

# Cert-RS – 5º EnCSIRTs

Marcos Straub

Leandro Bertholdo

# 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)



# 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.



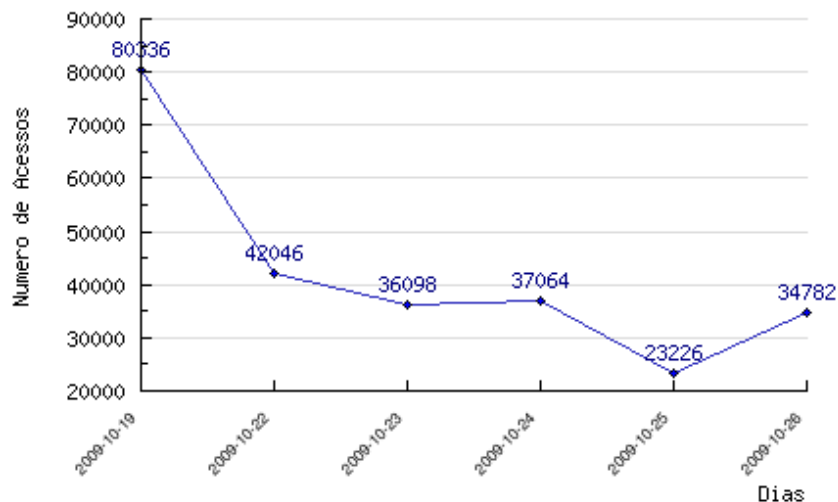
# Serviços

- 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**

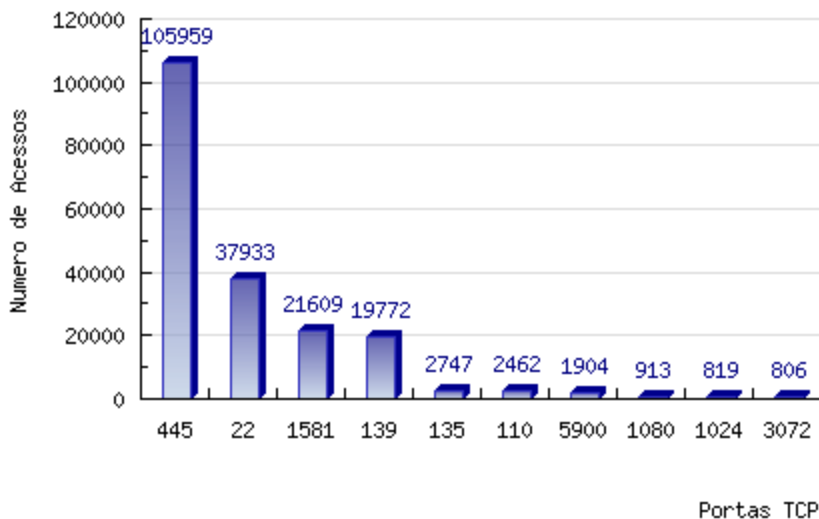
# Serviços

**Total de Acessos**  
Gerado por CERT-RS em 26/10/2009



**Total de Acessos a portas TCP - Semanal**

Gerado por CERT-RS em 26/10/2009  
Período de 19/10/2009 a 26/10/2009



**HoneyNet.BR**

# Serviços

- Consulta aos Flows
- Views por Instituição
- NFSEN

Home Graphs Details Alerts Stats Plugins continuous / shadow [Bookmark URL](#) Profile: **ufrgs**

Profile: ufrgs

TCP UDP ICMP other

Tue Oct 27 07:05:00 2009 Flows/s any protocol

Select  Display:  << < | ^ > >> >

▼ Statistics timeslot Oct 27 2009 - 08:05

Channel:	Flows:					Packets:						
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	tcp:	
<input checked="" type="checkbox"/> rnp	175.9 /s	168.1 /s	7.5 /s	0.3 /s	0.0 /s	381.4 /s	369.2 /s	11.8 /s	0.3 /s	0.1 /s	2.4 Mb/s	2.4 Mb

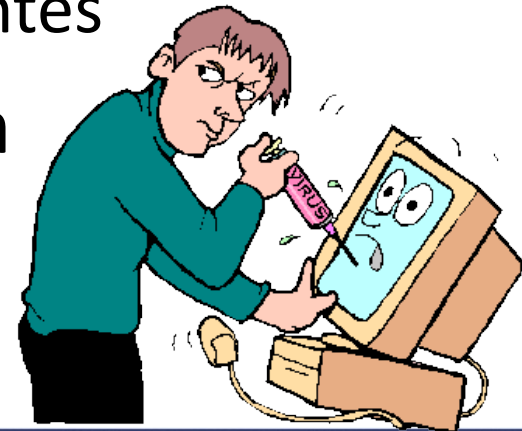
Display:  Sum  Rate

Netflow Processing

live  
**ufrgs**  
 Unipampa  
 PoP-RS  
 Enlaces  
 Colocation  
 MetroPOA  
 cefet-bg  
 CEFET-PEL  
 CEFET-SVS  
 CEFET-SUL  
 CMPA  
 CPOR  
 EAFA-RS  
 EAFA-RS  
 Embrapa-CNPT  
 Embrapa-CNPUV  
 Embrapa-CPACT  
 Embrapa-CPPSUL  
 Embrapa-SNT  
 FACCAT  
 Fapa  
 FAPERGS  
 FEE  
 Feevale  
 FSG  
 FURG  
 INMETRO  
 La\_Salle  
 PUCRS  
 Santa\_Casa  
 UCPEL  
 UCPEL  
 UCS  
 UFPEL  
 UFPEL  
 UFSM  
 Unijui  
 Unisc  
 unisinos  
 Univates-Fates  
 UPF  
 Urcamp  
 Emater  
 ativ\_maliciosa  
 Hospital-Conceicao  
 New Profile ...

# Ações contra atividades maliciosas de 2010

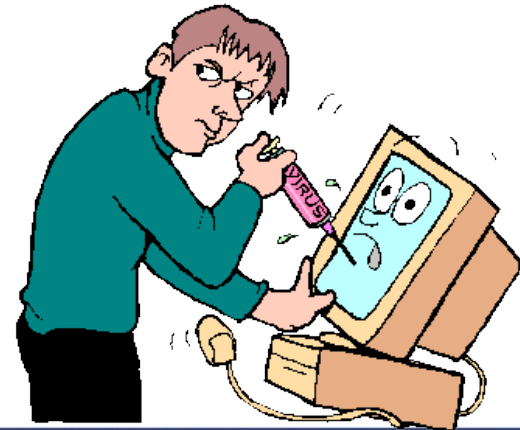
- Reunião e Workshop da Rede Tchê.
- Cursos em conjunto com a ESR-POA/RNP.
  - Introdução a segurança de redes
  - Análise Forense e Tratamento de Incidentes
- Plugin por protocolo/portas do NFSen
- Loghost com análise de logs OSSEC
  - Implementar ações pró-ativas





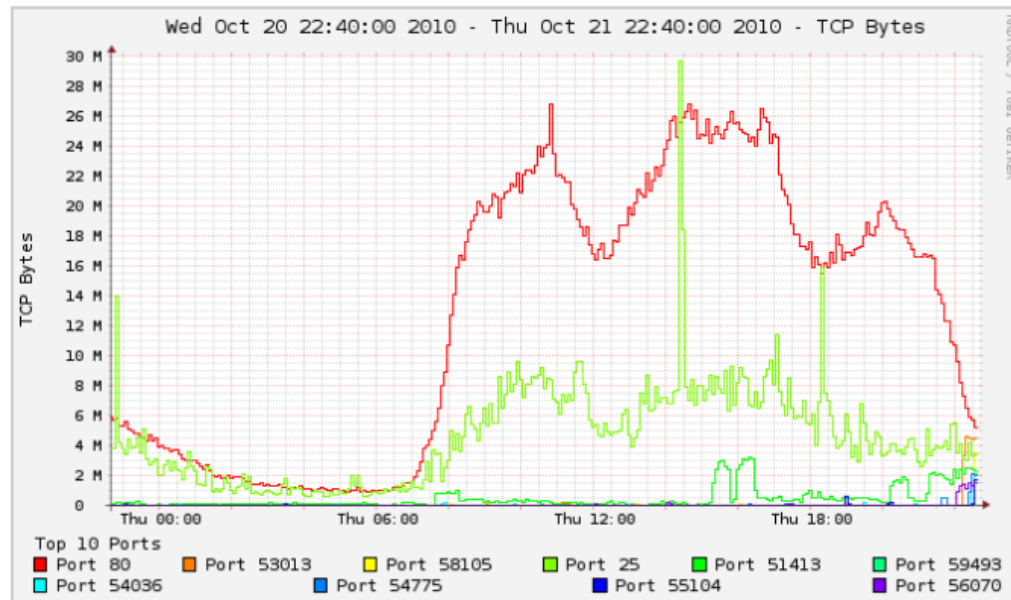
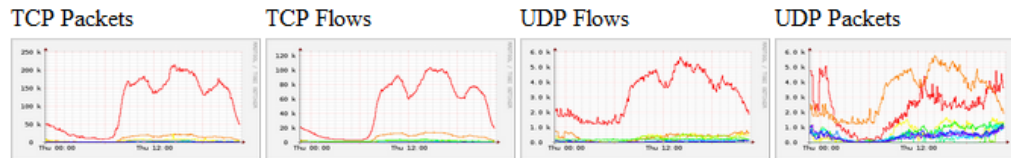
# Ações contra atividades maliciosas de 2010

- 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.



# Obrigado

**Perguntas ou sugestões?**

[marcos@tche.br](mailto:marcos@tche.br)

[cert@pop-rs.rnp.br](mailto:cert@pop-rs.rnp.br)