Cert-RS – 5º EnCSIRTs

Marcos Straub

Leandro Bertholdo

CERT RS
Computer Emergency Team - Rio Grande do Sul

Rede Tchê

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

CERTRS
Computer Emergency Team - Rio Grande do Sul

Rede Tchê

Serviços

- Contenção de ataques no backbone acadêmico
- Notificação e tratamento de incidentes.
- Acompanhamento para que os eventos tenham o tratamento adequado!
- Auxílio aos clientes na implementação de serviços com requisitos de segurança
- Análise de vulnerabilidades sob demanda

Serviços

- Lista de segurança InfoSeg

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

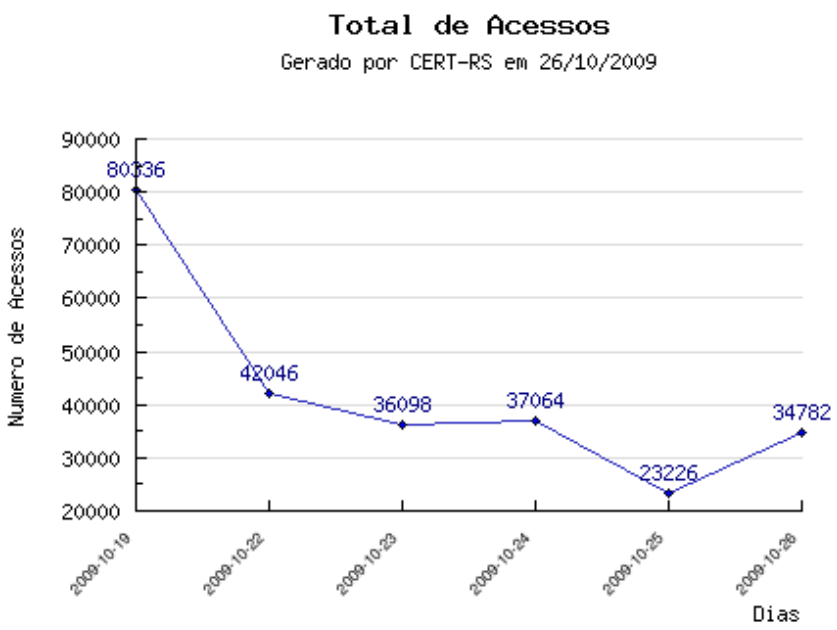
- Criada em 1998
- Lista voltada aos administradores de redes
- Firewalls, configurações, ataques
- Notificação de vulnerabilidades.

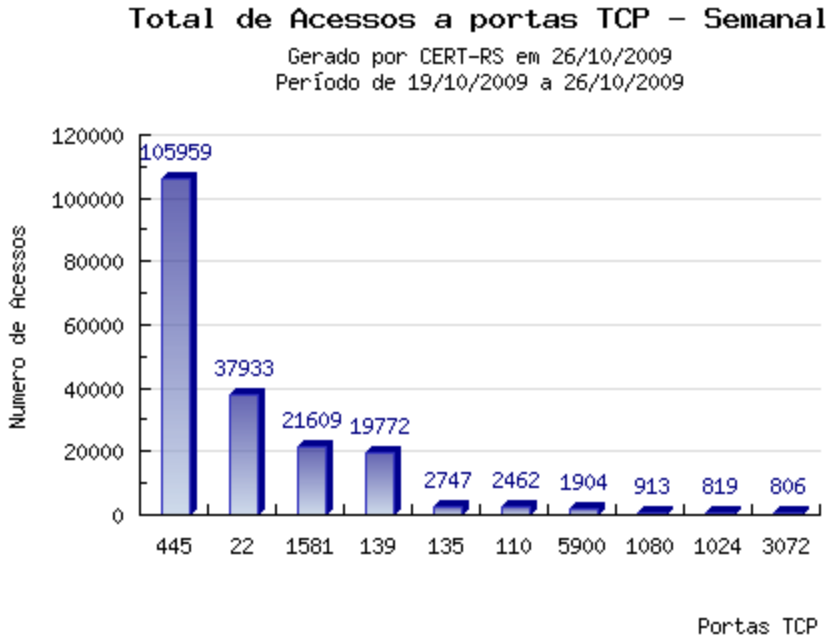
Serviços

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

Honeynet.BR

Serviços

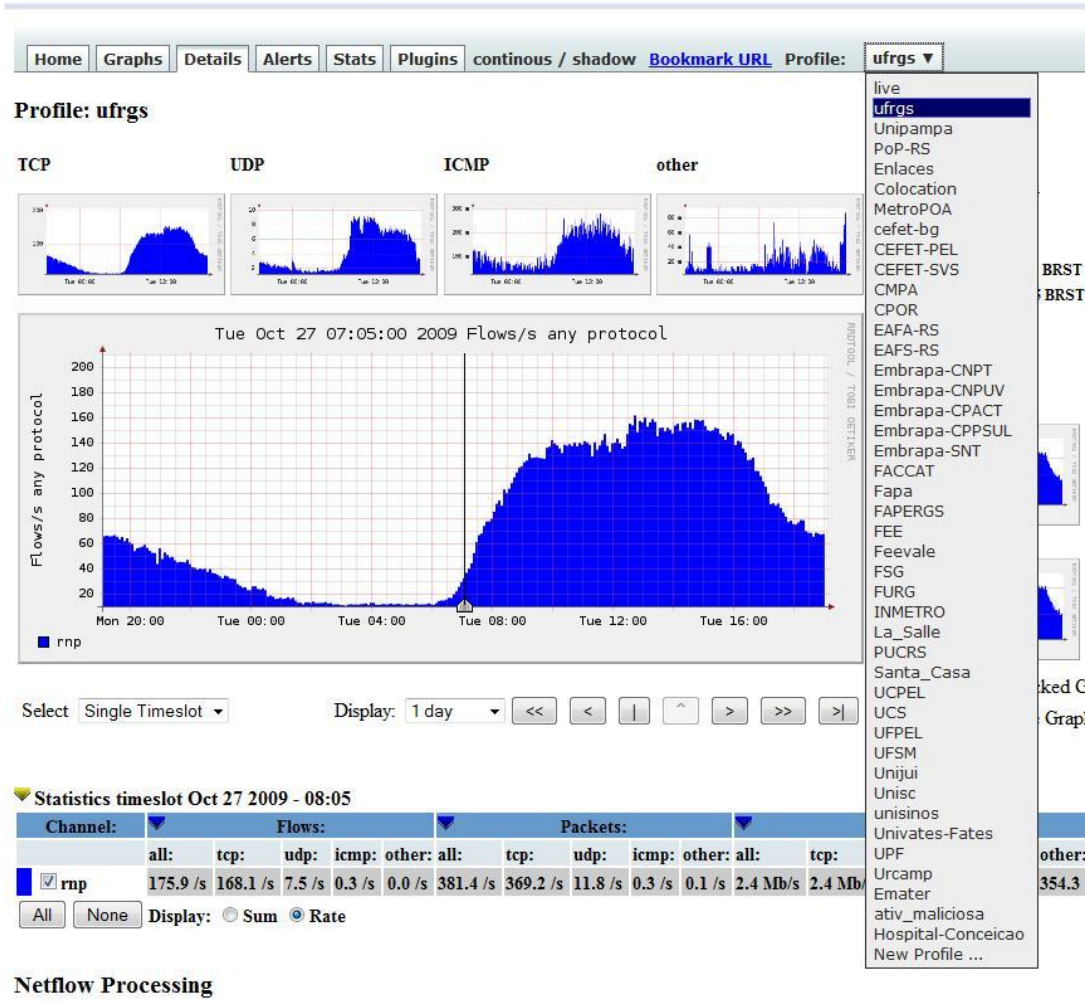




Honeynet.BR

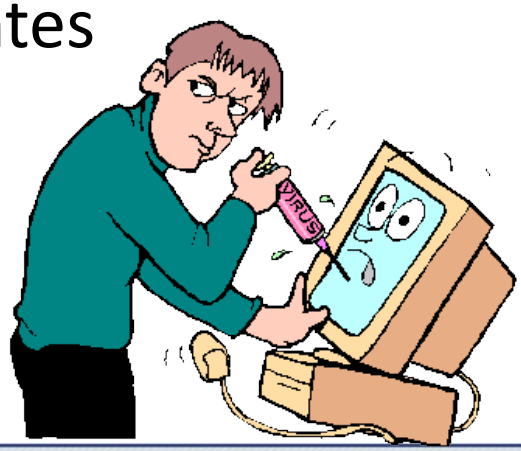
Serviços

- Consulta aos Flows
- Views por Instituição
- NFSEN



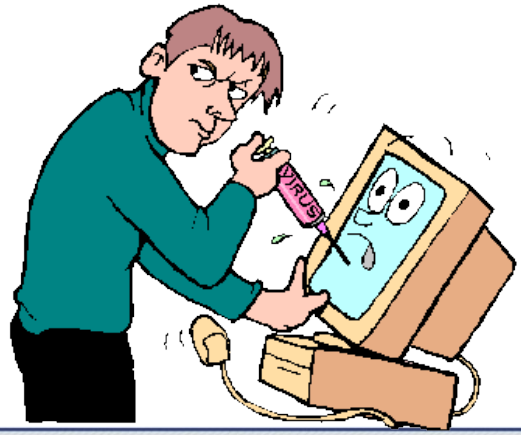
Ações contra atividades maliciosas de 2010

- Reunião e Workshop da Rede Tchê.
- Cursos em conjunto com a ESR-POA/RNP.
  - Introdução a segurança de redes
  - Análise Forense e Tratamento de Incidentes
- Plugin por protocolo/portas do NFSen
- Loghost com análise de logs OSSEC
  - Implementar ações pró-ativas



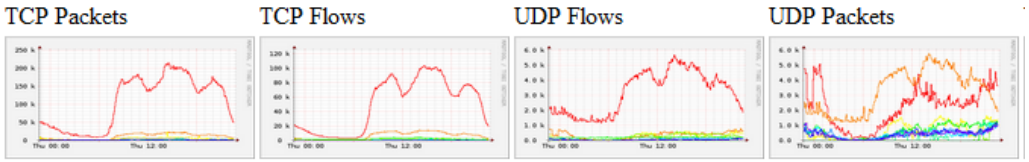
Ações contra atividades maliciosas de 2010

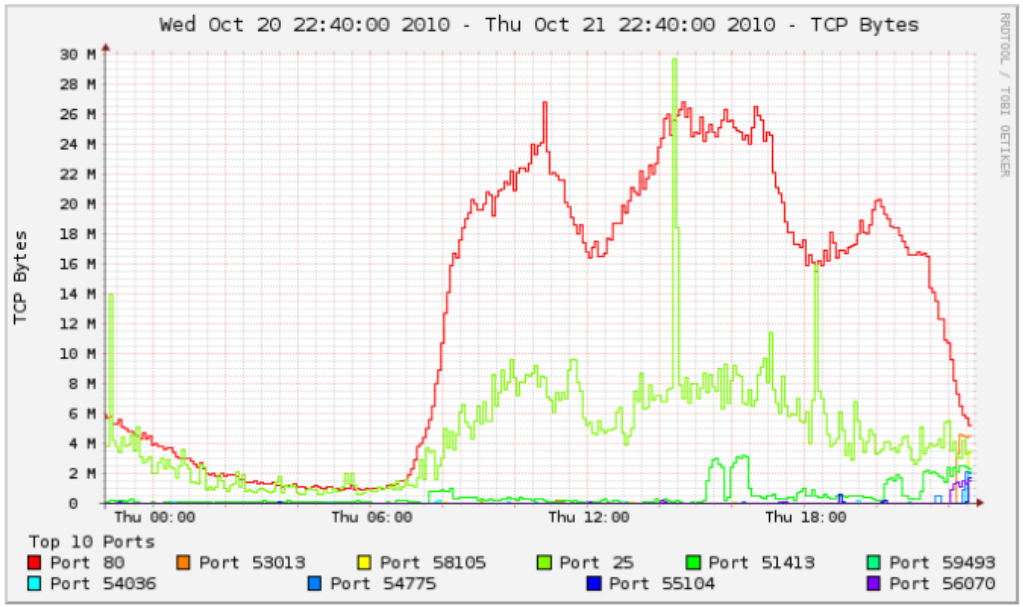
- Auxílio aos clientes para desestimular o uso do NAT.



Ações contra atividades maliciosas de 2010

Port Tracker





Problemas Enfrentados em 2010

- Equipe novamente!
  - Bolsistas (4 até 6 horas)
  - PoP-RS x Cert-RS x **MetroPOA**
  - Alta rotatividade (concursos)
  - Falta de profissionais qualificados

Eventuais ações junto a RNP

- 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

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

Eventuais ações junto a RNP

- Ações para maior colaboração entre CSIRTs
  - Wiki com procedimentos.
  - Intranet com acesso limitado.
  - Listas de e-mail para divulgação de trabalhos e troca de conhecimento (chaves PGP, politica de uso da lista).
  - Eventos por videoconferência.

CAIS

Obrigado

Perguntas ou sugestões?

marcos@tche.br

cert@pop-rs.rnp.br