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

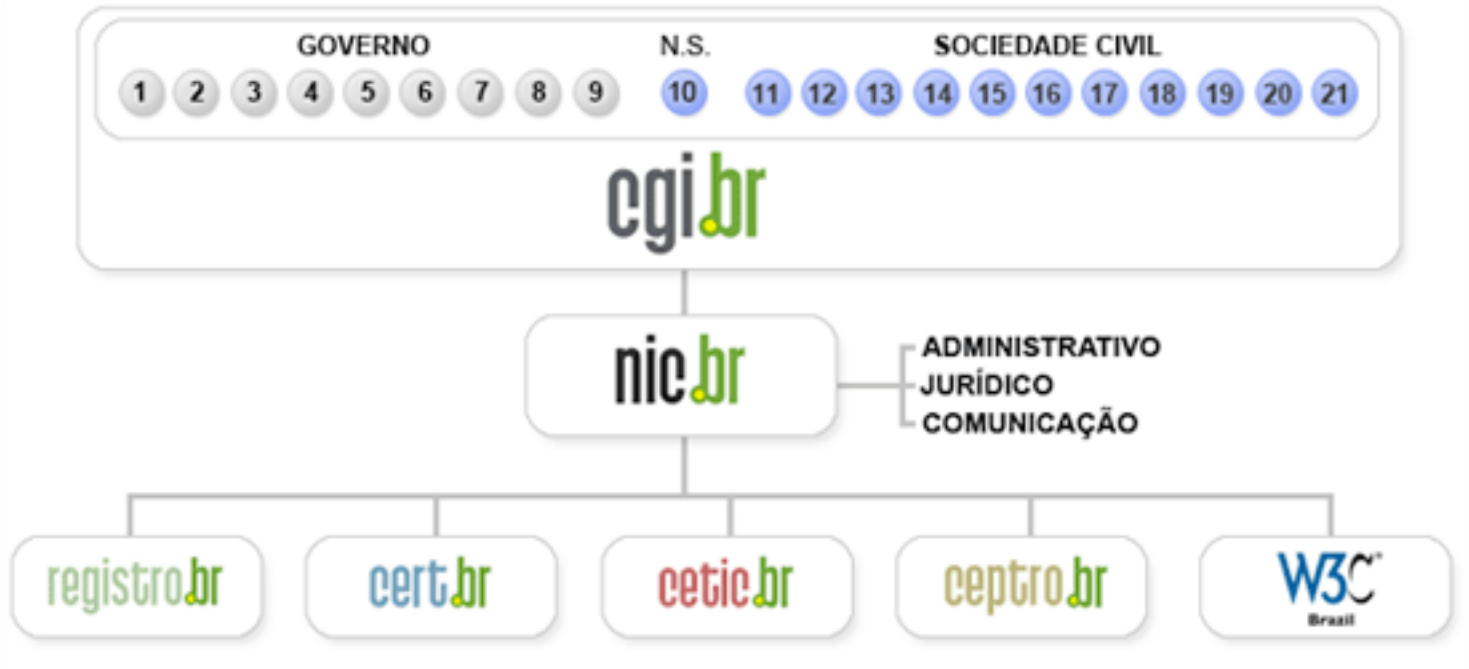
Comitê Gestor da Internet no Brasil – CGI.br

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

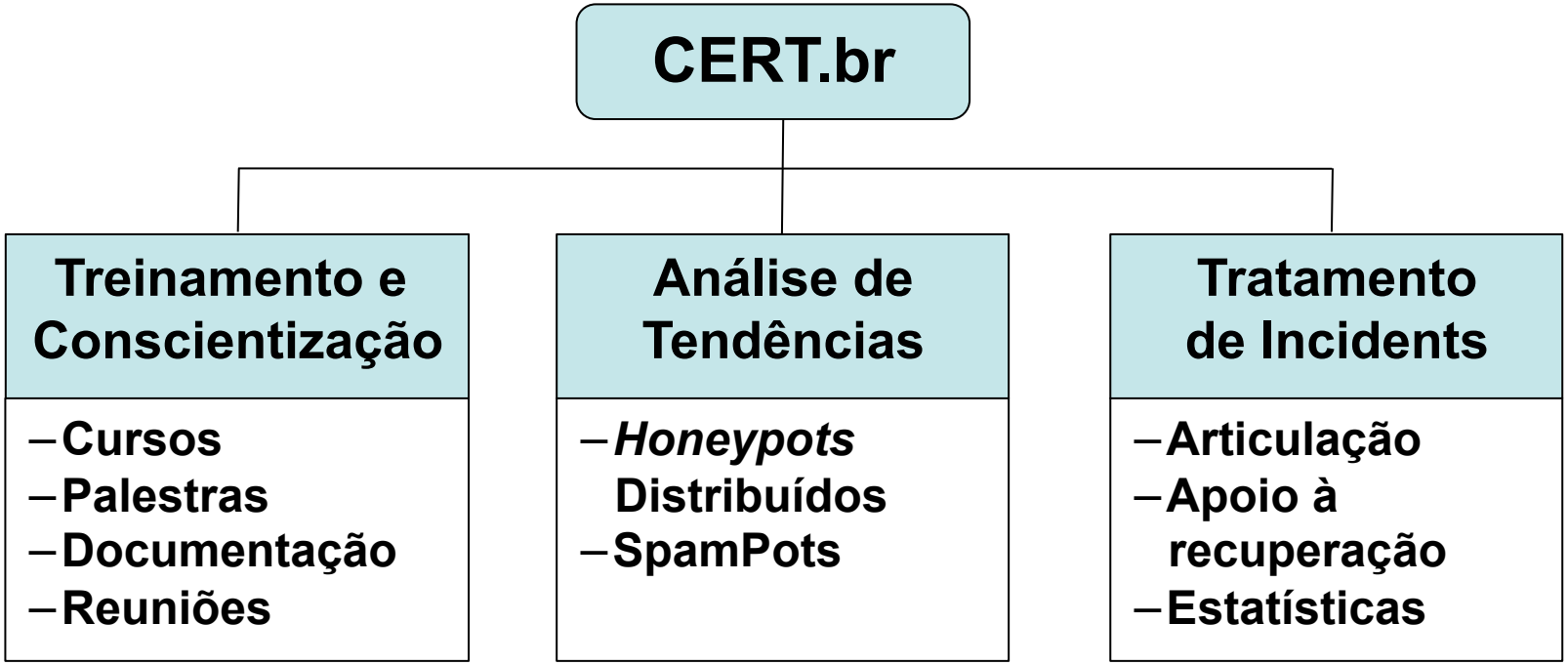
11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

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



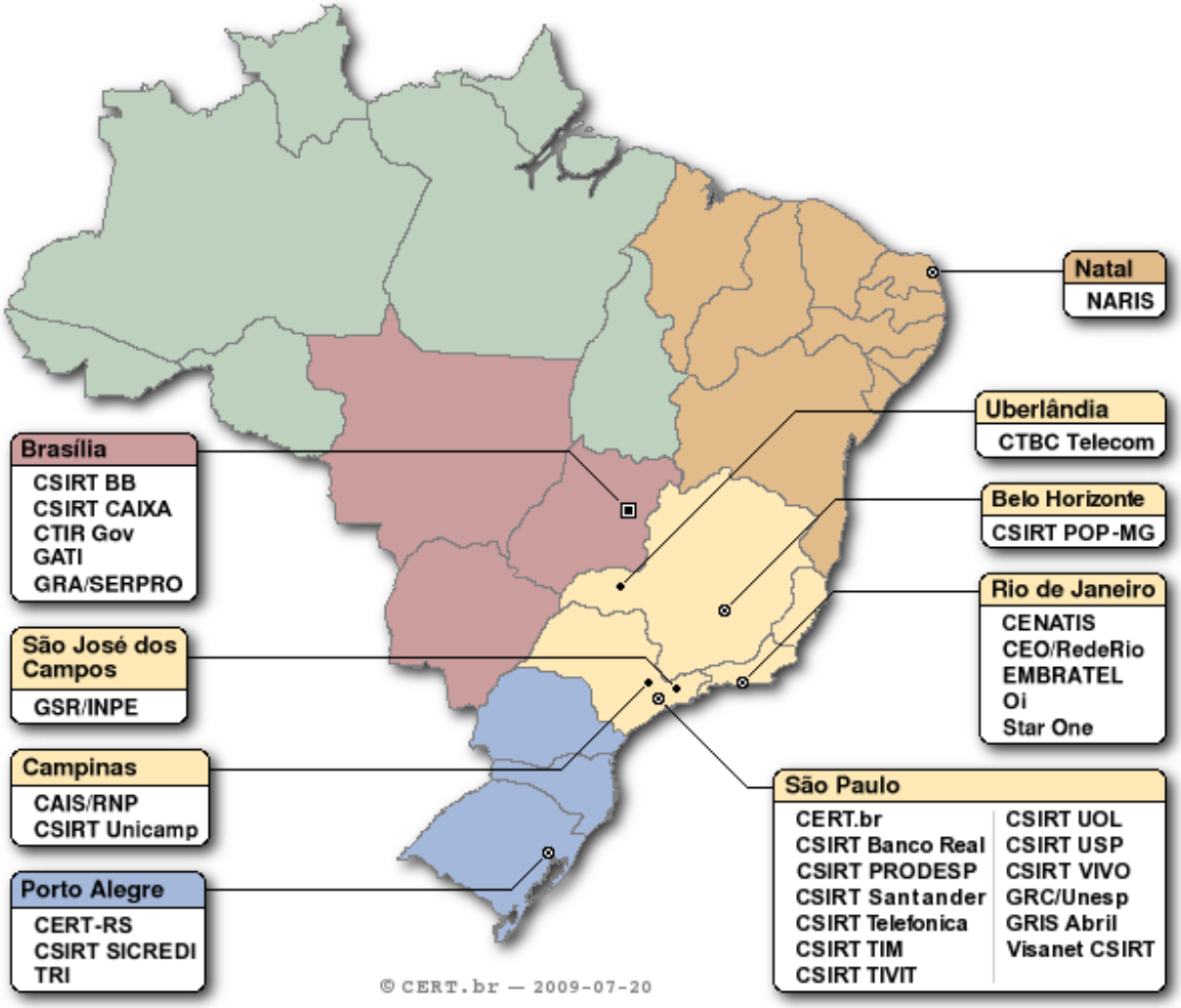
Parcerias Internacionais:

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



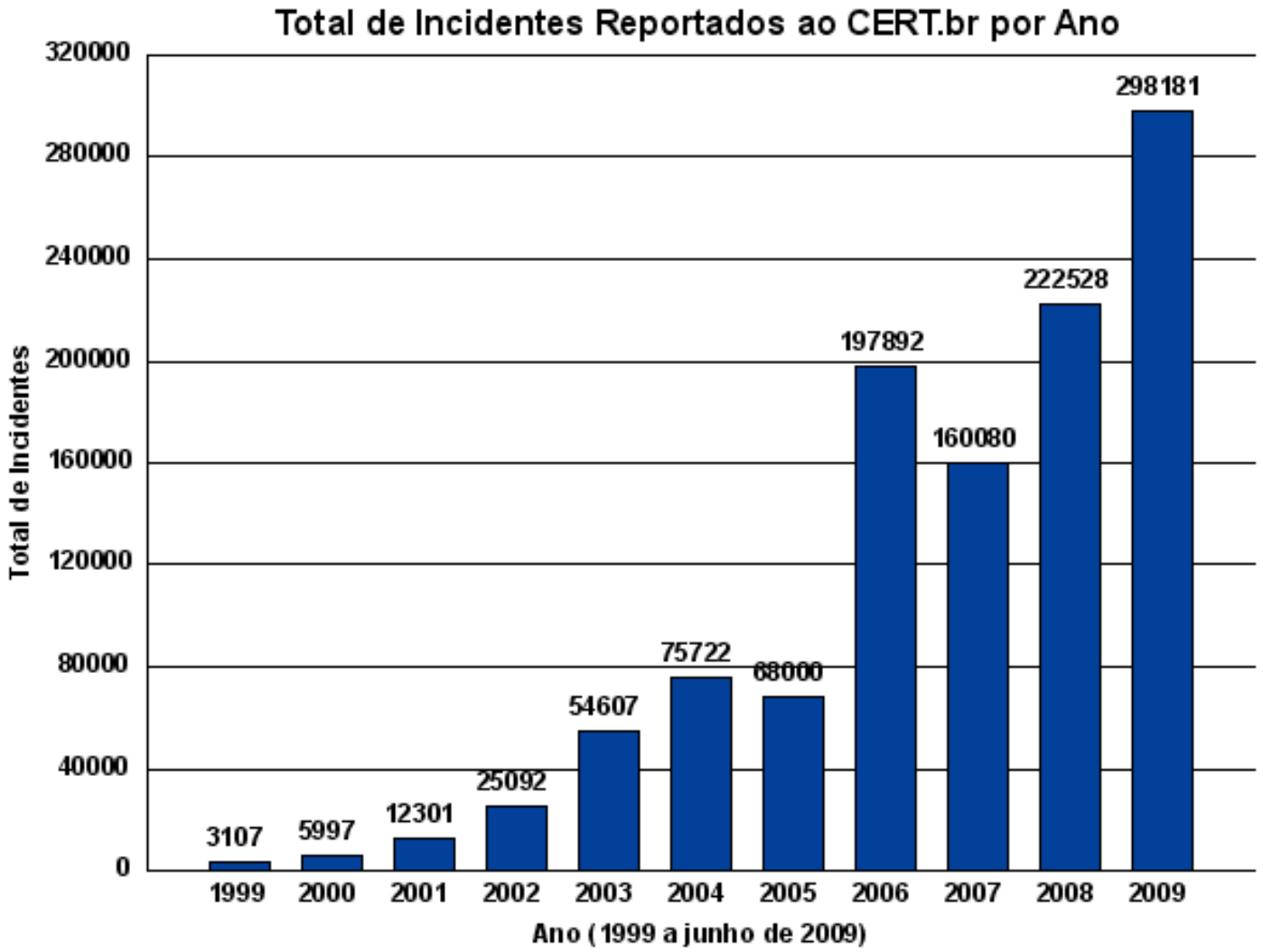
http://www.cert.br/contato-br.html

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/**

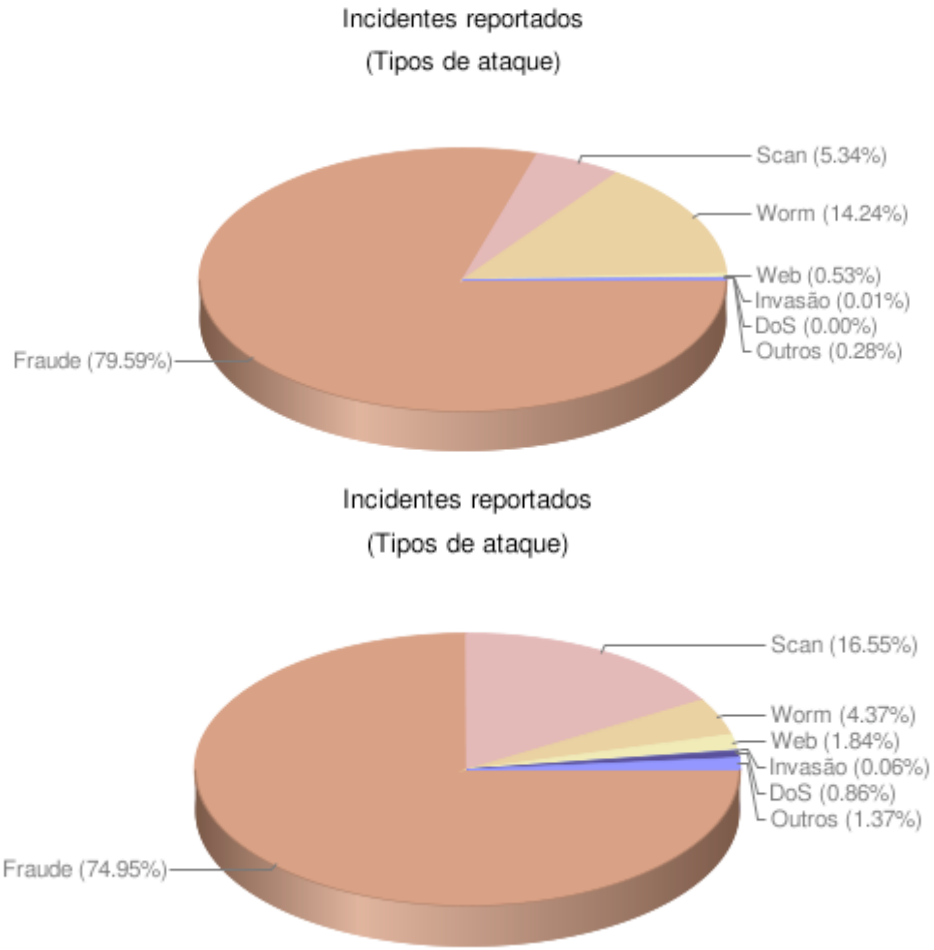
Incidentes Reportados ao CERT.br



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

Incidentes Reportados ao CERT.br – Tipos (2/2)

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

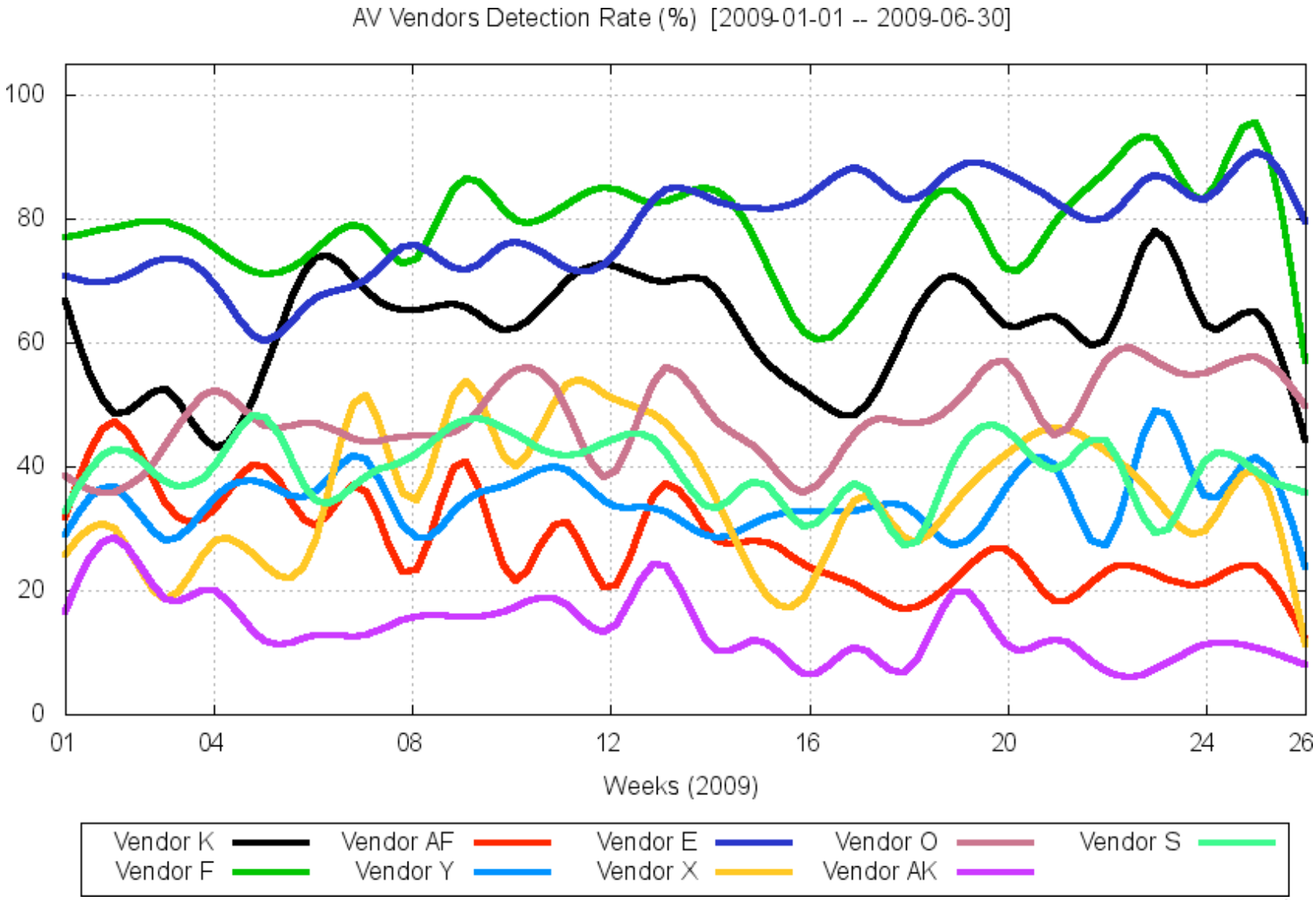
- **Em nome das mais variadas instituições e com tópicos diversos**
- **Com *links* para códigos maliciosos (cavalos de tróia)**

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

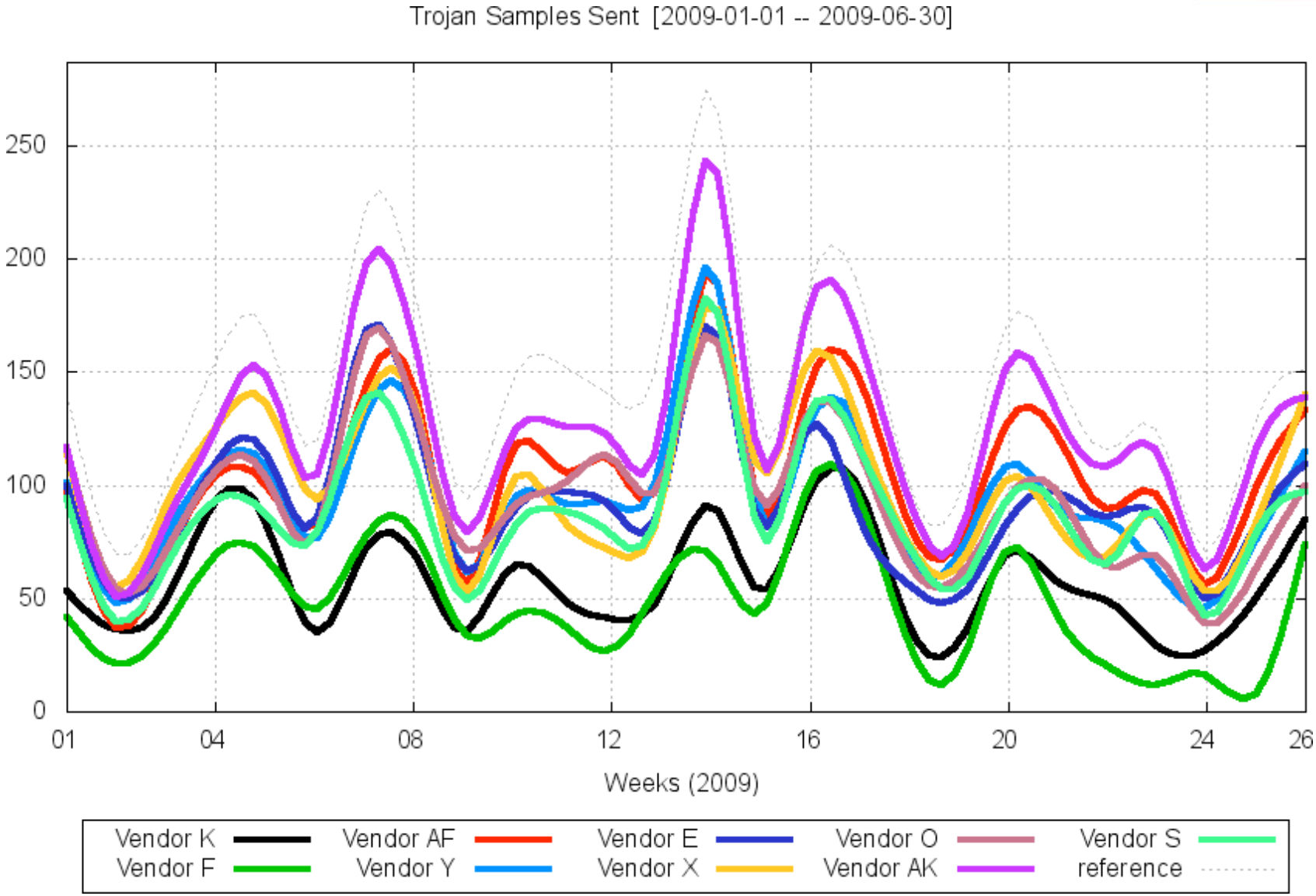
2008/2009: Detalhes dos Códigos e URLs

	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 origem	78	64
Nomes de arquivos	8.297	2.879
URLs únicas	17.376	4.973
Códigos maliciosos únicos (*hashes* criptográficos únicos)	14.256	3.740

1º Semestre/2009: Eficiência dos Antivírus



1º Semestre/2009: Exemplares Enviados

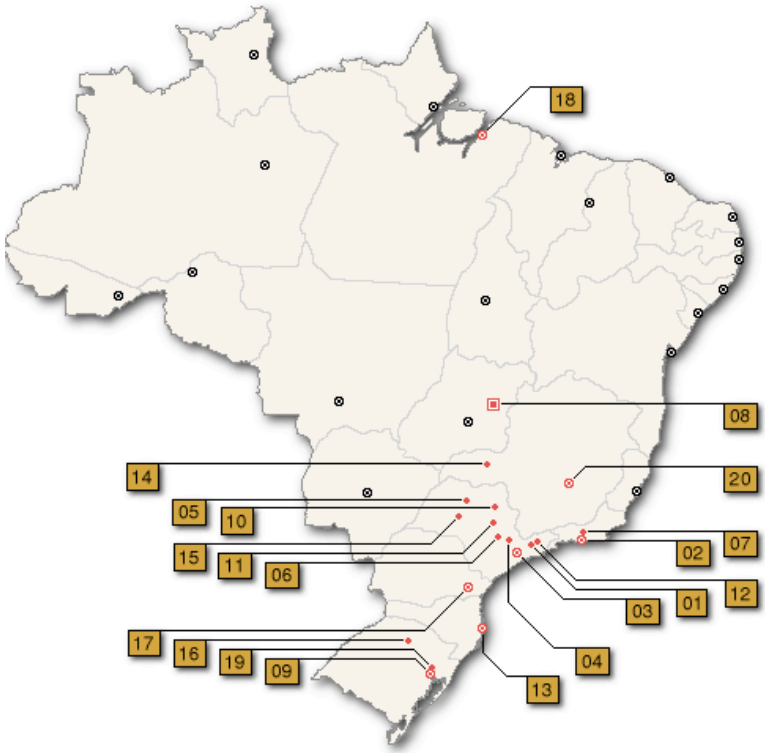


Análise de Tendências

Projeto *Honeypots* Distribuídos

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

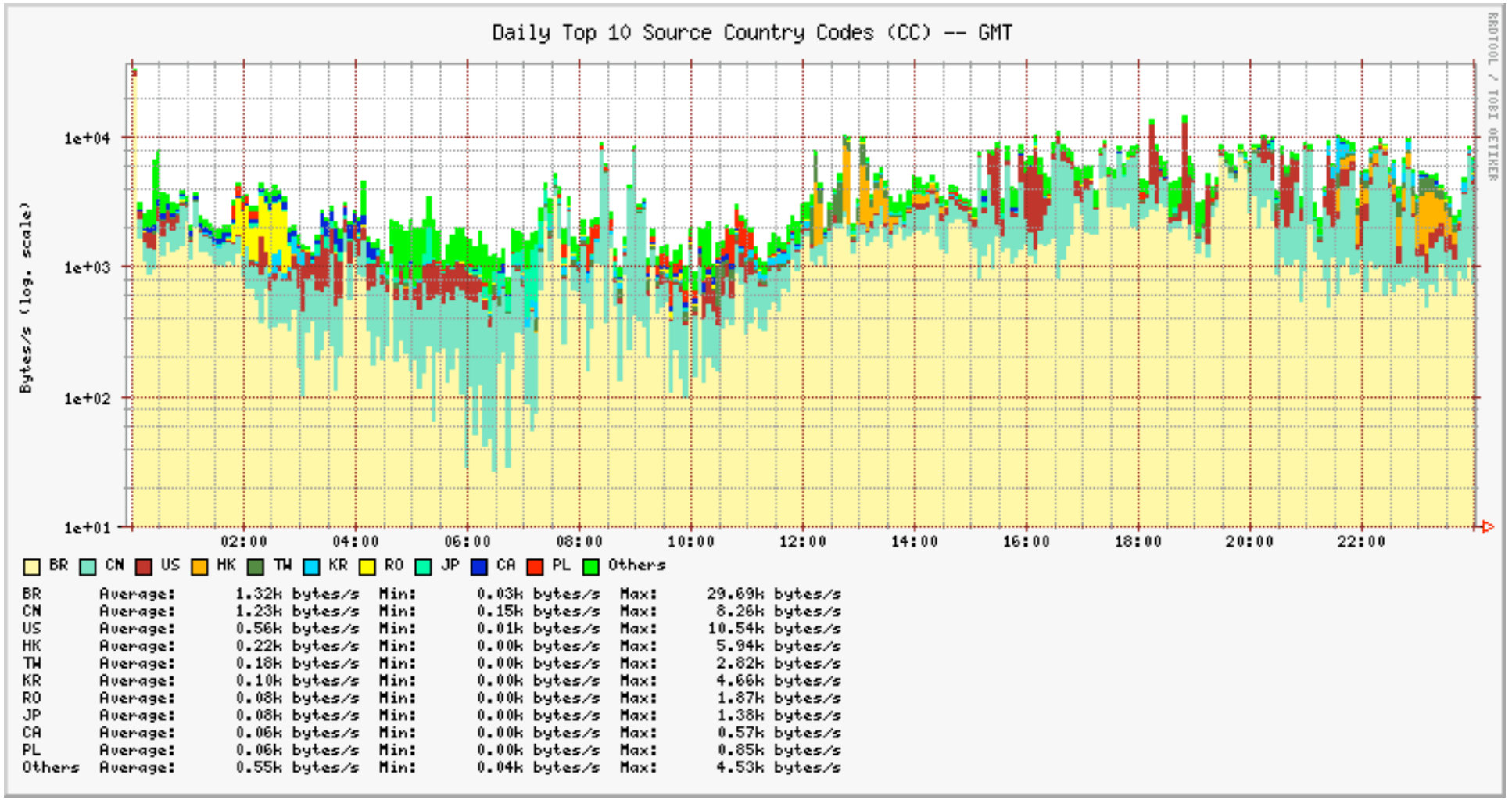
- **37 instituições, entre academia, governo, indústria e instituições financeiras**
- **Baseado em trabalho voluntário**
- **http://www.honeypots-alliance.org.br/**



Utilização dos dados coletados para:

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

Estatísticas Públicas dos Ataques Registrados



Projeto SpamPots

- **Implementado pelo CERT.br**

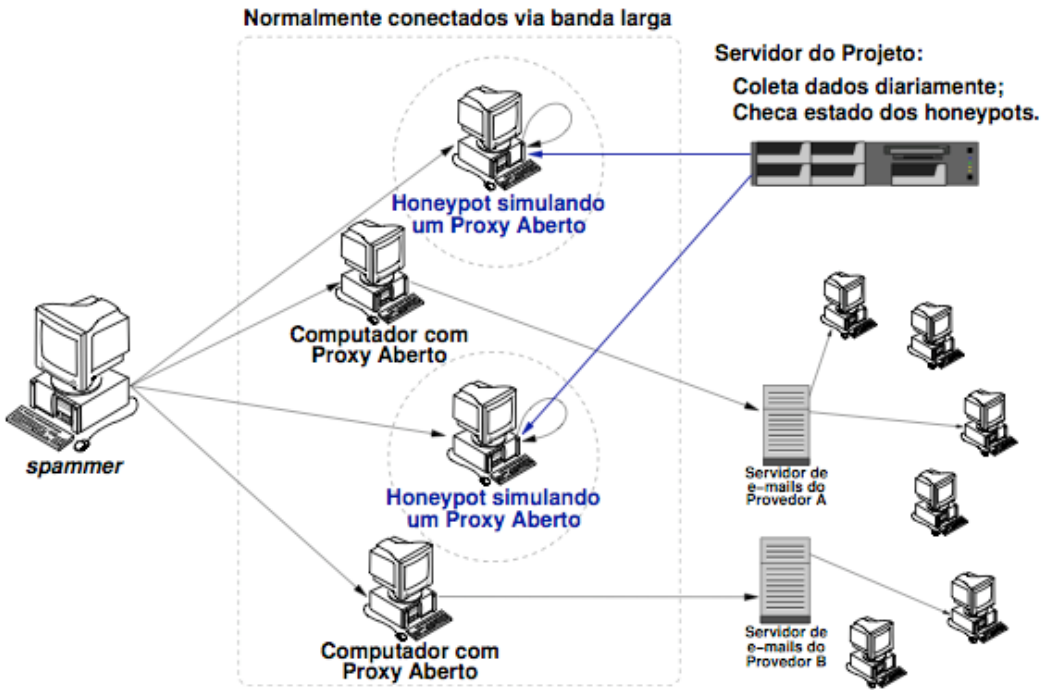
- **Financiado pelo NIC.br/CGI.br**
  - **Como parte dos trabalhos da Comissão Anti-Spam**
  - **Para gerar métricas sobre o abuso de máquinas de usuários finais para o envio de *spam***

- **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/

Considerações Finais

- **Cenário atual**
  - ***Softwares* com muitas vulnerabilidades**
  - **Pressão econômica para lançar, mesmo com problemas**
- **Só haverá melhorias quando**
  - **O processo de desenvolvimento de *software* incluir**
    - **Levantamento de requisitos de segurança**
    - **Testes que incluam casos de abuso (e não somente casos de uso)**
  - ***Secure Software Development* se tornar parte da formação de projetistas e programadores**
  - **Provedores e operadoras forem mais pró-ativos**

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/