O Cert-RS e a segurança na rede acadêmica

Marcos Straub

Leandro Bertholdo

CERT RS
Computer Emergency Team - Rio Grande do Sul

Rede Tchê

Sumário

- Introdução
- Missão
- Serviços
- Incidentes reportados ao Cert-RS
- Ações contra atividades maliciosas
- Desafios

Introdução

- Criado oficialmente em 1997
- 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

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.

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	novo 2 semanas atrás	CERT-RS	Nobody 3 min atrás	0 0
175997	2 host(s) identificado(s) como origem de Spam -	novo 2 dias atrás	CERT-RS	Nobody 2 min atrás	0 0
176251	1 host(s) identificado(s) como origem de Spam -	novo 40 horas atrás	CERT-RS	Nobody 2 min atrás	0 0
176255	2 host(s) identificado(s) como origem de Spam -	novo 40 horas atrás	CERT-RS	Nobody 2 min atrás	0 0
176495	1 host(s) identificado(s) como origem de Spam -	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

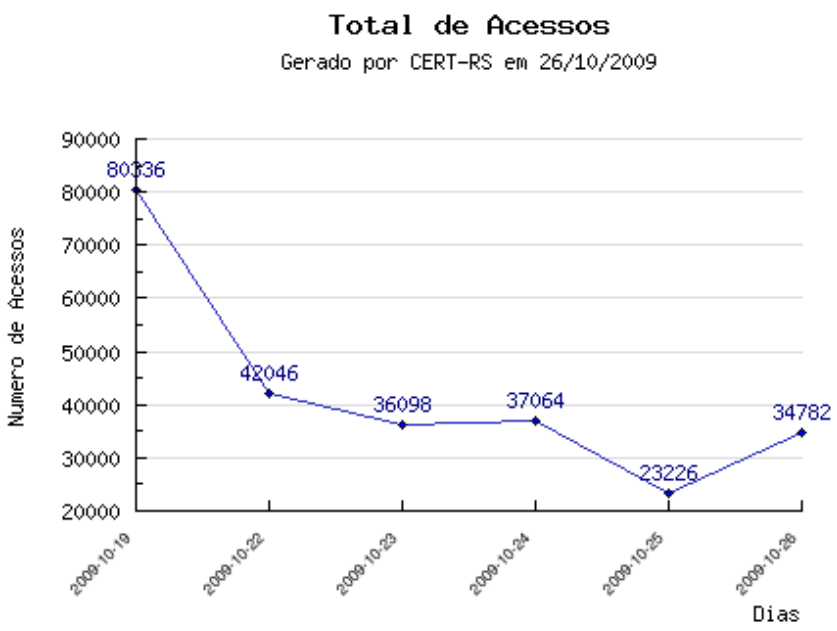
- Criada em 1998
- Lista voltada aos administradores de redes
- Firewalls, configurações, ataques
- Notificação de vulnerabilidades.

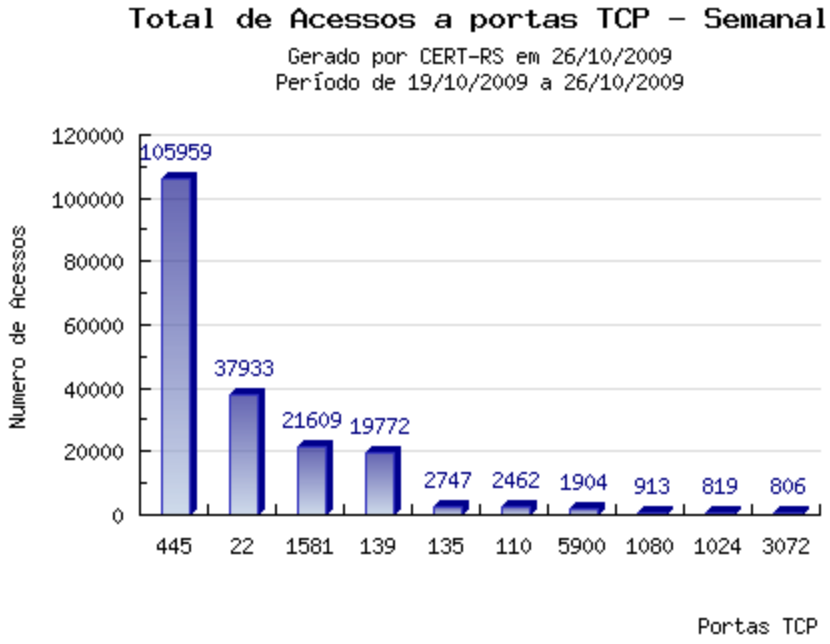
Serviços

- Honeypots
  - Sistema desenvolvido para ser atacado, comprometido
  - Consórcio Brasileiro de Honeypots
  - Parceria com o CERT.br
  - Análise de Tendências e Early Warning
  - 4 Honeypots no estado (Cert-RS,TRI, Unisinos, UPF)

Honeynet.BR

Serviços



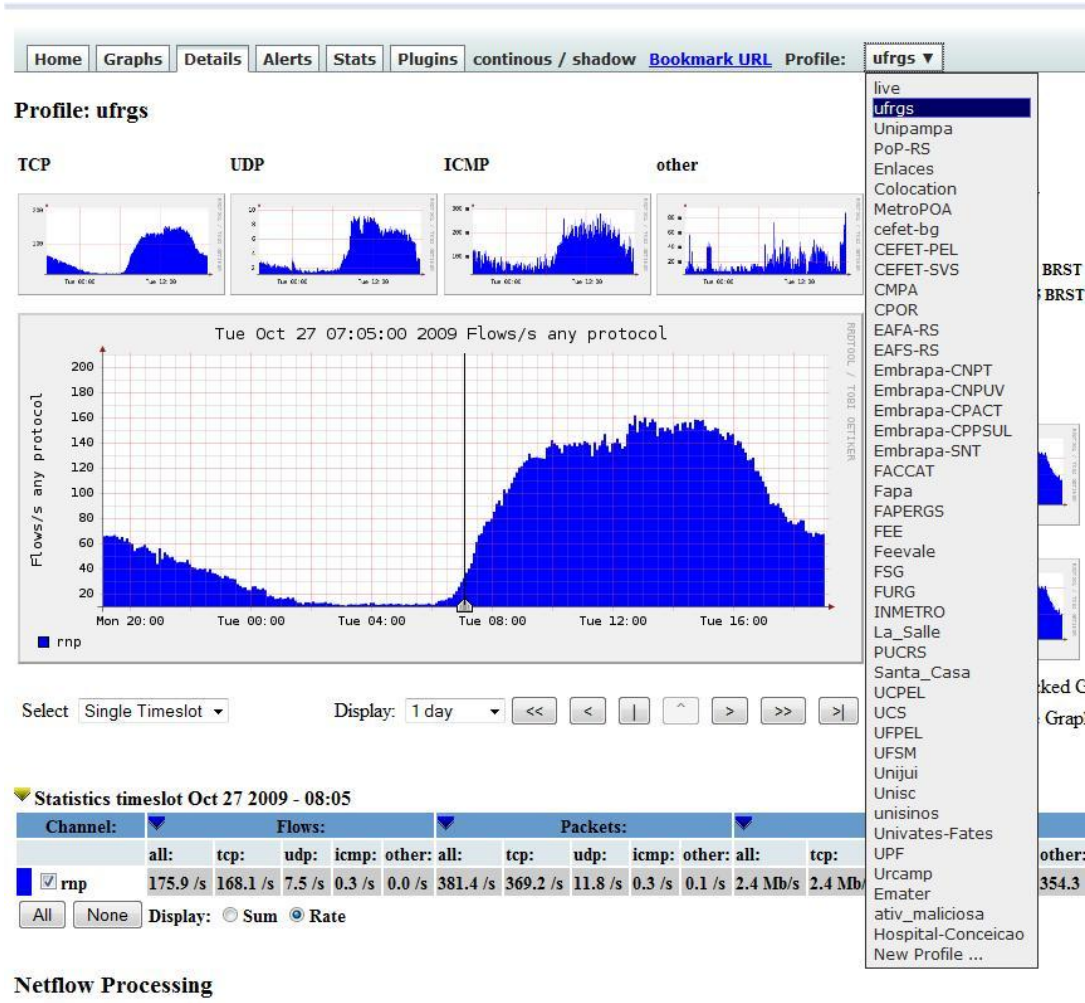


http://cert-rs.tche.br/index.php/estatisticas

Honeynet.BR

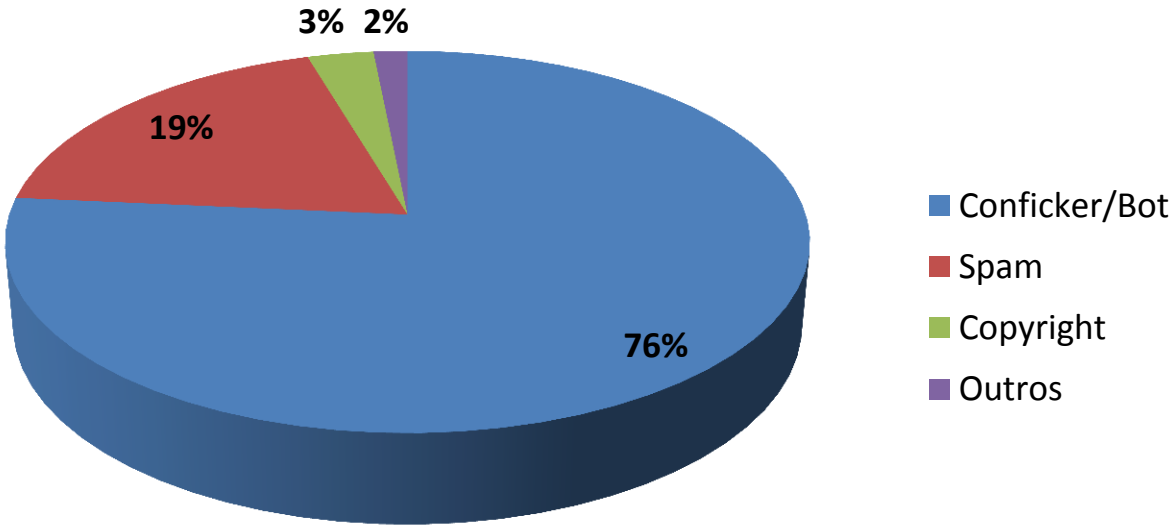
Serviços

- Consulta aos Flows
- Views por Instituição
- NFSEN



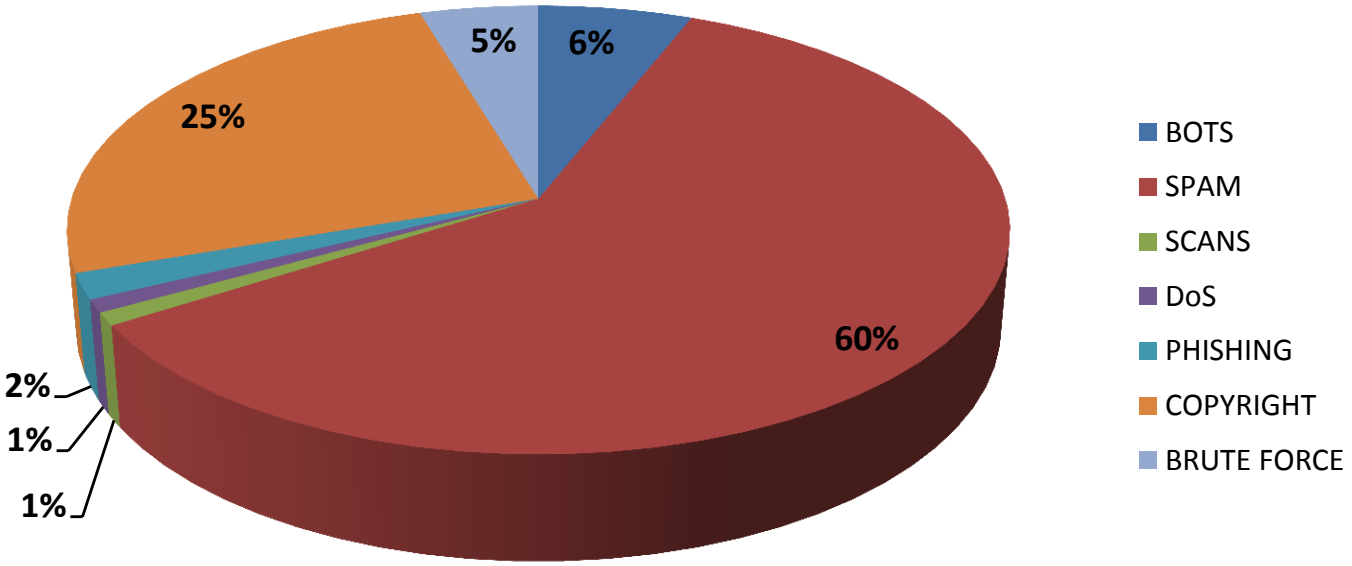
Incidentes Reportados

Incidentes de 2009



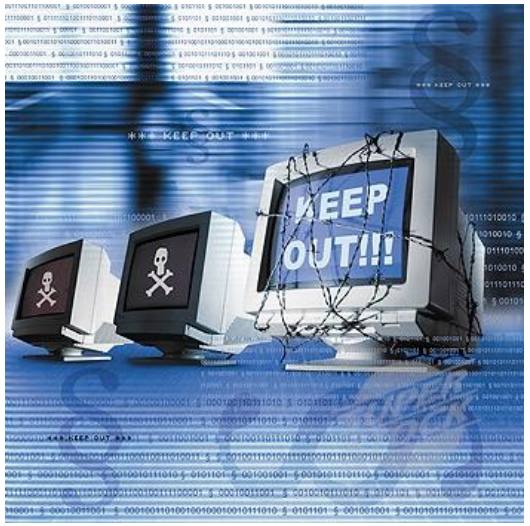
Incidentes Reportados

Incidentes de 2010



Incidentes mais reportados

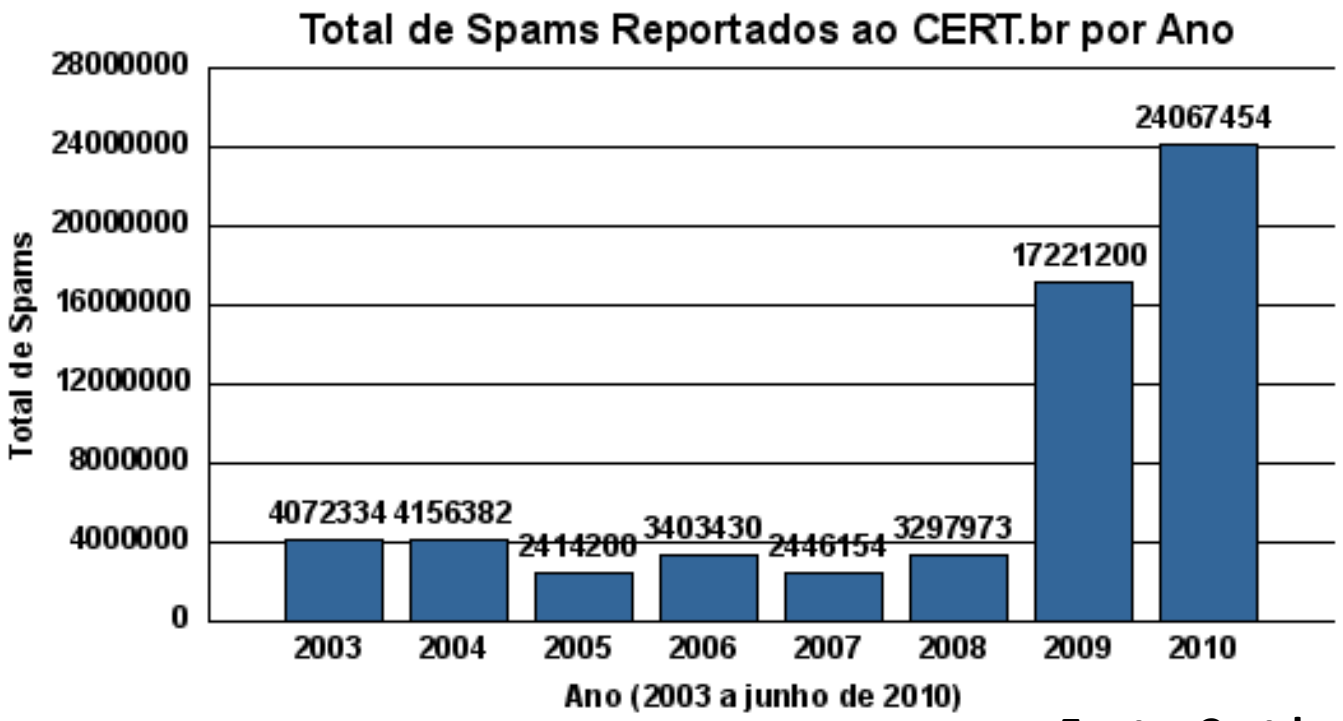
- SPAM
- Copyright/Pirataria
- Scans/Varreduras
- Bots
- Phishing/Defacement
- DOS



Incidentes – Conficker em 2009

- Grande aumento no número de incidentes em 2009 devido ao Conficker.
- Dos 9733 incidentes, 7511 eram sobre o Conficker.

Incidentes - SPAMs



Fonte: Cert.br

Incidentes - SPAMs

- Mensagens de e-mail não solicitadas
- 92,2% de SPAMs, ou 1 em cada 1,08 mensagen
- Quase sempre oriundos de botnets
  - Relatórios Symantec: botnets 95% de todo o SPAM
    - 41% deles são gerados pela botnet Rustock

Fonte: http://www.messagelabs.com

Incidentes - SPAMs

- Brasil: 2º lugar na lista cbl.abuseat.org
- Pirataria + banda larga + recursos hardware

country	Count	%total
Total	9419842	100
IN	1413253	15.00
BR	1230731	13.07

Incidentes – Copyright/Pirataria

- Bittorrent
  - Download de filmes e jogos
- MetroPOA a giga
  - Aumento no número de incidentes?
  - Redução de banda nas redes de acesso

Incidentes – Phishing

- Fraudes com objetivo de obter informações sigilosas
- Mensagens Phishing cada vez mais trabalhadas
  - Usuário leigo é uma vítima certa
    - Recadastro bancário
    - Amor esquecido
    - Celebridades (Michael Jackson)

Incidentes – Phishing

comunicação digital itaú

Protocolo: 48589759

Informamos que seu dipositivo iToken encontra-se desatualizado perante o servidor de acesso Bankline.

A atualização é obrigatória e deve ser realizada em até 2 dias úteis a partir de hoje.

O Itaú disponibiliza a versão 2.05 no caminho abaixo:

Iniciar atualização

Central de Segurança e Monitoramento - Itaú S/A
Verificador Anti-Spam.

O Banco Itaú garante o sigilo dos seus dados. Acesse o site do Banco Itaú e conheça a nossa política de privacidade. Por favor, não retorne este e-mail. Para nos contatar utilize o Fale Conosco do site do Banco Itaú.

Incidentes – Phishing

Incidentes – Defacement

- Desfiguração de sites
  - Exploram vulnerabilidades do servidor ou da aplicação
    - Ex: PHP e Joomla

Incidentes – Defacement

Ações contra atividades maliciosas

- Participações no DISI da RNP
- Cursos em conjunto com a ESR-POA/RNP

Desafios

- Instituições conectadas a giga no Metropoa
- Auxiliar os clientes da RedeTchê na adoção de boas práticas de e-mail (www.antispam.br)
- Desestimular o uso do NAT na rede Tchê
  - Falsa sensação de segurança
  - Dificuldade em rastrear o incidente
  - Pendrives, mensagens de e-mail, etc.

Obrigado

Sugestões?

www.cert-rs.tche.br

Marcos Straub

marcos@tche.br