Apresentando o Cert-RS

Marcos Straub

Leandro Bertholdo

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

CERT RS
Computer Emergency Team - Rio Grande do Sul

Sumário

- Introdução
- Missão
- Equipe
- Serviços Mantidos
- Ações contra atividades maliciosas.
- Eventuais ações junto ao Cais/RNP

Introdução

- Criado em 1995
- Hoje é sediado e mantido pela equipe do PoP-RS
- Responde pelos incidentes da Rede Tchê
  - Mais de 170.000 usuário conectados (pesquisa 2007)

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

Cert-RS

Rede Tchê

Missão

- Responder por incidentes na rede acadêmica do RS (Rede Tchê) e clientes do POP-RS/RNP
- Prover a coordenação e o apoio necessário para a resolução de incidentes.
- Eventualmente atender a alguns

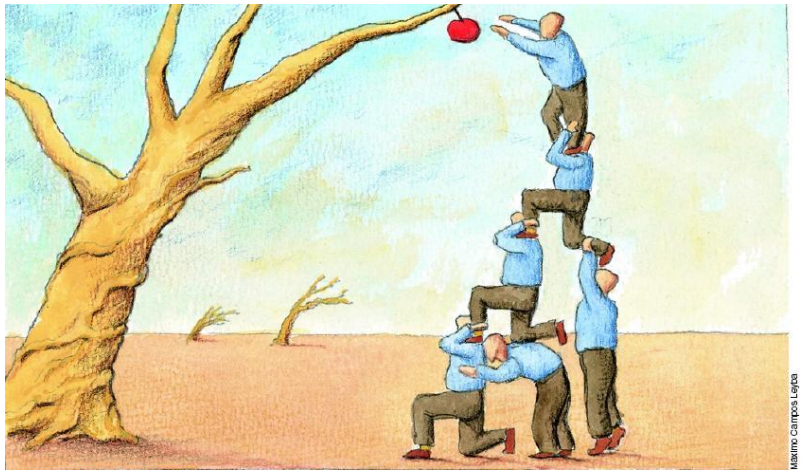
"usuários finais"

Missão

- Estabelecer um trabalho colaborativo com outras entidades, como os operadores da justiça, provedores de acesso e backbones.
- Concientizar sobre a necessidade da segurança na Internet.

Equipe

- Coordenador
- 3 bolsistas em tempo parcial



Serviços

- Contenção de ataques.
- Notificação e tratamento de incidentes.
- Acompanhamento para que os eventos tenham o tratamento adequado!

Serviços

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 - 200.236.36.0 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 - 200.236.32.0 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 - 200.236.36.0 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 - 143.54.35.0 cais@cais.rnp.br	novo 16 horas atrás	CERT-RS	Nobody 2 min atrás	0 0

Serviços

- Lista de segurança InfoSeg

http://listas.pop-rs.rnp.br/mailman/listinfo/infoseg

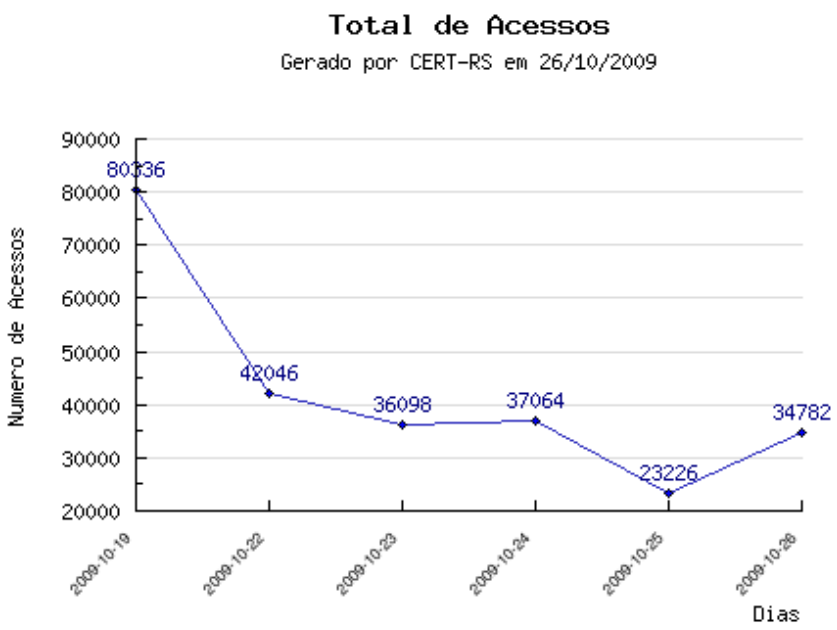
- Criada em 1998
- Lista voltada aos administradores de redes
- Firewalls, configurações, ataques
- Notificação de vulnerabilidades.

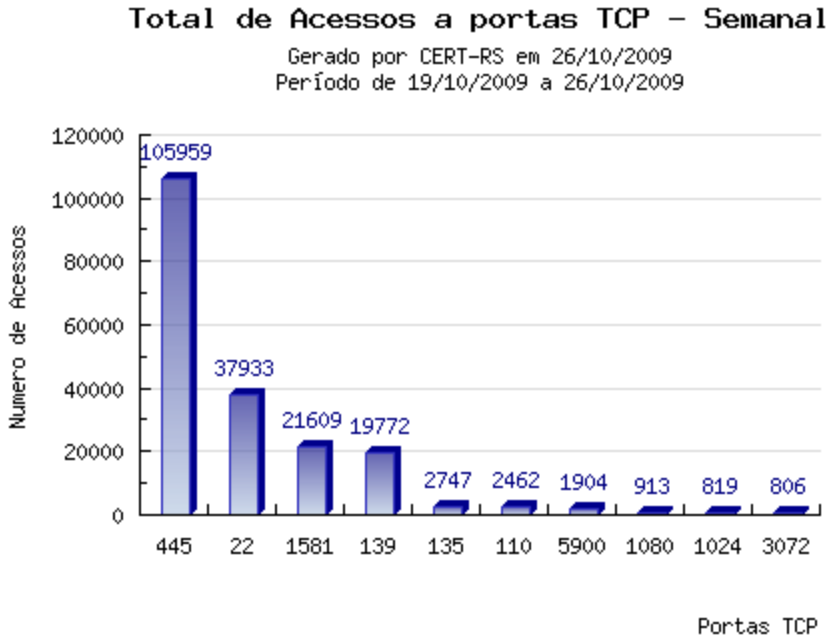
Serviços

- Honeypots
  - Consórcio Brasileiro de Honeypots
  - Parceria com o CERT.br
  - Análise de Tendências e Early Warning
  - Gráficos de Acessos UDP, TCP e Total para análise de tendências

Honeynet.BR

Serviços

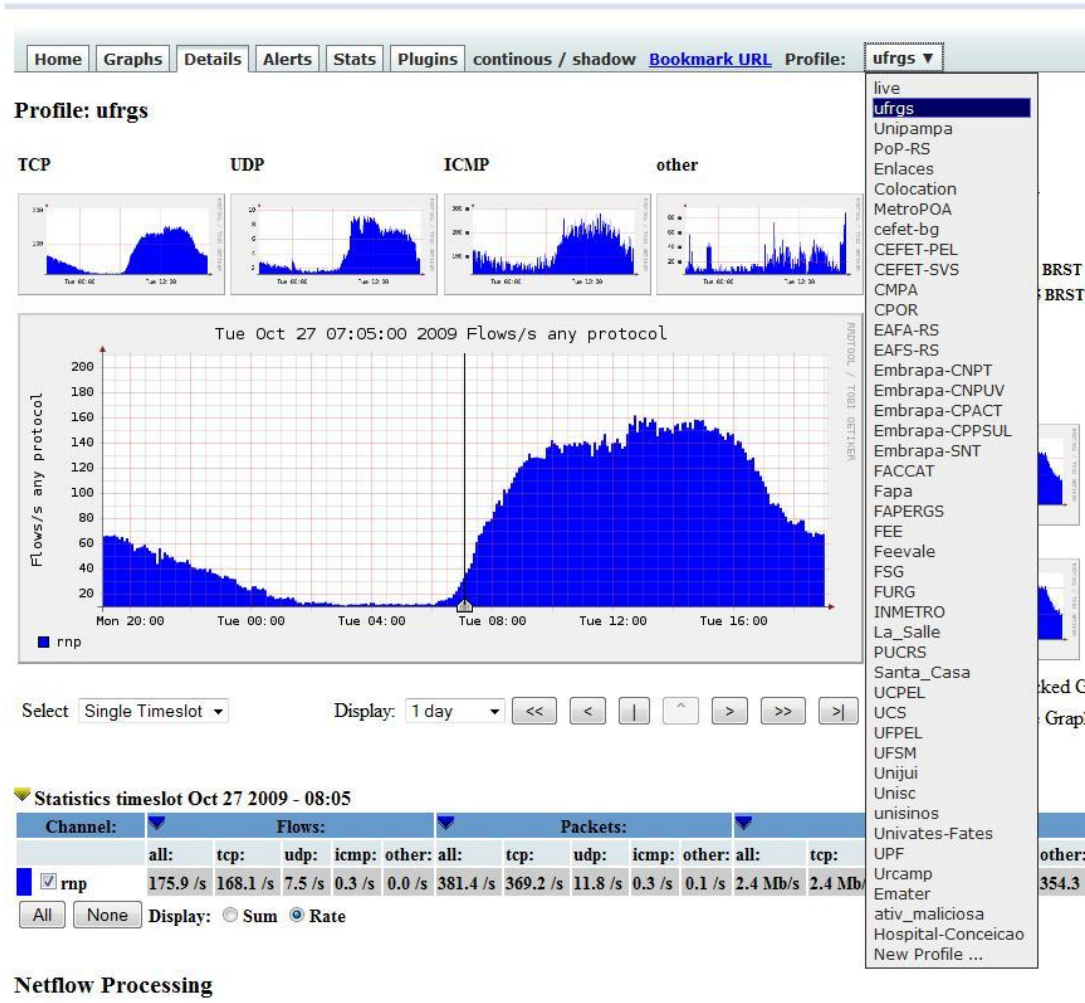




Honeynet.BR

Serviços

- Consulta aos Flows
- Views por Instituição
- NFSEN



Serviços

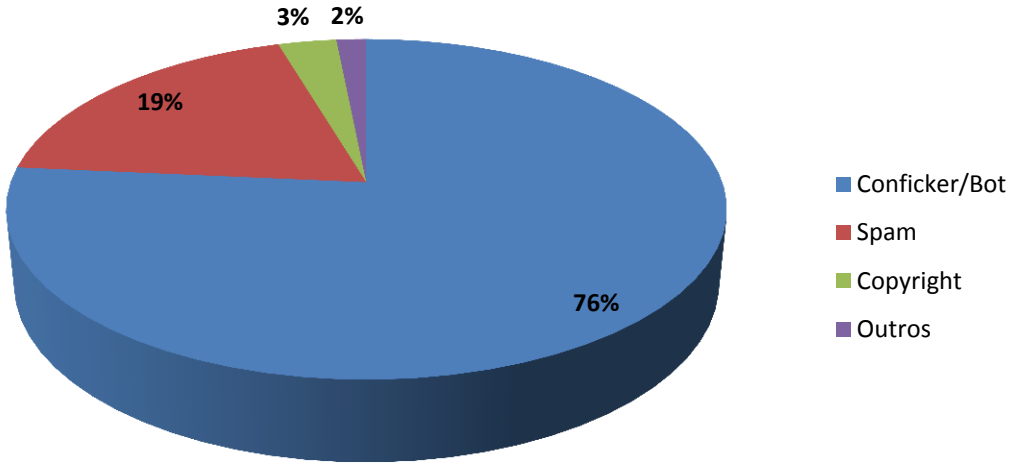
- Novo site do Cert-RS
- Atualização Dinâmica
  - RSS
- Fácil administração
- Mais bonitinho ;)

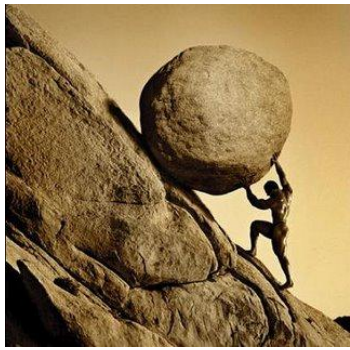
Ações contra atividades maliciosas

- Participações no DISI da RNP
- Palestras nas reuniões da Rede Tchê
- Cursos em conjunto com a ESR-POA/RNP

Dificuldades encontradas

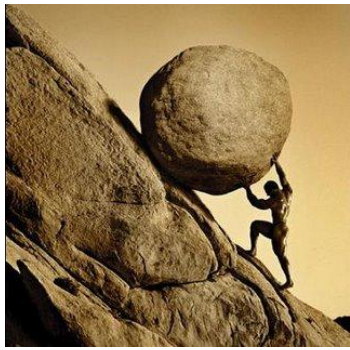
Cerca de 9200 incidentes desde janeiro de 2009!





Dificuldades encontradas

- Equipe!
  - Bolsistas (4 até 6 horas)
  - Sem dedicação exclusiva (PoP-RS x Cert-RS)
  - Alta rotatividade (concursos)



Eventuais ações junto a RNP

- Sujestão 1:
  - Isolamento de atividades maliciosas no backbone da RNP e contabilização dos dados. (blackhole solicitada ao CEO por comunidades e/ou rotas /32)

Eventuais ações junto a RNP

- Sujestão 2:
  - Disponibilizar os incidentes em formato IODEF - Incident object Description and Exchange Format (draft e rfc3067)

Obrigado

Perguntas?