Segurança da Internet no Brasil:
Estudos e Iniciativas

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

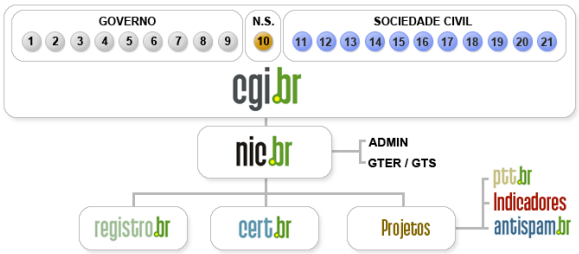
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br
http://www.cert.br/

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

Agenda

- Sobre o CGI.br e o CERT.br
- Indicadores do CGI.br
- Estatísticas do CERT.br
- Iniciativas de 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

http://www.cgi.br/sobre-cg/

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
- Manutenção de estatísticas sobre incidentes de segurança
- 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® Program
- Coordenação do “Consórcio Brasileiro de Honeypots”
- Membro do FIRST e da Honeynet Research Alliance
- Anti-Phishing Working Group (APWG) Research Partner

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 (2)

TIC Domicílios

Tabela 10 - População segundo PNAD 2003 = 173.966.052

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 (3)

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 - Freqüência de atualização do antivírus
- 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 Domícilios

F1 - Problemas de Segurança Encontrados Usando a Internet

Percentual sobre o total de usuários Internet

	Nenhum	Vírus (com acesso não autorizado)	Virus (com danos em SW ou HW)	Abuso de Informação pessoal	Fraude	Outro	Não lembra
Total	40,99	19,64	7,13	1,67	0,94	1,10	0,24

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
Total	69,76	19,33	22,09

F3 - Freqüência 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

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
Total	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
Total	95,72	59,46	54,11	49,48	42,33	21,12	29,21	69,62	38,33	19,69

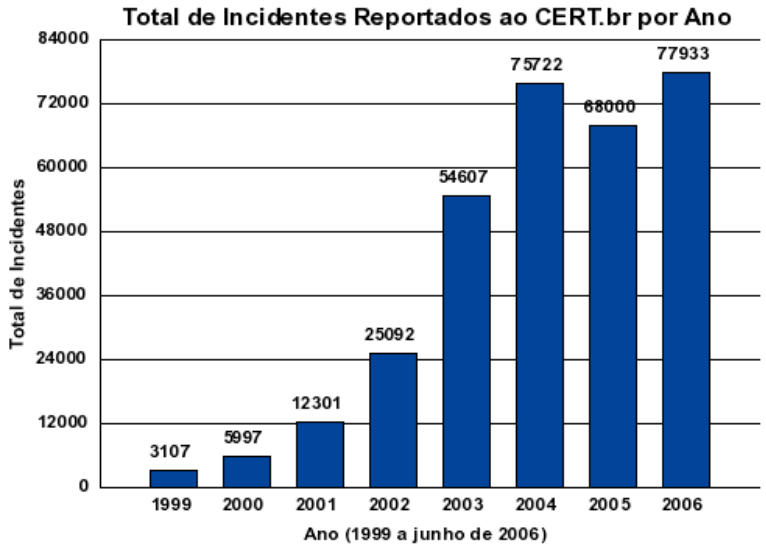
E3 - Freqüência de Atualização do Antivírus

Percentual sobre o total de empresas com acesso à Internet

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

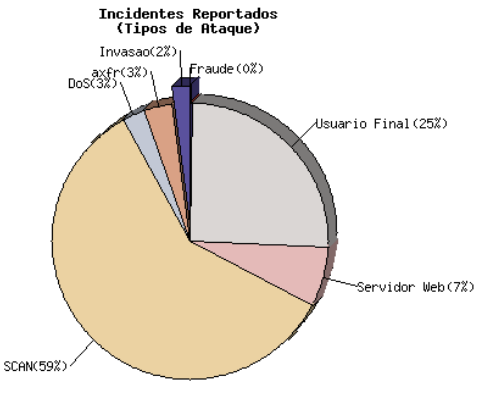
Estatísticas do CERT.br

Notificações de Incidentes: 1999-2006

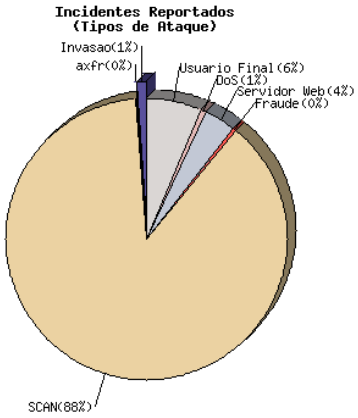


Evolução dos Tipos de Ataques

2000

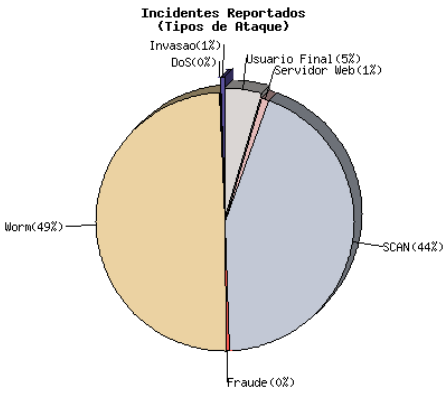


2001

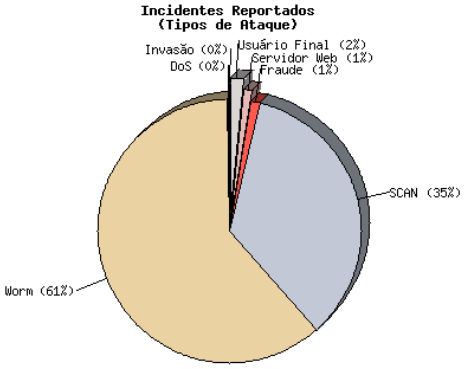


Evolução dos Tipos de Ataques (cont)

2002

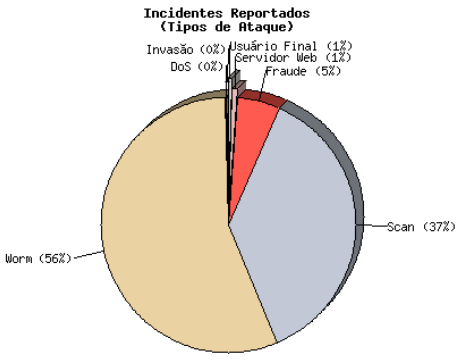


2003

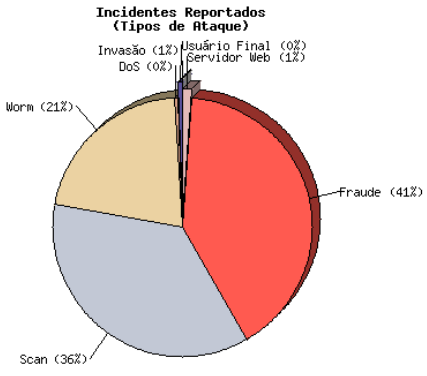


Evolução dos Tipos de Ataques (cont)

2004



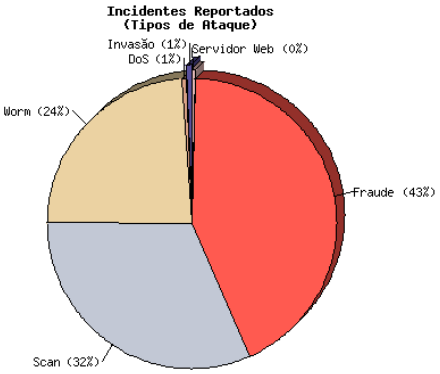
2005



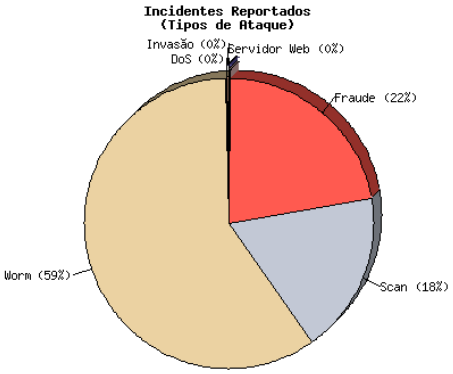
Evolução dos Tipos de Ataques (cont)

2006

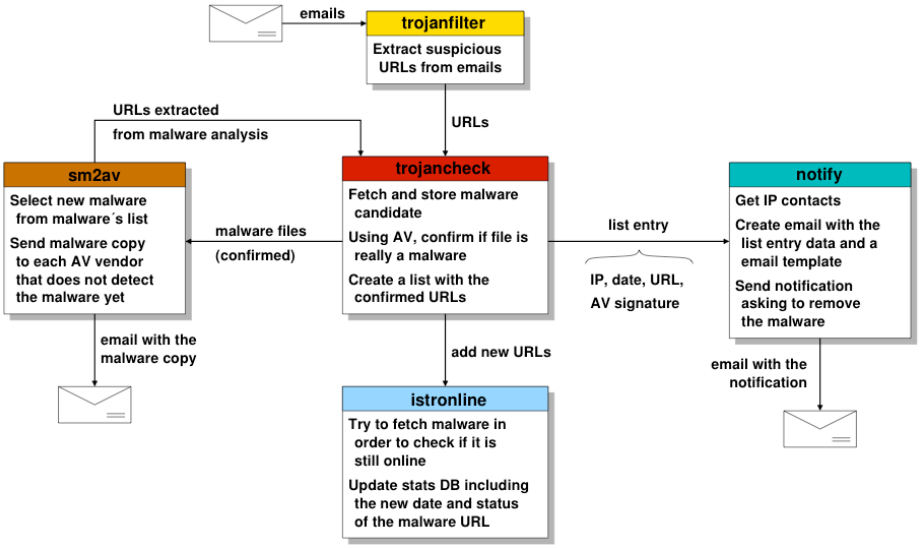
1º Trimestre:



2º Trimestre:



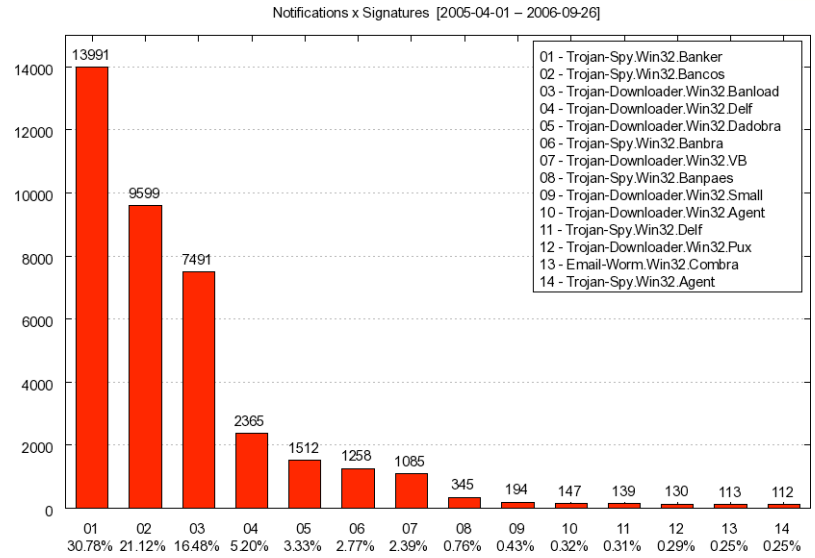
Tratamento de Incidentes Envolvendo Fraudes



Estatísticas de 01/04/2005 a 26/09/2006

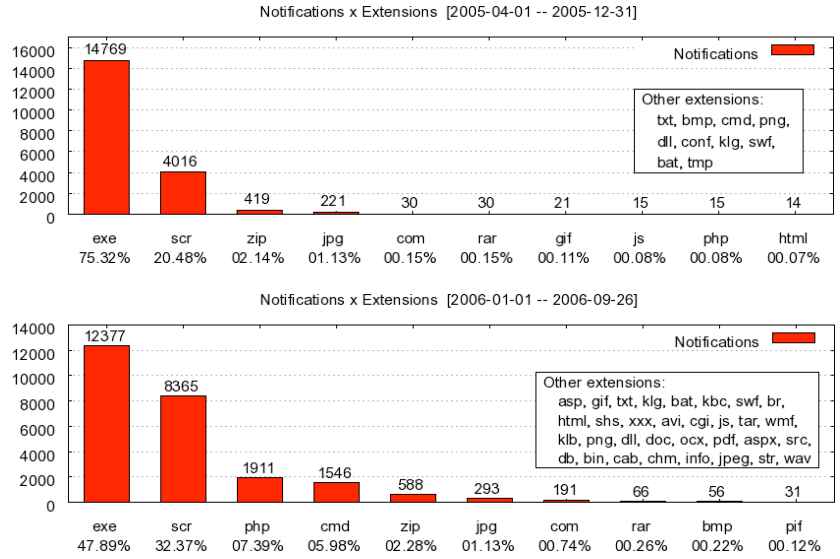
Categoria	Número
Domínios que estavam hospedando *trojans*	6.284
Contatos únicos para os domínios	2.552
Extensões usadas pelos arquivos de *trojans*	68
Nomes de arquivos utilizados pelos *trojans*	14.237
Nomes de máquinas (*hosts*) envolvidas	10.818
Endereços IP únicos	4.686
Países para os quais estavam alocados os IPs	75
E-mails de notificação enviados pelo CERT.br	23.709
URLs únicas encontradas no período	33.946
Assinaturas de antivírus (agrupadas)	161
Assinaturas de antivírus (com variantes)	2.418

Assinaturas Mais Comuns

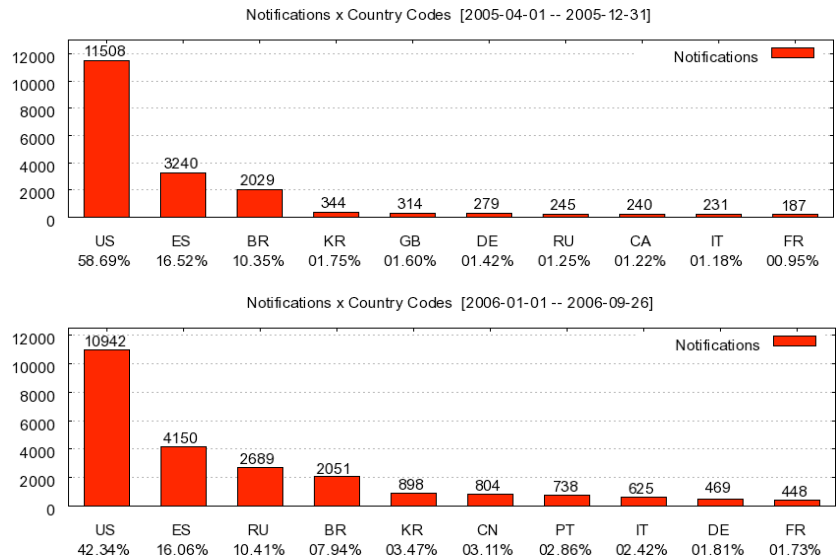


Fonte das assinaturas: Kaspersky Lab.

Extensões Mais Comuns



Países para os quais Estavam Alocados os IPs



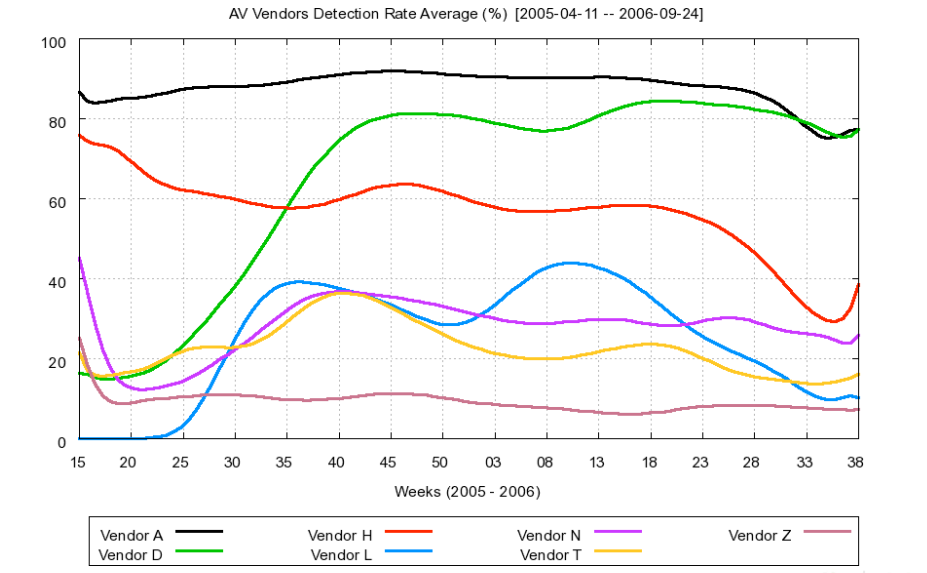
Eficiência dos Antivírus: 06/04/2005 a 26/09/2006

Empresa de Antivírus	Exemplares testados	Exemplares não detectados	Exemplares detectados	Taxa de detecção (%)
Vendor A	26.492	3.164	23.328	88,06
Vendor B	5.651	1.019	4.632	81,97
Vendor C	790	240	550	69,62
Vendor D	26.526	8.300	18.226	68,71
Vendor E	26.342	8.787	17.555	66,64
Vendor F	26.513	8.856	17.657	66,60
Vendor G	26.219	10.512	15.707	59,91
Vendor H	26.527	11.576	14.951	56,36
Vendor I	15.337	7.559	7.778	50,71
Vendor K	17.888	10.846	7.042	39,37
Vendor L	22.462	15.142	7.320	32,59
Vendor N	26.215	18.592	7.623	29,08
Vendor O	26.160	18.653	7.507	28,70
Vendor P	21.988	15.836	6.152	27,98
Vendor Q	26.524	19.168	7.356	27,73
Vendor T	26.509	20.595	5.914	22,31
Vendor Z	26.281	23.906	2.375	9,04

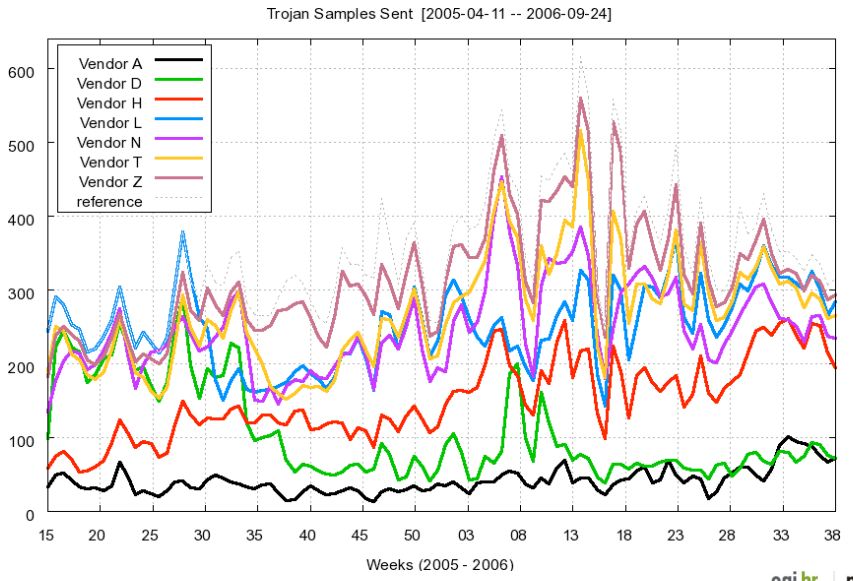
Apenas **2** fabricantes com taxa de detecção acima de **80%**

~70% dos fabricantes com menos de **40%** de taxa de detecção

Taxa de Detecção: 11/04/2005 a 24/09/2006



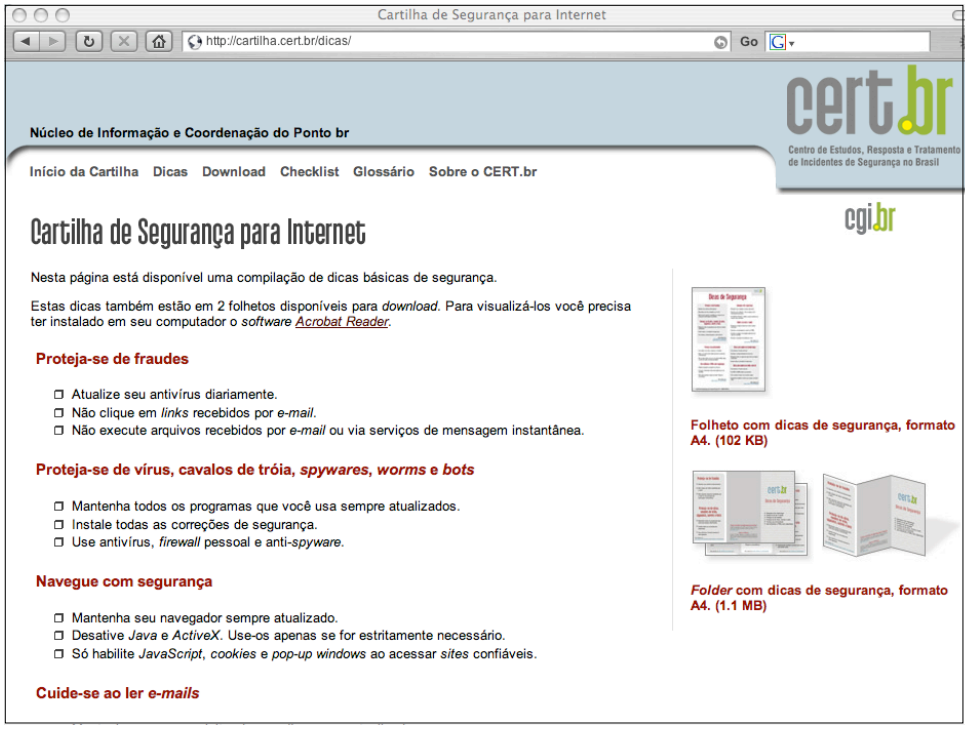
Exemplares enviados: 11/04/2005 a 24/09/2006



Iniciativas para Aumentar a Segurança

Ações em Diversas Frentes

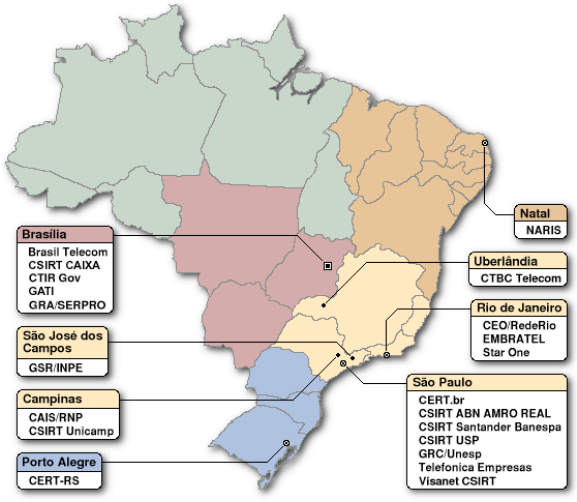
- Não há solução única
  - Combinar soluções e tecnologias
  - Investir em treinamento e atualização dos profissionais
- Educação de usuários é fundamental
  - vetores disseminação de worms/vírus
  - alvos de engenharia social (trojans, fraudes, etc)
- Materiais gratuitos disponíveis
  - Práticas de Segurança para Administradores de Redes Internet
    http://www.cert.br/seg-adm-redes/
  - Cartilha de Segurança para Internet
    http://cartilha.cert.br/
  - Site Antispam.br
    http://www.antispam.br/


Cartilha de Segurança para Internet
http://cartilha.cert.br/dicas/
Go
Núcleo de Informação e Coordenação do Ponto br
cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Início da Cartilha Dicas Download Checklist Glossário Sobre o CERT.br
cgi.br
Cartilha de Segurança para Internet
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.
Proteja-se de fraudes
Atualize seu antivírus diariamente.
Não clique em links recebidos por e-mail.
Não execute arquivos recebidos por e-mail ou via serviços de mensagem instantânea.
Proteja-se de vírus, cavalos de tróia, spywares, worms e bots
Mantenha todos os programas que você usa sempre atualizados.
Instale todas as correções de segurança.
Use antivírus, firewall pessoal e anti-spyware.
Navegue com segurança
Mantenha seu navegador sempre atualizado.
Desative Java e ActiveX. Use-os apenas se for estritamente necessário.
Só habilite JavaScript, cookies e pop-up windows ao acessar sites confiáveis.
Cuide-se ao ler e-mails
Folheto com dicas de segurança, formato A4. (102 KB)
Folder com dicas de segurança, formato A4. (1.1 MB)


Antispam.br ::
http://www.antispam.br/
Go
Comitê Gestor da Internet no Brasil
Sobre o NIC.br | Indicadores | Antispam.br | PTT.br
nic.br
Núcleo de Informação e Coordenação
antispam.br
Início - Administradores de redes - Estatísticas - Sobre o 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
ok
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.
Participe da campanha
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.
cert.br
Cartilha de Segurança para Internet
nic.br
Indicadores
registro.br
cgi.br
Comitê Gestor da Internet no Brasil
nic.br
Núcleo de Informação e Coordenação
registro.br
Registro de Domínios para a Internet no Brasil
cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes

Compartilhar Informações e Experiências é Fundamental

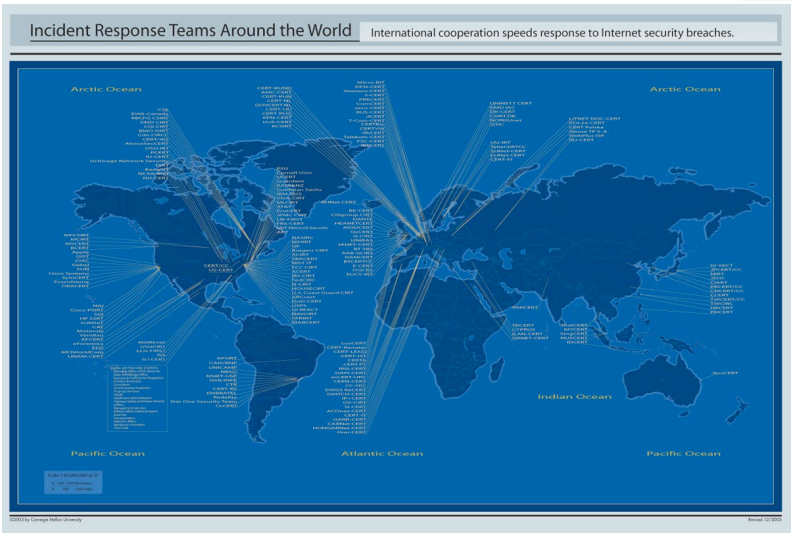
cert.br



CSIRTs Brasileiros
http://www.cert.br/contato-br.html

cgi.br nic.br

Também com Grupos de Outros Países



CSIRTs no Mundo
http://www.cert.org/csirts/

Referências

- Esta palestra
  http://www.cert.br/docs/palestras/
- Indicadores do CGI.br
  http://www.nic.br/indicadores/

- Antispam.br
  http://www.antispam.br/
- Material de Apoio para CSIRTs
  http://www.cert.br/csirts/
- Cartilha de Segurança para Internet
  http://cartilha.cert.br/
- Cursos Oficiais do CERT® Program ministrados pelo CERT.br
  http://www.cert.br/cursos/