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/

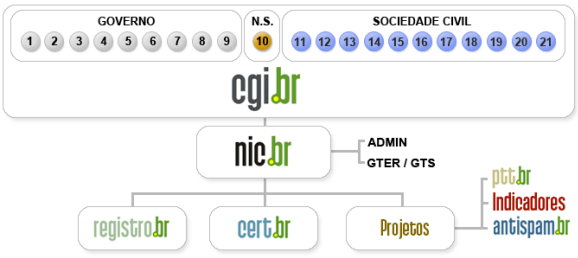
Motivação

- Analisar estastísticas 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 Honeypots”

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 domicilios (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 - Freqüência de atualização do antivírus
  - J - Spam
    - J1 - Recebimento de spam na principal conta de e-mail de uso pessoal
    - J2 - Freqüência 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)	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
Região							
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	-
Faixa Etária							
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	-	-

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
Total	69,76	19,33	22,09
Renda			
< 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
Faixa Etária			
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

TIC Domicílios (cont)

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
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 - Freqüência 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

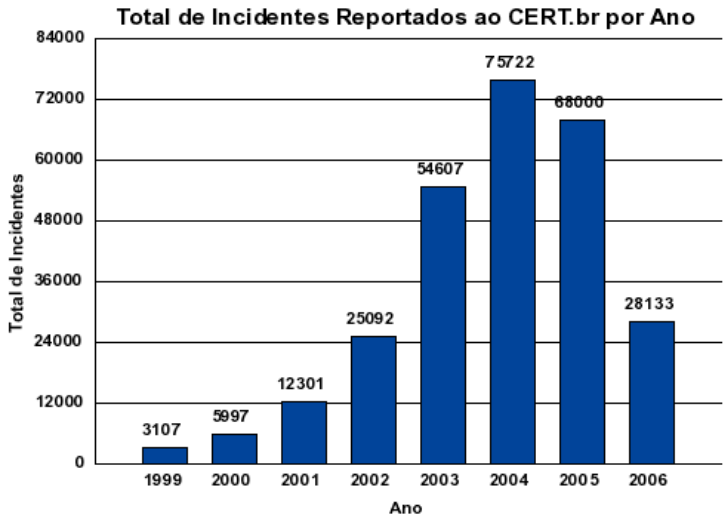
E3 - Freqüência de Atualização do Antivírus

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

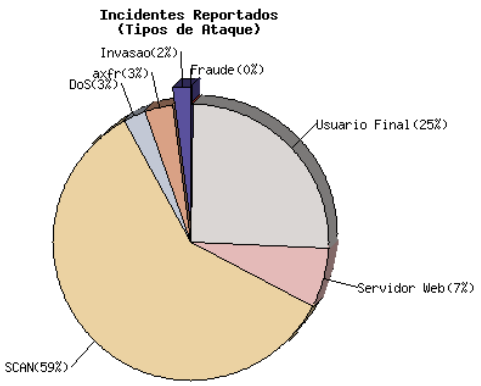
Notificações de Incidentes: 1999-2006



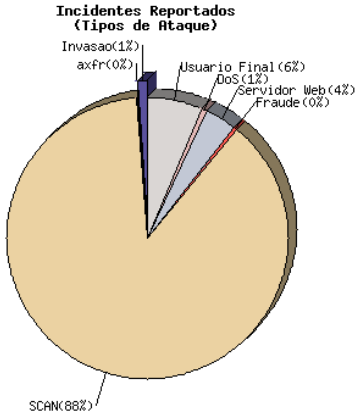
Obs.: Os dados de 2006 são referentes ao primeiro trimestre do ano.

Evolução dos Tipos de Ataques

2000

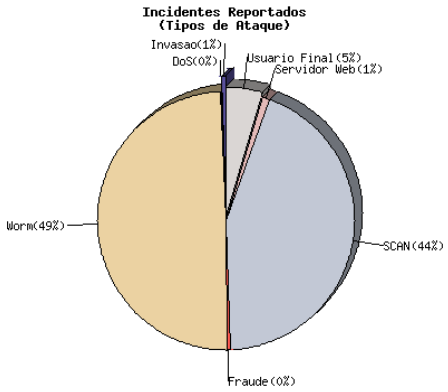


2001

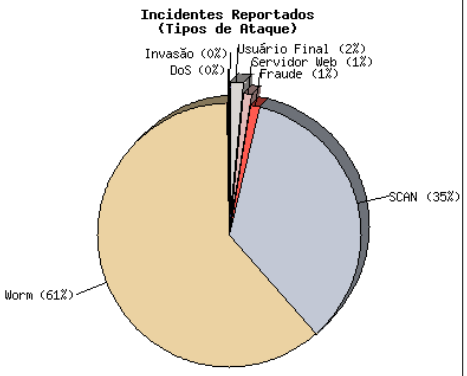


Evolução dos Tipos de Ataques (cont)

2002

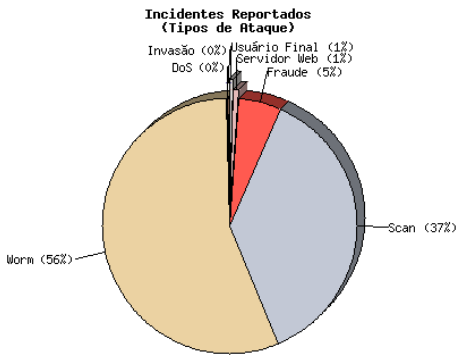


2003

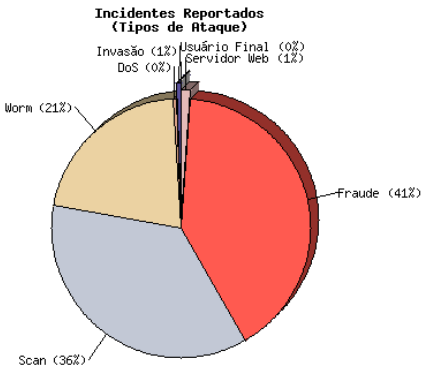


Evolução dos Tipos de Ataques (cont)

2004

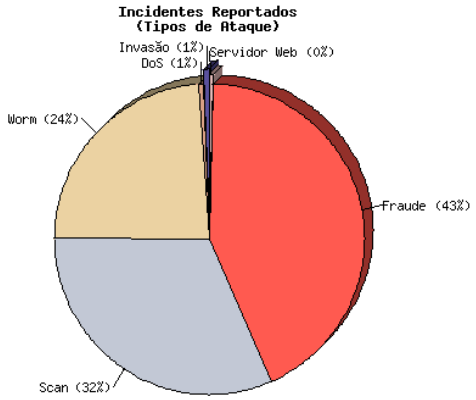


2005



Evolução dos Tipos de Ataques (cont)

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
  - Dedicação 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/
http://www.cert.org/archive/pdf/03tr001.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

- 1os *keyloggers* enviados por e-mail, ataques de força bruta

2002-2003

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

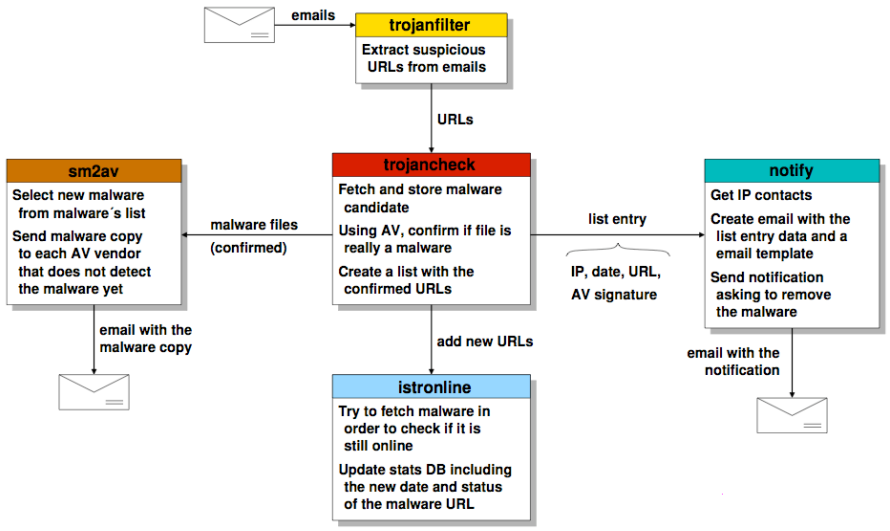
2003-2004

- 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

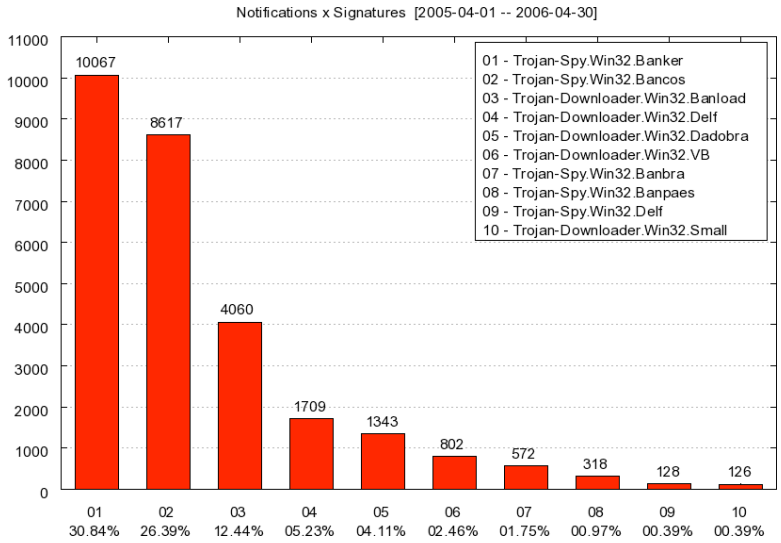
Tratamento de Incidentes Envolvendo Fraudes



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

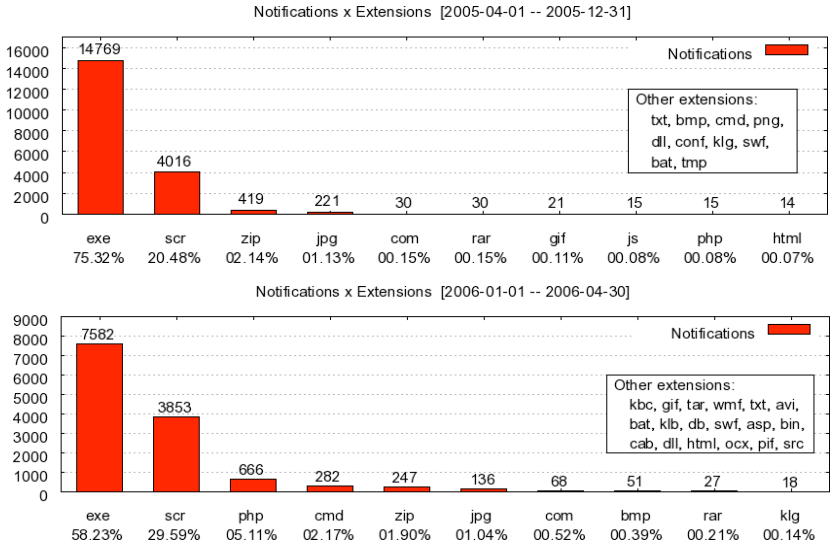
Categoria	Número
Domínios que estavam hospedando *trojans*	3.807
Contatos únicos para os domínios	1.782
Extensões usadas pelos arquivos de *trojans*	45
Nomes de arquivos utilizados pelos *trojans*	9.520
Nomes de máquinas (*hosts*) envolvidas	6.137
Endereços IP únicos	3.166
Países para os quais estavam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

Assinaturas Mais Comuns

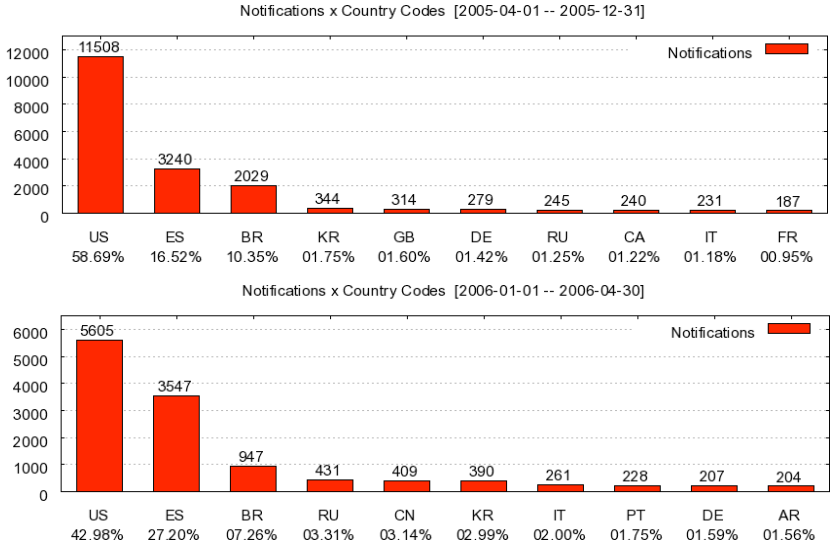


Fonte das assinaturas: Kaspersky Lab.

Extensões Mais Comuns



Países para os quais Estavam Alocados os IPs



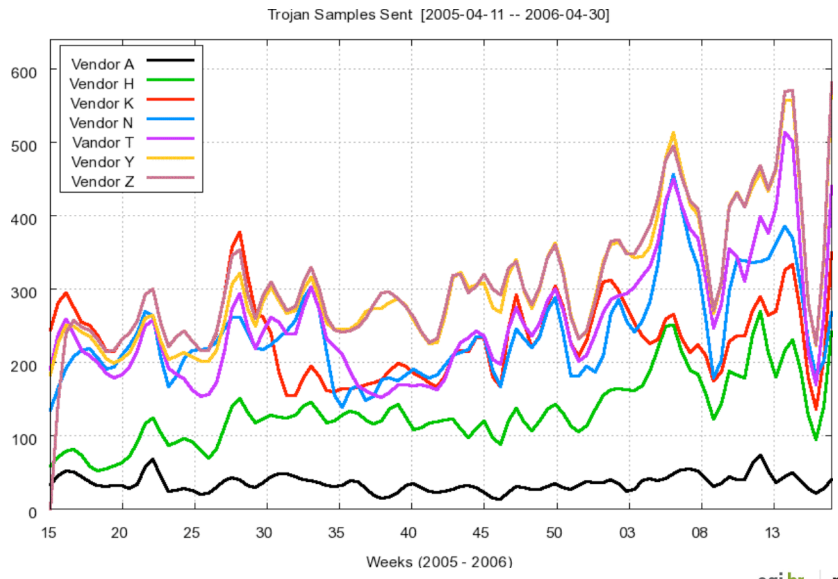
Eficiência dos Antivírus: 06/04/2005 a 30/04/2006

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%

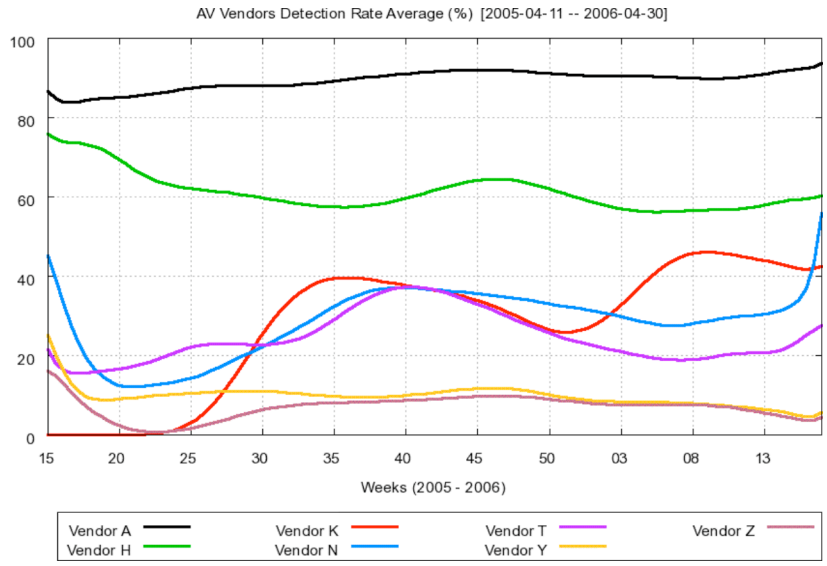
Apenas **1** AV com taxa de detecção de **90%**

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

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



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

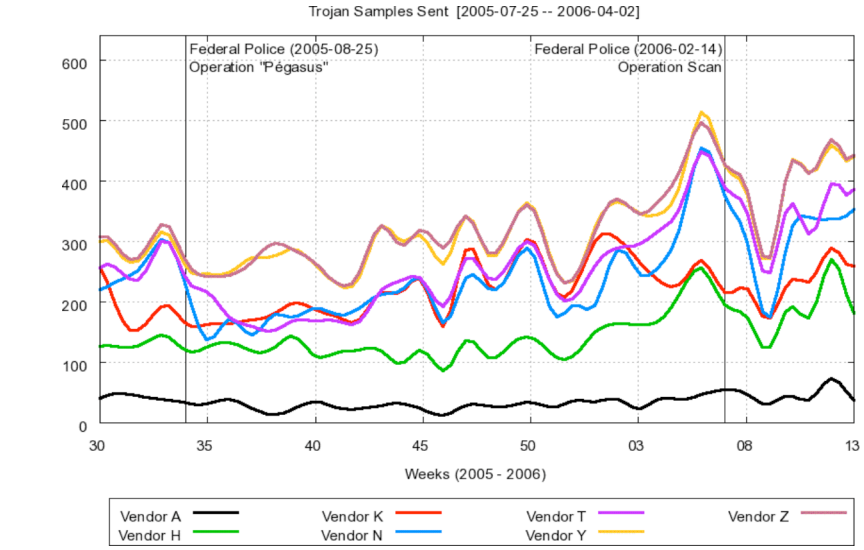


Operações da Polícia Federal

Combatendo fraudes via Internet

- **2001: Operação *Cash Net***, 17 pessoas presas
  - 1as 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

Operações da Polícia Federal (cont)



O Spam Visto como Incidente de Segurança

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…

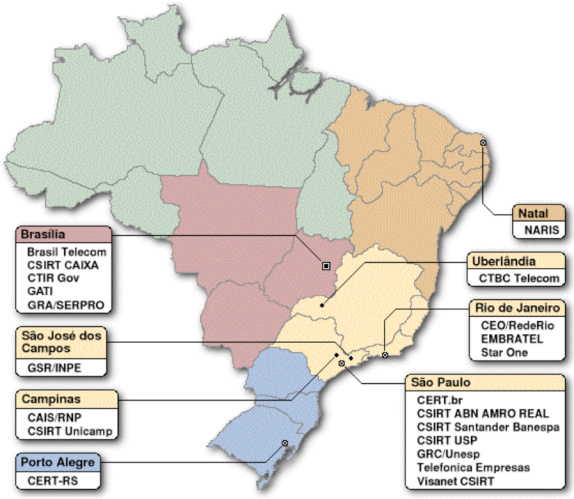
http://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/

Iniciativas para Aumentar a Segurança

Ações em Diversas Frentes

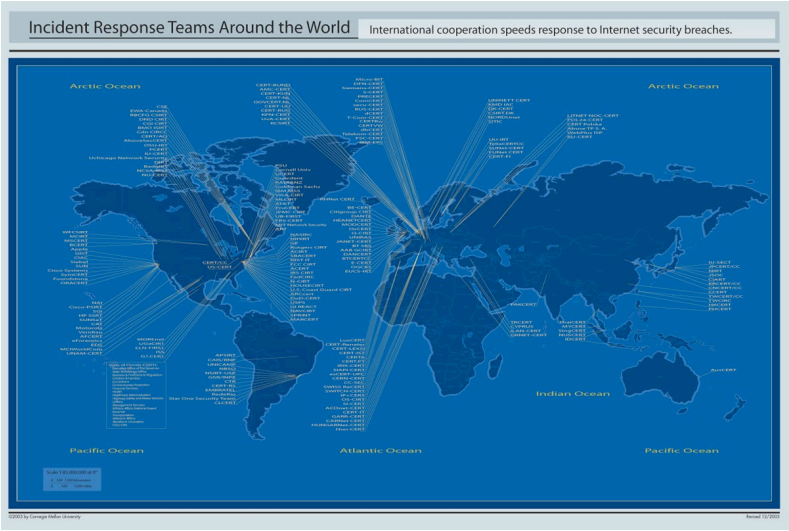
- Não há solução única
  - Combinar soluções e tecnologias, investir em treinamento e atualização dos profissionais
- Educação de usuários é fundamental
  - vetores disseminação de vírus/*worms*/*bots*
  - alvos de engenharia social (cavalos de tróia, fraudes, etc)
- Compartilhar informações e experiências
- 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



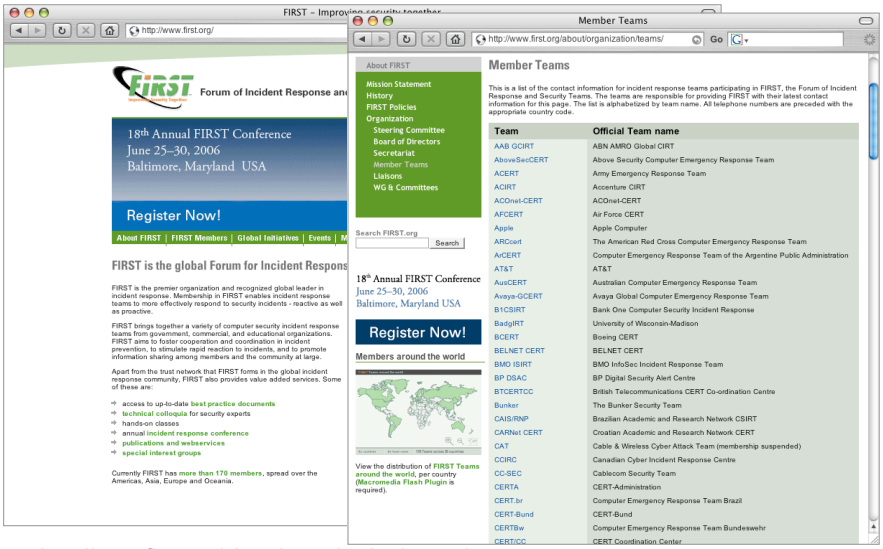
CSIRTs Brasileiros
http://www.cert.br/contato-br.html

CSIRTs no Mundo



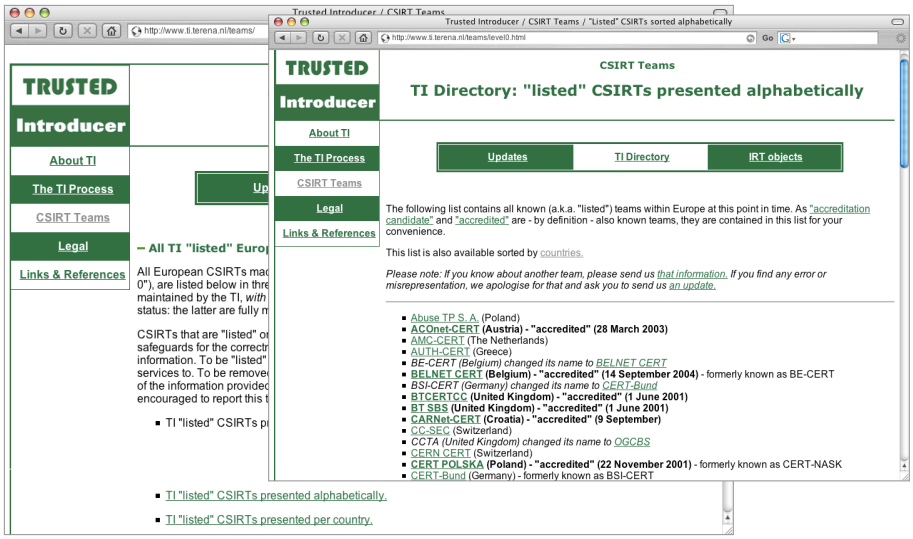
Fonte: http://www.cert.org/csirts/

CSIRTs Membros do FIRST



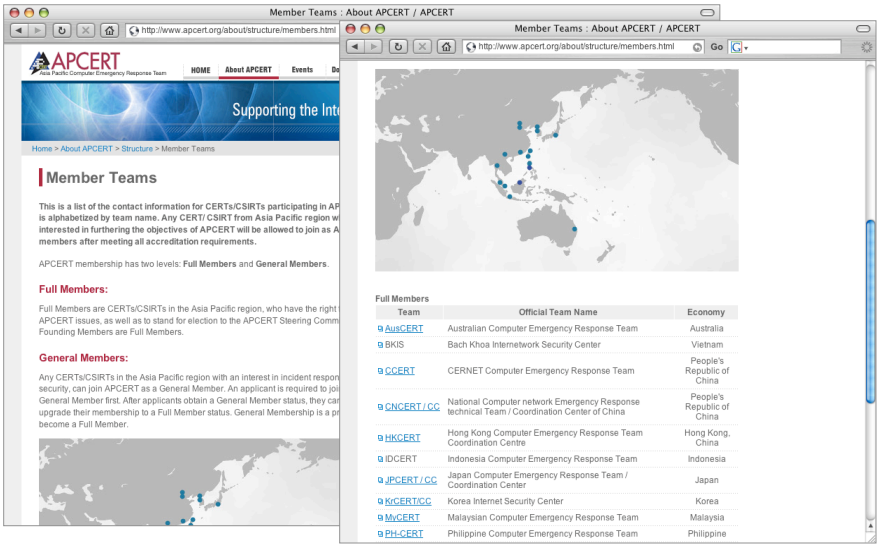
Fonte: http://www.first.org/about/organization/teams/

CSIRTs Europeus



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

CSIRTs na Ásia e Oceania



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 reorganizaçáo do conteúdo
- Folders com dicas mais importantes

Cartilha: Página Principal

Cartilha: Dicas de Segurança

Cartilha: Glossário

Site antispam.br

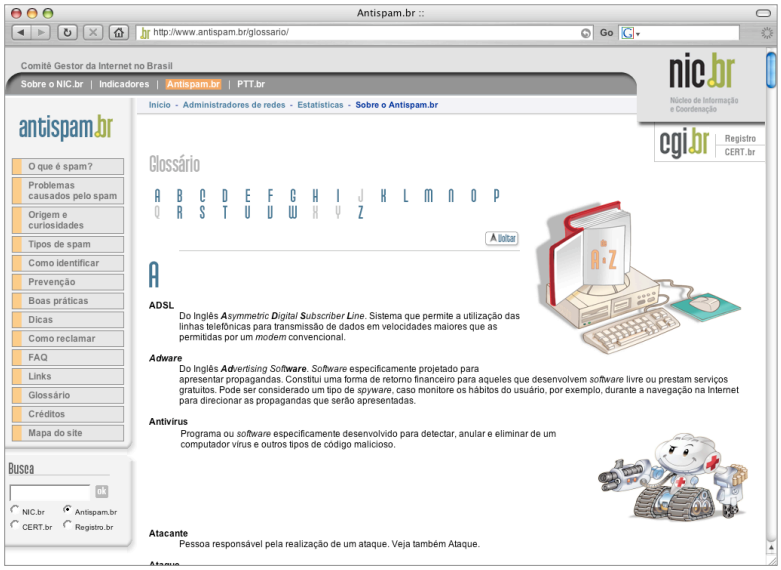
Antispam.br: Página Principal

Antispam.br: Tipos de Spam - códigos maliciosos

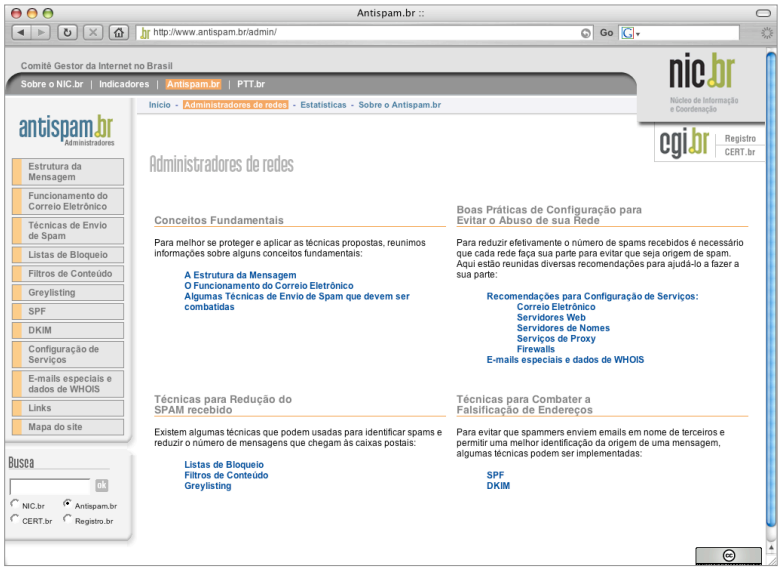
Antispam.br: Tipos de Spam - fraudes

Antispam.br: Dicas

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

Monitoramento e Acompanhamento de tendências

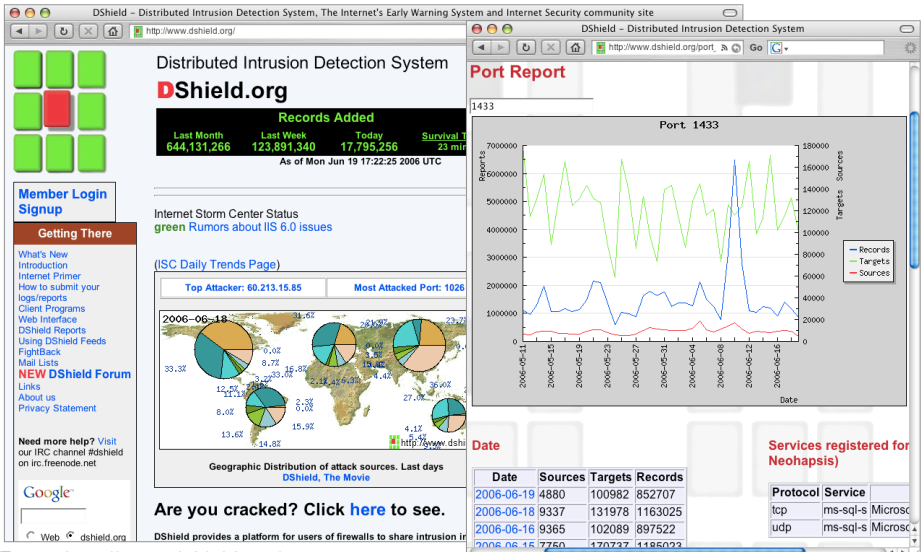
Acompanhamento de Tendências

- 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 Honeypots

Internet Storm Center

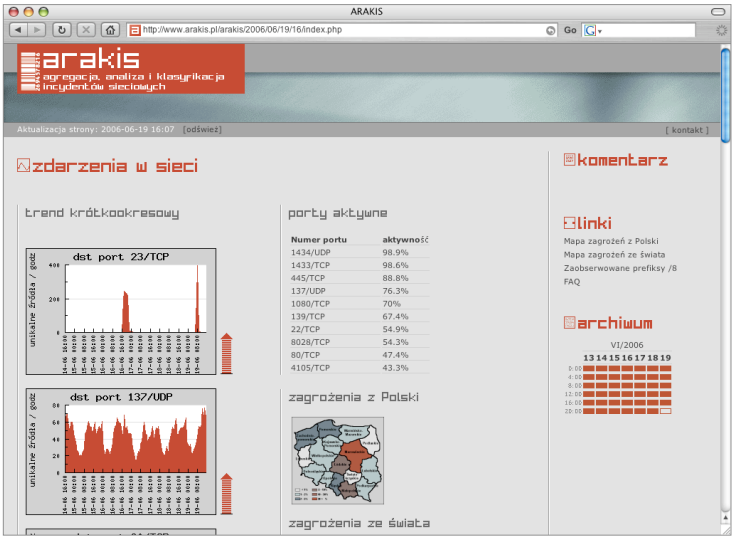
Fonte: http://isc.sans.org/

Internet Storm Center (cont)



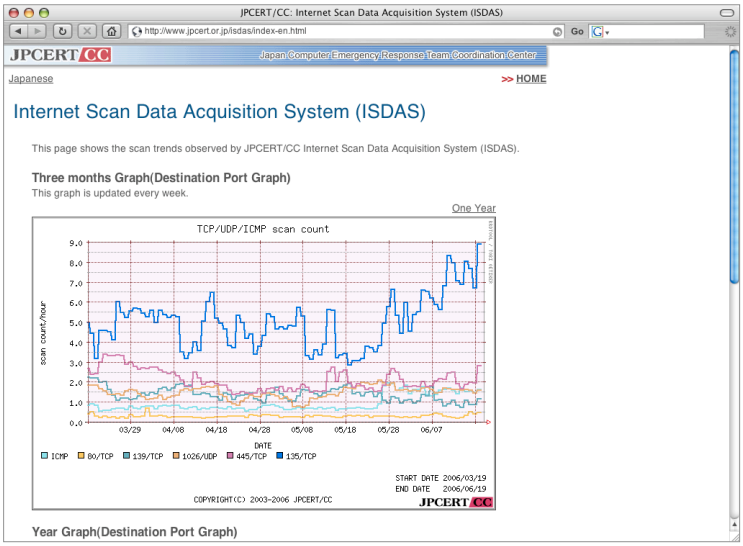
Fonte: http://www.dshield.org/

ARAKIS



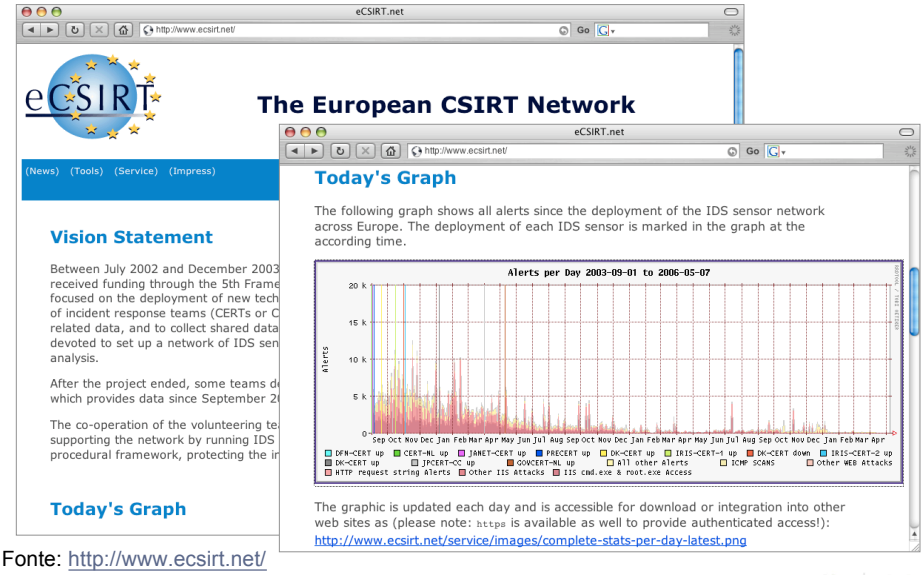
Fonte: http://www.arakis.pl/

ISDAS - *Internet Scan Data Acquisition System*



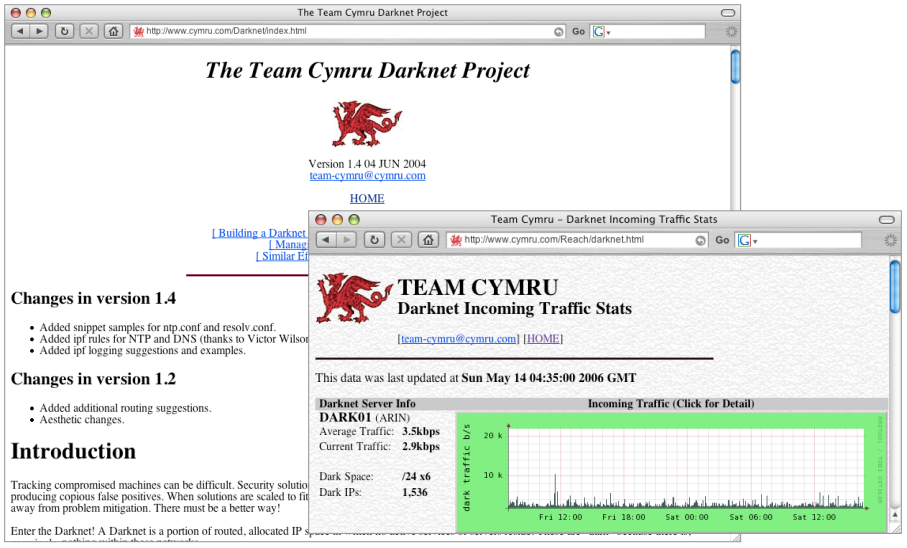
Fonte: http://www.jpcert.or.jp/isdas/index-en.html

eCSIRT.net - *The European CSIRT Network*



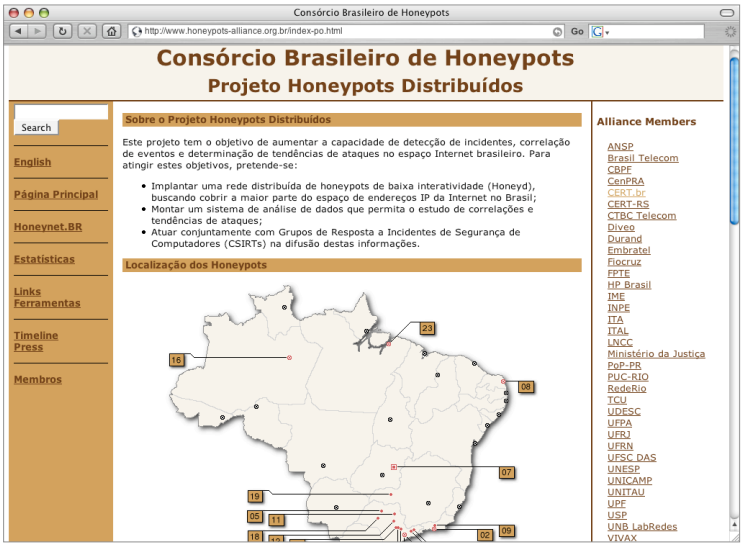
Fonte: http://www.ecsirt.net/

The Team Cymru Darknet Project



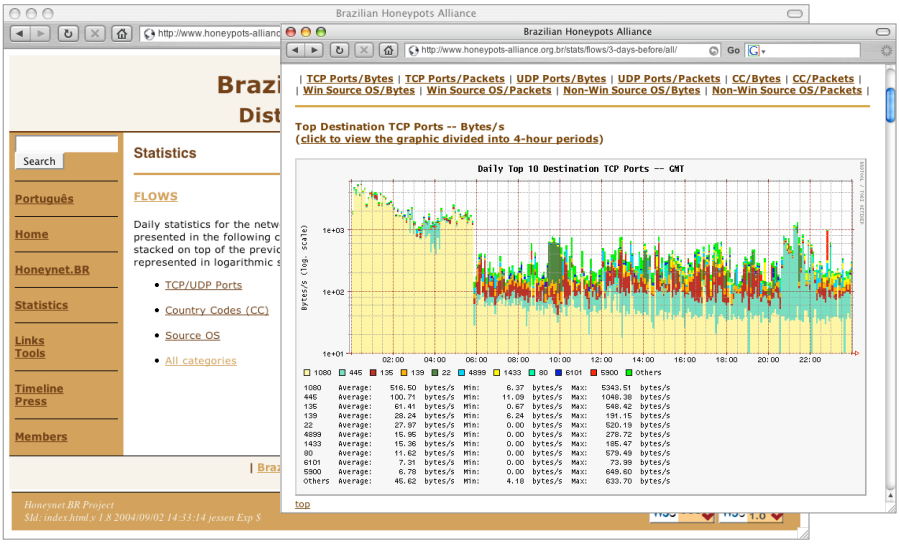
Fonte: http://www.cymru.com/Darknet/

Concórcio Brasileiro de *Honeypots*



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

Concórcio Brasileiro de *Honeypots*



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

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/