Incidentes de Segurança e Registro no SGIS/RNP

Diego Torres

VI Workshop do PoP-RS/RNP e Reunião da Rede Tchê

Porto Alegre, Outubro 2016

PoP-RS

Rede Tchê

Sumário

- Introdução
- Objetivos
- SGIS
- Incidentes e Vulnerabilidades
- Ações
- Desafios

Introdução

- Centro de Resposta a Incidentes de Segurança
- Pioneiro – Fundado em Agosto de 1997
- SGIS – Sistema de Gestão de Incidentes de Segurança, desenvolvido pelo CAIS.

Objetivos

- Responder por incidentes na Rede Tchê e clientes do POP-RS/RNP
- Auxiliar na resolução de incidentes e vulnerabilidades
- Aumentar a conscientização sobre a necessidade de segurança na internet

SGIS

- Sistema de Gestão disponível para todos clientes da RNP
- Facilitar o tratamento de incidentes
- Interface Web para gerar relatórios e indicadores
- Distingue Vulnerabilidade e Incidente
- Cadastro de Instituições e as redes responsáveis

Mensagem SGIS – CAIS

Antes de encerar este incidente junto ao CAIS, certifique-se que:
1. O incidente foi investigado e identificado:
2. O incidente foi corrigido, garantindo que ele não voltará a acontecer.

Para encerar o incidente, acesse o sistema SGIS (link abaixo) e atualize o status do incidente:
"https://sgis.rnp.br/incidents/[redacted]"

O incidente pode também ser encerrado mediante resposta dessa mensagem, conforme segue:

Para incidentes tratados e corrigidos, substitua o campo "Assunto"/"Subject" por:
[CAIS #[redacted]] - [RESOLVIDO]

Para incidentes com informações insuficientes ou cujo host denunciado não pertença a Instituição, substitua o campo "Assunto"/"Subject" por:
[CAIS #[redacted]] - [CAIS-AJUDA]

Aguardamos seu retorno, certos de sua colaboração, e nos colocamos a disposição
para quaisquer esclarecimentos.

Caso você não seja a pessoa apropriada para receber este tipo de mensagem, por
favor nos informe a quem devemos contactar para resolver este incidente.

Atenciosamente,

CAIS/RNP

###
CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)
Rede Nacional de Ensino e Pesquisa (RNP)
#   #
cais@cais.rnp.br   http://www.rnp.br/servicos/seguranca
Tel. 019-37873300   Fax. 019-37873301
Chave PGP disponivel   http://www.rnp.br/cais/cais-pgp.key
###

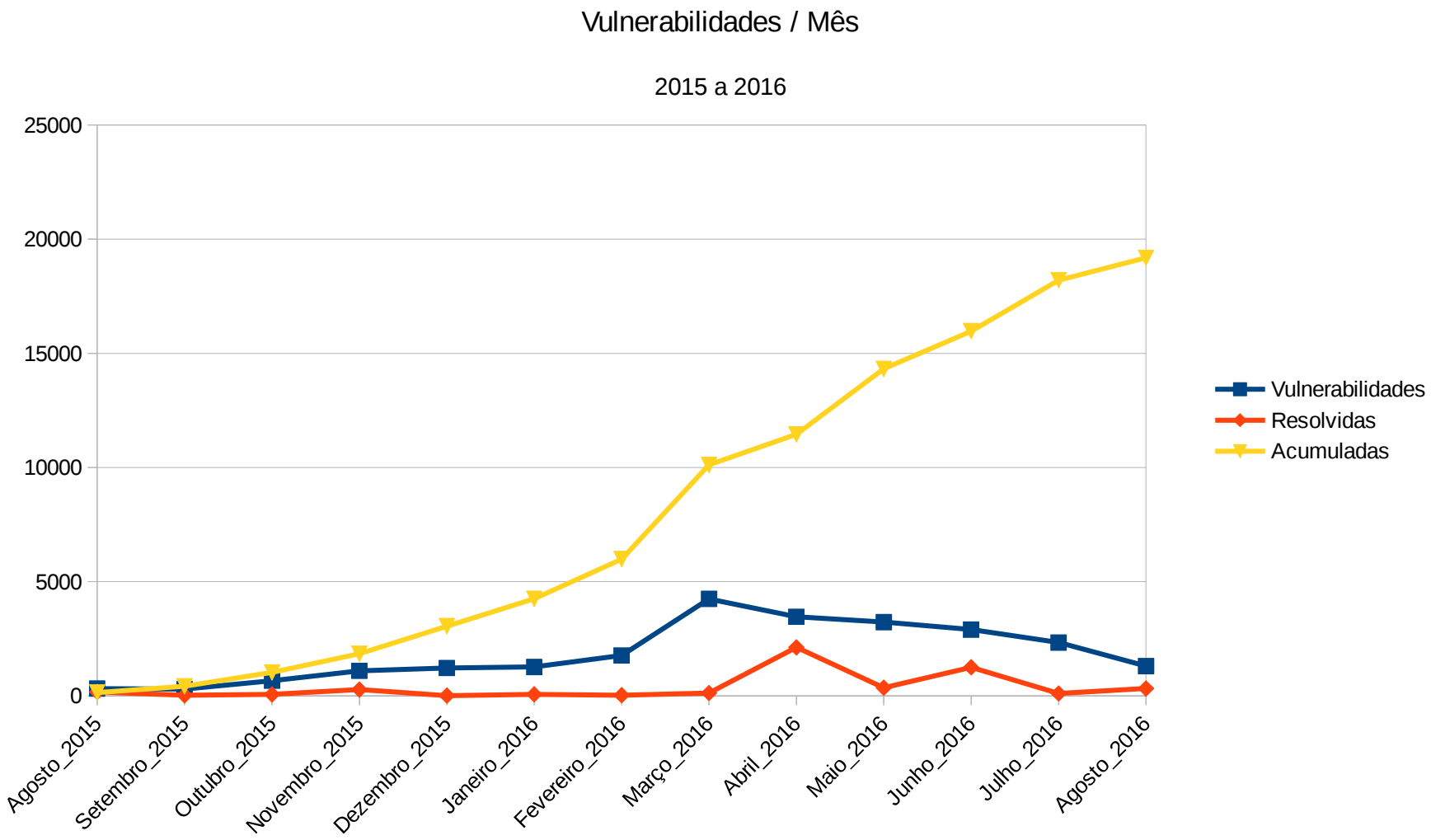
Data e hora UTC(+0),IP Origem, Porta Origem, Protocolo, WebServer, Vulnerabilidade
[redacted]

Vulnerabilidades e Incidentes

- Vulnerabilidade: é uma falha ou fraqueza no projeto, implementação, operação, ou gestão de um sistema que pode ser explorada para violar as políticas de segurança do sistema.

IETF RFC 2828 – tradução livre

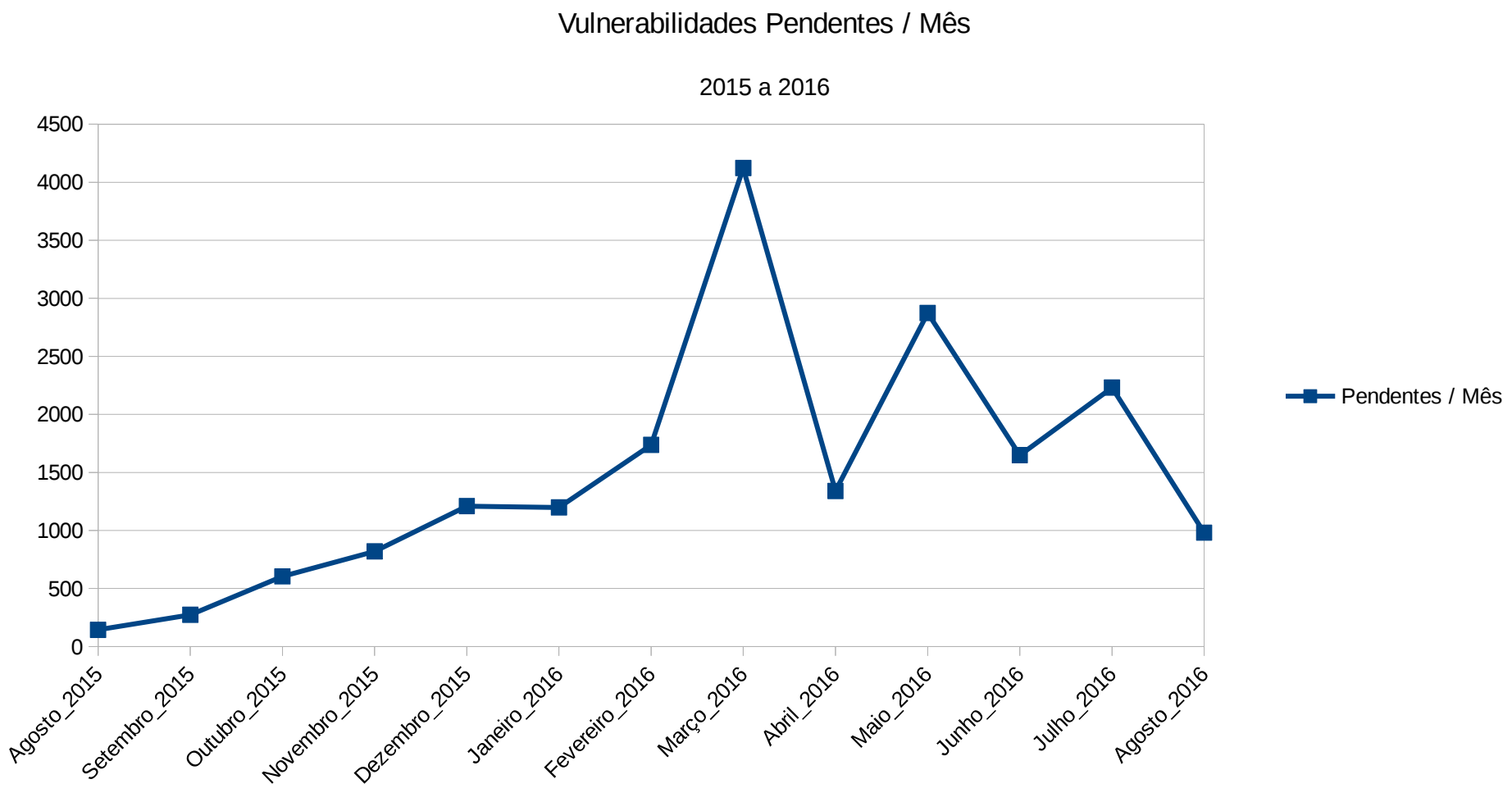
Vulnerabilidades



PoP-RS

Rede Tchê

Vulnerabilidades



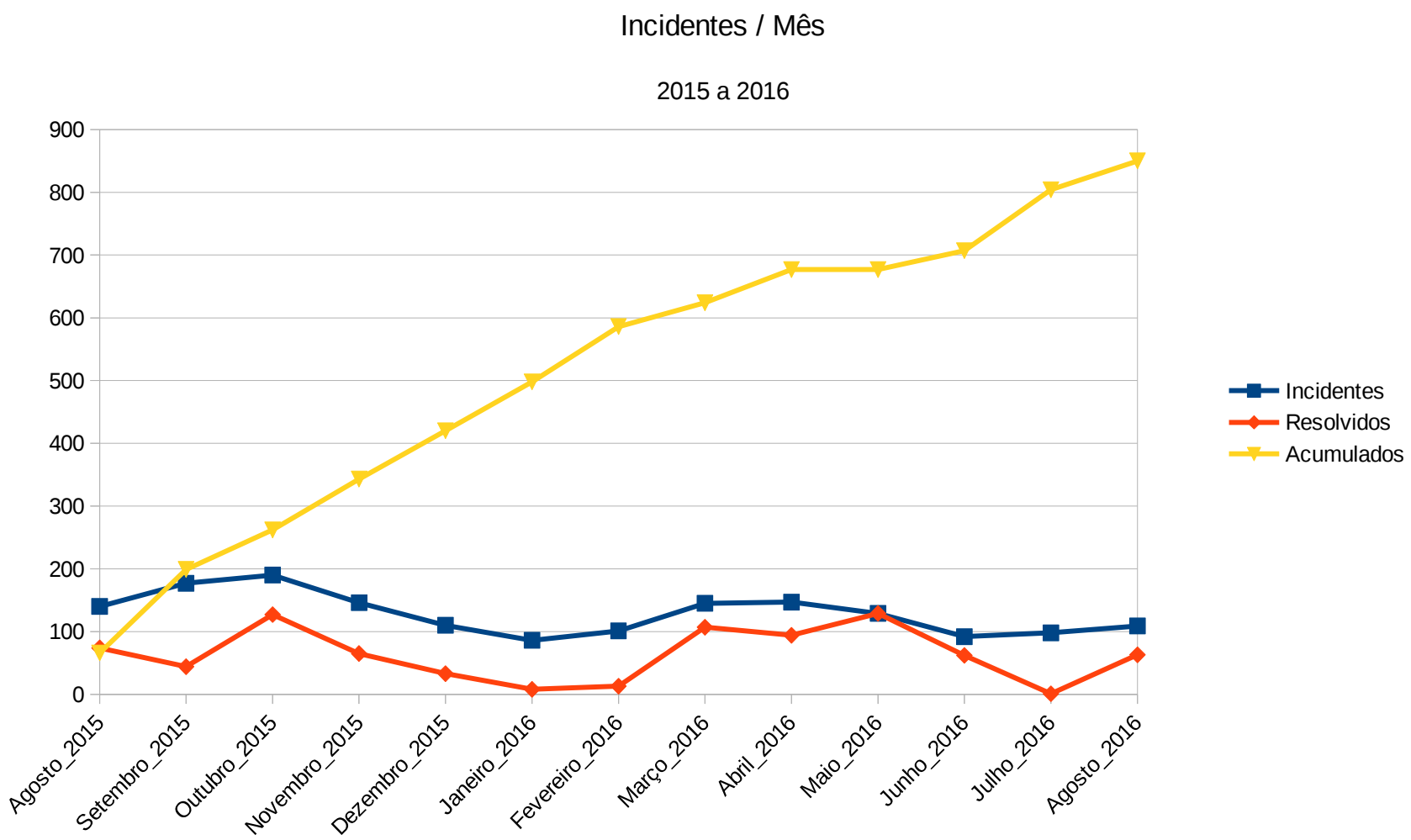
PoP-RS

Rede Tchê

Vulnerabilidades

- Média de resolução (vuln. / mês) : 408,75
- Média de vuln. informadas / mês : 2007,17
- Número de vuln. Pendentes de 2015 a 2016: 19181

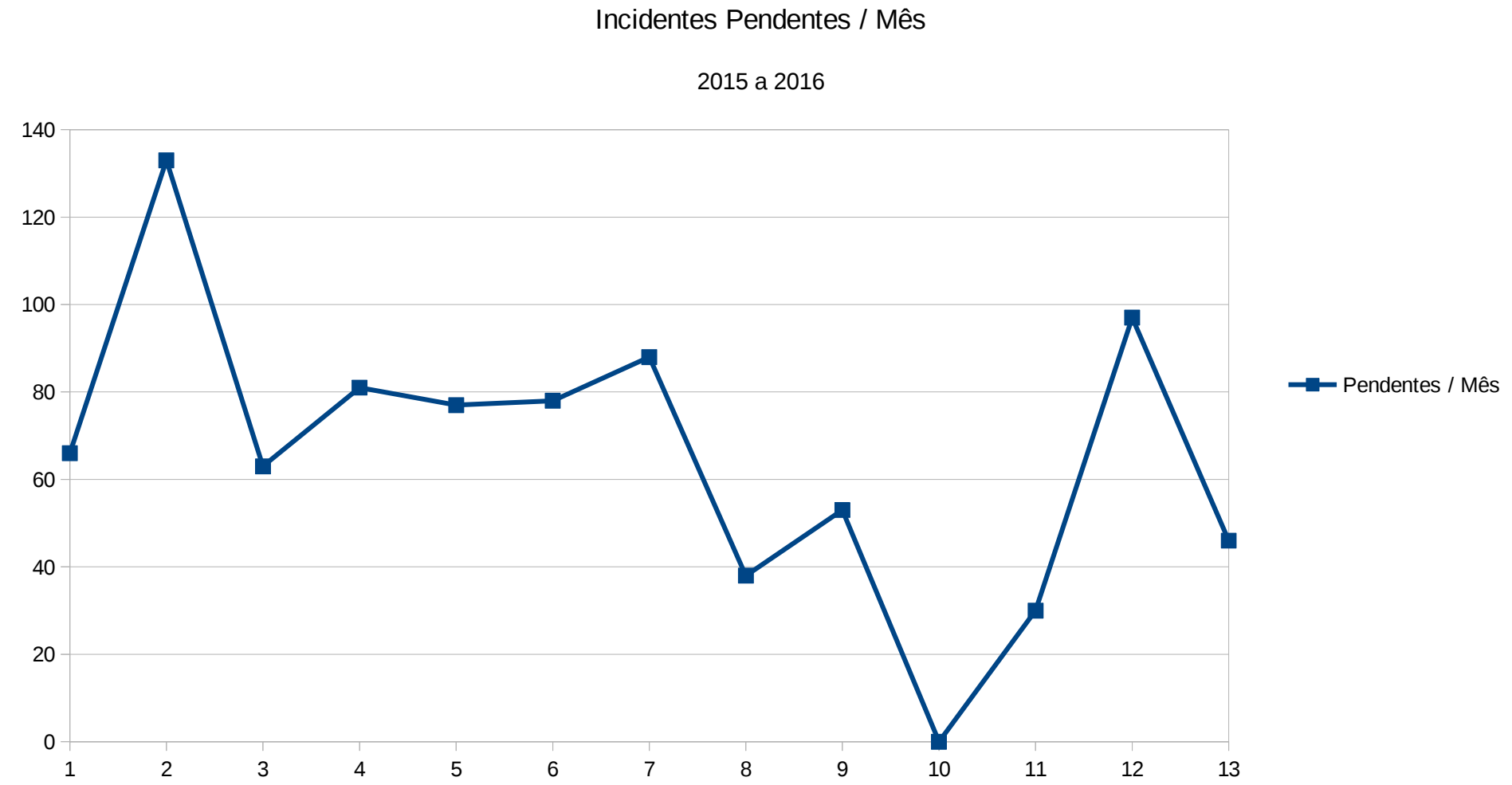
Incidentes



PoP-RS

Rede Tchê

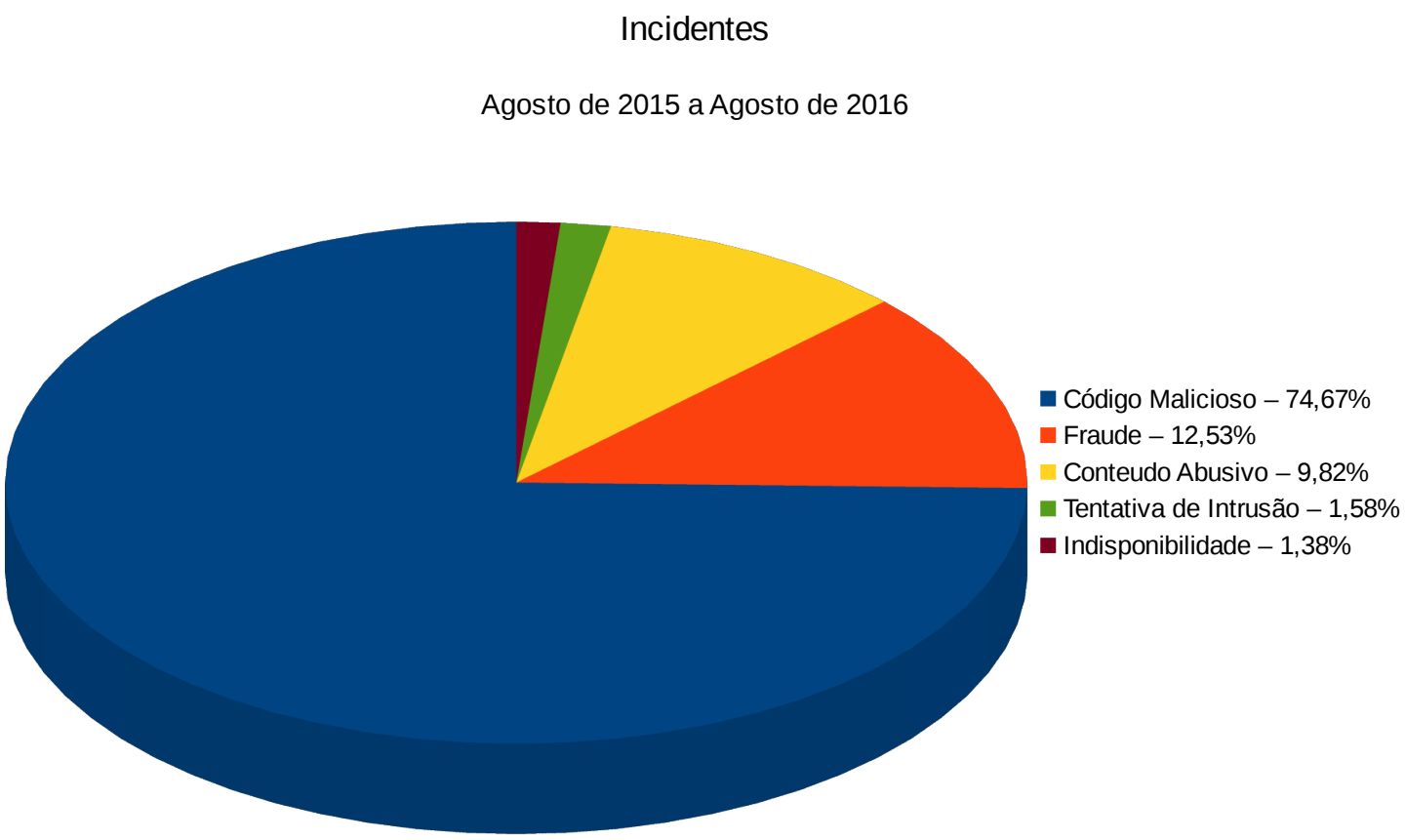
Incidentes



PoP-RS

Rede Tchê

Principais Incidentes



PoP-RS

Rede Tchê

Incidentes mais reportados

- SPAM
- PortMapper / Varreduras
- Violação de Copyright / Pirataria
- Bots
- Phishing

SPAM

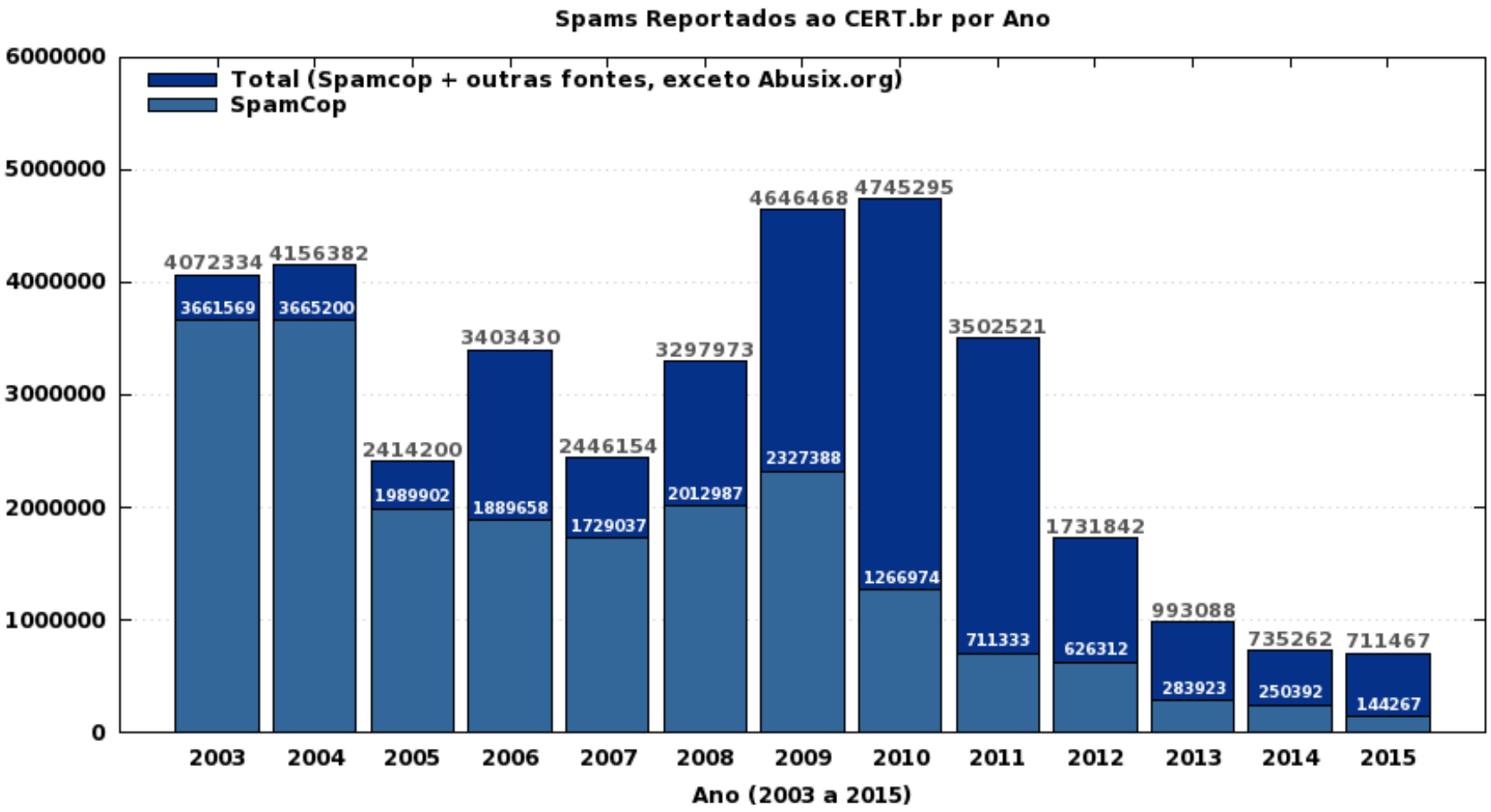


Imagem retirada do site cert.br às 14 horas e 20 minutos, dia 23 de Setembro de 2016

PoP-RS

Rede Tchê

Varreduras / PortMapper

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2015

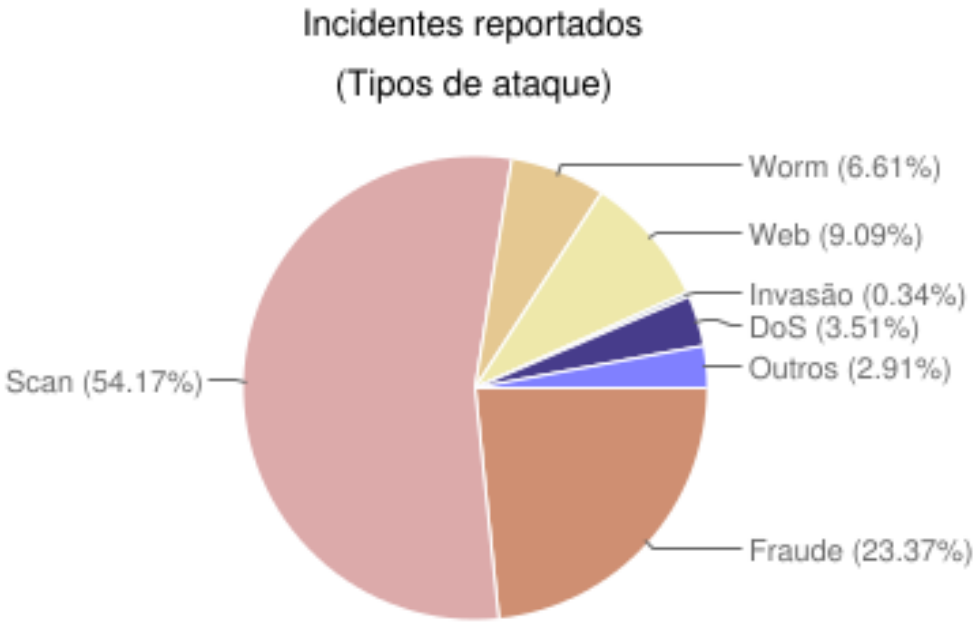
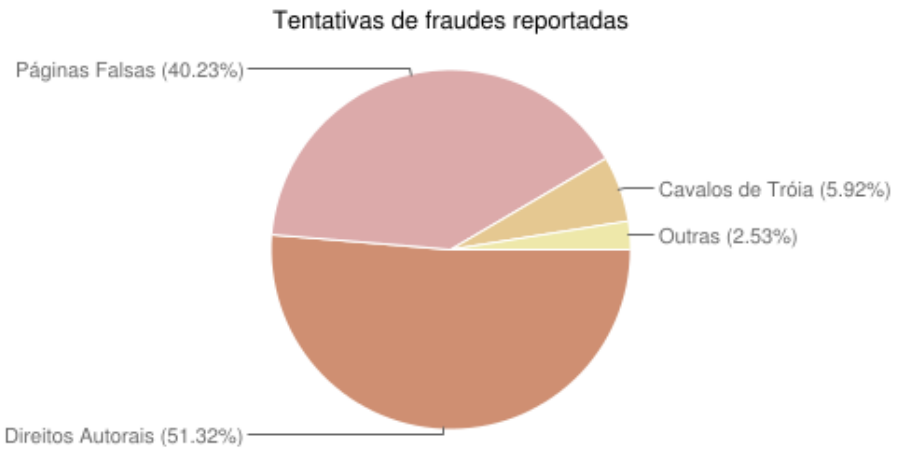


Imagem retirada do site cert.br às 15 horas e 35 minutos, dia 26 de Setembro de 2016

Violação de Copyright / Pirataria

- Bittorrent
  - Download de filmes e jogos

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2015



Legenda:

- **Cavalos de Tróia**: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
- **Páginas Falsas**: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.
- **Direitos Autorais**: Notificações de eventuais violações de direitos autorais.
- **Outras**: Outras tentativas de fraude.

Imagem retirada do site cert.br às 15 horas e 30 minutos, dia 26 de Setembro de 2016

$Date: 2016/03/15 13:13:33 $

Desafios

- Auxiliar clientes em boas práticas de segurança.
- Desestimular o uso do NAT na Rede Tchê.
  - Falsa sensação de segurança
  - Dificuldade em rastrear o incidente

Obrigado!

Dúvidas?

Contatos:

cert-rs.tche.br

Diego Torres

diego@pop-rs.rnp.br