Principais incidentes e vulnerabilidades de segurança dos clientes do PoP-PR

André Landim

CAIS - Centro de Atendimento a Incidentes de Segurança / RNP

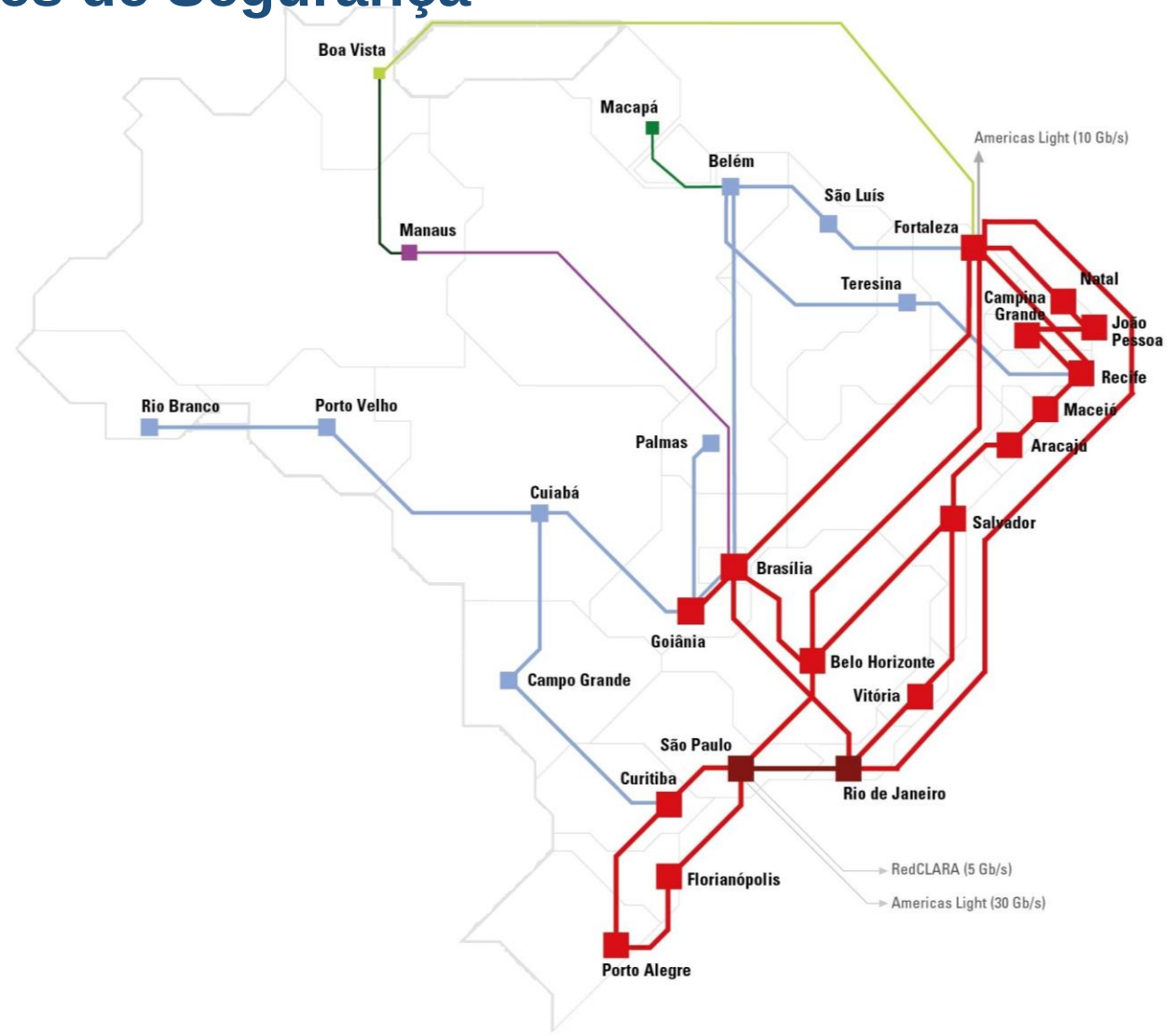
Agenda

- [ ] Contextualização
- [x] Principais Números
- [ ] Situação dos Clientes do PoP-PR
- [ ] O que Fazer?
- [ ] Dúvidas

Contextualização

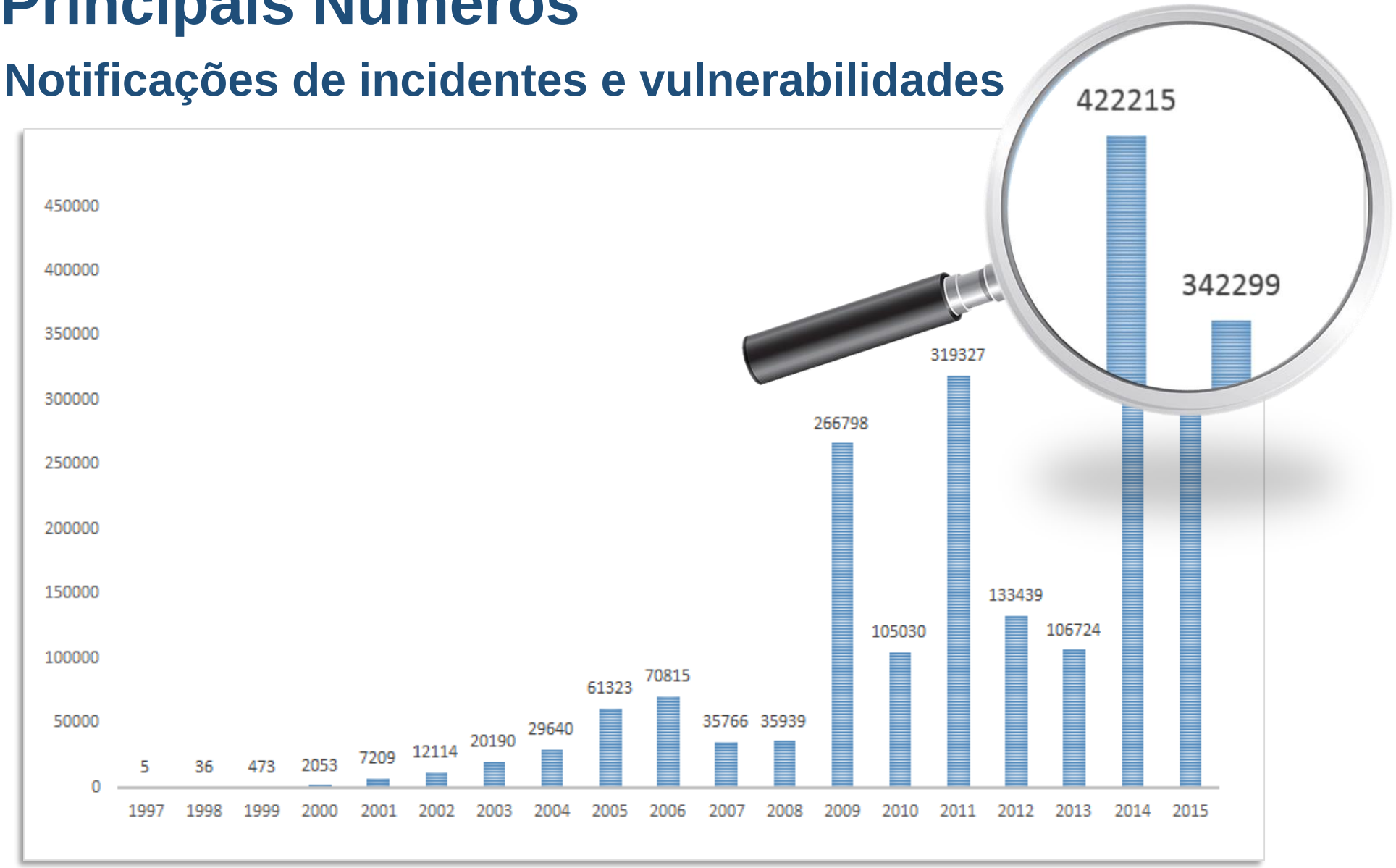
CAIS – Centro de Atendimento a Incidentes de Segurança

- **CSIRT de coordenação da Rede Ipê, desde 1997.**
- **Cerca de 1.100 Instituições.**
- **422.215 Notificações em 2014.**



Principais Números

Notificações de incidentes e vulnerabilidades

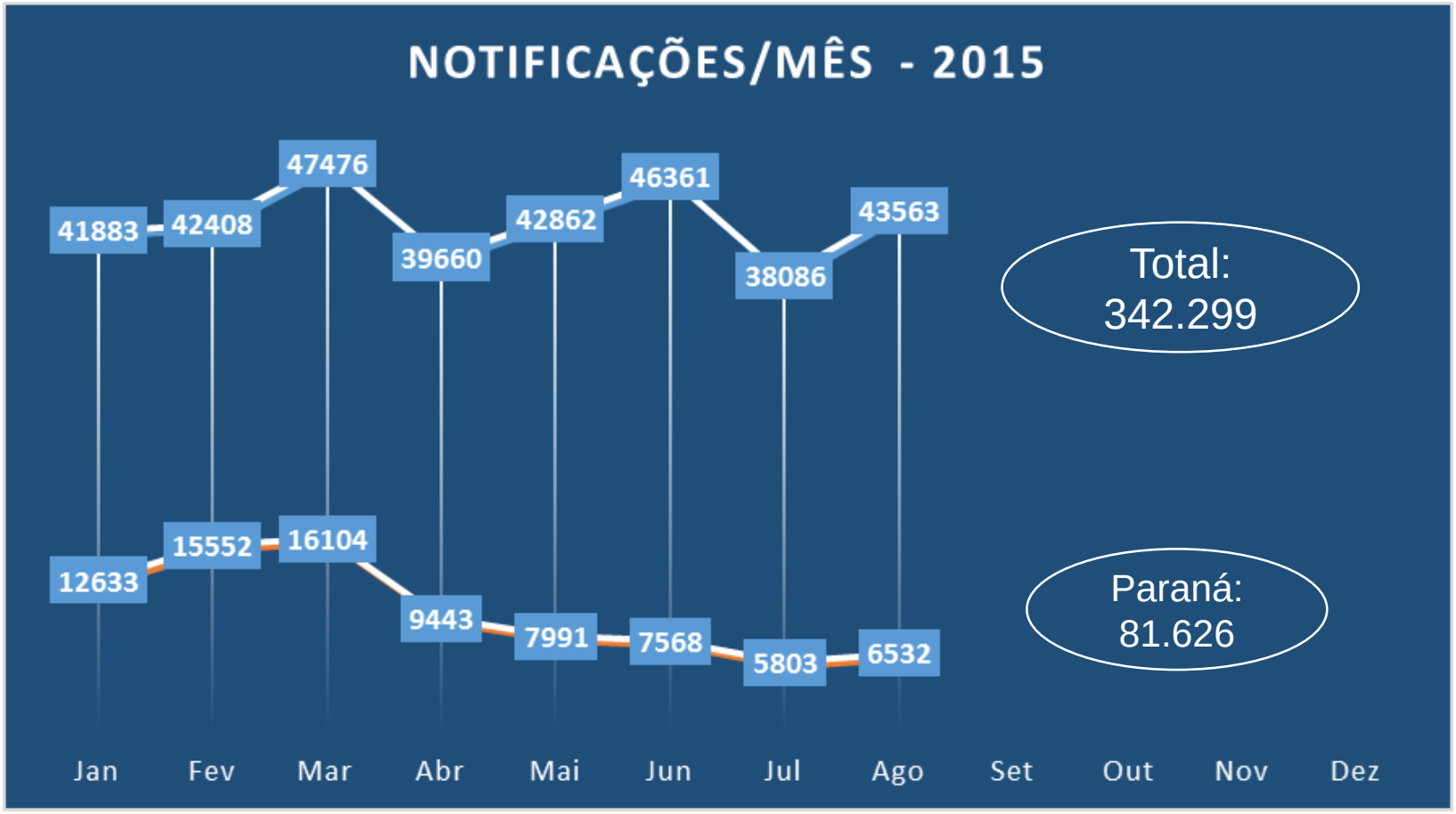


Ano	Incidentes/dia
2009	731
2010	288
2011	875
2012	365
2013	292
2014	1157
2015	938

* Dados até 08/2015.

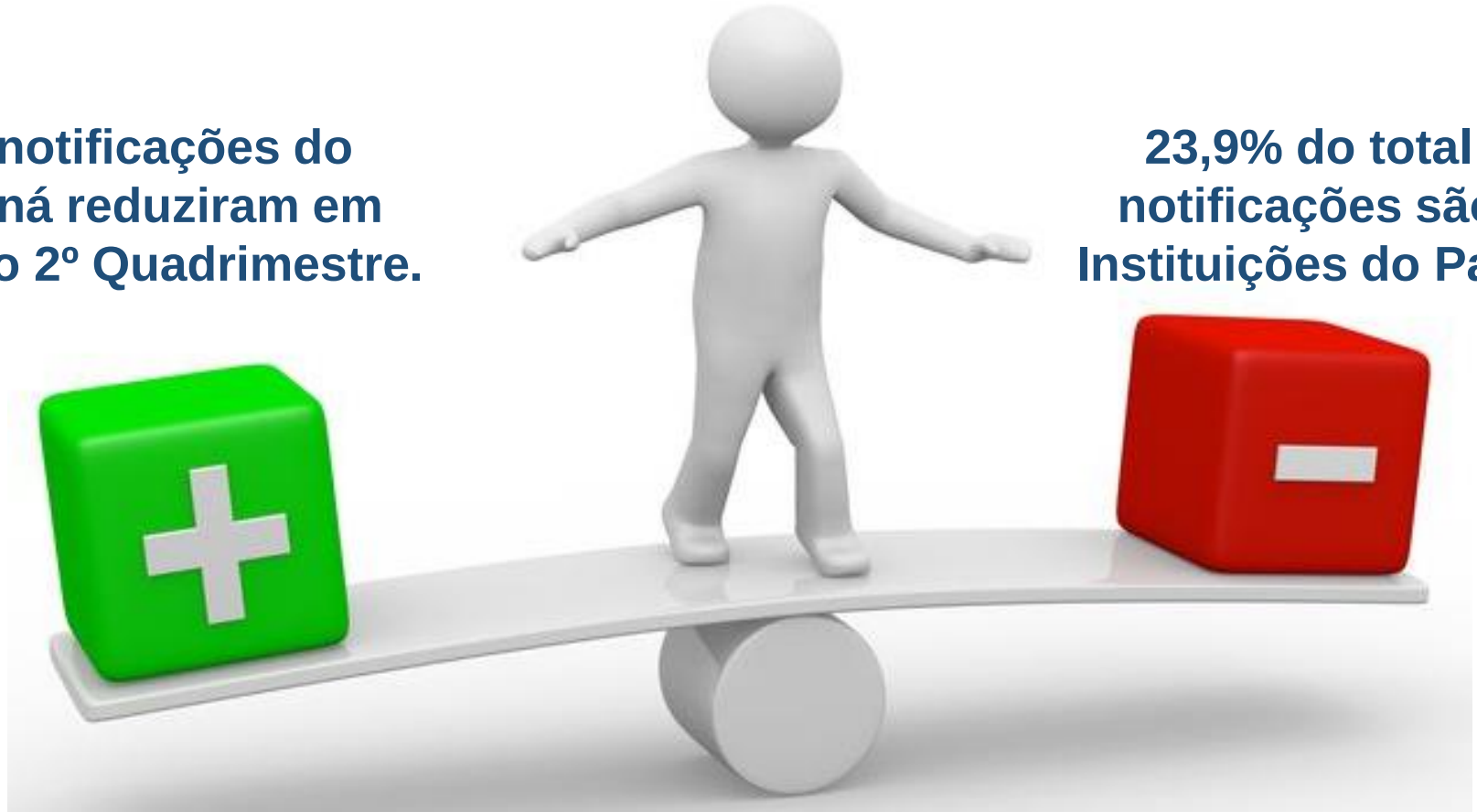
Principais Números

Notificações de incidentes e vulnerabilidades



Situação dos Clientes do PoP-PR

As notificações do Paraná reduziram em 48% no 2º Quadrimestre.



23,9% do total de notificações são de Instituições do Paraná.

Situação dos Clientes do PoP-PR

Incidentes e Vulnerabilidades

Notificações	81626
Tentativa de intrusão	80262
Código Malicioso	1208
Intrusão	84
Conteudo Abusivo	34
Fraude	31
Indisponibilidade de serviço ou informação	4
Segurança da informação	2
Prospecção por informações	1

Situação dos Clientes do PoP-PR

Incidentes e Vulnerabilidades

Tentativa de Intrusão

Exploração de vulnerabilidades para intrusão ou indisponibilidade de serviços

SNMP

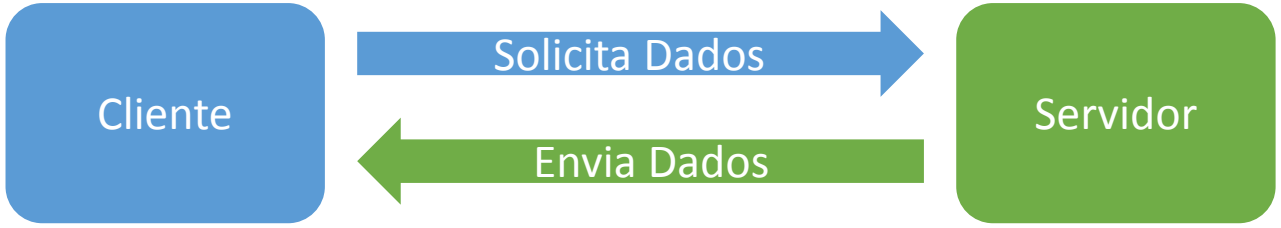
Netbios

NTP

Protocolos UDP

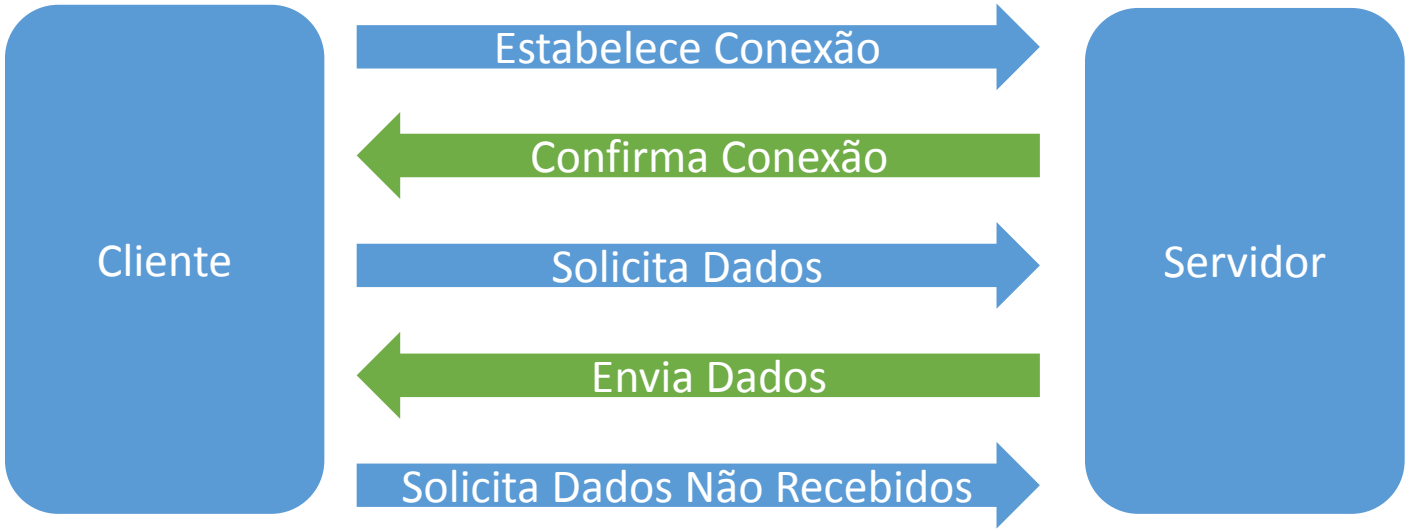
Situação dos Clientes do PoP-PR

Funcionamento da vulnerabilidade



Protocolo UDP

- Funcionamento mais simples
- Mais rápido por ter menos controles
- Não estabelece conexão
- Menos seguro em relação ao recebimento de dados (Transporte)



Protocolo TCP

- Funcionamento mais complexo
- Mais controles
- Estabelece conexão antes de transmitir os dados
- Solicita retransmissão dos dados não recebidos
- Mais seguro em relação ao recebimento de dados (Transporte)

Situação dos Clientes do PoP-PR

Incidentes e Vulnerabilidades

IP: 11.11.11.11

IP Spoofing

Técnica de mascaramento (*spoofing*) de pacotes IPs para evitar identificação, utilizando endereços de remetentes falsificados.

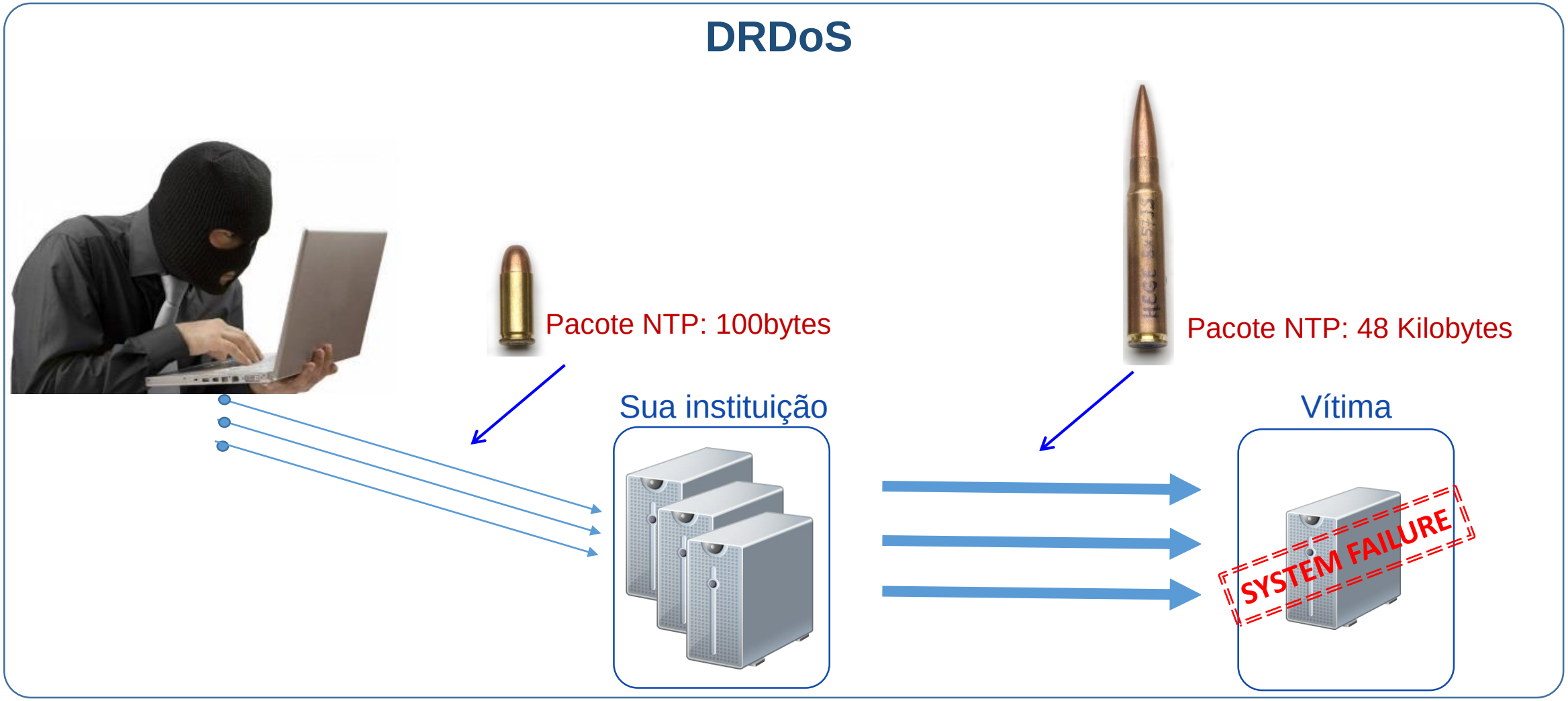
IP Destino: 22.22.22.22
IP Origem: 33.33.33.33

IP: 22.22.22.22

IP: 33.33.33.33

Situação dos Clientes do PoP-PR

Incidentes e Vulnerabilidades – Tentativa de Intrusão



O Que Fazer?

SNMP

- Desativar SNMP v1 e v2c e utilizar SNMP v3.
- Restringir o acesso SNMP para hosts específicos através de ACLs.
- Restringir todas as saídas SNMP através da utilização de views.
- Desativar o protocolo SNMP nos dispositivos que não precisarem de gerenciamento.

O Que Fazer?

NTP

- Atualizar o servidor NTP para a versão atual.
- Revisar lista de servidores para realizar o sincronismo.
- Adicionar regra para ignorar pedidos “default”.
- Restringir acesso ao servidor somente às redes internas.

O Que Fazer?

Netbios

- Revisar as configurações do servidor de forma a permitir somente consultas internas.
- Caso este serviço não seja utilizado, recomendamos a desativação do mesmo.

O Que Fazer?

O sistema SGIS (Sistema de Gestão de Incidente de Segurança)

- Interface web para o tratamento de incidentes
- Tratamento de notificações duplicadas
- Segregação entre Incidentes e Vulnerabilidades
- Tratamento de Origem e Destino dos incidente
- Sistema disponível para todas as Organizações Usuárias
- Indicadores e Relatórios gerenciais on-line
- Envio de arquivo XML com dados das notificações (IODEF)
- Ferramentas colaborativas (Wiki)

Situação dos Clientes do PoP-PR

O sistema SGIS (Sistema de Gestão de Incidente de Segurança)

sgis.rnp.br

Suas Dúvidas

Obrigado,

André Landim.