# Iniciativas em Tratamento de Incidentes de Segurança

Cristine Hoepers
cristine@cert.br

Klaus Steding-Jessen
jessen@cert.br

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

cert@cert.br

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

# Roteiro

- CGI.br, CERT.br e a história do Tratamento de Incidentes no Brasil
- cenário internacional
- iniciativas de cooperação
- problemas e desafios
- possíveis ações

# CGI.br

Comitê Gestor da Internet no Brasil (CGI.br)

- criado pela Portaria Interministerial nº 147, de 31 de maio de 1995
- alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003

Composto por 21 membros, sendo:

- 9 representantes do Governo Federal
- 4 representantes do setor empresarial
- 4 representantes do terceiro setor
- 3 representantes da comunidade científica e tecnológica
- 1 representante de notório saber em assuntos de Internet

# CGI.br (cont.)

Algumas atribuições definidas no Decreto Presidencial nº 4.829:

- **articular as ações relativas à 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

# CGI.br (cont.)


cgi.br
Comitê Gestor da Internet no Brasil
nic.br
Núcleo de Informação e Coordenação
cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil
registro.br
Registro de Domínios para a Intenet no Brasil
ptt.br
Ponto de Troca de Tráfego

# História dos CSIRTs no Brasil

- agosto/1996: o CGI.br publicou o relatório: “Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil”[1], com os seguintes requisitos:
  - ser uma organização neutra
  - atuar como ponto focal para tratamento de incidentes envolvendo redes brasileiras
  - facilitar o processo de tratamento de incidentes e troca de informações
  - orientar tecnicamente os que a ela recorrerem para sanar falhas de segurança

[1] http://www.nic.br/grupo/historico-gts.htm

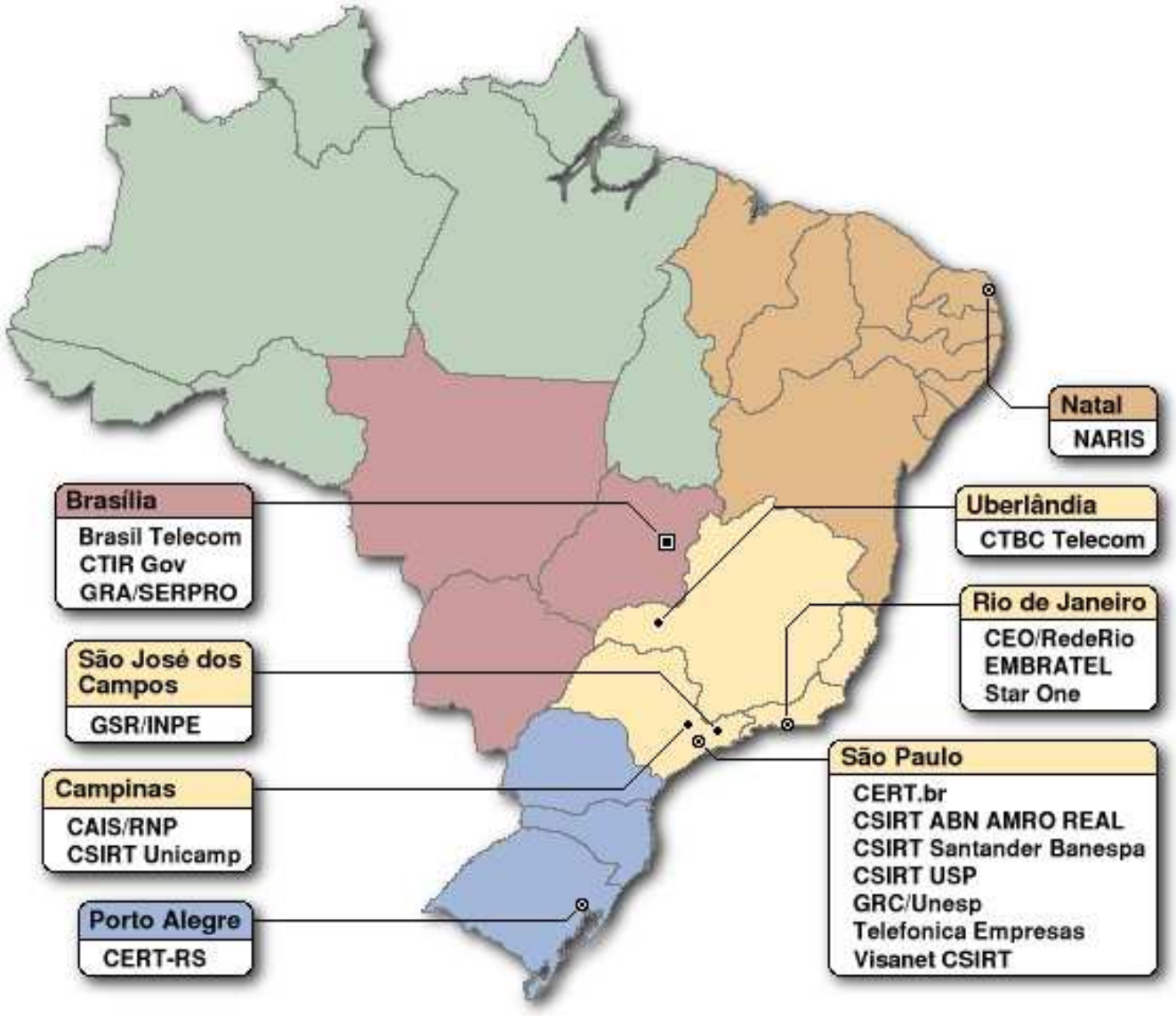
# História dos CSIRTs no Brasil (cont.)

- junho/1997: O CGI.br criou o CERT.br (inicialmente chamado NBSO – NIC BR Security Office)
- agosto/1997: são criados o CAIS/RNP[2] e o CERT-RS[3]
- 1999: diversas outras instituições anunciaram seus CSIRTs, entre elas operadoras de telecom e universidades
- 2003: mais de 20 CSIRTs formados. Iniciada a página de contatos de CSIRTs no Brasil: http://www.cert.br/contato-br.html
- 2004: Criação do CTIR Gov, no âmbito da Administração Pública Federal

[2] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf

[3] http://www.cert-rs.tche.br/cert-rs.html

# CSIRTs no Brasil




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

# CSIRTs no Brasil (cont.)

## Projeto iNOC-DBA BR

Sistema de comunicação imediata entre operadores de redes e CSIRTs, baseado em telefonia IP.

- 120 telefones IP distribuídos pelo CGI.br para:
  - 100 maiores AS (*Autonomous Systems*) do Brasil
  - 20 CSIRTs (reconhecidos pelo CERT.br)

iNOC-DBA (Internet Network Operation Centers – Dial By AS Number), a global hotline phone system which directly interconnects the Network Operations Centers and Security Incident Response Teams

# Atividades atuais do CERT.br

- atua como ponto focal para notificações de incidentes envolvendo redes brasileiras (domínio .br e IPs alocados ao Brasil)
- produz documentos em português sobre boas práticas
  - 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/)
- mantém estatísticas sobre incidentes e spam
- ministra cursos do CERT/CC sobre Tratamento de Incidentes

# Cenário Internacional

# FIRST

## Forum of Incident Response and Security Teams

- "*brings together a variety of computer security incident response teams from government, commercial, and academic organizations*"
- "*FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.*"

Fonte: http://www.first.org/

# APCERT

## Asia Pacific Computer Emergency Response Team

- "*It is a coalition of CSIRTs, from 12 economies across the Asia Pacific region.*"
- "*Any CSIRT from Asia Pacific Region, who is interested to furthering the objectives of APCERT, will be allowed to join as APCERT members after meeting all member accreditation requirements.*"

Fonte: http://www.apcert.org/

# TF-CSIRT

## Collaboration of Security Incident Response Teams

- "*Task Force established under the auspices of the TERENA Technical Programme to promote the collaboration between CSIRTs in Europe.*"
- "*activities of TF-CSIRT are focused on Europe and neighbouring countries*"
- "*Services for CSIRTs: Trusted Introducer for CSIRTs in Europe*"

Fonte: http://www.terena.nl/tech/task-forces/tf-csirt/index.html

# TI

## Trusted Introducer for CSIRTs in Europe

- "*TI provides European CSIRTs with a public repository that lists all known European CSIRTs*"
- "*An important pre-requisite for mutual trust is shared and accurate operational knowledge about one another.*"
- "*The TI accreditation service is meant to do just that: facilitate trust by formally accrediting CSIRTs that are ready to take that step.*"

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

# EGC

## European Government CSIRTs group

- "*EGC is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe.*"
- "*Current members: CERTA (France), CERT-Bund (Germany), CERT-FI (Finland), GOVCERT.NL (The Netherlands), SITIC (Sweden), UNIRAS (United Kingdom)*"

Fonte: http://www.bsi.de/certbund/EGC/index_en.htm

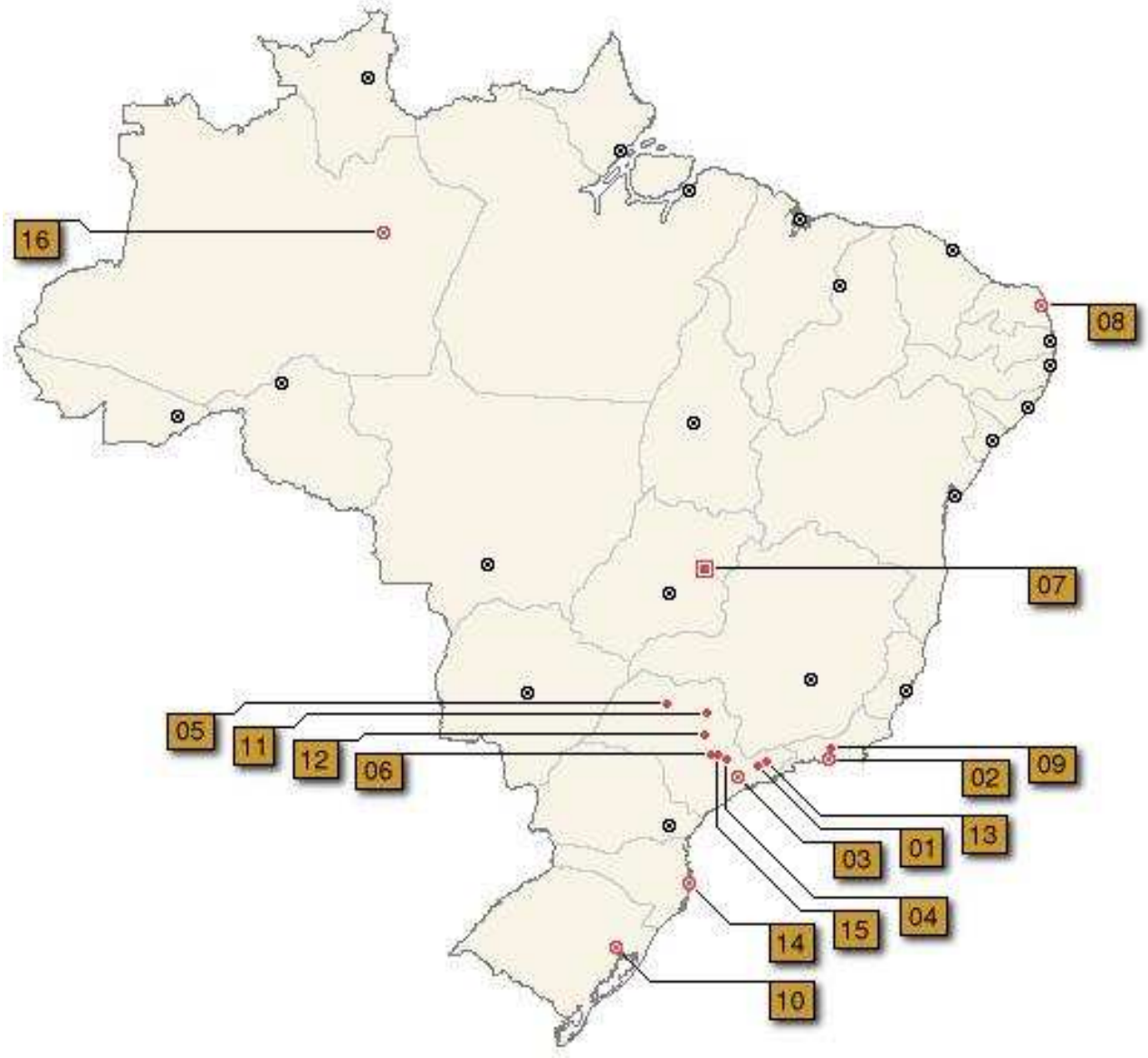
# Algumas Iniciativas de Cooperação no Brasil

# Projeto Honeypots Distribuídos

- coordenação: CenPRA/MCT e CERT.br
- 27 instituições parceiras:
  - academia, governo, teles, empresas
- honeypots distribuídos no Brasil
  - em diversos AS e em diferentes localidades
- com base em trabalho voluntário
- mantém estatísticas públicas
  - flows diários das atividades combinadas dos honeypots

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

# Projeto Honeypots Distribuídos (cont.)




Cidades onde os honeypots estão localizados.

# Projeto Honeypots Distribuídos (cont.)

Uso, pelo CERT.br, dos dados dos honeypots em Tratamento de Incidentes

- identificação de assinaturas de atividades maliciosas/abusivas conhecidas
  - worms, bots, scans, spam e outros
- notificação dos responsáveis pelas redes de IPs alocados ao Brasil
  - fornecidas dicas de recuperação

# Ações Antifraude

- trabalho conjunto entre algumas instituições financeiras e o CERT.br
- trocas de informações sobre técnicas e sites hospedando páginas clonadas ou códigos maliciosos
- CERT.br é um Anti-Phishing Working Group Research Partner (http://www.antiphishing.org/)
  - notifica os sites hospedando os malwares
  - interage com sites internacionais para agilizar retirada de malwares do ar
  - envia novos exemplares para mais de 20 fabricantes de antivírus

# CT-Spam do CGI.br

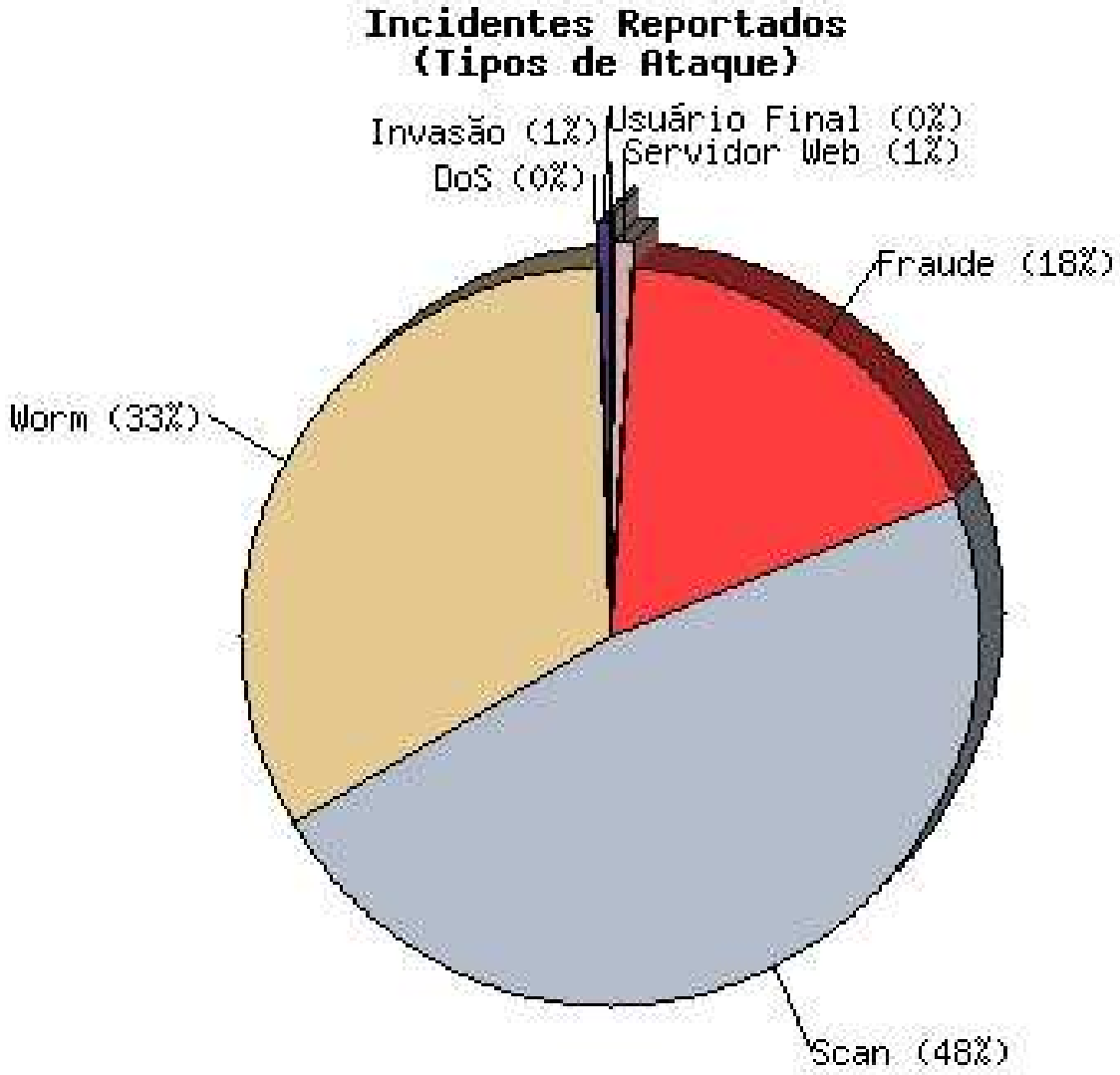
Missão da Comissão de Trabalho sobre Spam:

- propor uma estratégia nacional de combate ao spam
- articular as ações entre os diferentes atores
- documentos escritos:
  - “Tecnologias e Políticas para Combate ao Spam”
  - “Análise Técnica de Algumas Legislações sobre Spam”
- desenvolver um site anti-spam
  - dicas para usuários
  - melhores práticas para administradores de redes

http://www.cgi.br/eventos/int-ctspam.htm

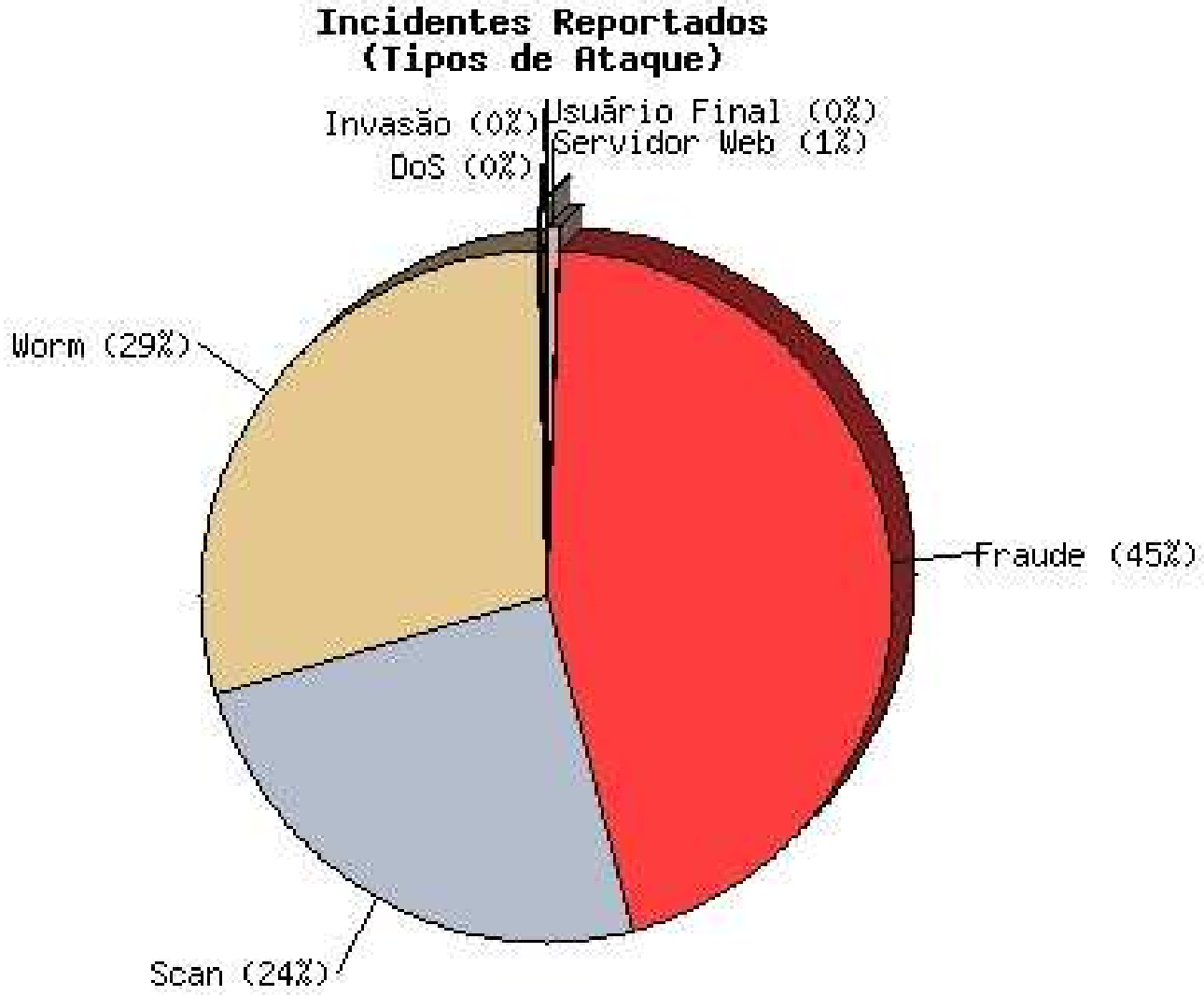
# Problemas e Desafios

# Incidentes Notificados em 2005/01




Total de incidentes: 12.438

# Incidentes Notificados em 2005/02




Total de incidentes: 17.542

# Principais Ameaças

- ataques automatizados
  - worms, bots, etc
- enfoque dos ataques nos usuários
  - aumento no uso de banda larga
  - máquinas sem cuidado com segurança
  - vítimas de fraudes, malwares, spywares, engenharia social
  - usadas para práticas de negação de serviço, envio de spam, harvesting de e-mails, entre outras

# Desafios no Tratamento de Incidentes no Brasil

- dificuldades de comunicação via e-mail
  - perda de e-mails devido a filtros anti-spam
  - dificuldade de notificar malwares e outros tipos de códigos barrados por antivírus
- dificuldades no tratamento das notificações
  - dificuldade para priorização
  - equipes sem perfil técnico
- contatos desatualizados

# Desafios no Tratamento de Incidentes no Brasil (cont.)

- atuar em casos de usuários finais ou redes terceirizadas
- interagir em todo processo de segurança
  - prevenção, proteção e políticas
- expandir o trabalho pró-ativo
  - usar os conhecimentos das tendências de ataques para direcionar a conscientização de seu público alvo, treinamentos, desenvolvimento de software, etc

# Possíveis Ações

- anunciar mais amplamente os CSIRTs
- promover workshops/treinamentos para aqueles que estão recebendo e respondendo as notificações
- iniciar cooperação com outros grupos da mesma área
  - produção de documentos
  - troca de informações sobre boas práticas e casos de sucesso