Segurança da Internet no Brasil e Atuação do CERT.br

Cristine Hoepers

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br

Núcleo de Informação e Coordenação do Ponto br - NIC.br
Comitê Gestor da Internet no Brasil - CGI.br

Agenda

- **Estrutura do CGI.br, NIC.br e CERT.br**
- **Missão do CERT.br e seu papel na segurança da Internet no Brasil**
- **Incidentes mais freqüentes**
- **Considerações finais**

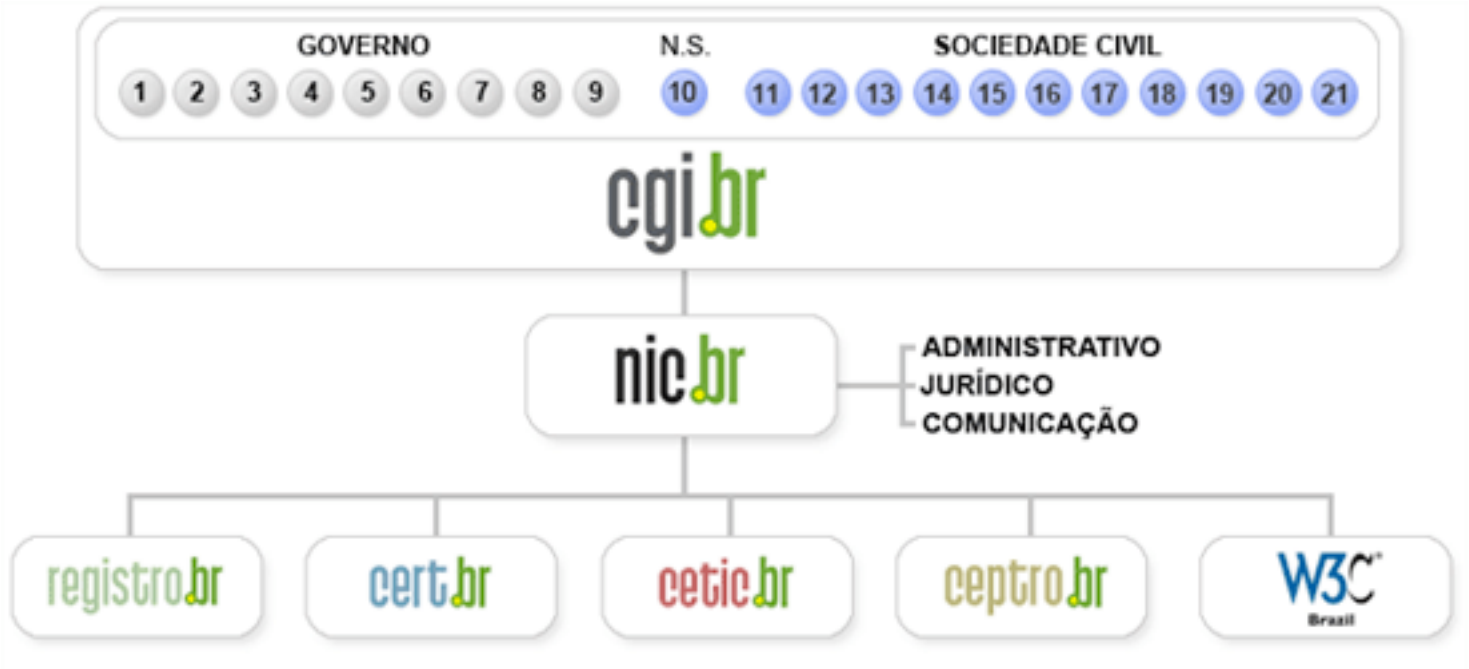
Comitê Gestor da Internet no Brasil – CGI.br

Dentre as atribuições 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.**

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

Estrutura do CGI.br e NIC.br



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

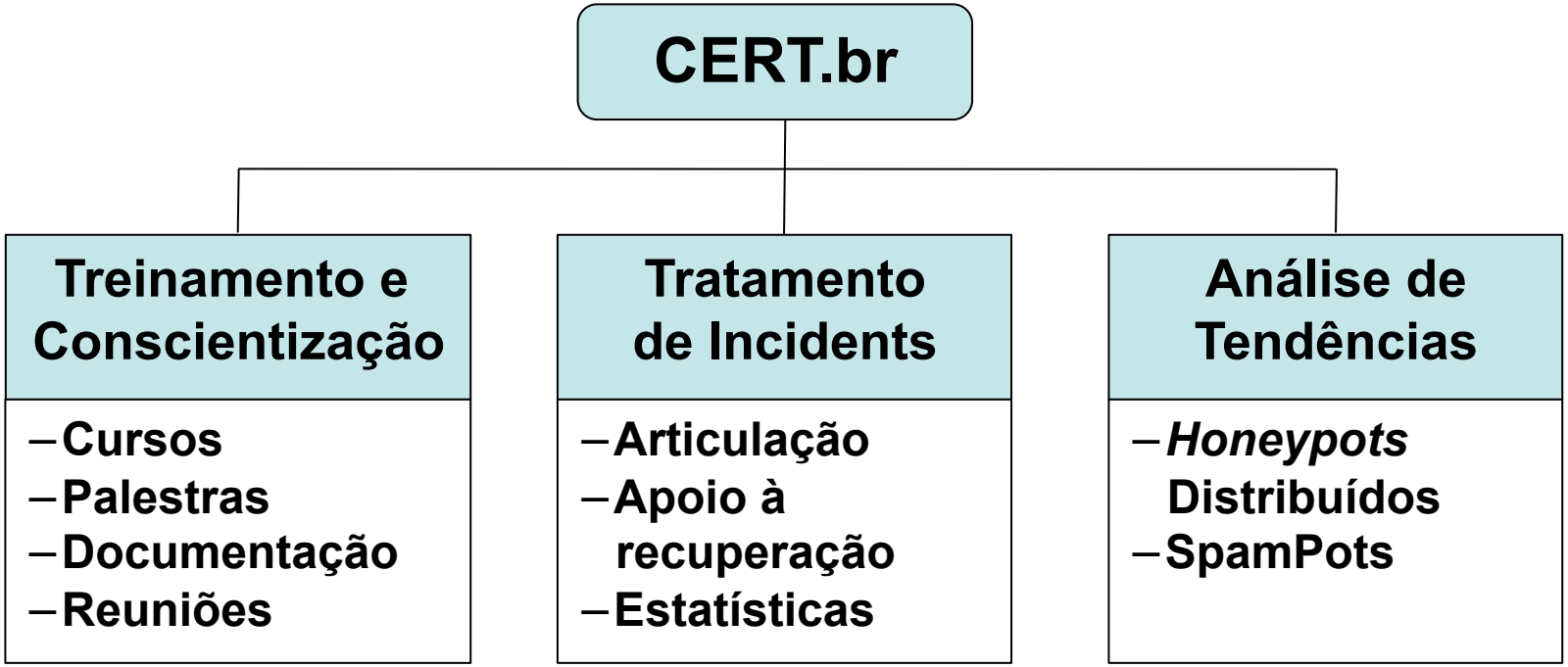
11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

CERT.br

- **Criado em 1997 para tratar incidentes segurança em computadores, envolvendo redes conectadas à Internet brasileira, exercendo as seguintes funções:**
  - **Ser um ponto de contato nacional para notificação de incidentes de segurança**
  - **Prover a coordenação e o apoio necessário no processo de resposta a incidentes**
  - **Estabelecer um trabalho colaborativo com outras entidades, como os operadores da justiça, provedores de acesso e serviços e backbones**
  - **Auxiliar novos CSIRTs a estabelecerem suas atividades**
  - **Aumentar a conscientização sobre a necessidade segurança na Internet**

Missão e Serviços do CERT.br:
http://www.cert.br/missao.html
Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil:
http://www.nic.br/grupo/historico-gts.htm

Atividades do CERT.br



Parcerias Internacionais:

SEIPartner CERT Courses

APWG RESEARCH PARTNER www.antiphishing.org

FIRST Improving Security Together MEMBER

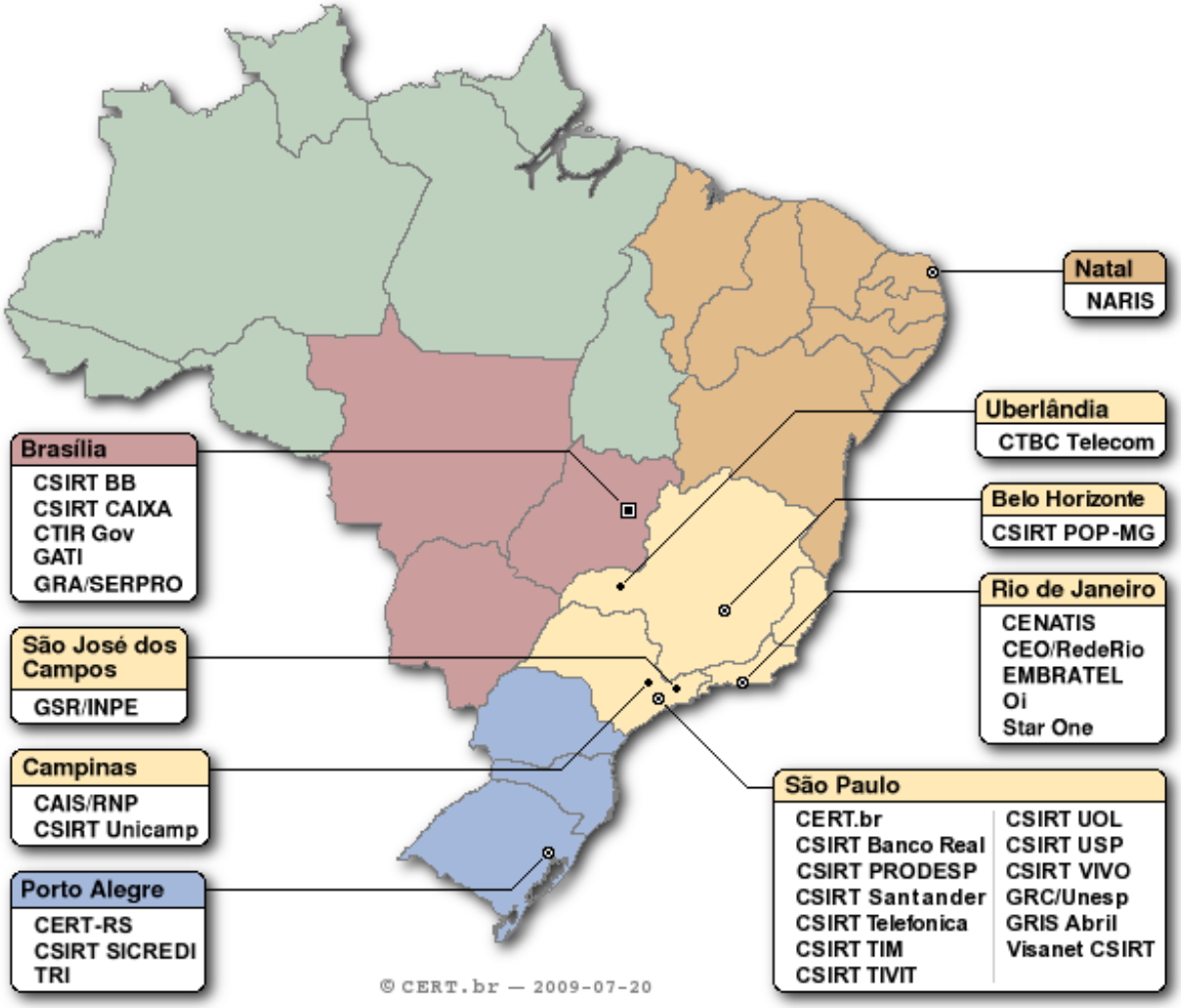
The Honeynet PROJECT®

Apoio e Treinamento para Novos CSIRTs

- **Auxílio no estabelecimento das atividades**
  - **Reuniões, palestras, treinamentos, etc**
- ***SEI/CMU Partner* desde 2004, licenciado para ministrar os cursos do *CERT® Program* no Brasil:**
  - **http://www.cert.br/cursos/**
    - ***Information Security for Technical Staff***
    - ***Overview of Creating and Managing Computer Security Incident Response Teams***
    - ***Fundamentals of Incident Handling***
    - ***Advanced Incident Handling for Technical Staff***
  - **320+ profissionais segurança treinados**
    - **máximo de 25 participantes por turma**

Grupos de Tratamento de Incidentes (CSIRTs/CERTs) no Brasil

Setor	CSIRTs
Resposabilidade Nacional	CERT.br
Redes de Governo	CTIR Gov, GATI, GRA/SERPRO, CSIRT Prodesp
Setor Financeiro	CSIRT BB, CSIRT CAIXA, CSIRT Banco Real, CSIRT Sicredi, CSIRT Santander, Visanet CSIRT
Telecom/ISP	CTBC Telecom, EMBRATEL, StarOne, Oi, CSIRT Telefonica, CSIRT TIM, CSIRT UOL, CSIRT VIVO
Redes Acadêmicas e de Pesquisa	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CSIRT USP, GRC/UNESP, TRI
Outros	CSIRT TIVIT, GRIS Abril



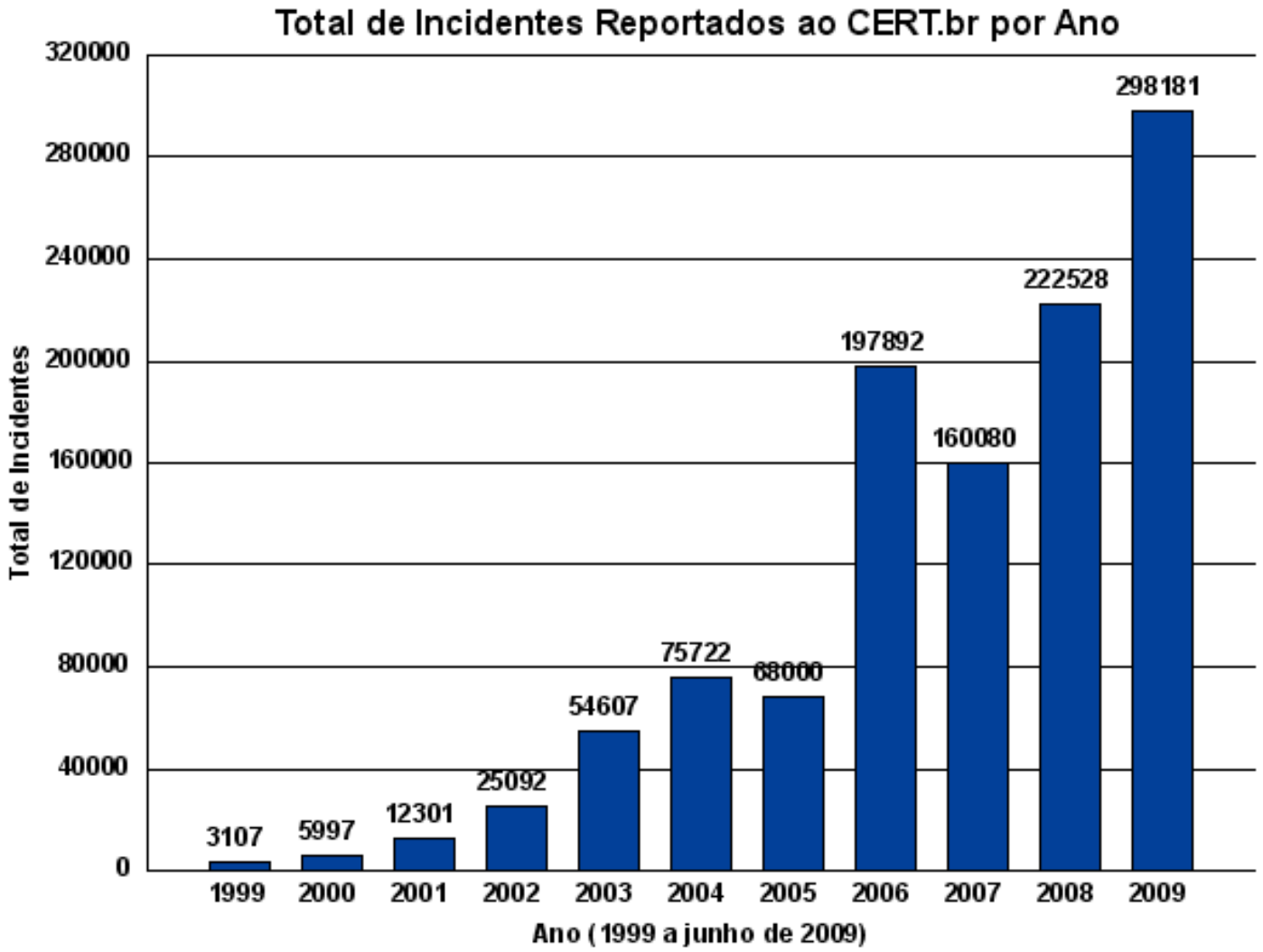
http://www.cert.br/contato-br.html

Tratamento de Incidentes

Tratamento de Incidentes

- **Articulação das ações para o tratamento de incidentes envolvendo redes brasileiras**
  - **Contato nacional para notificação de incidentes de segurança**
  - **Manutenção de estatísticas sobre as notificações de incidentes recebidas**
    - http://www.cert.br/stats/incidentes/
    - http://www.cert.br/stats/spam/
  - **Desenvolvimento de documentos de boas práticas para usuários e administradores de redes**
    - **Práticas de Segurança para Administradores de Redes Internet** http://www.cert.br/seg-adm-redes/
    - **Cartilha de Segurança para Internet** http://cartilha.cert.br/

Incidentes Reportados ao CERT.br



http://www.cert.br/stats/incidentes/

Categorias – Tipos de Incidentes (1/2)

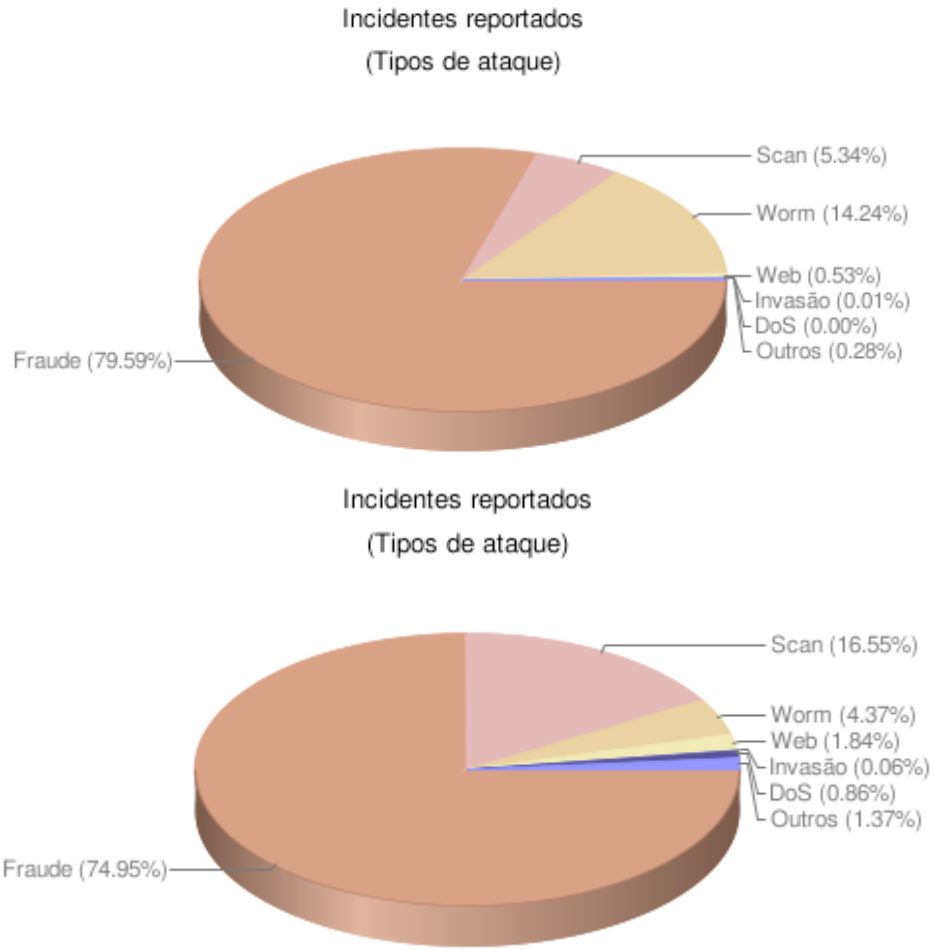
- **`scan`:** notificações de **varreduras** em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente **utilizado por atacantes para identificar potenciais alvos**, pois **permite associar possíveis vulnerabilidades aos serviços habilitados em um computador**.
- **`worm`:** notificações de atividades maliciosas relacionadas com o **processo automatizado de propagação de códigos maliciosos** na rede, como **worms e bots**.
- **`dos` (DoS – *Denial of Service*):** notificações de ataques de **negação de serviço**, onde o atacante utiliza um computador ou um conjunto de computadores para **tirar de operação um serviço, computador ou rede**.
- **`invasão`:** um ataque bem sucedido que resulte no **acesso não autorizado a um computador ou rede.**

Categorias – Tipos de Incidentes (2/2)

- **`web`:** um caso particular de ataque visando especificamente o **comprometimento de servidores Web ou desfigurações de páginas na Internet.**
- **`fraude`:** entram nesta categoria as **tentativas de fraude**, que incluem:
  - *e-mails* com *links* para códigos maliciosos;
  - eventuais violações de direitos autorais.
- **`outros`: notificações de incidentes que não se enquadram nas categorias anteriores.**

Distribuição entre as categorias

2009 – 1º e 2º trimestres



Enfoque dos atacantes:

- **Ataques a usuários finais**
- **Motivação financeira**

Características das tentativas de fraude:

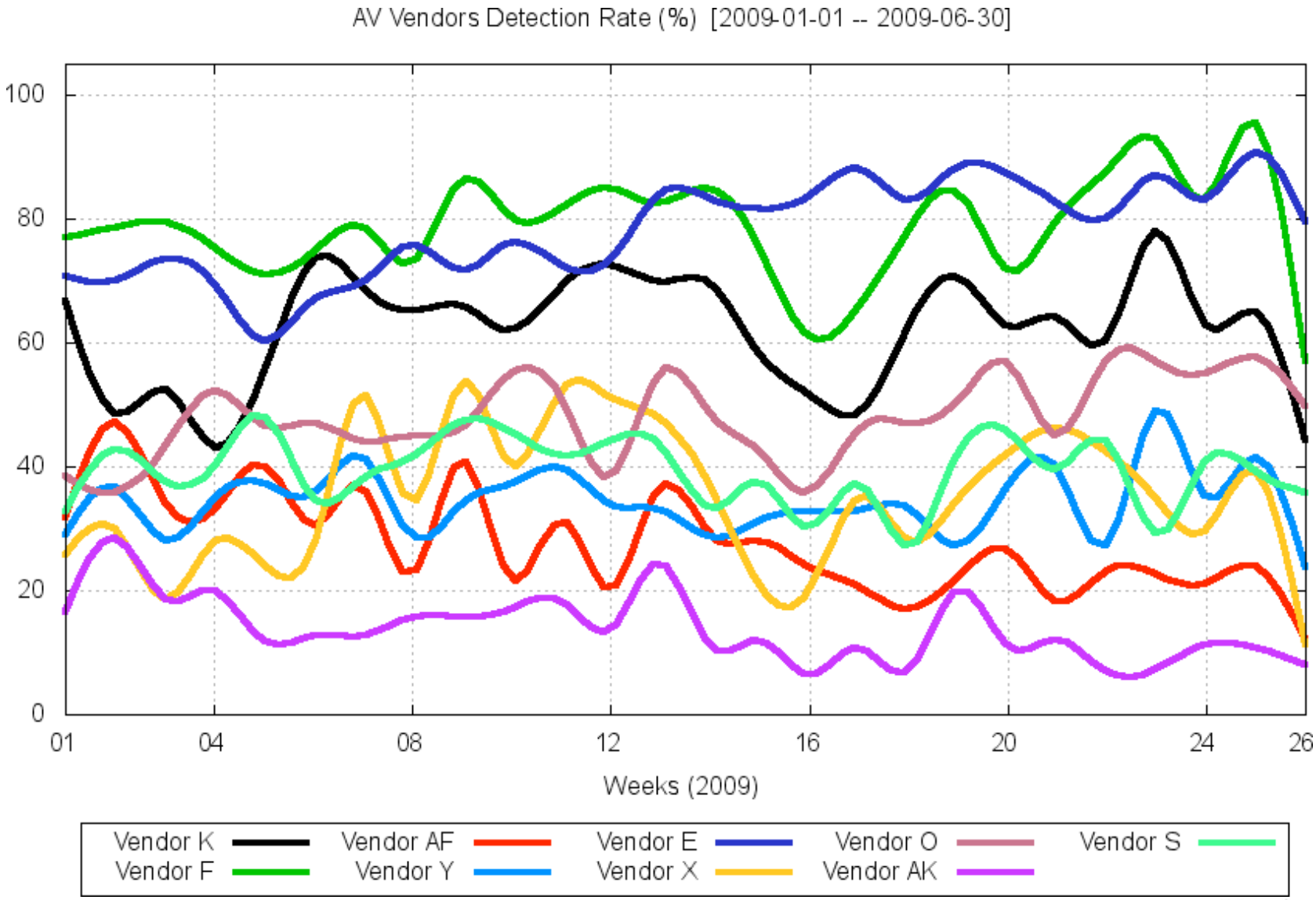
- **Eventuais violações de direitos autorais**
- ***Spams***
  - **Em nome das mais variadas instituições e com tópicos diversos**
  - **Com *links* (URLs) para códigos maliciosos (cavalos de tróia)**

http://www.cert.br/stats/incidentes/

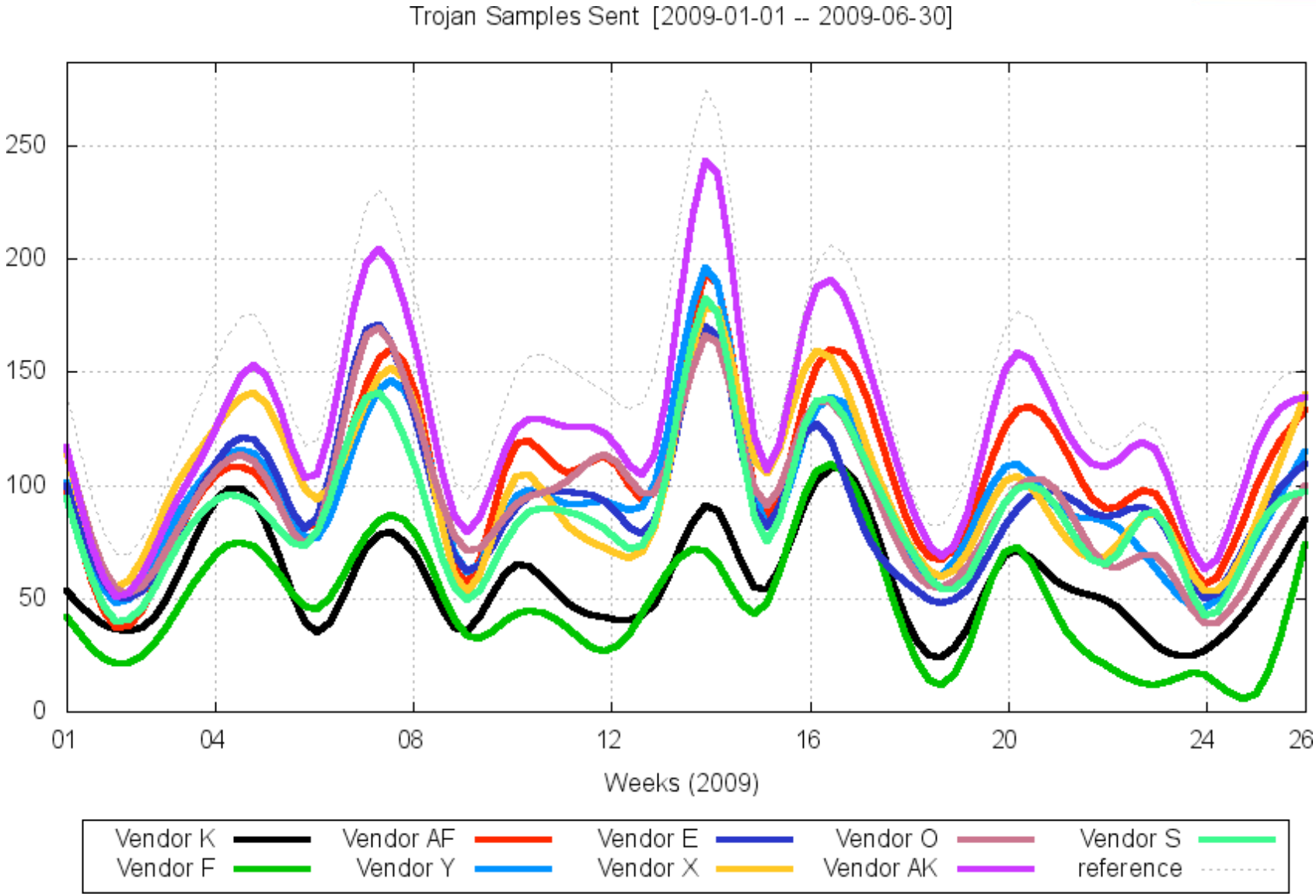
2008/2009: Detalhes dos Códigos e URLs Reportados nas Tentativas de Fraude

	2008	2009 1º Sem.
Assinaturas de antivírus ("famílias")	447	935
Assinaturas de antivírus (únicas)	6.085	1.564
Domínios	5.916	2.048
Extensões de arquivos usadas	112	65
Endereços IP únicos	3.921	1.595
Países de onde estavam hospedados	78	64
Nomes de arquivos	8.297	2.879
URLs únicas	17.376	4.973
Códigos maliciosos novos únicos (assinaturas criptográficas únicas)	14.256	3.740

1º Semestre/2009: Eficiência dos Antivírus



1º Semestre/2009: Exemplares Enviados

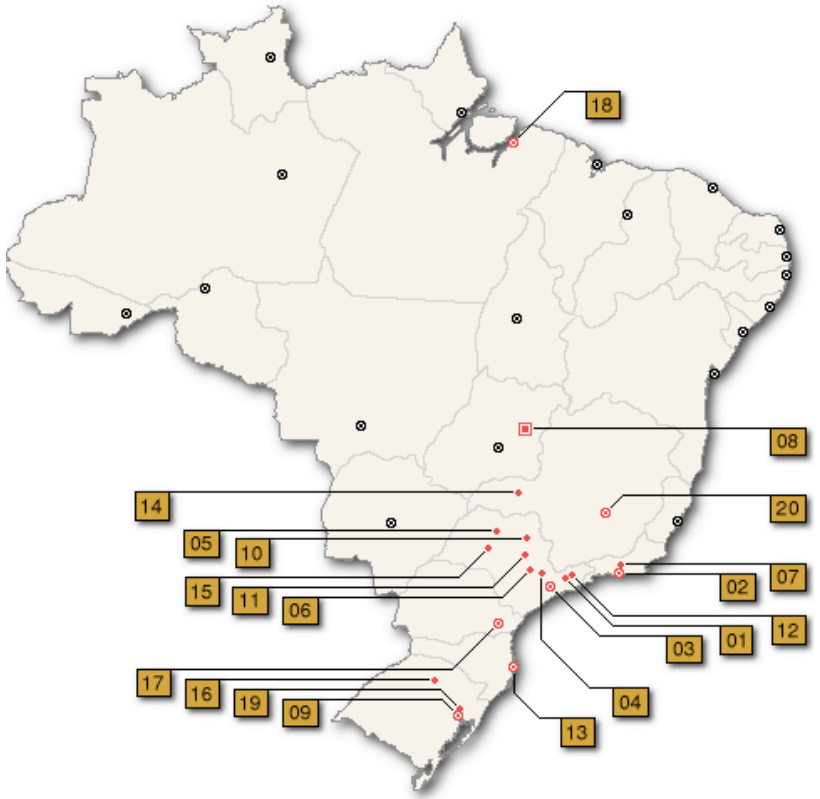


Análise de Tendências

Projeto *Honeypots* Distribuídos

Objetivo: aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro

- **37 instituições, entre academia, governo, indústria e instituições financeiras**
- **Baseado em trabalho voluntário**
- **http://www.honeypots-alliance.org.br/**

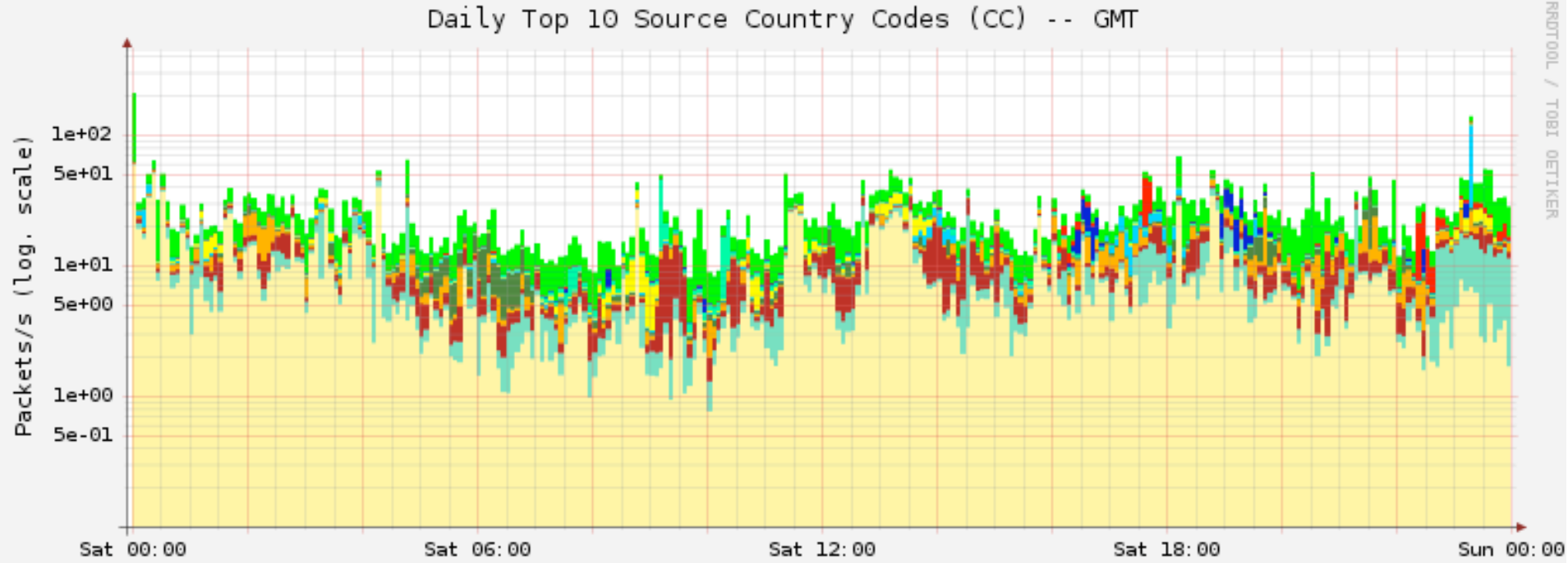


Fornece um termômetro das atividades maliciosas na Internet do Brasil

Utilização dos dados coletados para:

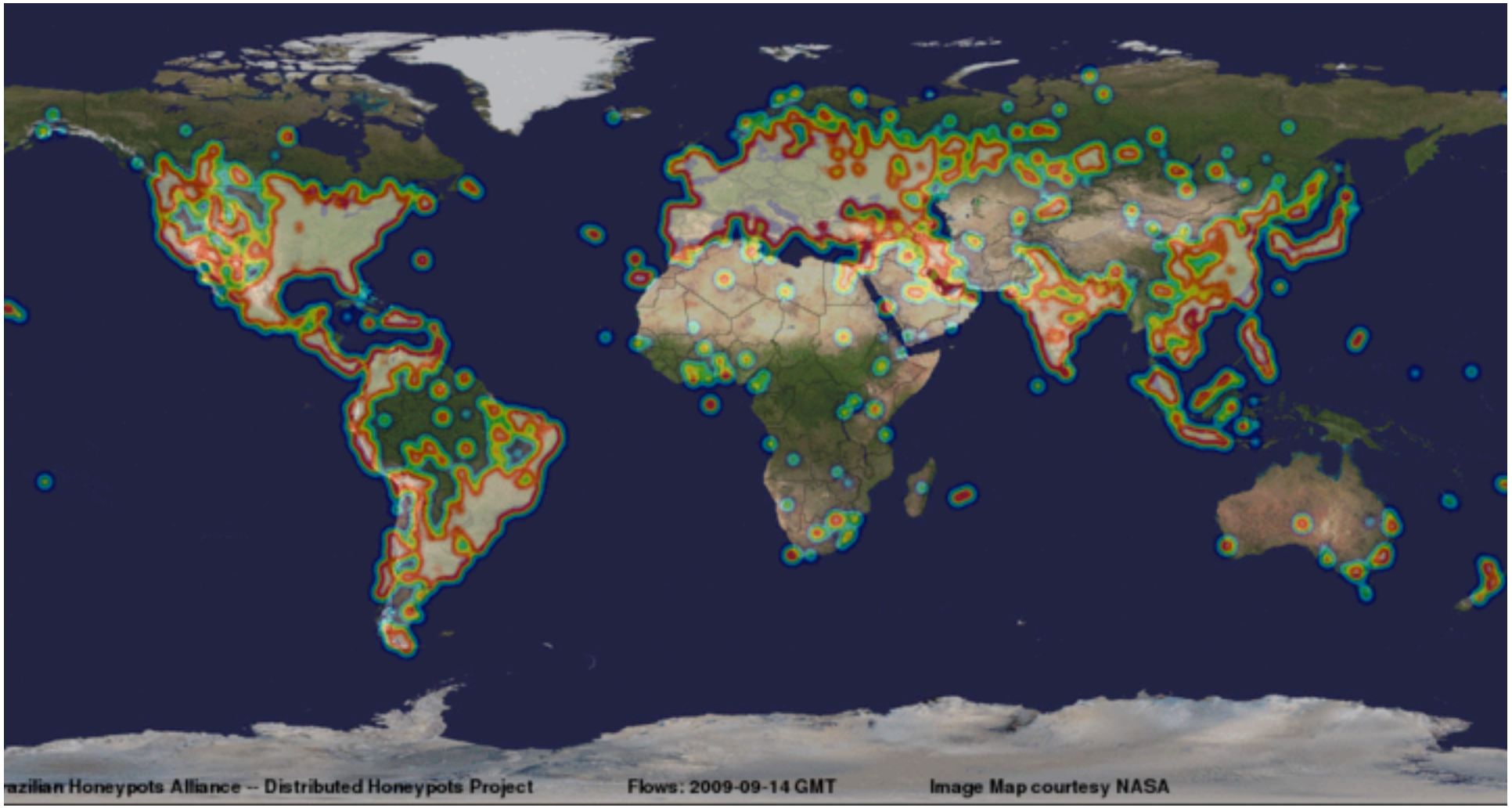
- **Notificação das redes originadoras dos ataques**
- **Geração de estatísticas públicas**

Estatísticas Públicas dos Ataques Registrados



BR	Average:	7.77	pkts/s	Min:	0.76	pkts/s	Max:	59.08 pkts/s
CN	Average:	2.50	pkts/s	Min:	0.31	pkts/s	Max:	24.34 pkts/s
US	Average:	2.33	pkts/s	Min:	0.24	pkts/s	Max:	13.88 pkts/s
AR	Average:	1.68	pkts/s	Min:	0.07	pkts/s	Max:	17.41 pkts/s
TW	Average:	0.94	pkts/s	Min:	0.05	pkts/s	Max:	24.75 pkts/s
CA	Average:	0.87	pkts/s	Min:	0.03	pkts/s	Max:	90.73 pkts/s
JP	Average:	0.85	pkts/s	Min:	0.03	pkts/s	Max:	6.35 pkts/s
RU	Average:	0.69	pkts/s	Min:	0.10	pkts/s	Max:	32.02 pkts/s
GB	Average:	0.54	pkts/s	Min:	0.00	pkts/s	Max:	10.75 pkts/s
VE	Average:	0.53	pkts/s	Min:	0.00	pkts/s	Max:	26.40 pkts/s
Others	Average:	7.24	pkts/s	Min:	2.16	pkts/s	Max:	143.71 pkts/s

Novas Estatísticas a Serem Lançadas



Projeto SpamPots

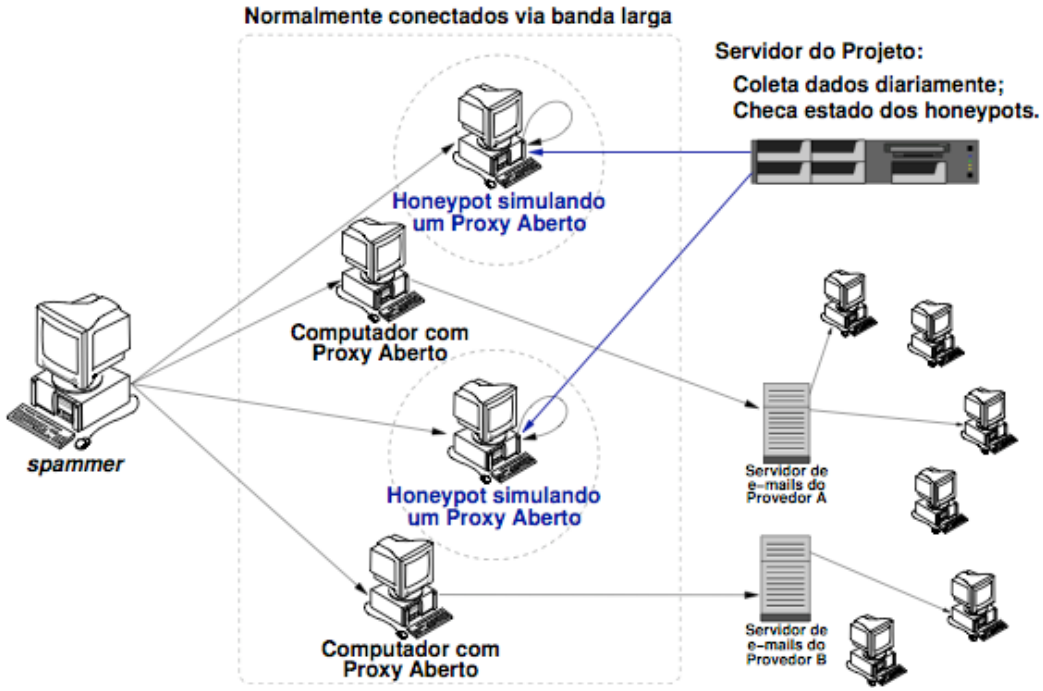
- **Implementado pelo CERT.br**
- **Financiado pelo NIC.br/CGI.br**
  - **Como parte dos trabalhos da Comissão Anti-Spam**
  - **Para gerar métricas sobre o abuso de máquinas de usuários finais para o envio de *spam***

- **Implantação de 10 *honeypots** de baixa-interatividade, simulando ser *proxies* abertos e capturando *spam***
  - **Em 5 operadoras de banda-larga**
    - **2 cabo e 3 ADSL**
    - **1 residencial e 1 empresarial em cada**

* *Honeypot* é um tipo de sensor usado para simular serviços e registrar as atividades maliciosas.
Fonte: http://www.cert.br/docs/whitepapers/honeypots-honeynets/

Resultados – Abuso das Redes Brasileiras

Dias de coleta:	**466**
***E-mails* capturados:**	**524.585.779**
Destinatários:	**4.805.521.964**
Destinatários/*e-mail*:	**≈ 9.1**
***E-mails*/dia:**	**≈ 1.2 Milhões**
IPs únicos:	**216.888**
ASNs únicos:	**3.006**
***Country Codes*:**	**165**



Principais Resultados:

- **99.84% das conexões eram originadas do exterior**
- **os spammers consumiam toda a banda de upload disponível**
- **mais de 90% dos spams eram destinados a redes de outros países**

http://www.cert.br/docs/whitepapers/spampots/

Outras Atividades

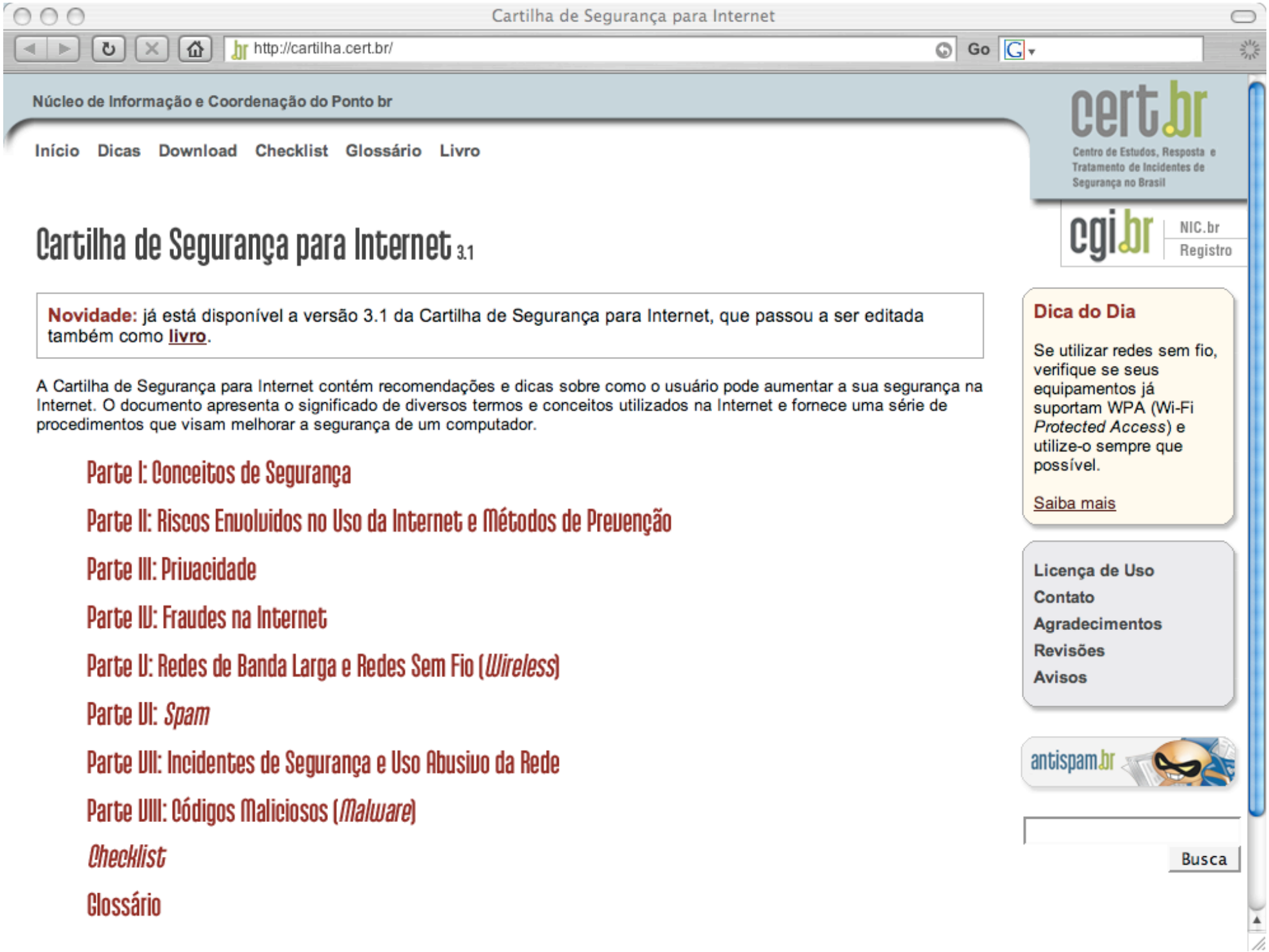
Material para Administradores e Usuários

Materiais gratuitos disponíveis

- **Práticas de Segurança para Administradores de Redes Internet**
  http://www.cert.br/seg-adm-redes/
  - **boas práticas em configuração, administração e operação segura de redes conectadas à Internet**

- **Cartilha de Segurança para Internet**
  http://cartilha.cert.br/

- **Site Antispam.br – no escopo das atividades da Comissão de Trabalho Anti-Spam do CGI.br**
  http://www.antispam.br/


Cartilha de Segurança para Internet
http://cartilha.cert.br/
Go
Núcleo de Informação e Coordenação do Ponto br
Início Dicas Download Checklist Glossário Livro
cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
cgi.br
NIC.br
Registro
Cartilha de Segurança para Internet 3.1
Novidade: já está disponível a versão 3.1 da Cartilha de Segurança para Internet, que passou a ser editada também como livro.
A Cartilha de Segurança para Internet contém recomendações e dicas sobre como o usuário pode aumentar a sua segurança na Internet. O documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.
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
Glossário
Dica do Dia
Se utilizar redes sem fio, verifique se seus equipamentos já suportam WPA (Wi-Fi Protected Access) e utilize-o sempre que possível.
Saiba mais
Licença de Uso
Contato
Agradecimentos
Revisões
Avisos
antispam.br
Busca

Cartilha de Segurança para Internet 3.1

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.

Folheto com dicas de segurança, formato A4. (106 KB)

***Folder* com dicas de segurança, formato A4. (1.1 MB)**

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*

- ❒ Mantenha o programa leitor de *e-mails* sempre atualizado.
- ❒ Desative a visualização de *e-mails* em HTML.
- ❒ Desative as opções de execução automática de arquivos anexados.
- ❒ Desative a execução de *JavaScript* e *Java*.

Cartilha de Segurança para Internet 3.1

Livro Completo

A partir da versão 3.1 a Cartilha de Segurança para Internet passou a ser editada também como livro. Nesta página você encontra o prefácio do Livro e o arquivo para download.

Prefácio

A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças.

Produzido pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil -- CERT.br, com o apoio do Comitê Gestor da Internet no Brasil -- CGI.br, o documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.

Nós esperamos que esta Cartilha possa auxiliá-lo não só a compreender as ameaças do ambiente Internet, mas também a manter seu sistema mais seguro. Gostaríamos ainda de lembrar que é muito importante ficar sempre atento ao usar a Internet, pois somente aliando medidas técnicas a boas práticas é possível atingir um nível de segurança que permita o pleno uso da Internet.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, por favor, entre em contato através do endereço `doc@cert.br`.

Equipe do CERT.br
Outubro de 2006

Estrutura da Cartilha

Este documento conta com oito partes, que dividem o conteúdo em diferentes áreas relacionadas com a segurança da Internet, além de um glossário, um *checklist* e uma compilação de dicas rápidas.

- **Parte I: Conceitos de Segurança**
  Apresenta conceitos gerais de segurança de computadores, importantes para o entendimento dos

Livro Completo para download (886 KB)

Cartilha de Segurança para Internet, versão 3.1 / CERT.br -- São Paulo: Comitê Gestor da Internet no Brasil, 2006.

ISBN: 978-85-60062-06-5
ISBN: 85-60062-06-8

antispam.br

Tipos de spam

Voltar

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.
- **Cavalo de tróia:** 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.

antispam.br

Tipos de spam

Voltar

Fraudes

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial. Então, atacantes têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet.

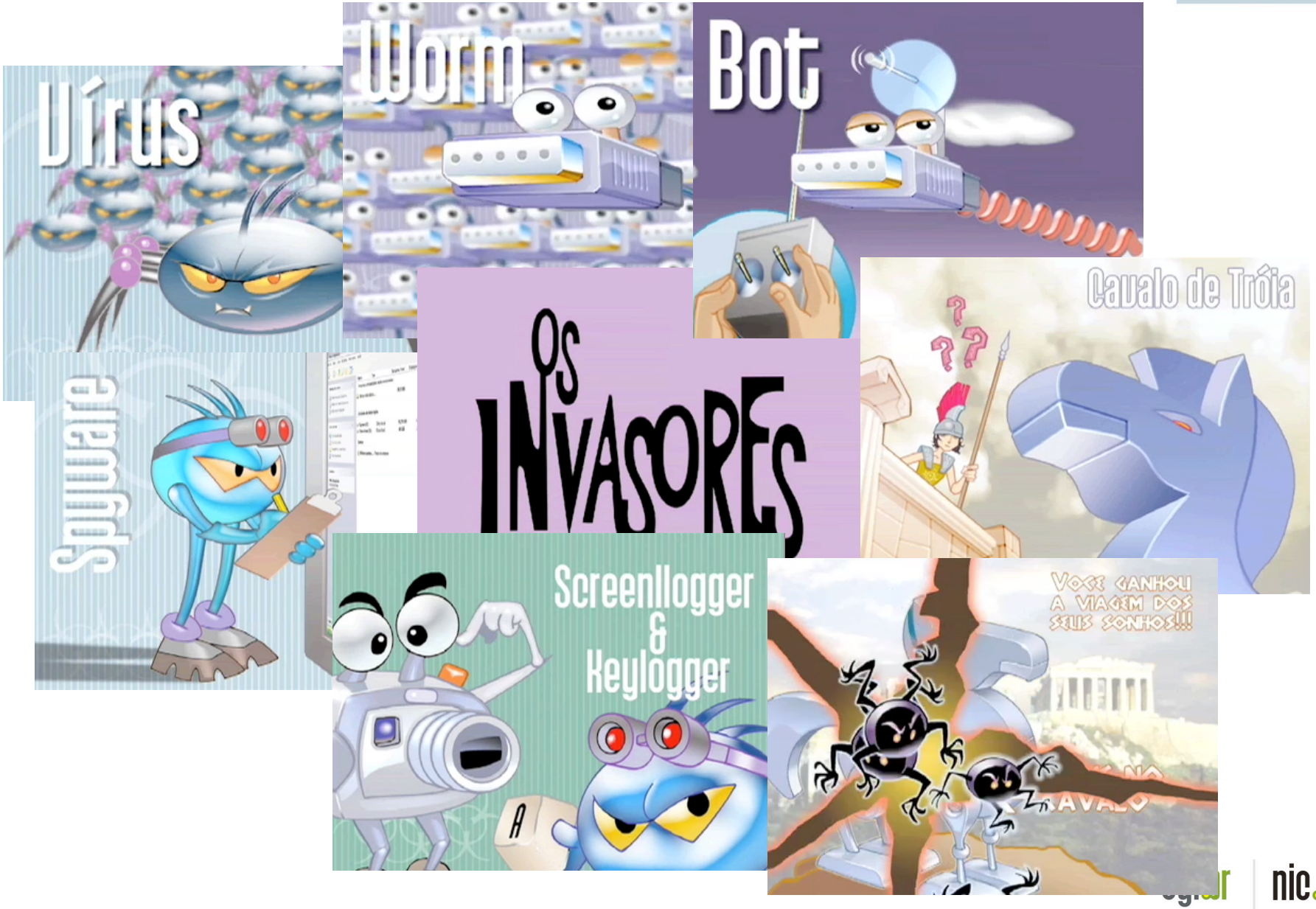
Para obter vantagens, os fraudadores têm utilizado amplamente *e-mails* com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados. Desta forma, é muito importante que usuários de Internet tenham certos cuidados com os *e-mails* que recebem e ao utilizarem serviços de comércio eletrônico ou *Internet Banking*.

Sumário

Golpes (*Scams*)

Vídeo 1: Navegar é Preciso

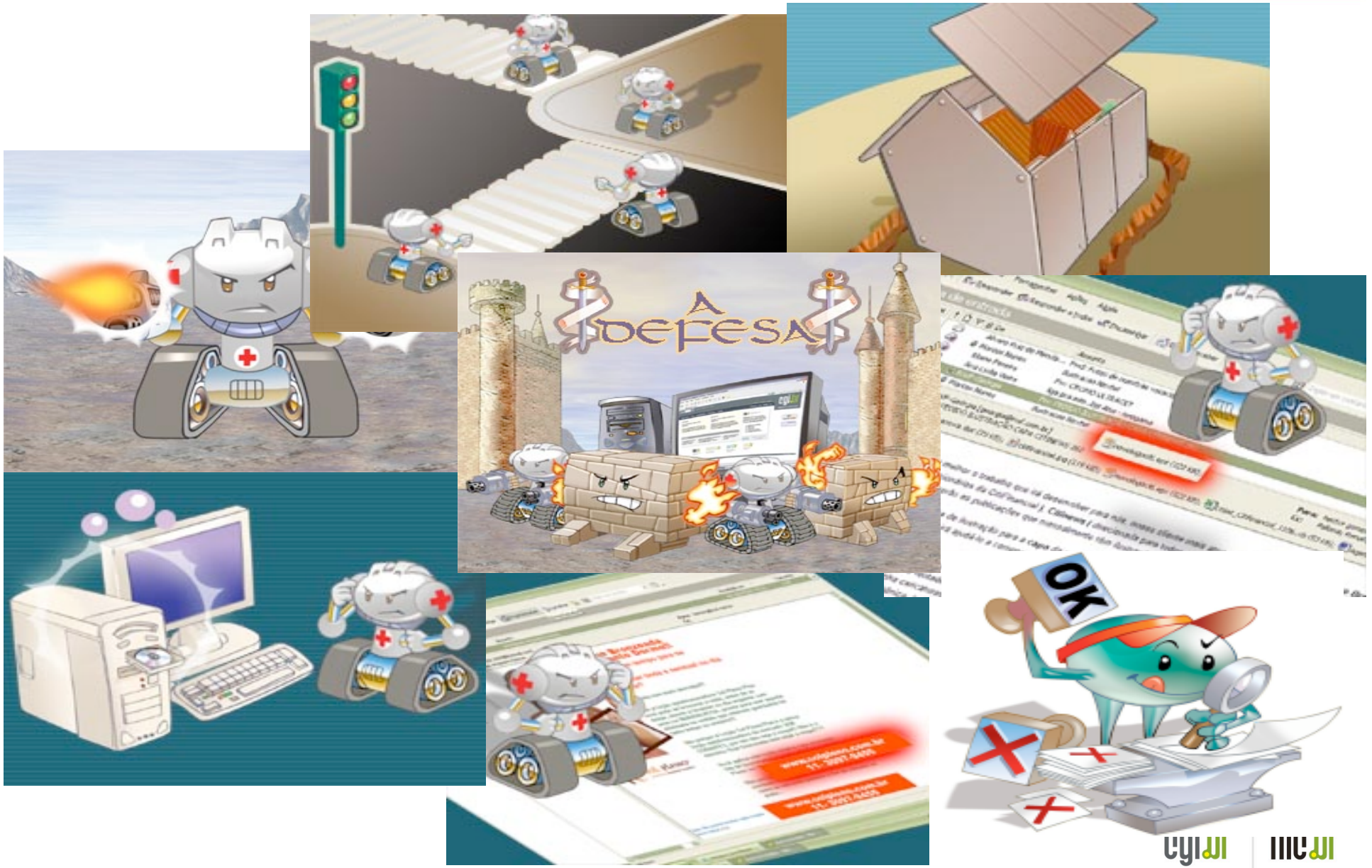
Vídeo 2: Os Invasores



Vídeo 3: Spam


SPAM
SPIT
OU
SPIM
Spaum (online)
Localizar um contato...
Você tem 5 solicitações....
Oscar- Freelas para redator....
Robert- La donna é mobile...
Rodrigon-
SUPER SOFT
10,00

Vídeo 4: A Defesa



Links Relacionados

- **CGI.br - Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do Ponto br**
  http://www.nic.br/
- **CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/