

# Segurança na Internet

Marcelo H. P. C. Chaves  
mhp@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br  
<http://www.cert.br/>

Comitê Gestor da Internet no Brasil - CGI.br  
<http://www.cgi.br/>

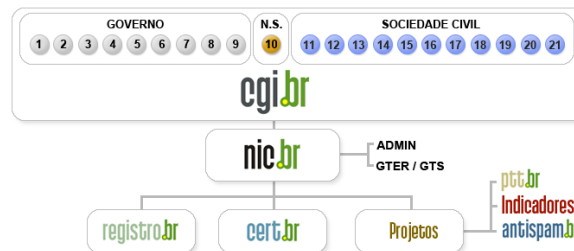
## Motivação

- Analisar estatísticas sobre segurança na Internet, para entendermos o problema
- Discutir a evolução dos problemas de segurança desde a concepção da Internet até os dias atuais
- Discutir possíveis formas de proteção, isto é, o que podemos fazer para nos proteger no uso da Internet
- Apresentar iniciativas que visam aumentar a segurança no uso da Internet

## Agenda

- Sobre o CGI.br e o CERT.br
- Indicadores do CGI.br
- Estatísticas do CERT.br
- Evolução dos Problemas de Segurança
- O Spam Visto como Incidente de Segurança
- Formas de Proteção
- Iniciativas para Aumentar a Segurança
- Referências

## Comitê Gestor da Internet no Brasil



- 1 – Ministério da Ciência e Tecnologia (Coordenação)  
 2 – Ministério das Comunicações  
 3 – Casa Civil da Presidência da República  
 4 – Ministério da Defesa  
 5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior  
 6 – Ministério do Planejamento, Orçamento e Gestão  
 7 – Agência Nacional de Telecomunicações (Anatel)  
 8 – Conselho Nacional de Desenvolvimento Científico e Tecnológico  
 9 – Fórum Nacional de Secretários Estaduais para Assuntos de C&T  
 10 – Representante de Notório Saber em assuntos de Internet

- 11 – provedores de acesso e conteúdo  
 12 – provedores de infra-estrutura de telecomunicações  
 13 – indústria de bens de informática, telecomunicações e software  
 14 – segmento das empresas usuárias de Internet  
 15-18 – representantes do terceiro setor  
 19-21 – representantes da comunidade científica e tecnológica

## Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na Internet;
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**

## Atividades do CERT.br

- Articulação das ações para resposta a incidentes envolvendo redes brasileiras, por exemplo:
  - Combate a fraudes: contato com *sites* envolvidos para remoção de códigos maliciosos; envio de novos exemplares para fabricantes de antivírus; troca de informações técnicas com instituições financeiras
- Manutenção de estatísticas sobre incidentes de segurança e sobre spam
- Desenvolvimento de documentos de Boas Práticas para usuários e administradores de redes
- Fomento à criação de novos Grupos de Segurança e Resposta a Incidentes (CSIRTs) no Brasil
- Oferecimento de cursos oficiais do CERT®/CC
- Coordenação do “Consórcio Brasileiro de Honey pots”

## Parcerias Internacionais do CERT.br

- Forum of Incident Response and Security Teams (FIRST)  
Full member  
<http://www.first.org/membership/>
- Anti-Phishing Working Group (APWG) Research Partner  
<http://www.antiphishing.org/>
- Honeynet Research Alliance Member  
<http://honeynet.org/alliance/>

## Indicadores do CGI.br

## Indicadores do CGI.br

- Parceria com o IBGE e IBOPE/NetRatings
- Pesquisas TIC Domicílios e TIC Empresas 2005, realizadas para o CGI.br, pelo Instituto Ipsos Opinion  
<http://www.nic.br/indicadores/>

### Objetivos:

- Produzir e divulgar com periodicidade indicadores oficiais sobre penetração e uso da Internet;
- Fornecer subsídios para a elaboração de políticas públicas que garantam o acesso às TICs no Brasil;
- Acompanhar, monitorar e avaliar o impacto sócio econômico das TICs;
- Permitir a comparabilidade da realidade brasileira com outros países.

## Indicadores do CGI.br (cont)

### TIC Domicílios

Tabela 10 - Amostra da TIC Domicílios

	População PNAD 2003	Entrevistas	Overcota Internet
Total	173.966.052	8048	492

B1 - Proporção de Domicílios com Computador = 16,91%

*Percentual sobre o total de domicílios (8540 domicílios entrevistados)*

B2 - Proporção de Indivíduos com Acesso ao com Computador em Casa = 11,37%

*Percentual sobre o total da população (8540 domicílios entrevistados)*

B3 - Proporção de Indivíduos que Usaram o Computador, de qualquer Local

*Percentual sobre o total da população (8540 domicílios entrevistados)*

	< 3 meses	Entre 3 e 6 meses	Entre 6 e 12 meses	+ 12 meses	Nunca usou
Percentual	29,72	3,21	3,64	8,63	54,79

## Indicadores do CGI.br (cont)

### TIC Domicílios

C1 - Proporção de Domicílios com Internet = 21,43%  
*Percentual sobre o total de domicílios (8540 domicílios entrevistados)*

C2 - Proporção de Indivíduos com Acesso à Internet no Domicílio = 9,39%  
*Percentual sobre o total da população (8540 domicílios entrevistados)*

C5 - Proporção de Indivíduos que Acessaram à Internet, de qualquer Local  
*Percentual sobre o total da população (8540 domicílios entrevistados)*

	< 3 meses	Entre 3 e 6 meses	Entre 6 e 12 meses	+ 12 meses	Nunca usou
Percentual	24,41	2,65	2,26	2,93	67,76

## Indicadores do CGI.br (cont)

### Números relacionados com segurança:

- TIC Domicílios
  - F - Segurança
    - F1 - Problemas de segurança encontrados usando a Internet
    - F2 - Medidas de segurança tomadas com relação ao computador
    - F3 - Frequência de atualização do antivírus
  - J - Spam
    - J1 - Recebimento de spam na principal conta de e-mail de uso pessoal
    - J2 - Frequência de recebimento de spam na principal conta de e-mail de uso pessoal
    - J3 - Número de spams recebidos na principal conta de e-mail de uso pessoal
    - J4 - Tempo perdido com spams na principal conta de e-mail de uso pessoal
- TIC Empresas
  - E - Segurança
    - E1 - Problemas de segurança encontrados
    - E2 - Medidas de segurança adotadas
    - E3 - Frequência de atualização do antivírus
    - E4 - Uso de recursos de segurança para comunicação

## TIC Domicílios

### F1 - Problemas de Segurança Encontrados Usando a Internet

Percentual sobre o total de usuários Internet

(%)	Nenhum	Vírus (com acesso não autorizado)	Vírus (com danos em SW ou HW)	Abuso de Informação pessoal	Fraude	Outro	Não lembra
<b>Total</b>	40,99	19,64	7,13	1,67	0,94	1,10	0,24
<b>Região</b>							
RM SP	59,74	19,68	11,48	2,73	2,19	1,09	-
RM RJ	35,09	15,73	9,94	2,34	1,17	0,58	-
RM BEL	69,28	24	7,96	8,58	-	1,12	-
DF	36,34	20,45	8,92	2,55	-	0,42	-
<b>Faixa Etária</b>							
10-15	33,95	8,72	1,91	0,08	-	0,79	0,74
16-24	36,21	21,07	7,37	1,27	1,06	1,06	0,3
25-34	44,17	19,8	7,02	2,13	1,25	1,25	0,49
35-44	44,89	16,69	6,2	1,8	0,08	1,47	-
45-59	38,04	23,67	10,27	2,09	1,6	-	-
60 +	60,36	9,89	2,39	0,55	3,22	-	-

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

13/94

## TIC Domicílios (cont)

### F2 - Medidas de Segurança Tomadas com Relação ao Computador

Percentual sobre o total de usuários Internet que possuem computador

(%)	Antivírus	Firewall Pessoal	Software Anti-spyware
<b>Total</b>	69,76	19,33	22,09
<b>Renda</b>			
< R\$300	67,63	29,91	43,56
R\$301-500	25,21	10,9	16,49
R\$501-1000	51,97	17,89	24,62
R\$1001-1800	71,12	15,73	15,8
R\$1801 +	72,85	21,69	24,58
<b>Faixa Etária</b>			
10 -15	58,31	9,9	12,15
16-24	72,82	20,57	23,84
25-34	69,97	23,05	26,32
35-44	70,23	17,51	18,32
45-59	61,18	15,02	18,04
60 +	52,27	-	11,48

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

14/94

## TIC Domicílios (cont)

## F3 - Frequência de Atualização do Antivírus

Percentual sobre o total de usuários Internet que possuem computador

(%)	Diária	Semanal	Mensal	Trimestral	Não atualizou
Total	21,11	27,01	17,37	3,47	31,03
Região					
RM SP	16,42	31,7	18,18	2,9	30,81
RM RJ	24,2	27,5	16,5	6,6	25,19
RM BEL	12,34	28,16	13,93	7,91	37,66
DF	28,9	21,06	14	6,22	29,81
Faixa Etária					
10-15	6,13	25,3	23,56	-	45,02
16-24	18,84	31,5	20,01	3,69	25,96
25-34	28,09	22,54	13,89	3,75	31,73
35-44	20,57	26,59	18,6	3,1	31,14
45-59	14,87	25,71	15,34	3,16	40,92
60 +	18,24	13,32	6,78	2,77	58,89

## TIC Domicílios (cont)

## J1 - Recebimento de Spam na Principal Conta de E-mail de Uso Pessoal

Percentual sobre o total de pessoas que possuem conta de e-mail

	Sim	Não	Não sabe
Percentual	51,86	47,66	0,48

## J2 - Frequência de Recebimento de Spam na Principal Conta de E-mail de Uso Pessoal

Percentual sobre o total de pessoas que afirmaram ter recebido spam

	Diariamente	Toda semana	Todo mês
Percentual	45,71	37,79	13,93

## J3 - Número de Spams Recebidos na Principal Conta de E-mail de Uso Pessoal

Número médio de spams diários recebidos

	1-10	11-20	21-30	31-40	41-50	51-60	61-70	+ 71
Percentual	73,24	13,03	3,89	2,16	2,29	0,62	0,22	3,32

## J4 - Tempo Perdido com Spams na Principal Conta de E-mail de Uso Pessoal

Tempo médio gasto com spams, em minutos por dia

	1-5	6-10	11-15	16-20	21-25	26-30	+ 30
Percentual	61,78	23,02	7,65	3,47	0,63	1,78	1,67



## TIC Empresas

### E1 - Problemas de Segurança Encontrados

Percentual sobre o total de empresas com acesso à Internet

	Vírus	Worms ou Bots	Trojans	Acesso externo não autorizado	Acesso interno não autorizado	DoS	Desfiguração de Servidor Web
%	50,34	17,44	31,13	10,89	7,61	6,25	11,20

### E2 - Medidas de Segurança Adotadas

Percentual sobre o total de empresas com acesso à Internet

	Antivírus	Software Anti-spyware	Firewall	SSL HTTPS	Autenticação para usuários internos	Autenticação para usuários externos	IDS	Backup	Backup offsite	Programa de Treinamento para Funcionários
%	95,72	59,46	54,11	49,48	42,33	21,12	29,21	69,62	38,33	19,69

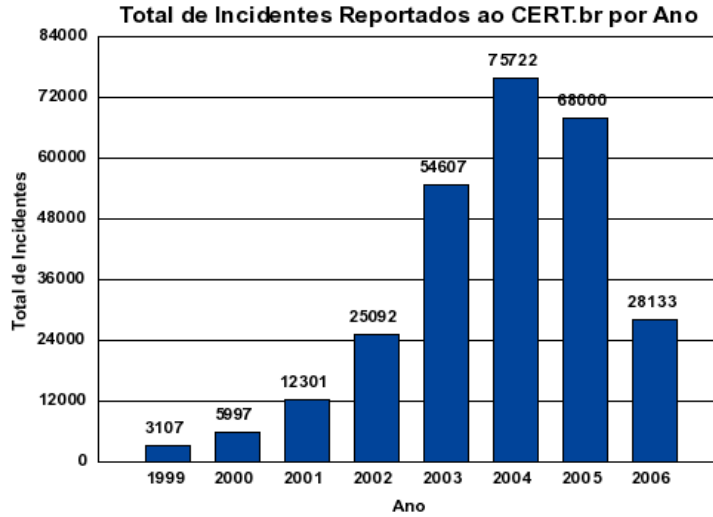
### E3 - Frequência de Atualização do Antivírus

Percentual sobre o total de empresas com acesso à Internet

	Diária	Semanal	Mensal	Trimestral	Semestral/Anual	Não atualizou
%	41,68	30,02	12,34	5,11	2,11	8,74

## Estatísticas do CERT.br

## Notificações de Incidentes: 1999-2006



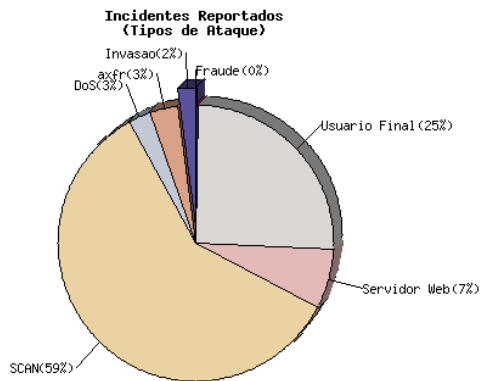
Obs.: Os dados de 2006 são referentes ao primeiro trimestre do ano.

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

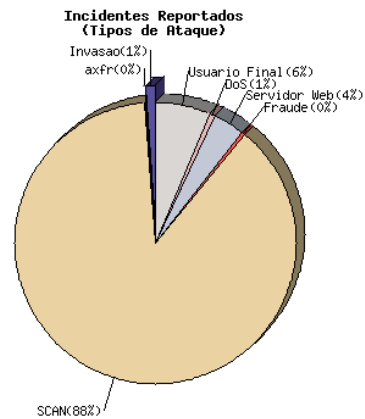
19/94

## Evolução dos Tipos de Ataques

2000



2001

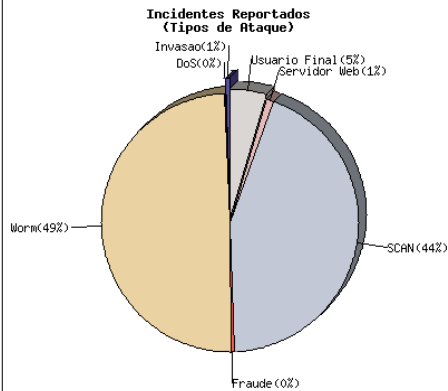


CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

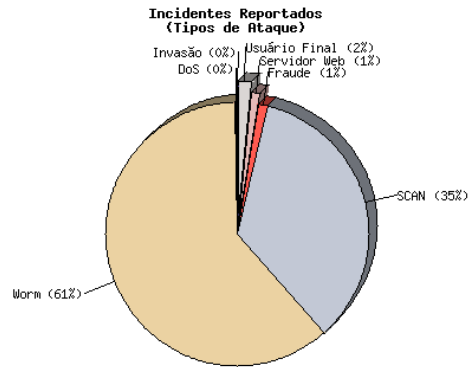
20/94

## Evolução dos Tipos de Ataques (cont)

2002



2003

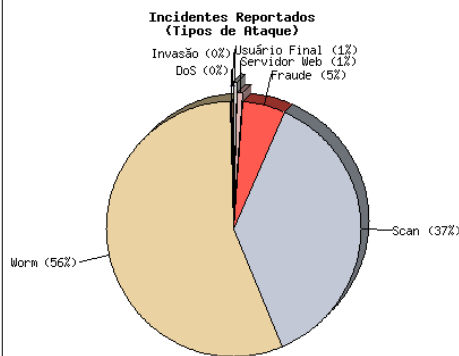


CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

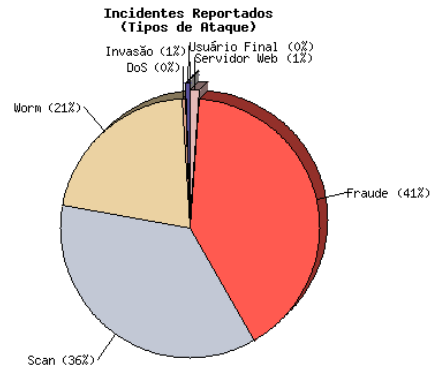
21/94

## Evolução dos Tipos de Ataques (cont)

2004



2005

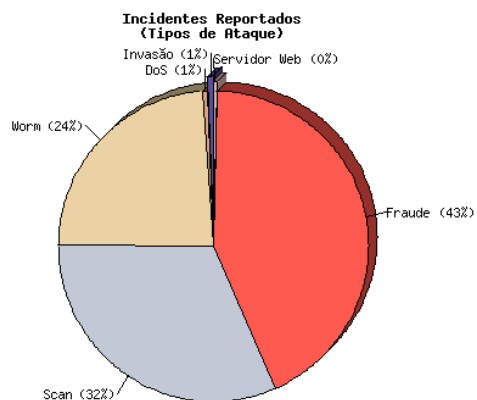


CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

22/94

## Evolução dos Tipos de Ataques (cont)

1º Trimestre de 2006:



## A Evolução dos Problemas de Segurança

## Final dos Anos 60

### Internet

- Projeção não considera implicações de segurança
- Comunidade de pesquisadores
- Confiança

## Anos 80

- Invasores com
  - Alto conhecimento
  - Dedicção por longos períodos para realização de poucos ataques
- “*Cookoo’s Egg: Traking a Spy Through the Maze of Computer Espionage*”, Cliff Stoll
  - 30+ sistemas invadidos
  - Contas/senhas óbvias
  - Vulnerabilidades em softwares
  - Tempo e persistência

<http://www.bookfinder.us/review4/0743411463.html>

## Final dos Anos 80

- Primeiro *worm* com implicações de segurança
  - Criado por Robert Morris Jr.
  - Explorava a combinação de vulnerabilidades no *sendmail*, *finger* e em configurações dos “r” *services*
  - Mais de 6000 computadores atingidos
    - Aproximadamente 10% da Internet na época
- Mobilização em torno do tema segurança
- Criação do CERT/CC 15 dias após

[ftp://coast.cs.purdue.edu/pub/doc/morris\\_worm/](ftp://coast.cs.purdue.edu/pub/doc/morris_worm/)

<http://www.cert.org/archive/pdf/O3tr001.pdf>

<http://www.ietf.org/rfc/rfc1135.txt>

## Glossário de Termos (1)

- **Vírus:**

programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus **depende** da execução do programa hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.
- **Worm:**

programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Fonte: <http://cartilha.cert.br/glossario/>

## Anos 1991-2001

- Início da utilização da “engenharia social” em grande escala
- Primeiros ataques remotos aos sistemas
- Popularização de: cavalos de tróia, furto de senhas, varreduras em busca de máquinas vulneráveis, captura de informações digitais (*sniffers*), ataques de negação de serviço, etc
- Primeiras ferramentas automatizadas para
  - Realizar invasões
  - Ocultar a presença dos invasores (*rootkits*)
- Sofisticação no processo de controle das ferramentas

## Anos 2002-2005

- Explosão no número de códigos maliciosos com diversos fins
  - *worms*, *bots*, cavalos de tróia, vírus, *spyware*
- Códigos com múltiplas funcionalidades
  - Múltiplos vetores de ataque, código eficiente, aberto e facilmente adaptável
- Permitem controle remoto
- Praticamente não existem interações por parte dos invasores

## Glossário de Termos (2)

- **Cavalo de tróia:**  
programa, normalmente recebido com um “presente”, que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.
- **Bot:**  
programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente.
- **Spyware:**  
termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Fonte: <http://cartilha.cert.br/glossario/>

## Situação Atual

### Característica dos Ataques

- Crime organizado
  - Aliciando *spammers* e invasores
  - Injetando dinheiro na “economia *underground*”
- **Botnets**
  - Usadas para envio de *scams*, *phishing*, invasões, esquemas de extorsão
- Redes mal configuradas sendo abusadas para realização de todas estas atividades
  - sem o conhecimento dos donos
- **Alvo migrou para usuários finais**



## Situação Atual (cont)

### Característica dos Atacantes

- Em sua maioria pessoal com pouco conhecimento técnico que utiliza ferramentas prontas
- Trocam informações no *underground*
- Usam como moedas de troca
  - Senhas de administrador/root
  - Novos *exploits*
  - Contas/senhas de banco
  - Números de cartão de crédito
  - *bots/botnets*

## Situação Atual (cont)

### Perfil dos Ataques / Principais Ameaças

- Sistemas operacionais e softwares desatualizados, vulnerabilidades freqüentes
- Códigos maliciosos explorando essas vulnerabilidades, em curto espaço de tempo
- Ferramentas automatizadas de ataque
- Vírus / *worms* / *bots*
- Ataques de força bruta
- Atacantes + *spammers*
- Fraudes / *scams* / *phishing* / crime organizado

## Glossário de Termos (3)

- **Scam:**  
esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.
- **Phishing:**  
mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Fonte: <http://cartilha.cert.br/glossario/>

## Fraudes via Internet

## Histórico das Fraudes via Internet no Brasil

### 2001

- 1<sup>os</sup> *keyloggers* enviados por e-mail, ataques de força bruta

### 2002-2003

- Casos de *phishing* e uso disseminado de servidores DNS comprometidos

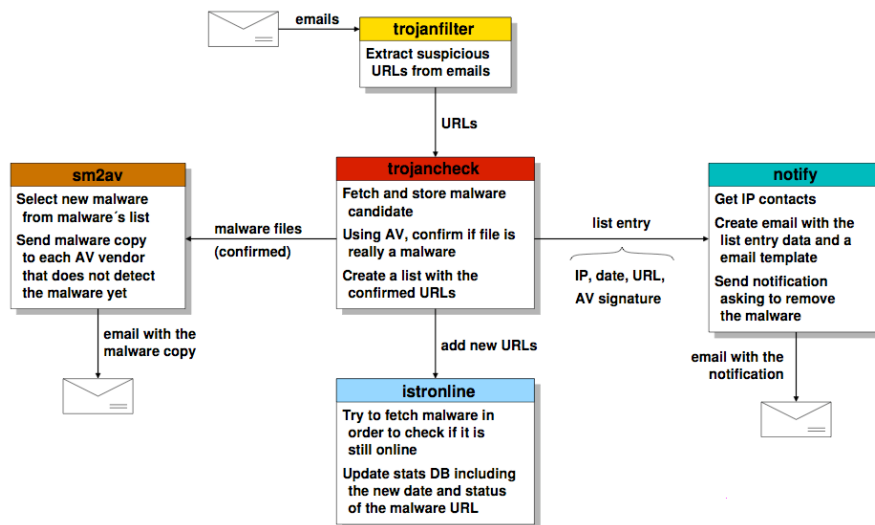
### 2003-2004

- Aumento dos casos de *phishing* mais sofisticados
  - Dados eram enviados dos *sites* falsificados para *sites* coletores
  - *Sites* coletores processavam os dados e os enviavam para contas de e-mail

### 2005-2006

- Spams usando nomes de diversas entidades e temas variados
  - *Links* para cavalos de tróia hospedados em diversos *sites*
  - Vítima raramente associa o spam recebido com a fraude bancária

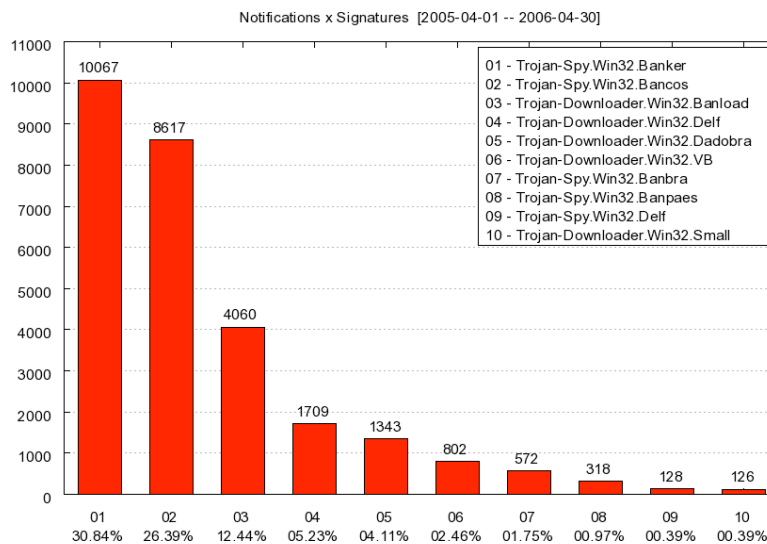
## Tratamento de Incidentes Envolvendo Fraudes



## Estatísticas de 01/04/2005 a 30/04/2006

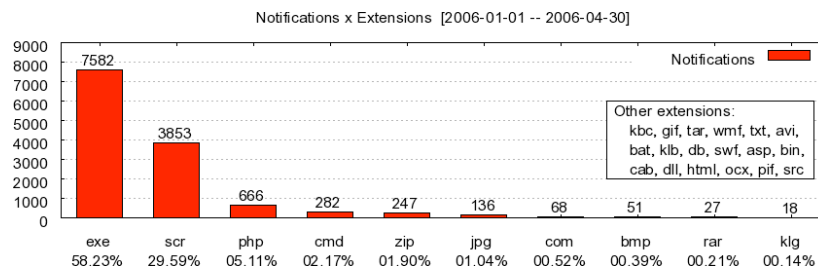
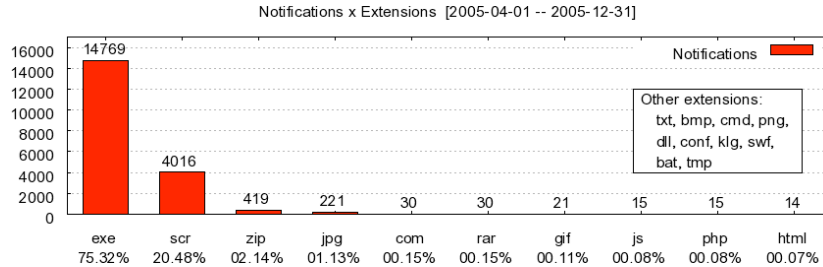
Categoria	Número
Domínios que estavam hospedando <i>trojans</i>	3.807
Contatos únicos para os domínios	1.782
Extensões usadas pelos arquivos de <i>trojans</i>	45
Nomes de arquivos utilizados pelos <i>trojans</i>	9.520
Nomes de máquinas ( <i>hosts</i> ) envolvidas	6.137
Endereços IP únicos	3.166
Países para os quais estavam alocados os IPs	68
<i>E-mails</i> de notificação enviados pelo CERT.br	15.556
URLs únicas encontradas no período	24.005
Diferentes assinaturas de antivírus	1.546

## Assinaturas Mais Comuns



Fonte das assinaturas: Kaspersky Lab.

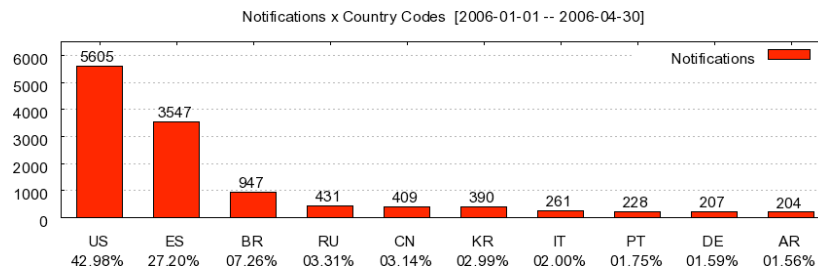
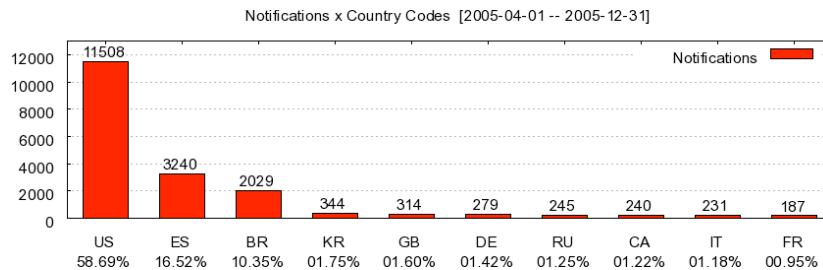
## Extensões Mais Comuns



CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

41/94

## Países para os quais Estavam Alocados os IPs



CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

42/94

### Eficiência dos Antivírus: 06/04/2005 a 30/04/2006

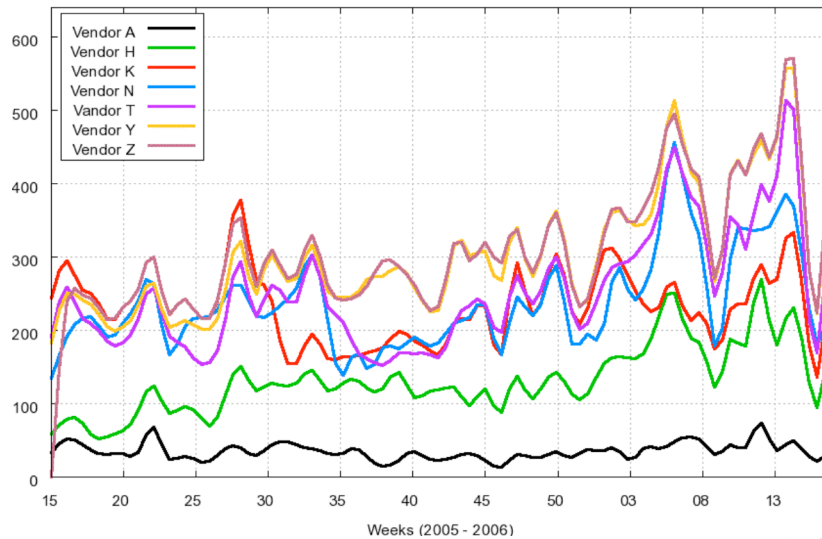
Empresa de Antivírus	Exemplares testados	Exemplares não detectados	Exemplares detectados	Taxa de detecção
Vendor A	18.634	1.913	16.721	89,73%
Vendor B	5.653	1.020	4.633	81,96%
Vendor D	18.519	5.475	13.044	70,44%
Vendor E	18.652	6.240	12.412	66,55%
Vendor F	18.665	6.857	11.808	63,26%
Vendor G	18.348	6.750	11.598	63,21%
Vendor H	18.666	7.324	11.342	60,76%
Vendor I	7.474	3.160	4.314	57,72%
Vendor K	14.603	8.873	5.730	39,24%
Vendor L	18.658	11.623	7.035	37,71%
Vendor N	18.371	12.866	5.505	29,97%
Vendor O	18.606	13.084	5.522	29,68%
Vendor P	14.126	10.162	3.964	28,06%
Vendor Q	18.541	13.395	5.146	27,75%
Vendor T	18.652	14.140	4.512	24,19%
Vendor Y	18.469	16.713	1.756	09,51%
Vendor Z	15.784	14.517	1.267	08,03%

Apenas 1 AV com taxa de detecção de 90%

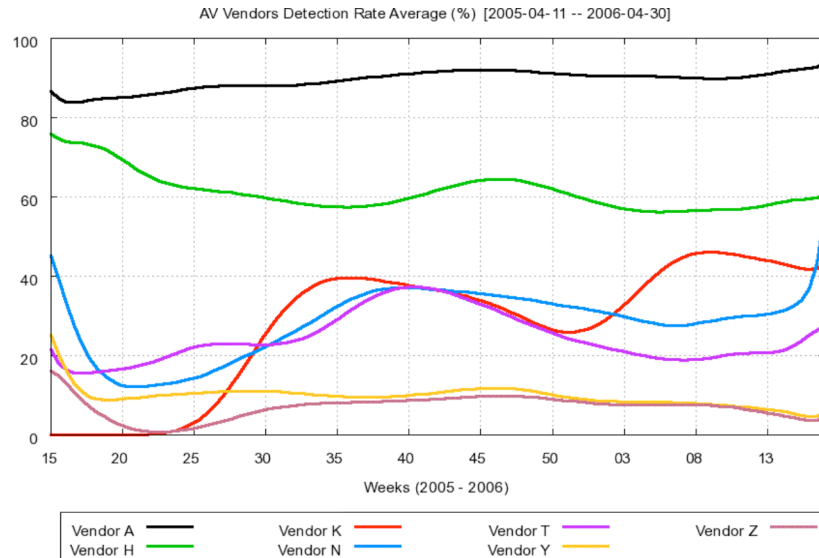
70% dos AV com menos de 40% de taxa de detecção

### Exemplares enviados: 11/04/2005 a 30/04/2006

Trojan Samples Sent [2005-04-11 -- 2006-04-30]



## Taxa de Detecção: 11/04/2005 a 30/04/2006



CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

45/94

## Operações da Polícia Federal

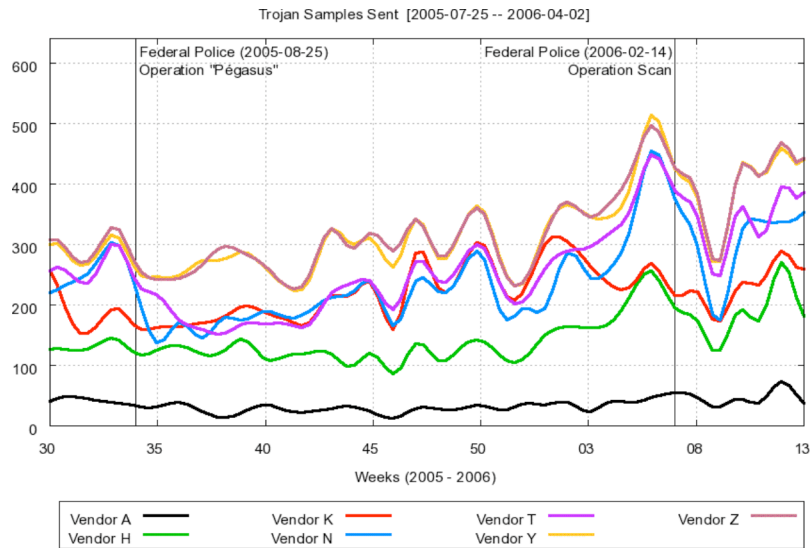
## Combatendo fraudes via Internet

- **2001: Operação Cash Net**, 17 pessoas presas
  - 1<sup>as</sup> implementações de *keylogger*, ataques de força bruta
- **2003: Operação Cavalo de Tróia I**, 27 pessoas presas
  - Spams, sites falsos, *{key,screen}loggers*, comprometimentos de DNS
- **2004: Operação Cavalo de Tróia II**, 64 pessoas presas
  - Organização criminosa, hierarquia, *{key,screen}loggers* sofisticados
- **2005: Operação Pégasus**, 85 pessoas presas
  - *{key,screen}loggers* ainda mais sofisticados, sobreposição de tela
- **2006: Operação Scan**, 63 pessoas presas
  - Líder tinha 19 anos, 9 eram menores de idade

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

46/94

## Operações da Polícia Federal (cont)



CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

47/94

## O Spam Visto como Incidente de Segurança

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

48/94



## Spam como Incidente de Segurança

Por que é importante tratá-lo como incidente

- Número grande de spams circulando na Internet
- Abuso dos computadores de usuários finais
  - Instalação de *bots*, utilizados para DDoS e envio de spam
- E-mail como vetor de propagação de vírus/*worms*
- Spam como meio para a prática de fraudes
- Bloqueio de spams apenas no destino não é ideal
  - Consumo de banda, disco, processamento
  - Contínuo esforço de configuração e de implantação de novas tecnologias

## Dificultando o Abuso da Sua Rede

*Spammers*, *bots*, *worms* e vírus usam o envio direto de e-mails de um cliente para um MTA destino para se propagar

- Fechar *proxies* e *relays* abertos
- Impedir o envio direto de e-mail a partir de estações clientes
  - Bloquear a porta 25/TCP para conexões de saída
  - Utilizar a porta 587/TCP (*mail submission port*)
- Implementar SMTP autenticado

## Combatendo a Falsificação de E-mails

Fraudadores e códigos maliciosos costumam forjar os remetentes das mensagens.

- **DKIM (*Domain Keys Identified Mail*)**
  - Técnica que permite checar o **cabeçalho** de uma mensagem (campo `From:`)
  - Consiste em assinar as mensagens para garantir a autenticidade do remetente
- **SPF (*Sender Policy Framework*)**
  - Técnica que permite checar o campo `MAIL FROM` do envelope de uma mensagem

## SPF

- Permite anunciar quais servidores podem enviar e-mail em nome de um domínio
- Anúncio feito via registro `TXT` do DNS

```
example.com. IN TXT "v=spf1 a mx ip4:192.0.2.32/27 -all"
```
- Permite checar se um e-mail foi enviado a partir de um servidor autorizado
- O anúncio e a checagem são operações independentes
- Diversas redes já estão utilizando SPF

## SPF (cont)

```
planalto.gov.br. 3204 IN TXT "v=spf1 ip4:200.181.15.0/24
ip4:200.198.192.192/27 ~all"

stj.gov.br. 10450 IN TXT "v=spf1 mx ip4:200.186.174.136 -all"

ctir.gov.br. 86137 IN TXT "v=spf1 mx -all"

caixa.gov.br. 3364 IN TXT "v=spf1 mx a:200.201.164.40
a:200.201.164.41 a:200.201.164.42 a:200.201.164.3 mx:200.201.166.143
mx:200.201.166.204 ~all"

cert.br. 86218 IN TXT "v=spf1 mx a:listas.cert.br -all"

uol.com.br. 3458 IN TXT "v=spf1 ip4:200.221.11.0/24
ip4:200.221.29.0/24 ip4:200.221.4.0/24 -all"

terra.com.br. 7200 IN TXT v=spf1 ip4:200.176.10.0/23 ip4:200.154.55.0/24
ip4:200.176.2.0/23 include:tmp-spf.terra.com.br include:ti-spf.terra.com.br
include:te-spf.terra.com.br -all
```

## Acompanhamento de Notificações de Abuso

- Criar e-mails da RFC 2142 (security@, abuse@).
- Manter os contatos de Whois atualizados
- O contato técnico do domínio deve ser um profissional que tenha contato com as equipes de abuso
- Redes com grupos de resposta a incidentes de segurança devem anunciar o endereço do grupo junto à comunidade
- Os endereços de contato não podem ter as mesmas regras anti-spam que o resto da organização

# Formas de Proteção

## Segurança desde o Princípio

- Planejamento do ambiente e da instalação
- Política de segurança
- Política de uso aceitável
- Investimento em treinamento
  - Administradores de redes
  - Desenvolvedores
  - Suporte, etc

## Política de Atualização e Correção

- Possuir uma política de atualização de sistemas operacionais e aplicação de *patches*
  - Sistema operacional (servidores e *desktops*)
  - Aplicativos
  - Hardware de rede
- Não aplicar apenas quando estiver sendo explorado
  - Tarde demais
- Seguir a política!

## Proteção da Rede Interna

Grande risco: propagação de códigos maliciosos internamente e de dentro para fora (*worms* e *bots*)

- Compartimentalização da rede
- Política de atualização e correção
- Política de conexão de equipamentos na rede interna
  - Terceirizados
  - *Notebooks* de funcionários
  - Redes *wireless*

## Segurança em Camadas

Não há uma solução única para resolver todos os problemas

- Combinar soluções
- *Firewall*, IDS, sistemas atualizados, serviços e aplicativos bem configurados, antivírus, etc
- Monitoramento dos registros de eventos (*logs*)
- Treinamento, atualização dos profissionais

## Ataques de Força Bruta contra SSH

Dicas de defesa:

- Utilizar senhas fortes em todas as contas
- Reduzir o número de equipamentos com serviço aberto
- Restringir a origem das conexões
- Acessar via chaves públicas
- Monitorar, monitorar, monitorar...

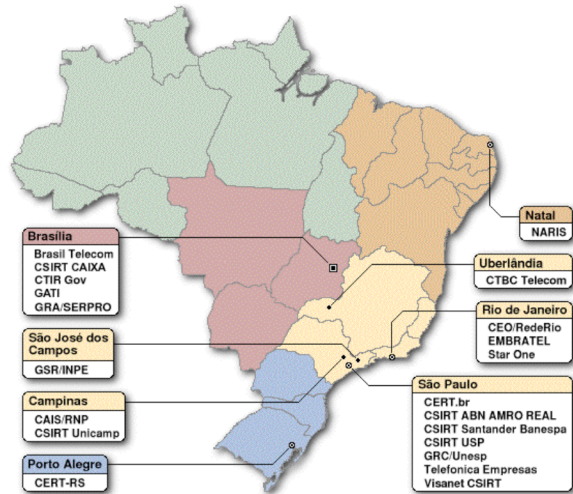
<http://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/>

# Iniciativas para Aumentar a Segurança

## Ações em Diversas Frentes

- Não há solução única
  - Combinar soluções e tecnologias, investir em treinamento e atualização dos profissionais
- Educação de usuários é fundamental
  - vetores disseminação de vírus/*worms/bots*
  - alvos de engenharia social (cavalos de tróia, fraudes, etc)
- Compartilhar informações e experiências
- Materiais gratuitos disponíveis
  - Cartilha de Segurança para Internet  
<http://cartilha.cert.br/>
  - Site Antispam.br  
<http://www.antispam.br/>
  - Práticas de Segurança para Administradores de Redes Internet  
<http://www.cert.br/docs/seg-adm-redes/>
- Monitoramento e acompanhamento de tendências

## Compartilhar Informações e Experiências é Fundamental



### CSIRTs Brasileiros

<http://www.cert.br/contato-br.html>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

63/94

## CSIRTs no Mundo

Incident Response Teams Around the World International cooperation speeds response to Internet security breaches.



Fonte: <http://www.cert.org/csirts/>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

64/94



## CSIRTs Membros do FIRST

The screenshot shows the FIRST website with a focus on the 'Member Teams' page. The page lists various incident response teams and their official names. A search bar is visible at the top of the member teams section.

Team	Official Team name
AAB GCIRT	ABN AMRO Global CERT
AboveSecCERT	Above Security Computer Emergency Response Team
ACERT	Army Emergency Response Team
ACERT	Accenture CERT
ACOnet-CERT	ACOnet-CERT
AF-CERT	Air Force CERT
Apple	Apple Computer
ARC4nt	The American Red Cross Computer Emergency Response Team
ACERT	Computer Emergency Response Team of the Argentine Public Administration
AT&T	AT&T
AusCERT	Australian Computer Emergency Response Team
Avaya-CERT	Avaya Global Computer Emergency Response Team
B1CSIRT	Bank One Computer Security Incident Response
BadgrT	University of Wisconsin-Madison
BOERT	Boeing CERT
BELNET CERT	BELNET CERT
BMO ISIRT	BMO InfoSec Incident Response Team
BP DSAC	BP Digital Security Alert Centre
BTCCERT	British Telecommunications CERT Co-ordination Centre
Bunker	The Bunker Security Team
CAIS/RNP	Brazilian Academic and Research Network CERT
CARNET CERT	Croatian Academic and Research Network CERT
CAT	Cable & Wireless Cyber Attack Team (membership suspended)
CCIRC	Canadian Cyber Incident Response Centre
CCSEC	Cablecom Security Team
CERTA	CERT-Administration
CERT.br	Computer Emergency Response Team Brazil
CERT-Bund	CERT-Bund
CERT@w	Computer Emergency Response Team Bundeswehr
CERTICC	CERT Coordination Center

Fonte: <http://www.first.org/about/organization/teams/>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

65/94

## CSIRTs Europeus

The screenshot shows the TI Directory website, which lists 'listed' CSIRTs in Europe. The page includes a navigation menu, a search bar, and a list of teams with their accreditation dates and names.

**CSIRT Teams**  
**TI Directory: "listed" CSIRTs presented alphabetically**

The following list contains all known (a.k.a. "listed") teams within Europe at this point in time. As "accreditation candidate" and "accredited" are - by definition - also known teams, they are contained in this list for your convenience.

This list is also available sorted by [countries](#).

Please note: if you know about another team, please send us [that information](#). If you find any error or misrepresentation, we apologise for that and ask you to send us [an update](#).

- Abuse TP S. A. (Poland)
- ACOnet-CERT (Austria) - "accredited" (28 March 2003)
- AMC-CERT (The Netherlands)
- AUTH-CERT (Greece)
- BE-CERT (Belgium) changed its name to BELNET CERT
- BELNET CERT (Belgium) - "accredited" (14 September 2004) - formerly known as BE-CERT
- BSI-CERT (Germany) changed its name to CERT-Bund
- BTCCERT (United Kingdom) - "accredited" (1 June 2001)
- BT SBS (United Kingdom) - "accredited" (1 June 2001)
- CARNET-CERT (Croatia) - "accredited" (9 September)
- CCSEC (Switzerland)
- CCTA (United Kingdom) changed its name to OGCBS
- CERN CERT (Switzerland)
- CERT POLSKA (Poland) - "accredited" (22 November 2001) - formerly known as CERT-NASK
- CERT-Bund (Germany) - formerly known as BSI-CERT

Fonte: <http://www.ti.terena.nl/teams/>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

66/94

## CSIRTs na Ásia e Oceania

The screenshot shows the 'Member Teams' page on the APCERT website. It features a map of the Asia-Pacific region with blue dots indicating member locations. Below the map is a table listing full members with their team names and countries.

Team	Official Team Name	Economy
<a href="#">AusCERT</a>	Australian Computer Emergency Response Team	Australia
<a href="#">BKIS</a>	Bach Khoa Internetwork Security Center	Vietnam
<a href="#">CCERT</a>	CERNET Computer Emergency Response Team	People's Republic of China
<a href="#">CNCERT/CG</a>	National Computer network Emergency Response technical Team / Coordination Center of China	People's Republic of China
<a href="#">HKCERT</a>	Hong Kong Computer Emergency Response Team Coordination Centre	Hong Kong, China
<a href="#">IDCERT</a>	Indonesia Computer Emergency Response Team	Indonesia
<a href="#">JPCERT/CC</a>	Japan Computer Emergency Response Team / Coordination Center	Japan
<a href="#">KICERT/CC</a>	Korea Internet Security Center	Korea
<a href="#">M-CERT</a>	Malaysian Computer Emergency Response Team	Malaysia
<a href="#">PH-CERT</a>	Philippine Computer Emergency Response Team	Philippine

Fonte: <http://www.apcert.org/about/structure/members.html>

# Cartilha de Segurança para Internet

## Cartilha de Segurança para Internet

Documento com recomendações e dicas para aumentar a segurança e proteção do usuário de ameaças na Internet.

- 2000: 1ª versão, em conjunto com a Abranet
- 2003: 2ª versão, ampliada, dividida em partes, também em HTML
- 2005: 3ª versão

Por que uma nova versão?

- Nos últimos anos surgiram novas ameaças
  - aumento no nº e nos tipos de fraude, uso em grande escala de códigos maliciosos
- e novas tecnologias
  - WPA, aumento da disponibilidade de dispositivos ligados em rede (celulares, PDAs), etc

## Cartilha de Segurança para Internet (cont)

Novidades na versão 3.0

- Incluídas novas situações na parte sobre Fraudes na Internet
- Novas tecnologias (WPA, celular, *bluetooth*)
- Criada uma parte dedicada a códigos maliciosos
- Mais de 50 novas entradas no Glossário
- Reformulação da página e reorganização do conteúdo
- Folders com dicas mais importantes

## Cartilha: Página Principal

cert.br

The screenshot shows the main page of the 'Cartilha de Segurança para Internet' website. The browser address bar shows 'http://cartilha.cert.br/'. The page header includes the 'cert.br' logo and the text 'Núcleo de Informação e Coordenação do Ponto br'. A navigation menu contains links for 'Início da Cartilha', 'Dicas', 'Download', 'Checklist', 'Glossário', and 'Sobre o CERT.br'. The main content area is titled 'Cartilha de Segurança para Internet' and features a red warning box: 'ATENÇÃO: Veja o aviso sobre a fraude envolvendo o nome do CERT.br e da Cartilha de Segurança para Internet'. Below this, a paragraph explains the handbook's purpose. A list of sections follows: 'Parte I: Conceitos de Segurança', 'Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção', 'Parte III: Privacidade', 'Parte IV: Fraudes na Internet', 'Parte V: Redes de Banda Larga e Redes Sem Fio (Wireless)', 'Parte VI: Spam', 'Parte VII: Incidentes de Segurança e Uso Abusivo da Rede', 'Parte VIII: Códigos Maliciosos (Malware)', 'Checklist', and 'Glossário'. On the right side, there is a 'Dica do Dia' section with a tip about mobile device security, a 'Sabe mais?' link, and a 'Copyright' section with links for 'Contato', 'Agradecimentos', and 'Revisões'. At the bottom of the page, it says 'CONIP 2006 - São Paulo - 27 a 29 de junho de 2006' and '71/94'. Logos for 'cgi.br' and 'nic.br' are in the bottom right corner.

## Cartilha: Dicas de Segurança

cert.br

The screenshot shows the 'Dicas de Segurança' page. The browser address bar shows 'http://cartilha.cert.br/dicas/'. The page header is identical to the main page. The main content area is titled 'Cartilha de Segurança para Internet' and states: 'Nesta página está disponível uma compilação de dicas básicas de segurança. Estas dicas também estão em 2 folhetos disponíveis para download. Para visualizá-los você precisa ter instalado em seu computador o software Acrobat Reader.' Below this, there are three sections of tips: 'Proteja-se de fraudes' with three bullet points, 'Proteja-se de vírus, cavalos de tróia, spywares, worms e bots' with three bullet points, and 'Navegue com segurança' with three bullet points. A fourth section, 'Cuide-se ao ler e-mails', is partially visible. On the right side, there are two download options: 'Folheto com dicas de segurança, formato A4, (102 KB)' and 'Folder com dicas de segurança, formato A4, (1.1 MB)'. Each option includes a small image of the respective document. At the bottom of the page, it says 'CONIP 2006 - São Paulo - 27 a 29 de junho de 2006' and '72/94'. Logos for 'cgi.br' and 'nic.br' are in the bottom right corner.

## Cartilha: Glossário

Cartilha de Segurança para Internet

Glossário

802.11  
Refere-se a um conjunto de especificações desenvolvidas pelo IEEE para tecnologias de redes sem fio.

**A**

**AC**  
Veja Autoridade certificadora.

**ADSL**  
Do Inglês *Asymmetric Digital Subscriber Line*. Sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidades maiores que as permitidas por um *modem* convencional.

**Adware**  
Do Inglês *Advertising Software*. Software especificamente projetado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem software livre ou prestam serviços gratuitos. Pode ser considerado um tipo de *spyware*, caso monitore os hábitos do usuário, por exemplo, durante a navegação na Internet para direcionar as propagandas que serão apresentadas.

# Site antispam.br

## Antispam.br: Página Principal

Comitê Gestor da Internet no Brasil

Sobre o NIC.br | Indicadores | **Antispam.br** | PTT.br

Inicio - Administradores de redes - Estatísticas - Sobre o Antispam.br

### antispam.br

- O que é spam?
- Problemas causados pelo spam
- Origem e curiosidades
- Tipos de spam
- Como identificar
- Prevenção
- Boas práticas
- Dicas
- Como reclamar
- FAQ
- Links
- Glossário
- Créditos
- Mapa do site

Busca

NIC.br Antispam.br  
CERT.br Registro.br

### O que é spam?

Veja os conceitos de spam e de spam zombies - que podem fazer com que você envie spam mesmo sem saber. Conheça também as motivações que levam tantas pessoas a enviar e-mails não solicitados.

### Participe da campanha

Divulgue esta iniciativa para estimular o uso cada vez mais saudável, correto e seguro das redes ligadas à Internet.

### Como identificar

O que você precisa saber para detectar spams. Saiba quais são as técnicas que estão sendo usadas para fazer o spam chegar em sua caixa de correio.

### Dicas de prevenção

Como se prevenir dos spams, que lotam as caixas de e-mails, demandam precioso tempo e atrapalham a evolução dos negócios.

### Não deixe seu computador se tornar um spam zombie

Se você não é cuidadoso ao usar a Internet e, entre outros procedimentos, não usa antivírus e não possui um firewall pessoal, você está correndo sério risco. Saiba o porquê.

egibr nic.br registro.br cert.br

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006 75/94

## Antispam.br: Tipos de Spam - códigos maliciosos

Comitê Gestor da Internet no Brasil

Sobre o NIC.br | Indicadores | **Antispam.br** | PTT.br

Inicio - Administradores de redes - Estatísticas - Sobre o Antispam.br

### antispam.br

- O que é spam?
- Problemas causados pelo spam
- Origem e curiosidades
- Tipos de spam
- Como identificar
- Prevenção
- Boas práticas
- Dicas
- Como reclamar
- FAQ
- Links
- Glossário
- Créditos
- Mapa do site

Busca

NIC.br Antispam.br  
CERT.br Registro.br

### Tipos de spam

**A lista**

### Códigos maliciosos

São programas que executam ações maliciosas em um computador. Diversos tipos de códigos maliciosos são inseridos em e-mails, contendo textos que se valem de métodos de engenharia social para convencer o usuário a executar o código malicioso em anexo. Em geral, estes códigos também são utilizados em spams enviados por fraudadores.

Dentre os códigos mais comuns enviados via spam, pode-se citar as seguintes categorias:

- Backdoor:** Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.
- Spyware:** Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.
- Keylogger:** Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.
- Screenlogger:** Forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.
- Cavale de tréia:** Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

egibr nic.br

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006 76/94

## Antispam.br: Tipos de Spam - fraudes

The screenshot shows the website interface for 'Tipos de Spam - fraudes'. The browser address bar shows 'http://www.antispam.br/tipos/fraudes/'. The page header includes 'Comitê Gestor da Internet no Brasil' and navigation links for 'Sobre o NIC.br', 'Indicadores', 'Antispam.br', and 'PTT.br'. The main content area is titled 'Tipos de spam' and features a sub-section for 'Fraudes'. The text explains that fraudsters often use e-mails to attack and steal data from servers of financial or commercial institutions. It also mentions that fraudsters use e-mails to obtain advantages, such as installing malicious code or accessing fraudulent pages. An illustration shows a hand holding a gun pointing at a computer monitor. A sidebar on the left contains a navigation menu with items like 'O que é spam?', 'Problemas causados pelo spam', and 'Busca'. The footer of the page displays 'CONIP 2006 - São Paulo - 27 a 29 de junho de 2006' and '77/94'.

## Antispam.br: Dicas

The screenshot shows the website interface for 'Dicas'. The browser address bar shows 'http://www.antispam.br/dicas/'. The page header is similar to the previous page. The main content area is titled 'Dicas' and provides advice on how to avoid spam. It includes sections for 'Preserve sua privacidade', 'Mantenha-se informado', and 'Proteja-se'. An illustration shows a computer monitor surrounded by flames and a barbed wire fence. The sidebar on the left is identical to the previous page. The footer of the page displays 'CONIP 2006 - São Paulo - 27 a 29 de junho de 2006' and '78/94'.

## Antispam.br: Glossário

## Antispam.br: Administradores



# Práticas de Segurança para Administradores de Redes Internet

## Práticas de Segurança para Administradores

- Reune um conjunto de boas práticas em configuração, administração e operação segura de redes conectadas à Internet
  - Recomendações para obter o mínimo necessário de segurança
- implantação destas práticas minimiza as chances de ocorrerem problemas de segurança
- facilita a administração das redes e recursos de forma segura
- recomendações apresentadas são eminentemente práticas
- Independentes de plataforma de software e hardware
- A maioria dos princípios expostos é genérica
- Dirigido ao pessoal técnico de redes conectadas à Internet (administradores de redes, sistemas e/ou segurança)

## seg-adm-redes: Página Principal

Núcleo de Informação e Coordenação do Ponto br English cert.br  
Home CSIRT's no Brasil Estatísticas Cursos Documentos Mapa do Site FAQ

Práticas de Segurança para Administradores de Redes Internet

Versão para Impressão (PDF)  
Versão 1.2  
16 de maio de 2003  
Copyright © NBSO

Sumário

- 1. Introdução
  - 1.1. Organização do Documento
  - 1.2. Como Obter este Documento
  - 1.3. Nota de Copyright e Distribuição
- 2. Políticas
  - 2.1. Políticas de Segurança
  - 2.2. Políticas de Uso Aceitável
- 3. Instalação e Configuração Segura de Sistemas
  - 3.1. Preparação da Instalação
  - 3.2. Estratégias de Particionamento
  - 3.3. Documentação da Instalação e Configuração
  - 3.4. Senhas de Administrador
  - 3.5. Instalação Mínima
  - 3.6. Desativação de Serviços Não Utilizados
  - 3.7. Instalação de Conexões
  - 3.8. Prevenção de Abuso de Recursos
    - 3.8.1. Controle de Relay em Servidores SMTP
    - 3.8.2. Controle de Acesso a Proxies Web
- 4. Administração e Operação Segura de Redes e Sistemas
  - 4.1. Educação dos Usuários
  - 4.2. Ajuste do Relógio
    - 4.2.1. Sincronização de Relógios
    - 4.2.2. Timezone

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006 83/94 egi.br nic.br

# Monitoramento e Acompanhamento de tendências

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006 84/94 egi.br nic.br

## Acompanhamento de Tendências

- Acompanhar listas de discussão e *sites* que mantenham notícias e estatísticas sobre o assunto
- Analisar registros de eventos (*logs*)
- Acompanhar projetos de *Early Warning* nacionais e internacionais
  - *Internet Storm Center*
  - ARAKIS
  - ISDAS - *Internet Scan Data Acquisition System*
  - eCSIRT.net - *The European CSIRT Network*
  - *The Team Cymru Darknet Project*
  - Concórcio Brasileiro de Honey pots

## Internet Storm Center

SANS - Internet Storm Center - Cooperative Cyber Threat Monitor And Alert System

http://isc.sans.org/

SANS Homepage SANS Bookstore SANS Reading Room SANS Portal

INTERNET STORM CENTER GREEN SANS FIRE Washington, DC SC July 5th - 13th 2006

Handler on Duty: Johannes Ullrich 17:14:44 UTC Jun 19 2006, 13:14:44 Jun 19 2006

Trends Top 10 Reports Contact About INFOCon Presentations Links XML print

Handler's Diary: Rumors about IIS 6.0 issues

Port Lookup: 80 go IP Lookup go

How to Join?

SANS FIRE: Meet your favorite handlers in person

Search

+ Port Graph + Port History + Today's Diary + Papers and Analysis - Survival Time - Database

SANS FIRE: Meet your favorite ISC handlers in person. (July 5th-13th, Washington DC)

Today's Diary

Show | default | stories

previous -

Rumors about IIS 6.0 issues (NEW)

Published: 2006-06-19, Last updated: 2006-06-19 16:55:48 UTC by Johannes Ullrich (Version: 2)(click to highlight changes)

Update: All feedback we received so far points to the microsoft.fr being an isolated issue.

Microsoft confirmed that this does not appear to be a 0-day exploit. The defaced website was outsourced and not under direct Microsoft control. No other Microsoft website was hit.

Some persistent rumors talk about a possible new exploit (0-day?) against IIS 6.0. The defacement of experts.microsoft.fr is used as evidence. At this point, we have nothing to support that claim. If you have any additional evidence, please [let us know](#). An image of the

Poll

Are you using a browser plugin to alert you of unsafe websites?

Yes, I use Netcraft's Plugin

Yes, I use Siteadvisor (McAfee)

Yes, I use something else or multiple plugins

No, I didn't know about it.

No, I am concerned about privacy

No, I don't think they help

No for some other reason

add comment

Vote

see results

Database Status

Reports Processed:  
Last Month: 644,131,266  
Last Week: 123,891,340  
Last 24hrs: 17,795,256

World Map

Fonte: <http://isc.sans.org/>

## Internet Storm Center (cont)

**Distributed Intrusion Detection System**  
**DShield.org**

**Records Added**  
 Last Month: 644,131,266  
 Last Week: 123,891,340  
 Today: 17,795,256  
 Sunday: 23 mil  
 As of Mon Jun 19 17:22:25 2006 UTC

**Internet Storm Center Status**  
green Rumors about LIS 6.0 issues

**(ISC Daily Trends Page)**  
 Top Attacker: 60.213.15.85  
 Most Attacked Port: 1026

**Port Report**  
 Port: 1433

**Geographic Distribution of attack sources. Last days**  
 DShield, The Movie

**Are you cracked? Click here to see.**  
 DShield provides a platform for users of firewalls to share intrusion logs

**Records**

Date	Sources	Targets	Records
2006-06-19	4880	100982	852707
2006-06-18	9337	131978	1163025
2006-06-16	9365	102089	897522
2006-06-15	7760	470737	1485023

**Services registered for Neohapsis)**

Protocol	Service
tcp	ms-sql-s Microsc
udp	ms-sql-s Microsc

Fonte: <http://www.dshield.org/>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006 87/94

cgi.br nic.br

## ARAKIS

**arakis**  
 agregacja, analiza i klasyfikacja incydentów sieciowych

Aktualizacja strony: 2006-06-19 16:07 [odtwórz] [kontakt]

**zdarzenia w sieci**

**trend krótkookresowy**

dst. port: 23/TCP

dst. port: 137/UDP

**porty aktywne**

Numer portu	aktywność
1434/UDP	98.9%
1433/TCP	98.6%
445/TCP	88.8%
137/UDP	76.3%
1080/TCP	70%
139/TCP	67.4%
22/TCP	54.9%
8026/TCP	54.3%
80/TCP	47.4%
4105/TCP	43.3%

**zagrożenia z Polski**

**zagrożenia ze świata**

**linki**  
 Mapa zagrożeń z Polski  
 Mapa zagrożeń ze świata  
 Zaobserwowane prefiksy /8  
 FAQ

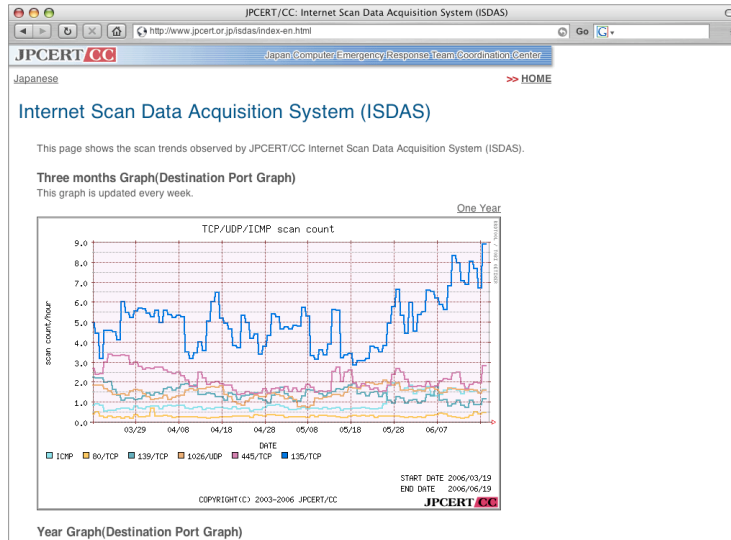
**archiwum**  
 VI/2006  
 13 14 15 16 17 18 19

Fonte: <http://www.arakis.pl/>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006 88/94

cgi.br nic.br

## ISDAS - Internet Scan Data Acquisition System

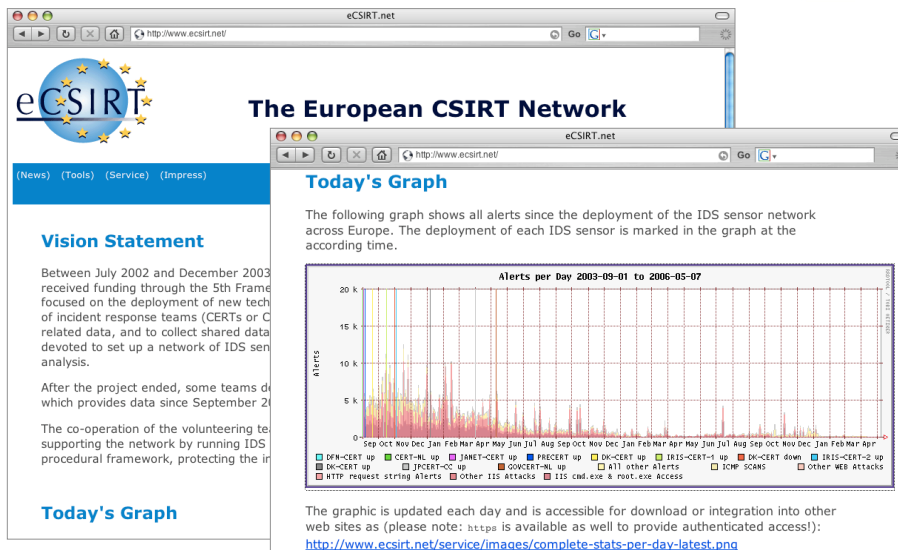


Fonte: <http://www.jpCERT.or.jp/isdas/index-en.html>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

89/94

## eCSIRT.net - The European CSIRT Network



Fonte: <http://www.ecsirt.net/>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

90/94

## The Team Cymru Darknet Project

The screenshot shows two browser windows. The top window displays the main project page with the title "The Team Cymru Darknet Project", a red dragon logo, and version information: "Version 1.4 04 JUN 2004 team-cymru@cymru.com". Below this is a "HOME" link and a list of "Changes in version 1.4" including added snippet samples for ntp.conf and resolv.conf, added ipt rules for NTP and DNS, and added ipt logging suggestions. "Changes in version 1.2" include additional routing suggestions and aesthetic changes. An "Introduction" section explains that tracking compromised machines is difficult and that the Darknet is a portion of routed, allocated IP space.

The bottom window shows the "TEAM CYMRU Darknet Incoming Traffic Stats" page. It features a red dragon logo and a green traffic graph. The graph shows "dark traffic b/s" over time, with a peak around 20 kbps. Text on the page includes: "This data was last updated at Sun May 14 04:35:00 2006 GMT", "Darknet Server Info DARK01 (ARIN)", "Average Traffic: 3.5kbps", "Current Traffic: 2.9kbps", "Dark Space: /24 x6", and "Dark IPs: 1,536".

Fonte: <http://www.cymru.com/Darknet/>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

91/94

## Concórdio Brasileiro de Honeypots

The screenshot shows the website for the "Consórcio Brasileiro de Honeypots Projeto Honeypots Distribuídos". The page has a search bar and a navigation menu on the left with links for "English", "Página Principal", "Honeynet.BR", "Estatísticas", "Links Ferramentas", "Timeline Press", and "Membros". The main content area includes a section "Sobre o Projeto Honeypots Distribuídos" with a description of the project's goals and a list of objectives: "Implantar uma rede distribuída de honeypots de baixa interatividade (Honeyd)", "buscando cobrir a maior parte do espaço de endereços IP da Internet no Brasil", and "Montar um sistema de análise de dados que permita o estudo de correlações e tendências de ataques".

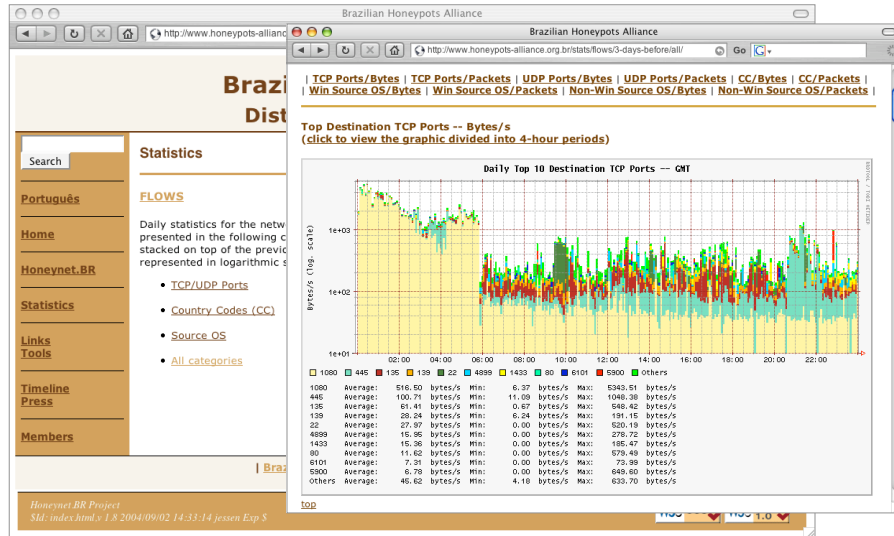
Below this is a section "Localização dos Honeypots" featuring a map of Brazil with numbered markers (16, 23, 02, 07, 09, 05, 11, 18, 06, 03) indicating the locations of honeypots across the country. To the right of the map is a list of "Alliance Members" including ANSP, Brasil Telecom, CBPF, CERPIA, CERT.br, CERT-RS, CTBC Telecom, Duxco, Durand, Embratel, Flocruz, FITE, HP-Brasil, JME, INPE, ITA, ITAL, LNCC, Ministério da Justiça, Pop-PB, PUC-RIO, RedeRio, TCU, UDESC, UFPA, UFPI, UFRN, UFSC-DAS, UNESP, UNICAMP, UNITAU, UFF, USP, UNB LabRedes, and VIVAX.

Fonte: <http://www.honeypots-alliance.org.br/>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

92/94

## Concórdio Brasileiro de Honeypots



Fonte: <http://www.honeypots-alliance.org.br/stats/>

CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

93/94

## Referências

- Esta palestra  
<http://www.cert.br/docs/palestras/>
- Indicadores do CGI.br  
<http://www.nic.br/indicadores/>
- Estatísticas do CERT.br  
<http://www.cert.br/stats/>
- Antispam.br  
<http://www.antispam.br/>
- Cartilha de Segurança para Internet  
<http://cartilha.cert.br/>
- Práticas de Segurança para Administradores de Redes Internet  
<http://www.cert.br/docs/seg-adm-redes/>
- Cursos Oficiais do CERT®/CC ministrados pelo CERT.br  
<http://www.cert.br/cursos/>



CONIP 2006 - São Paulo - 27 a 29 de junho de 2006

94/94