CERT-RS: Apresentação e Atuação

João Marcelo Ceron

Leandro Bertholdo

Sumário

- Introdução
- Estatísticas
- Principais Incidentes
- Medidas tomadas

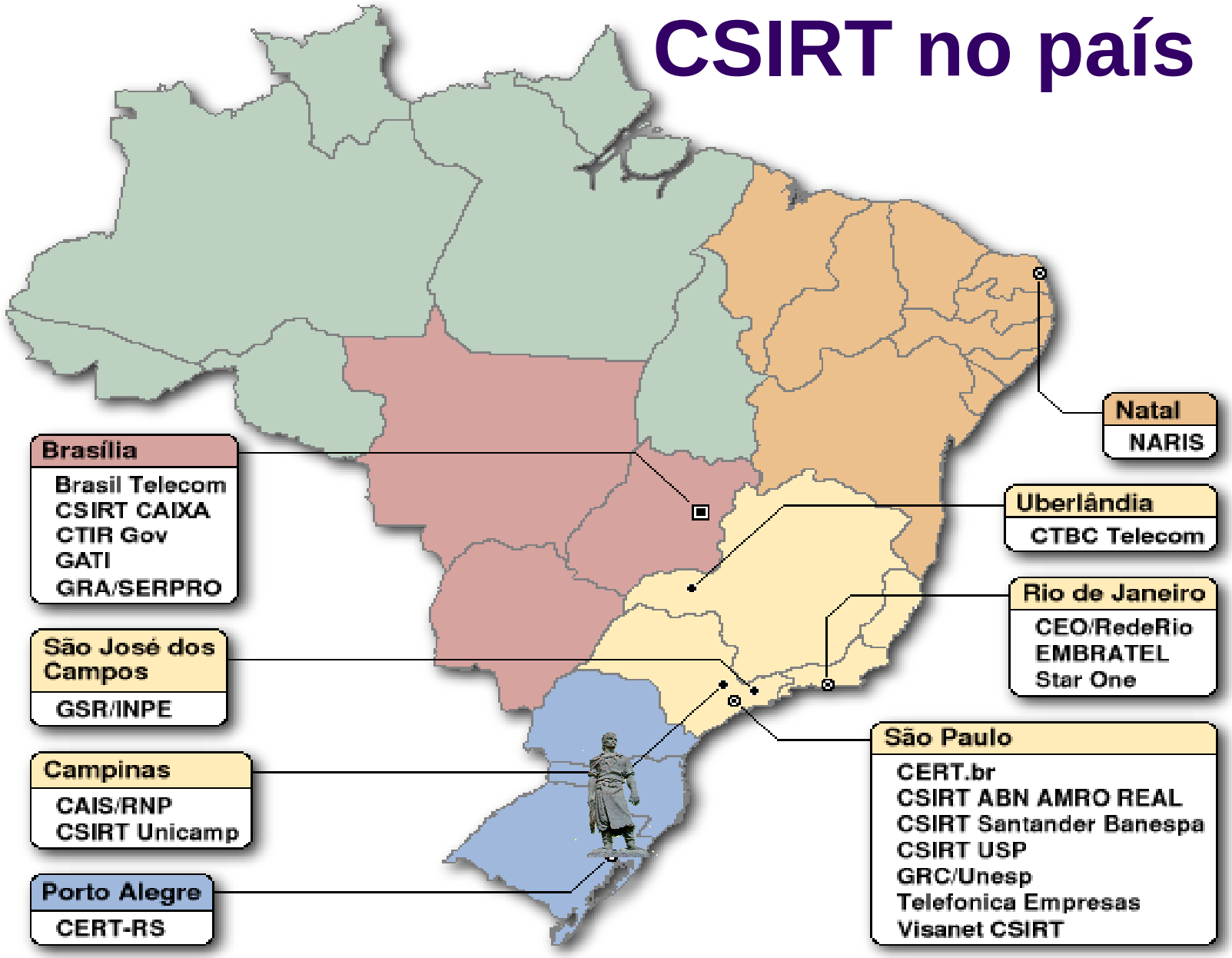
Introdução

- CERT-RS
  - Centro de resposta a incidentes de segurança
  - Fundado em 1995
  - Pioneiro no país
  - Responde por incidentes da Rede Tchê!
    - Mais de 170.000 usuários conectados

Missão

- responder por incidentes na rede acadêmica do Rio Grande do Sul
- prover a coordenação e o apoio necessário no processo de resposta incidentes
- estabelecer um trabalho colaborativo com outras entidades, como os operadores da justiça, provedores de acesso e serviços e backbones
- Aumentar a conscientização sobre a necessidade segurança na Internet

CSIRT no país



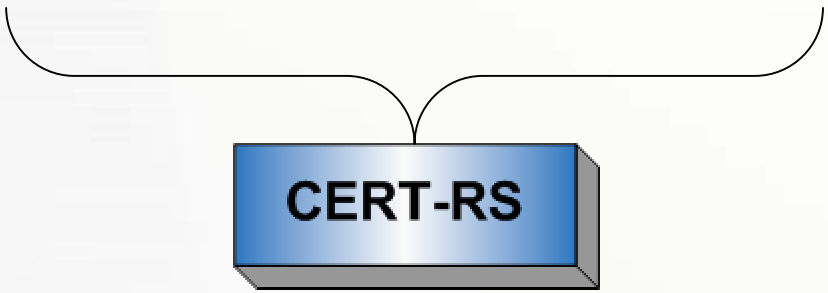
Atividades do CERT-RS

Resposta a Incidentes

alvos de ataques

outros CSIRTs

coordenação e cooperação



Trouble Tickets

RT por alto · Busca Simples · Tíquetes · Ferramentas · Preferências · Aprovação

Encontrado 8 tíquetes

Nova busca · Editar Busca · Avançado · Mostrar os Resultados · Atualização em lote

#	Assunto Requisitantes	Estado Criado	Fila Última atualização	Proprietário Atualizado em	Prioridade Tempo Restante
170451	Servidores DNS recursivos abertos cais@cais.rnp.br, cert@cert.br, cpdjlc@furg.br, henrique@pop-rs.rnp.br	novo 2 semanas atrás	CERT-RS	Nobody 3 min atrás	0 0
175997	2 host(s) identificado(s) como origem de Spam - 200.[illegible].0 cais@cais.rnp.br	novo 2 dias atrás	CERT-RS	Nobody 2 min atrás	0 0
176251	1 host(s) identificado(s) como origem de Spam - 200[illegible]2.0 cais@cais.rnp.br	novo 40 horas atrás	CERT-RS	Nobody 2 min atrás	0 0
176255	2 host(s) identificado(s) como origem de Spam - 200.[illegible].0 cais@cais.rnp.br	novo 40 horas atrás	CERT-RS	Nobody 2 min atrás	0 0
176495	1 host(s) identificado(s) como origem de Spam - [illegible].35.0 cais@cais.rnp.br	novo 16 horas atrás	CERT-RS	Nobody 2 min atrás	0 0

Estatísticas

- Manutenção de estatísticas sobre as notificações de incidentes recebidas

Estatísticas

(1 semestre de 2007)

Origem de spam	468
Varredura	107
Virus/worm	56
Bot	10
DNS recursivo	36
Defacement/Phising	14
D.o.S	7
Open Proxy	2

Total: 754

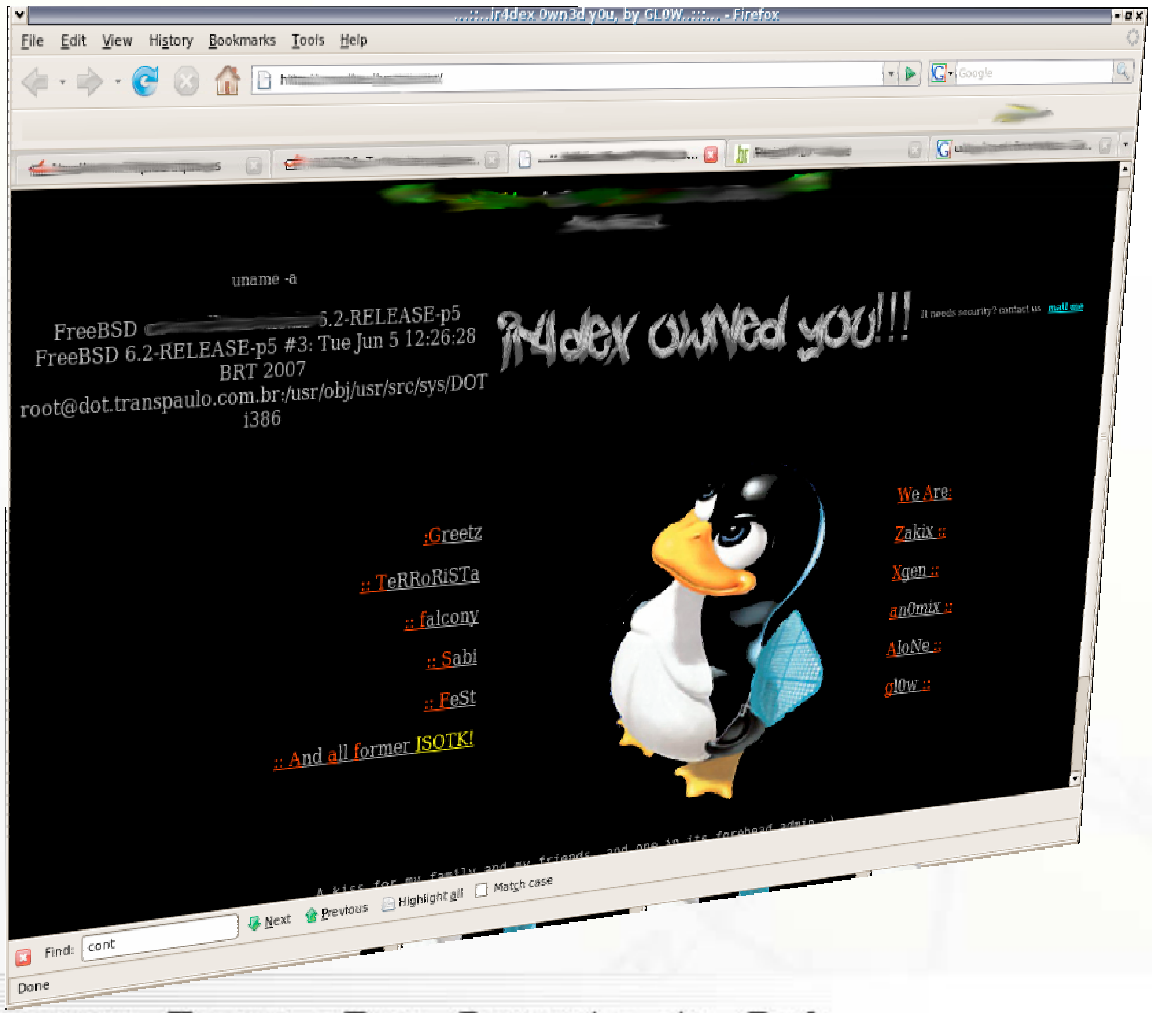
3.5 incidentes por dia

Principais incidentes

- Spams
  - Carga da rede/servidores
  - Virus/códigos maliciosos

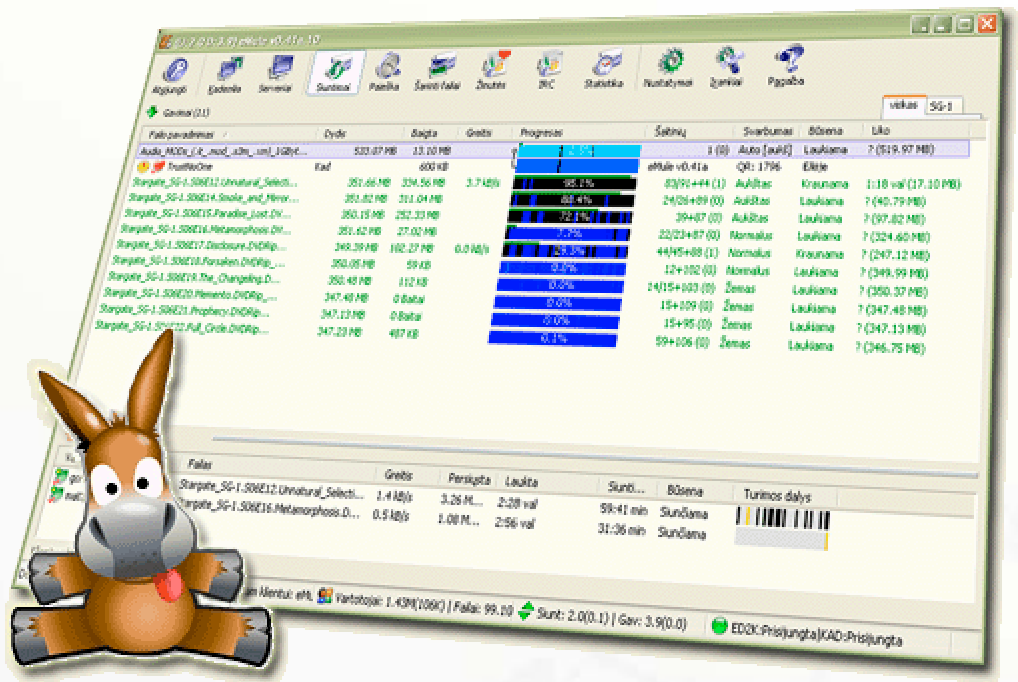
Principais incidentes

- Desfiguração



Principais incidentes

- P2P
  - Bittorrent
  - Kazaa
  - Emule
- Rede Comep
- Limitação de banda



Imagens do filme invares do CERT.br

Principais incidentes

- D.o.S (Denial of Service)
- D.D.o.S (Distributed Denial of Service)

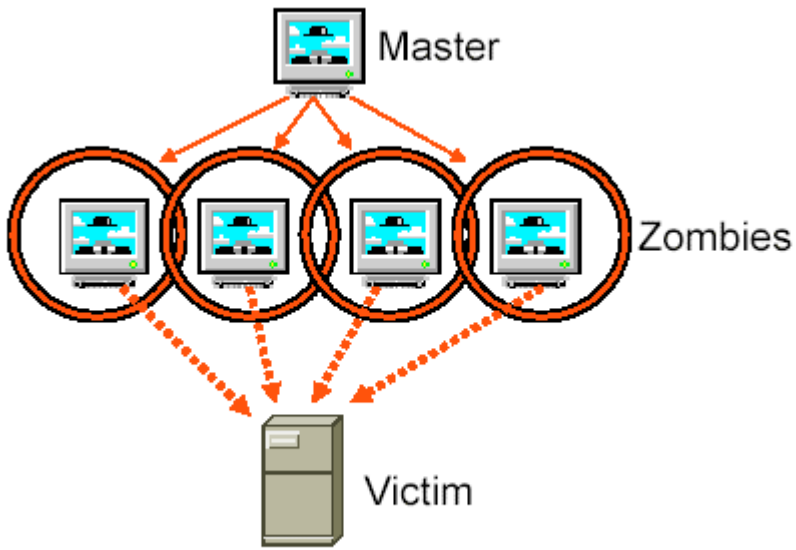
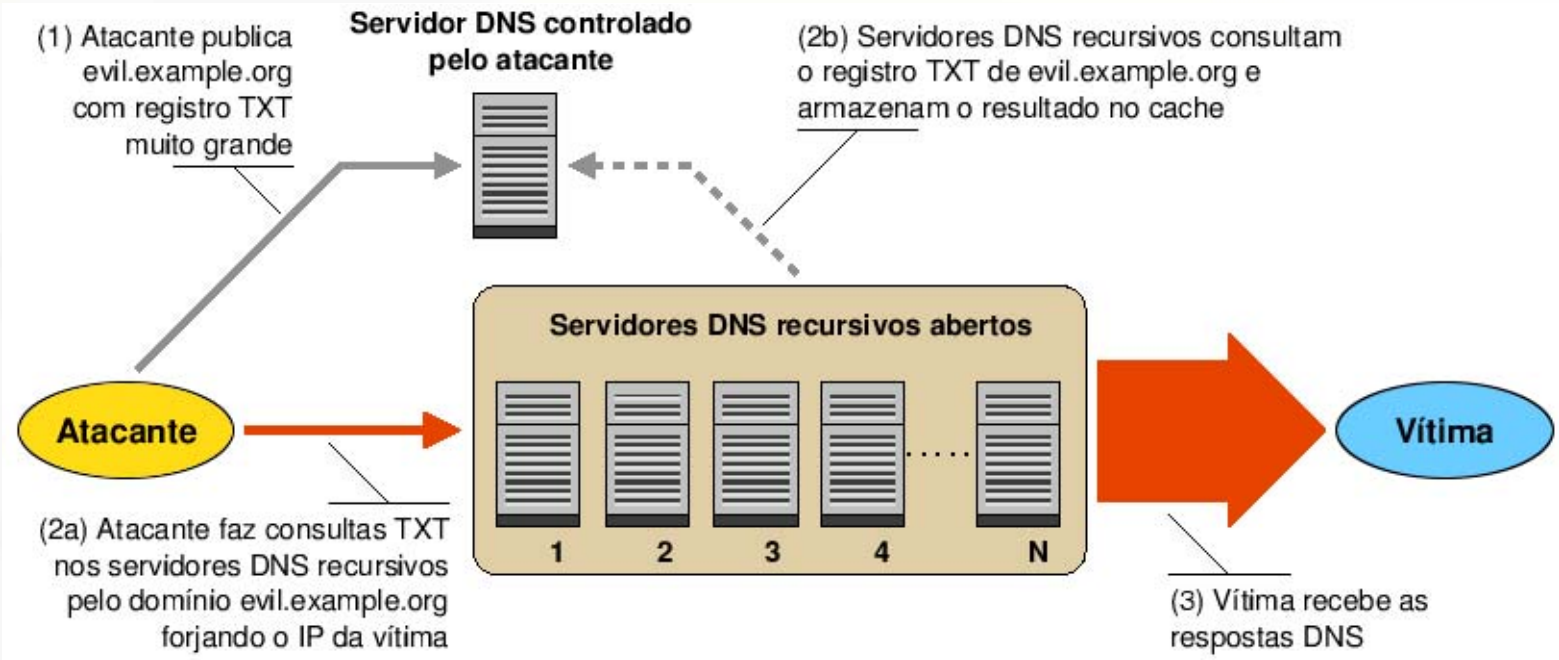


Figure 1-1: DDOS attack architecture

Principais incidentes

- DNS recursivos

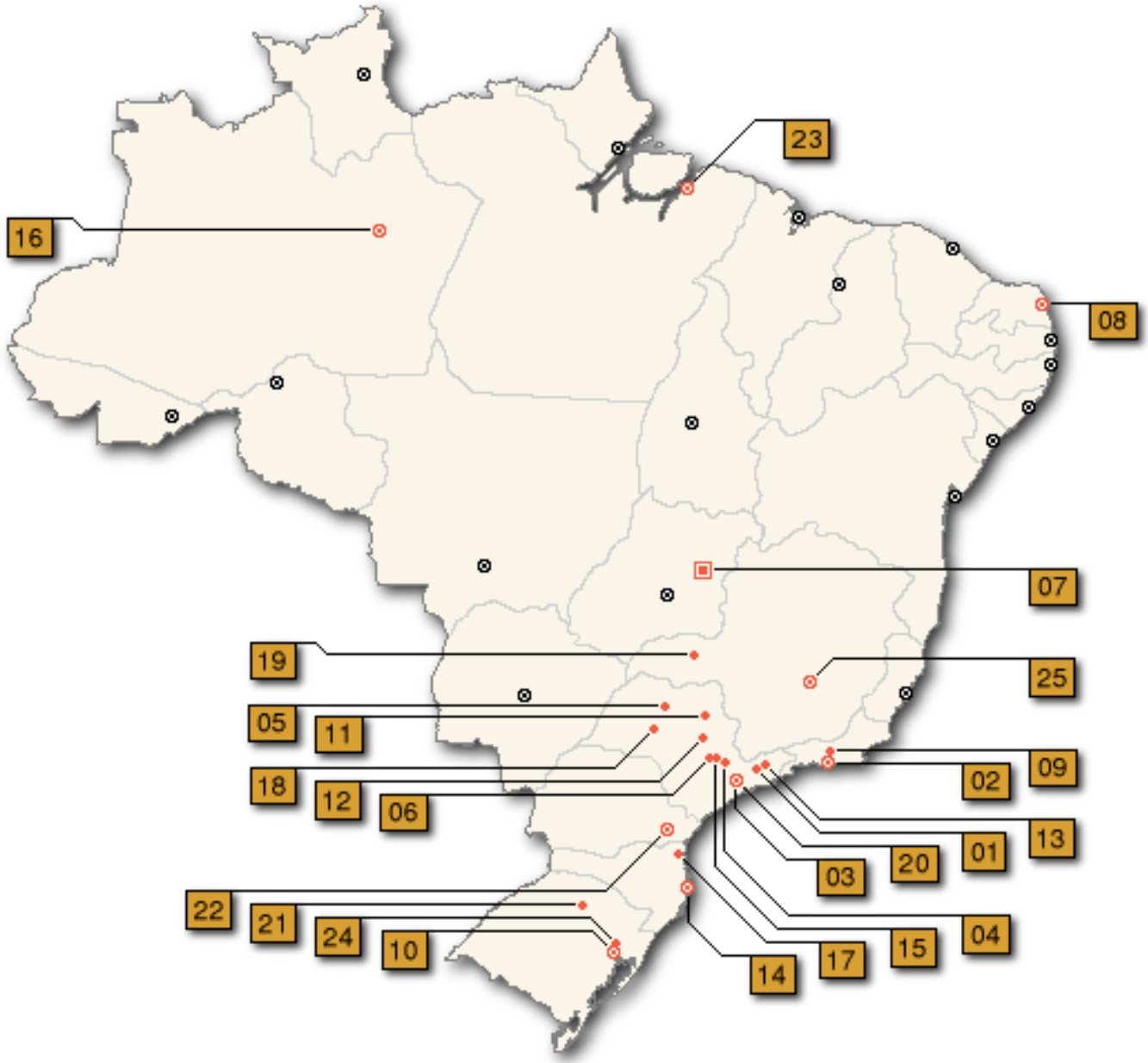


Atividades do CERT-RS

- Análise de Tendências e Early Warning
- Consórcio Brasileiro de Honeypots - Projeto Honeypots Distribuídos
- Parceria do CERT.br

Honeynet.BR

CERT-RS



Computer

Cert-RS
Computer Emergency Response Team - Rio Grande do Sul

www.cert-rs.tche.br

Menu

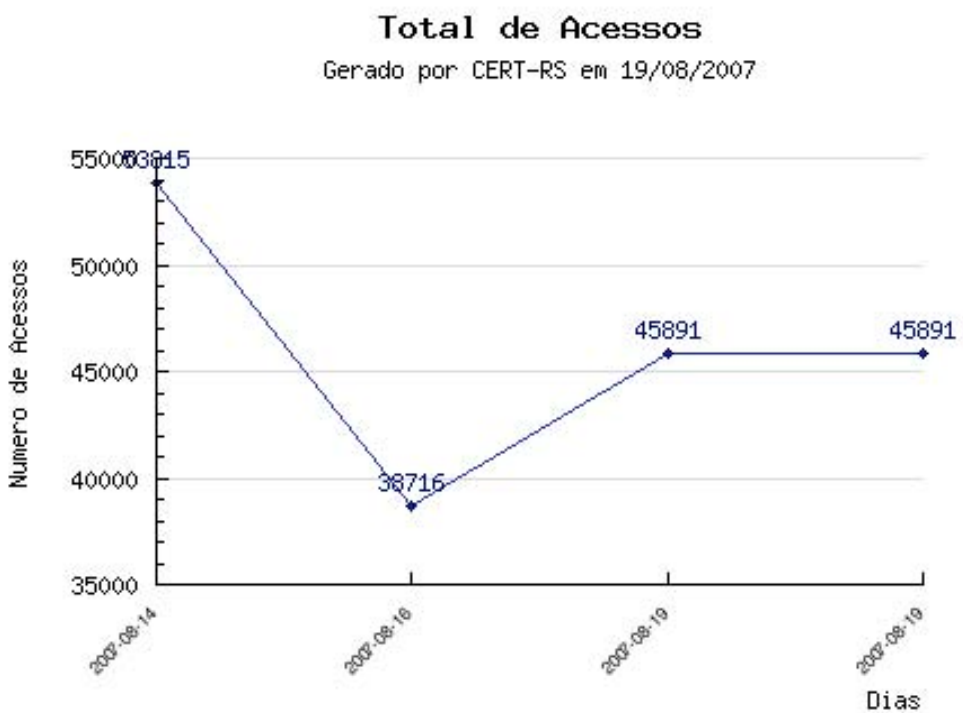
- Página Inicial
- Missão
- Clientes do CERT-RS
- Lista InfoSeg
- Feeds RSS
- Honeypots
- Estatísticas Honeypots
- Outros CERTs
- Documentos
- Ferramentas
- Contato

Projetos

cert.br Cartilha de Segurança para Internet

antispam.br

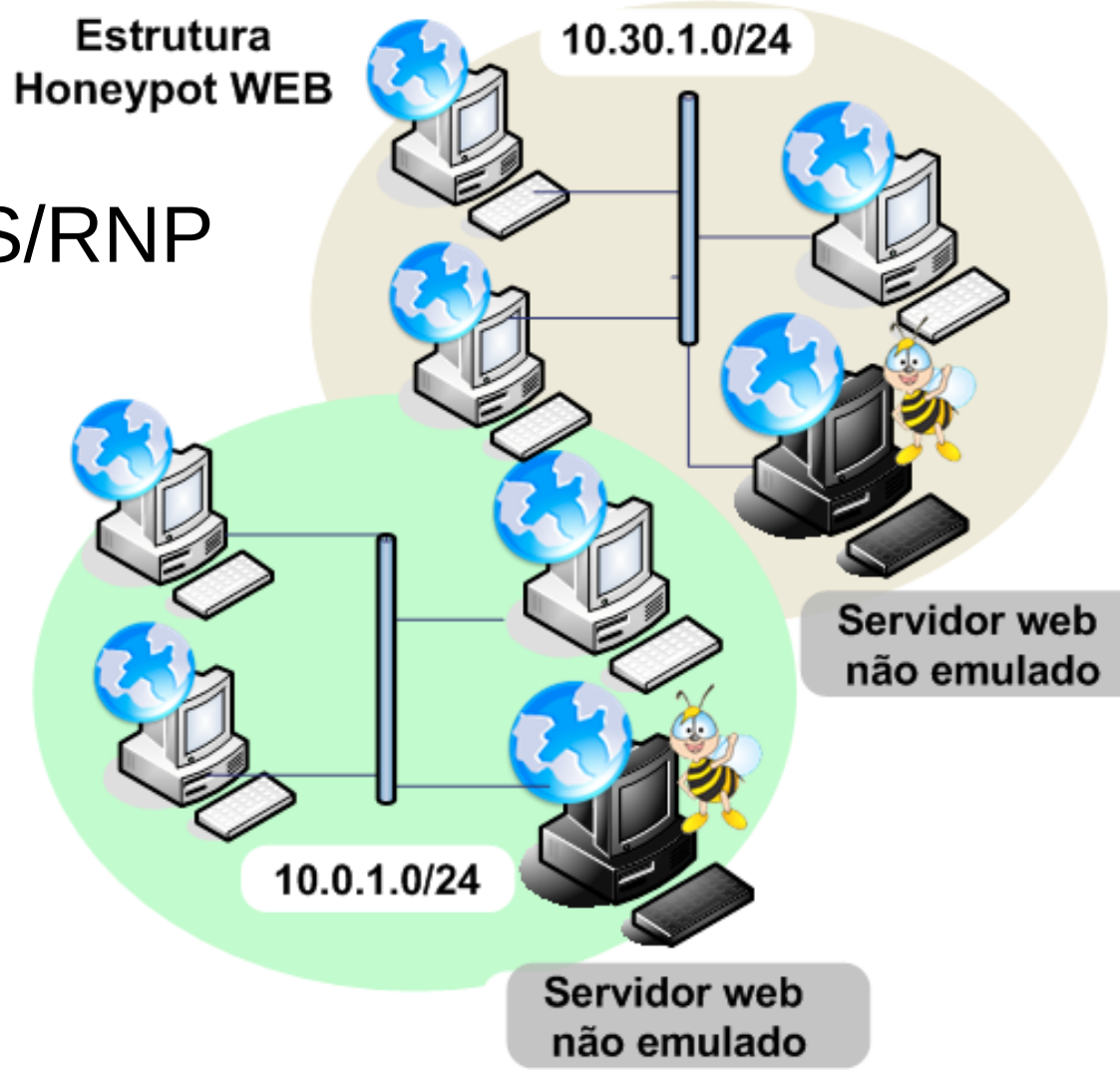
Honeypots Estatísticas - Total de Acessos



- Aumentar a conscientização sobre a necessidade segurança na Internet
- Publicações
  - Honeypots as a Security Mechanism - IEEE
  - HoneyPots Web: análise do tráfego malicioso Web – GTER/GTS
  - Experiências com 802.1x – GTER/GTS

Projetos

- Cursos – PoP-RS/RNP
- Honeypots Web



Projetos

Aplicação emulada	Total de acessos	% do total
PHP- Shell	1176	86,2%
PHP-BB	70	5,1%
PHP- Sysinfo	65	4,7%
Squirre Mail	53	3,8%
Total	**1364**	**100%**

Projetos

- VNC IC (I see)

Obrigado.

www.cert-rs.tche.br

João Marcelo Ceron

ceron@tche.br