



Serviço de Respostas a Incidentes de Segurança da RedeRio

Marita Maestrelli
mm@rederio.br

I Encontro de CSIRTs Acadêmicos
Rio de Janeiro/RJ – 25 e 26 maio de 2006

Roteiro

- **Apresentação da RedeRio**
- **Serviço de Respostas a Incidentes de Segurança**
- **Projetos**
- **Contato**



Backbone Acadêmico



RedeRio
de Computadores - FAPERJ

14 anos em 22/5/2006



Apresentação RedeRio

A Rede Rio é uma rede de computadores, integrada por universidades, centros de pesquisa e entidades governamentais (municipais, estaduais e federais) localizados no Estado do Rio de Janeiro.

É um dos principais instrumentos de desenvolvimento científico e tecnológico, além de oferecer serviços do governo ao cidadão do Estado do Rio de Janeiro.



A FAPERJ é o órgão responsável pela sua coordenação e pelo seu financiamento.

Fibra no RJ



Região Metropolitana do Rio de Janeiro



Serviço de Respostas à Incidentes de Segurança CEO – Coordenação de Engenharia Operacional

Início: Dezembro de 1999

Constituency:

- Universidades, Institutos de Pesquisa e Órgãos do Governo no Estado do Rio de Janeiro conectados ao AS2715, além dos AS21612 e AS14553;

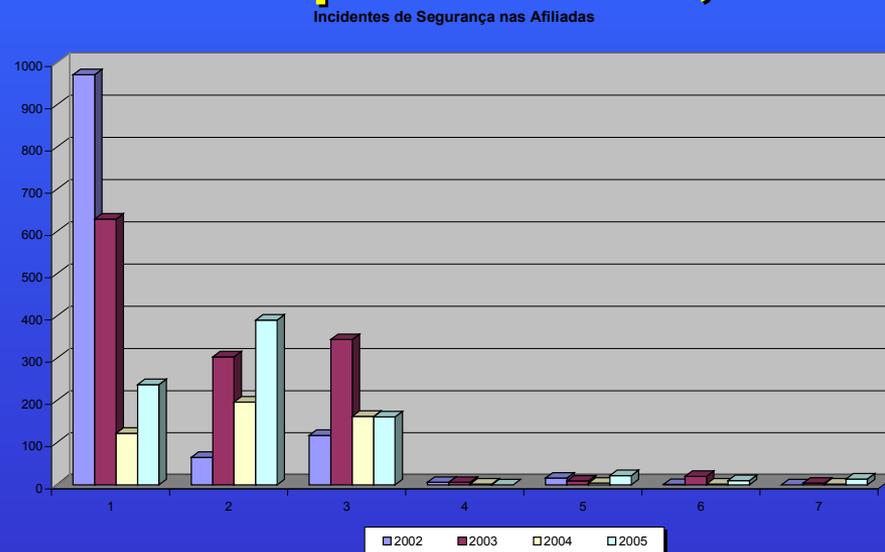
Equipe:

- Um responsável e uma bolsista;**
- Toda a equipe CEO;**

Atuação

Serviço de Respostas à Incidentes de Segurança CEO/RedeRio:

- Monitoramento e Alertas;
- Repasse para responsáveis e acompanhamento;
- Ajuda, se for necessário;
- Estatísticas;



Projetos

- **GRRW – cadastramento das afiliadas**
- **GRRW2 – Alertas de falhas**
- **Fluxo do Tráfego – Monitoramento visual**
- **Consórcio Brasileiro de Honeypots**



GRRW - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://grrw.redeRio.br/grrwphp/dados_inst.php?status=1&sigla=27

RedeRio Tráfego Roteador de borda - 200... | GRRW

Gerência da Rede Rio via WEB

Rio de Janeiro, -

Principal Voltar Preferências Buscas Logout

Lista de Instituições

- 0_BB-BGPO
- 1_RNP-CIGA
- 5_EDT
- 6_INT
- ABC
- BACK_RR_CIGA_CBPF
- BACK_RR_CIGA_CIN
- BACK_RR_CIGA_FIOCRUZ
- BACK_RR_CIGA_PUC
- BACK_RR_CIGA_UFRJ
- BB-CBPF
- BB-PUC
- BB-RNP
- BB-UFRJ
- BIORIO
- BNDES
- BPM
- CARDICA**
- CBPF
- CBPF/EN
- CBPF/PUC
- CECE/RJ
- CEDERJ
- CEFEY-RIO
- CEFEY/Química
- CENPES
- CEP
- CEPEL
- CETEM
- CETEP Petropolis
- CETEP Quintino
- CEUEL
- CH
- CNRJ
- CNEN
- CPIL
- CPRM

Interface: (up) Editar os dados Nova Ocorrência Adicionar ao GRRWAlert Acesso as Inativas

DADOS DE CONTATO

Instituição: Unicarica
 Contato: Gustavo
 Email: adolfo@unicarica.br; cclairanda@unicarica.br
 Telefone: 2563-1943 / 2502-1001 R:139
 Web: www.carica.br
 Endereço: Av. Paulo de Frontim, nº 568 - Rio Comprido - CNPJ - 31886146/0001-00

DADOS TÉCNICOS

Link/LP: 2Mbps/AssCom Link/LP antigo: 1/391469 - 1936010 - 1729212/1729219
 Roteador: ROUTER_PUC Equip.: ROUTER_PUC
 IP roteador: 200.20.94.81 IP equip.: 200.20.94.81
 Interface: 21 Tipo: Serial5/1
 IP rede: 200.20.91.72 IP interno: 200.20.156.1

HISTÓRICO DAS OCORRÊNCIAS

- + 274 - Concluída
- + 12/02/2004 - 15:16:00 - Jaime
Aumento de velocidade de 1Mbps para 2Mbps.
Troca da TELEMAR para AesCom.
- + 248 - Concluída
- + 10/11/2003 - 10:49:00 - naj
testando aviso

TRÁFEGO NA INTERFAÇA

Serial5/1 [23-05-2006 15:12:50]

Atual In: 507.6 kbits
 Atual out: 836.7 kb-its
 Max in: 1088.0 kb-its
 Max out: 2017.9 kb-its

PING PARA OS IPS

Pacotes: 2 Tamanho: 0 Ping

IP 200.20.91.73		Min	Max	Med	
Env.	Rec.	Perdas			
2	2	0 (0%)	0ms	1ms	0ms

IP 200.20.91.74		Min	Max	Med	
Env.	Rec.	Perdas			
2	2	0 (0%)	3ms	9ms	6ms

Done AS2715

- Importante localizar os responsáveis pelas redes envolvidas.
- Cadastro atualizado constantemente.
- Gerencia Integrada.
- Autenticação de usuários.
- Documentação da Rede.
- Acesso restrito.

GRRW2

GRRW - Status Sensitivo - Microsoft Internet Explorer

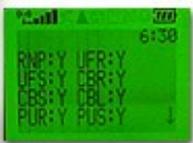
GRRW Status Sensitivo

CBPF2			
Status	Interface	Link	Inst
●	S6/5	128k	UNIF
●	S6/4	256K	SEFO
●	S6/3	2M	UVA
●	S6/2	1Mbps	FGV
●	S5/7	128K	IBPT
●	S5/6	1M	FBN
●	S5/5	256K	FAP
●	S5/4	2M	ON
●	S5/2	2Mbps	CEFF
●	S5/1	2M	IPLA
●	S5/0	2M	DAT
●	S3/7	512K	FLIN
●	S3/6	512K	IBAG
●	S3/5	2M	CEP
●	S3/4	1M	INT
●	S3/2	2Mbps	IME
●	S3/1	128K	IUP
●	S3/0	256K	ABC
●	S1/7	2Mbps	FCL
●	S1/6	64K	CPR
●	S1/5	1Mbps	CNE
●	S1/4	128kbps	ILT
●	S1/3	256K	DRM
●	S1/2	256kbps	AB
●	S1/1	2M	LNC
???	-	64K	FIN
			back

Sistema de Gerência Pró-Ativo



**Chamada
Alerta Vermelho**



Status SMS



Tecnologia WAP



Coordenação de Engenharia Operacional da Rede Rio

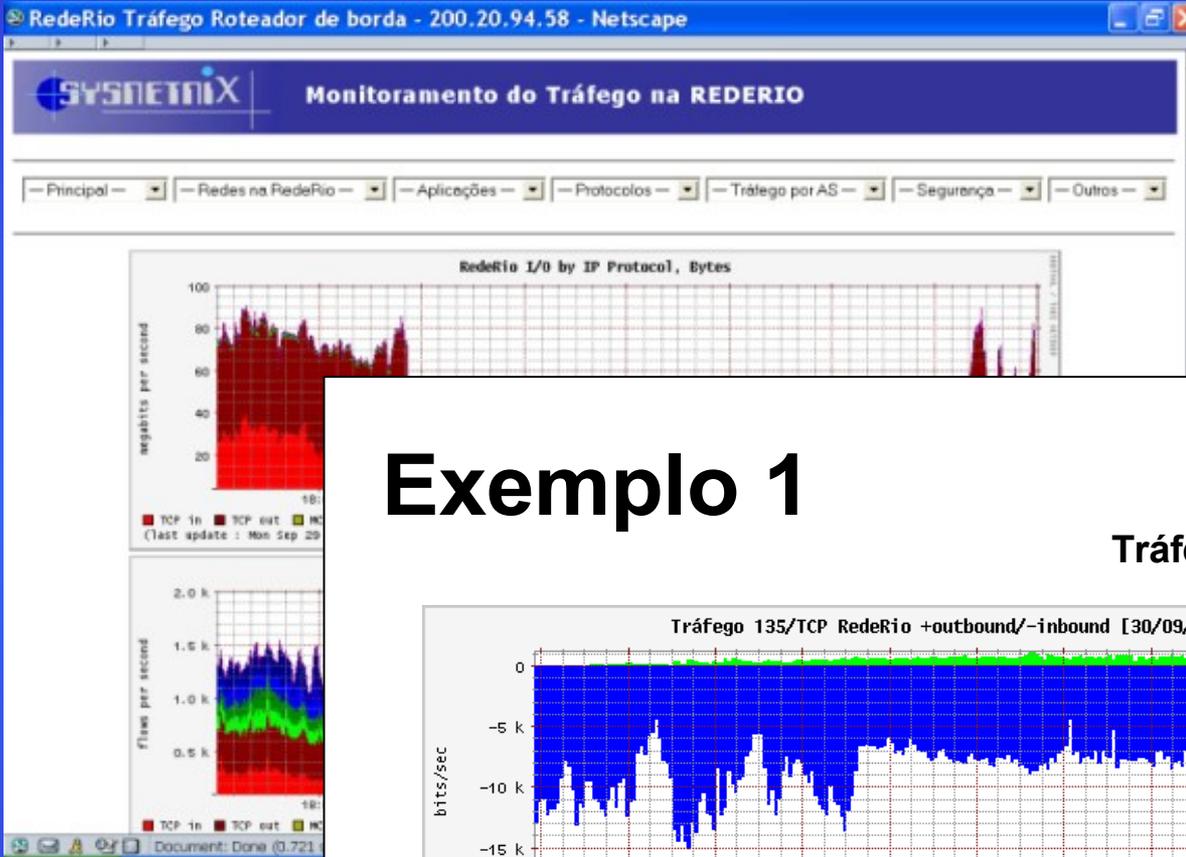
Painel Eletrônico



- Alertas de falhas: pode ser queda ou congestionamento no link;
- Sistema redundante;
- Gera relatórios WAP;
- Acesso restrito;

Fluxo do Tráfego

Facilidade em detectar incidentes visualmente

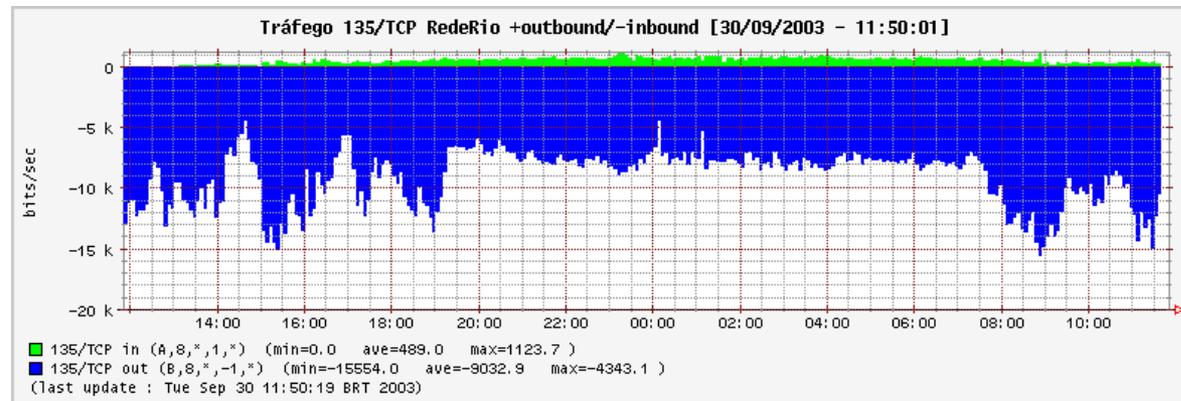


Sistema de Análise de Fluxo:

- 3) Por serviço
- 4) Por Rede (AS 2715)
Top 10
- 3) Por AS

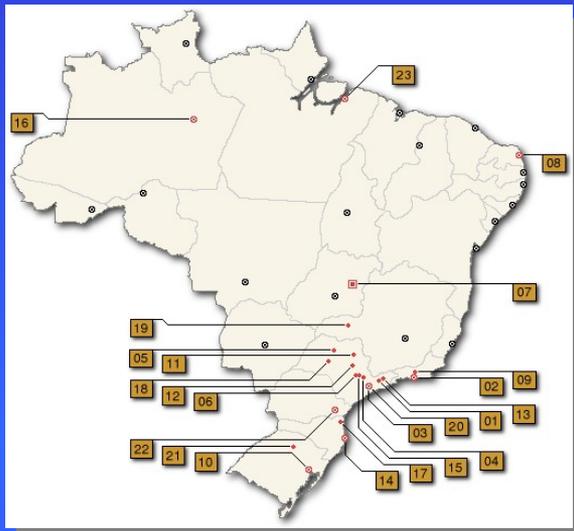
Exemplo 1

Tráfego: RPC MS-Windows



)
nas:

Honeypots



- **Coordenação: CERT.br e CenPRA**
- **Diversas máquinas no espaço Internet brasileiro**
- **<http://www.honeypots-alliance.org.br/index-po.html>**
- **Honeypots de Baixa Interatividade**
Os sistemas e serviços de rede são emulados e o sistema REAL é inacessível.
- **Arquitetura Sparc/Sun**
- **Emulam 4 redes diferentes**

Contato

Serviço de Respostas à Incidentes de Segurança CEO/RedeRio:

- Responsável: Marita Maestrelli
- E_mail: security@rederio.br
- Chave PGP:
<http://www.rederio.br/ceo/PGP/RedeRio.asc>
- Telefone: 21-2141-7124
- INOC-DBA: 2715*800

