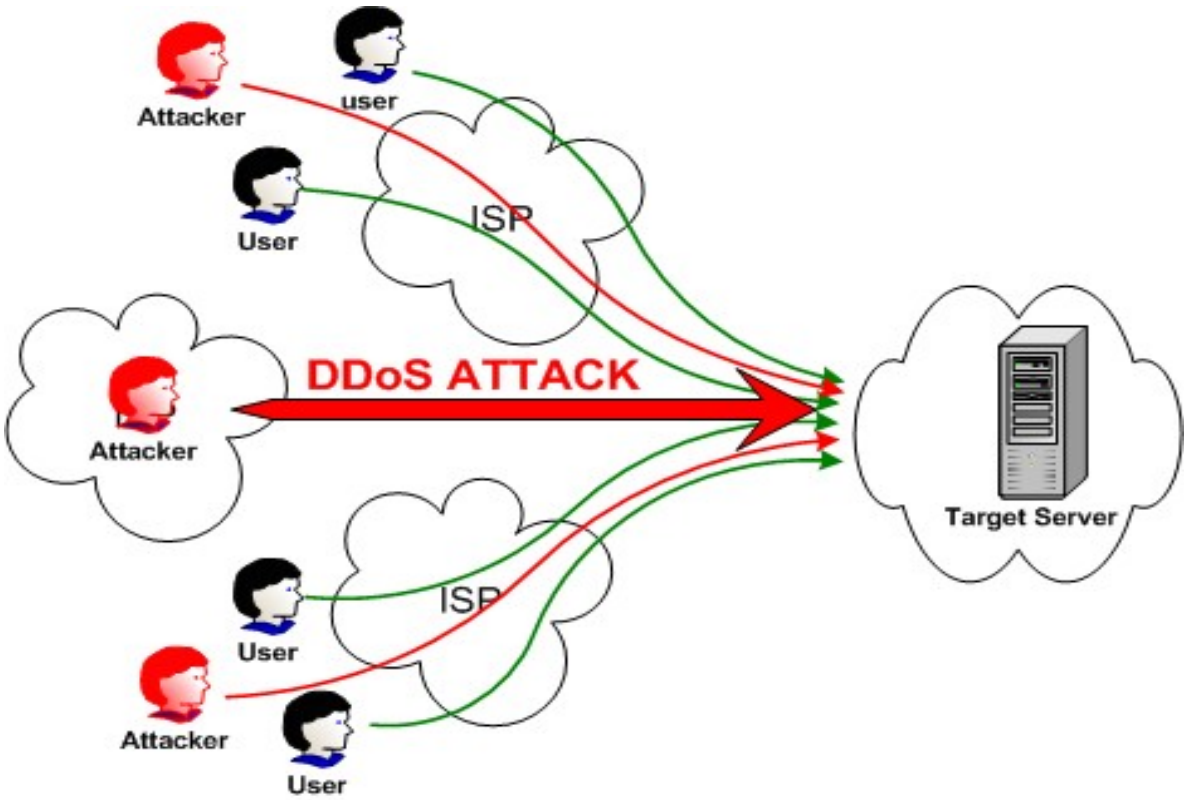
Combate à DDOS na rede acadêmica

Rildo Antonio de Souza
CAIS/RNP

RNP
MINISTÉRIO DA DEFESA
MINISTÉRIO DA CULTURA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
BRASIL GOVERNO FEDERAL

Definições - DDOS

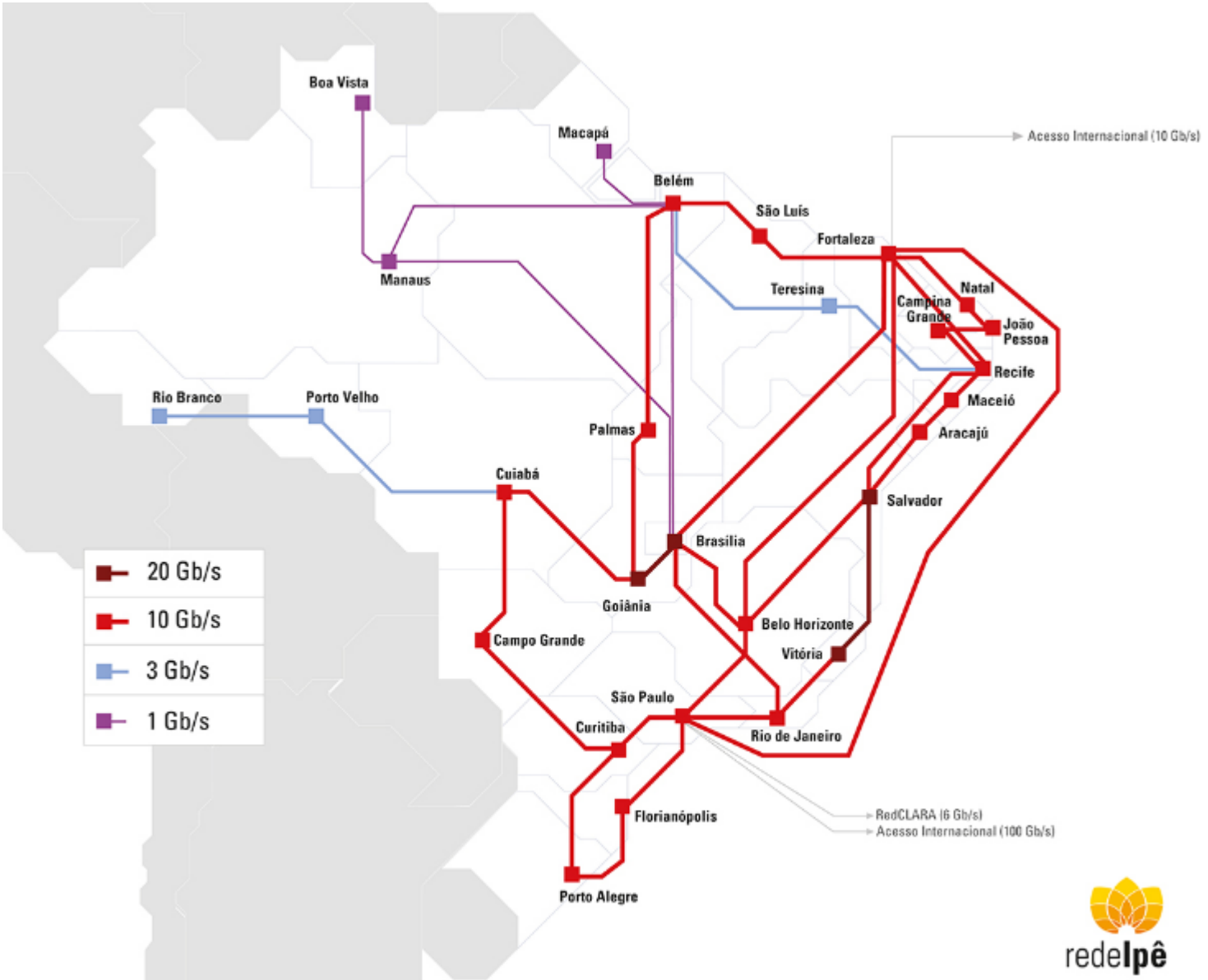
- DDOS – Ataque de negação de serviço distribuído



Definições – Rede Ipê

- 27 Pontos de Presença (PoP)
- Aproximadamente 1200 instituições
- Aproximadamente 3,5 milhões de usuários
- Quantidade inestimável de hosts

Definições – Rede Ipê



Definições – Ataques de Amplificação

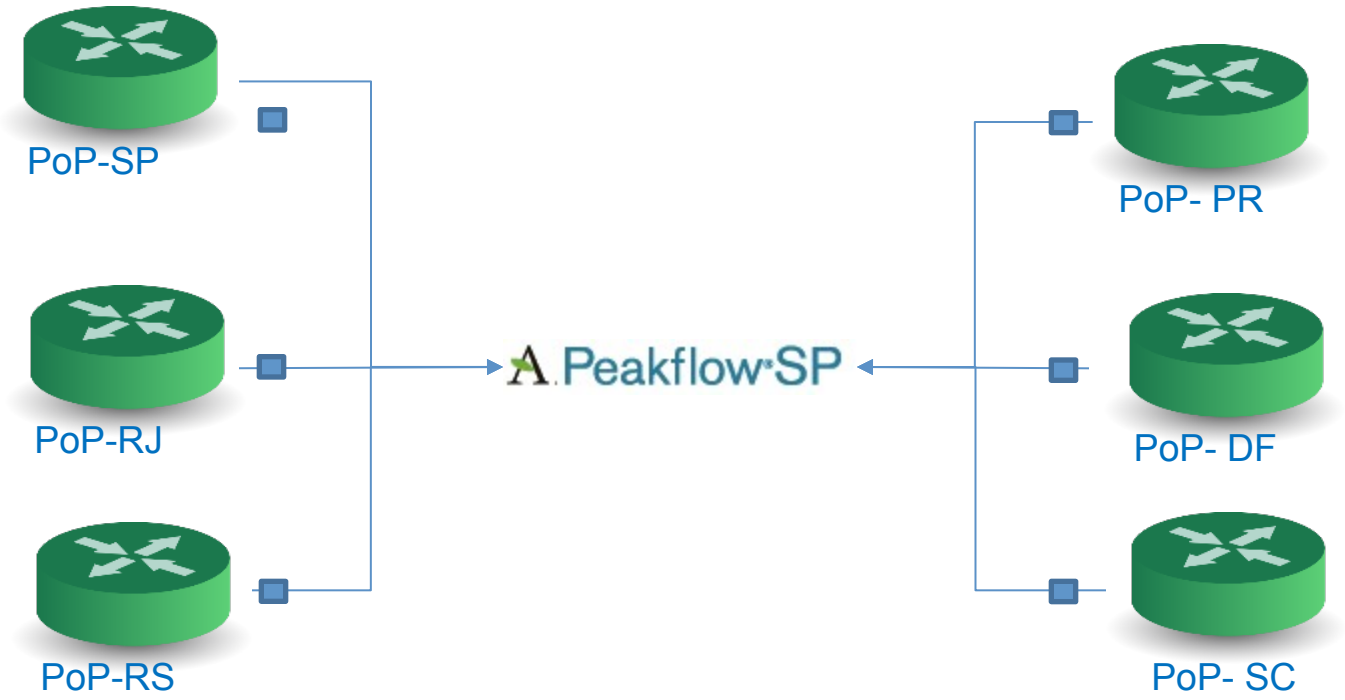
Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request

Fonte: US-CERT

Peakflow SP – O que é?

- Solução para detecção e tratamento de ataques de DDOS

Peakflow SP – Como funciona



Taxa média amostragem: 1/1000

Peakflow SP – Como funciona

- Comportamento
- Assinaturas

Gera alerta

Cenário Anterior do Peakflow SP na RNP

- Quantidade de alarmes alta
- Logs com mais de 4.000 linhas
- Necessidade de atuação rápida
- Dificuldade de separar eventos RNP vs eventos gerais (redes de trânsito)

Cenário Anterior do Peakflow SP na RNP

- Subutilizado
- Limitações da ferramenta
- Não gera / envia LOGs com evidências do ataque

Cenário Anterior do Peakflow SP na RNP

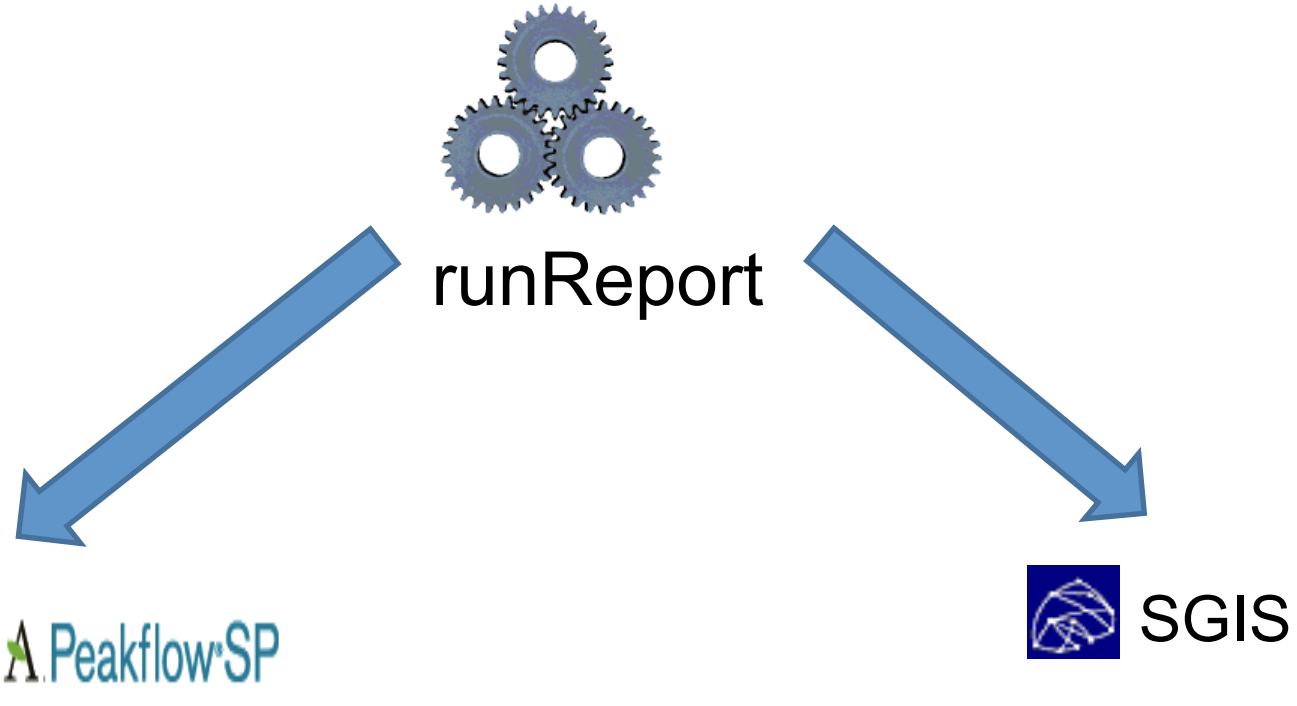
Briga de gato e rato

A solução

- Integração + Automação

A solução

- Integração + Automação



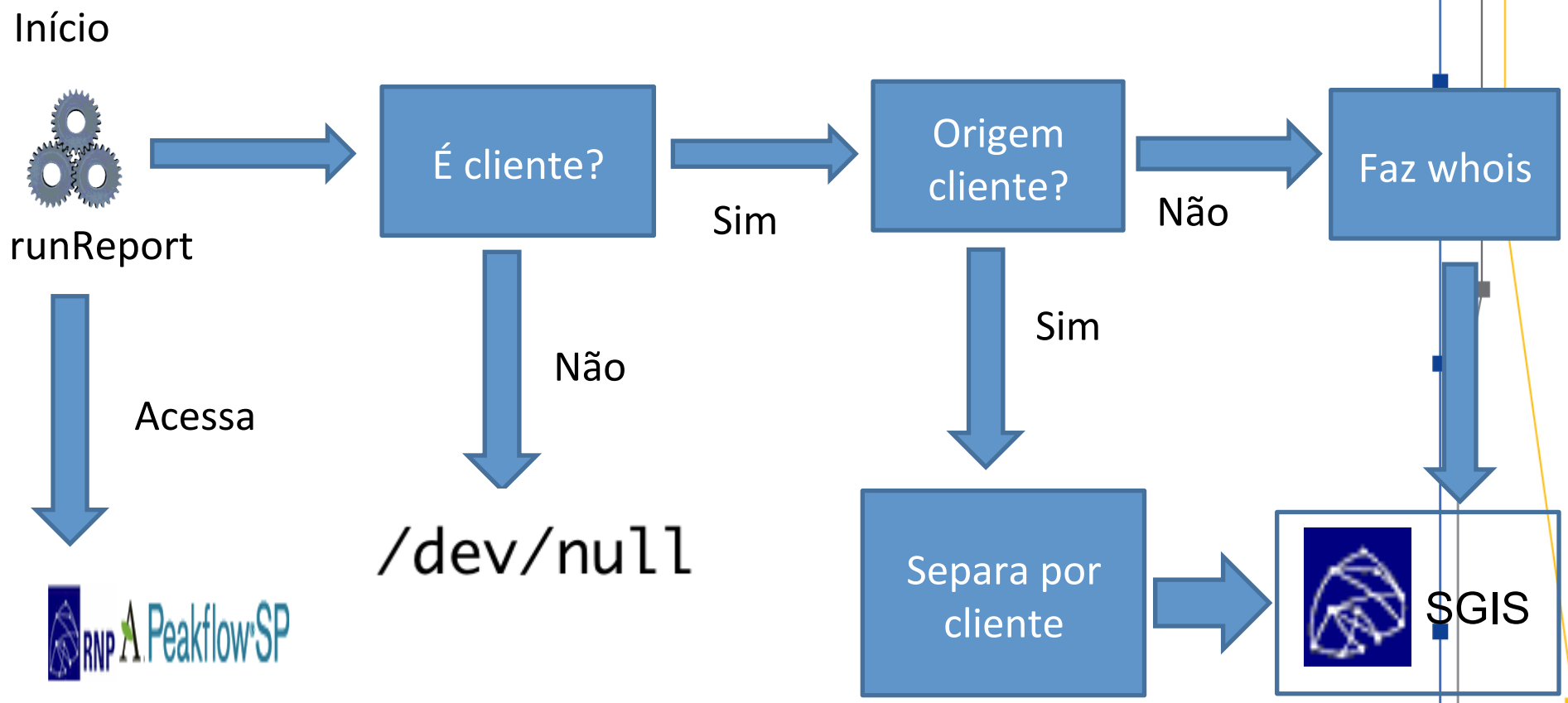
A solução

- Tecnologias utilizadas

Funcionamento da solução

- Controlar alarmes que devem ser monitorados
- Gerar flows para alarmes monitorados
- Uso da API do Peakflow
- Fácil atualização e manutenção

Como funciona a solução



Como funciona a solução

RNP origem

SC

Instituição é NOTIFICADA

do é ALERTADO

RNP des

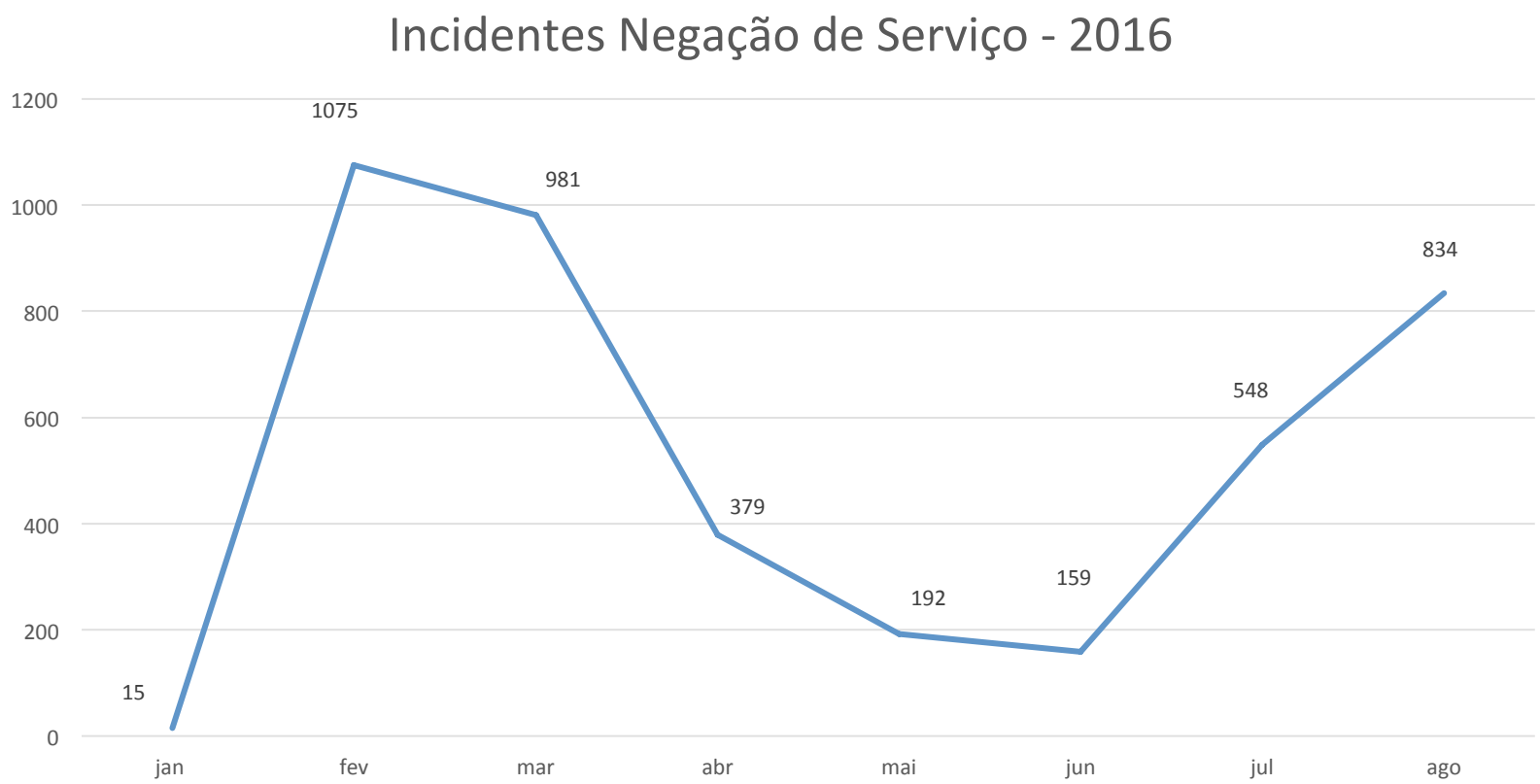
SC

tuição é ALERTADA

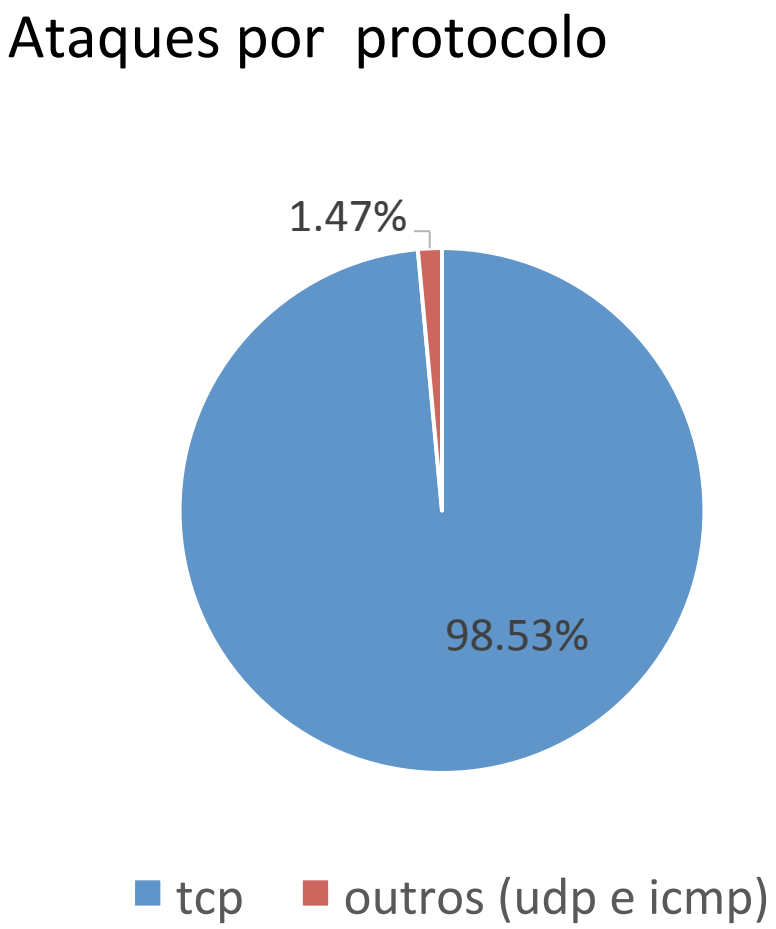
ante é NOTIFICADO

Dados Relevantes

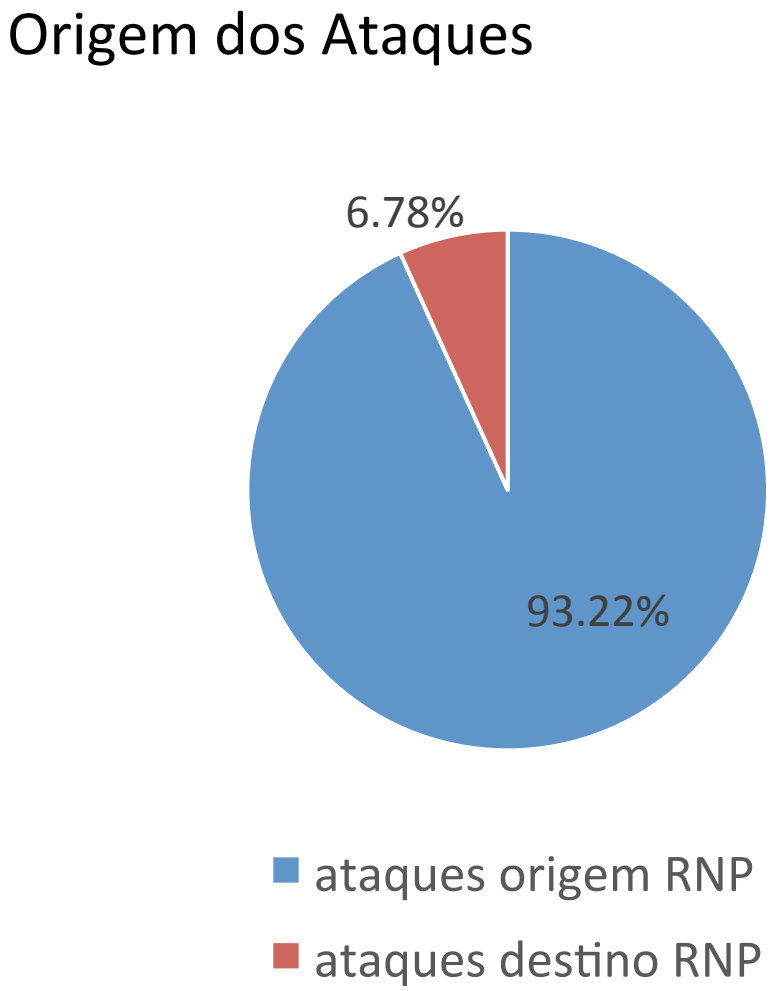
- Aumento no número de notificações de DDOS



Dados Relevantes



Dados Relevantes



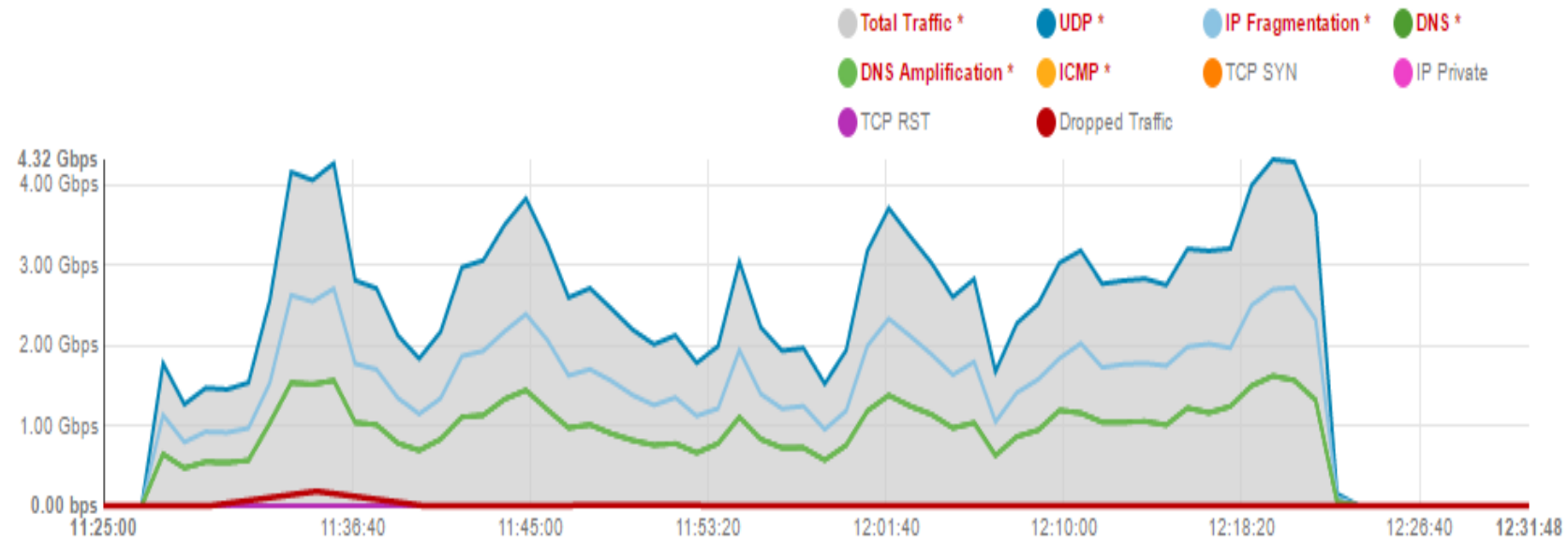
Dados Relevantes

Ataques coordenados

- Ataques DDOS com mais de 20 instituições envolvidas
- Instituições com 27 mil IPs envolvidos no ataque

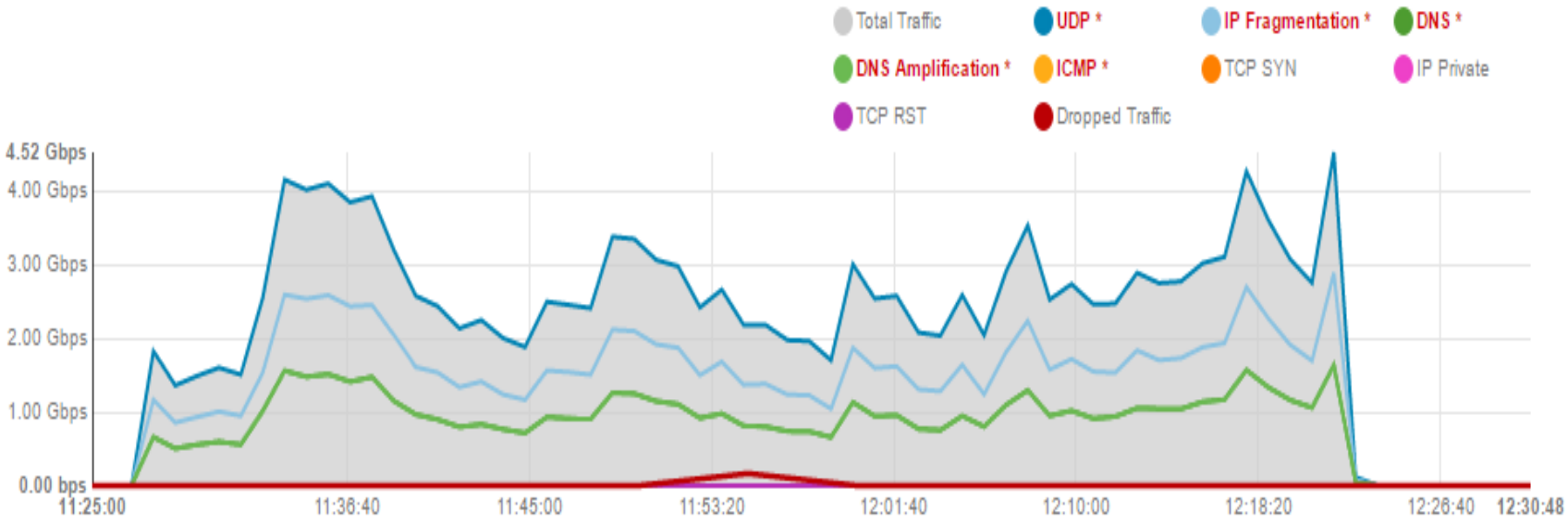
Dados Relevantes

Maiores ataques detectados - Volume



Dados Relevantes

Maiores ataques detectados - Volume



Resultados

- Número de notificações aumentaram muito
  Jan 2016 = 15 Incidentes
  Ago 2016 = 834 Incidentes

- Melhor análise dos ataques DDoS

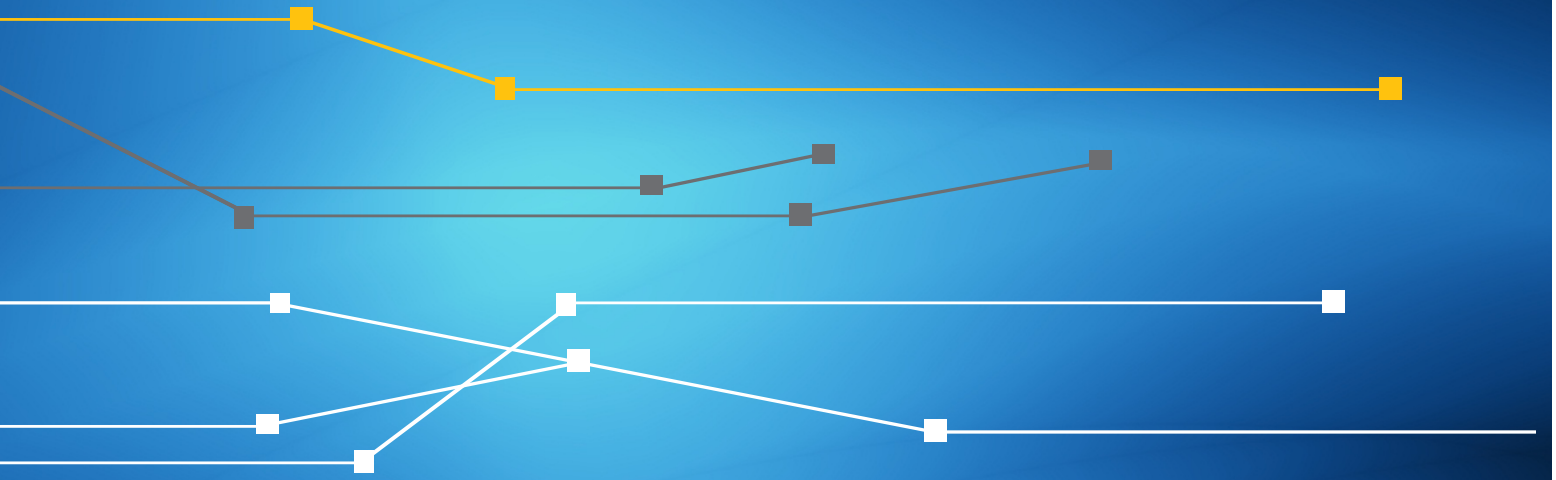
- Ataques entrando ou saindo da Rede Ipê agora são notificados

Desdobramentos

- Aumento da visão sobre a segurança do ambiente acadêmico

- Definição de estratégias para combate à ataques DDOS.

Dúvidas



Obrigado !!

Rildo Antonio de Souza – rildo.souza@rnp.br

RNP

MINISTÉRIO DA **DEFESA**

MINISTÉRIO DA **CULTURA**

MINISTÉRIO DA **SAÚDE**

MINISTÉRIO DA **EDUCAÇÃO**

MINISTÉRIO DA **CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**

BRASIL GOVERNO FEDERAL