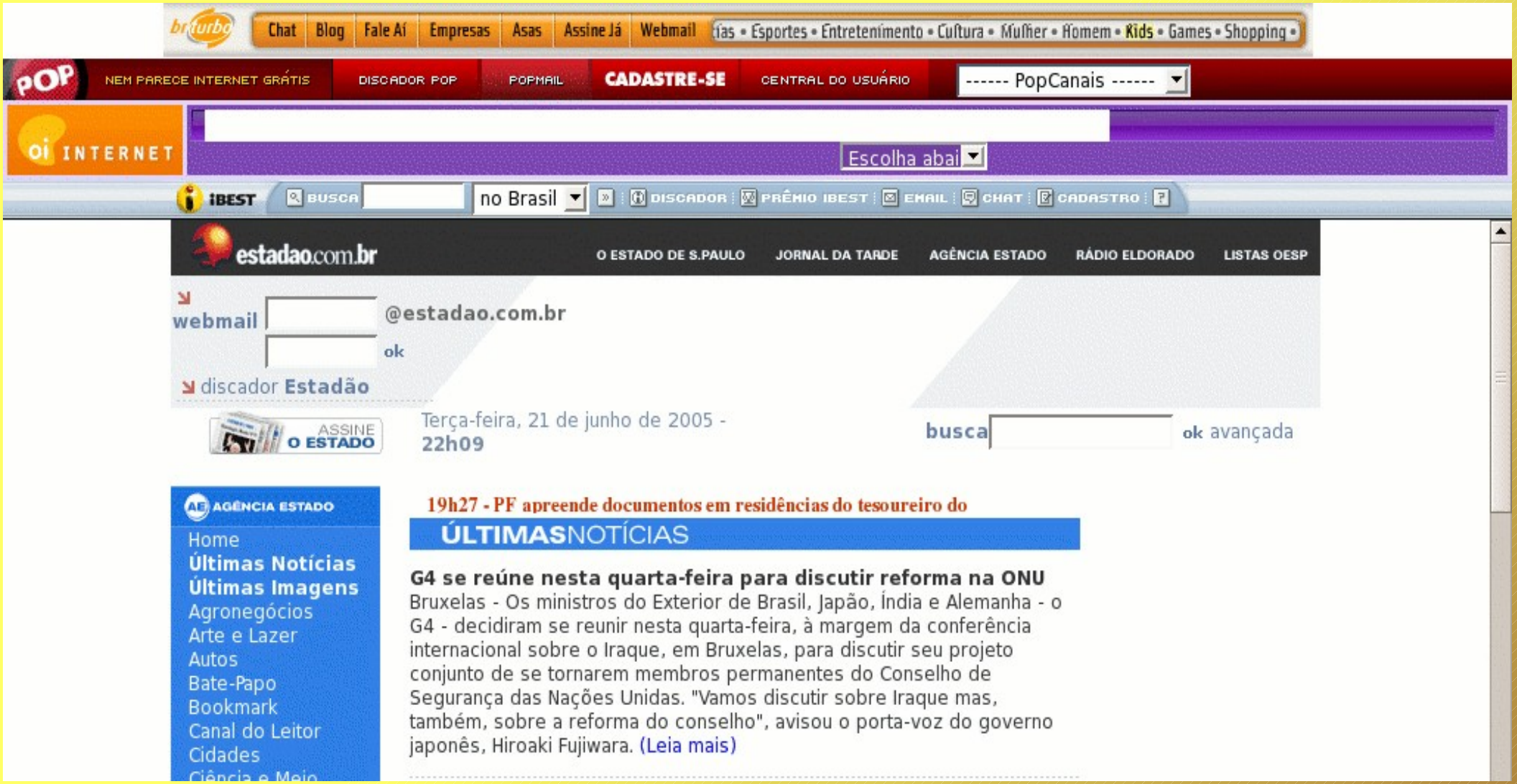
Estão disponíveis outras atualizações de segurança críticas:

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

Casos e Exemplos

CROSS SITE SCRIPTING



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

Contato

- Através do site ou e-mail

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

humberto@onda.com.br

Créditos

Sites consultados:

- Jus Navigandi
http://www1.jus.com.br/doutrina/texto.asp?id=3882

- Unicorp
http://www.unicorp.org.br/v2/eventos/basileia/evento_basileia.asp

- Wikipedia
http://www.wikipedia.org/

Créditos

- Figura Slide 1:
http://www.gnu.org/graphics/gnu-and-penguin-color-300x276.jpg

- Figura Slide 12:
http://www.cert.br/stats/spam/2005-may/total.html

- Figura Slide 13:
http://www.nbso.nic.br/stats/spam/

- Figura Slide 15:
http://www.nbso.nic.br/stats/incidentes/2005-jan-mar/total.html

- Figura Slide 16:
http://www.nbso.nic.br/stats/incidentes/

- Figura Slide 26:
http://www.idc.org.br/justica.gif

- Figura Slide 40 a 53, 55 a 57 e 59: Arquivo Pessoal