Panorama de incidentes de segurança nas redes acadêmicas brasileiras

Atanaí Sousa Ticianelli
Coordenador de segurança
Gestão de Incidentes de Segurança - GIS

Centro de Atendimento a Incidentes de Segurança – CAIS
Rede Nacional de Ensino e Pesquisa – RNP

CAIS

RNP

Ministério da Educação

Ministério da Ciência e Tecnologia

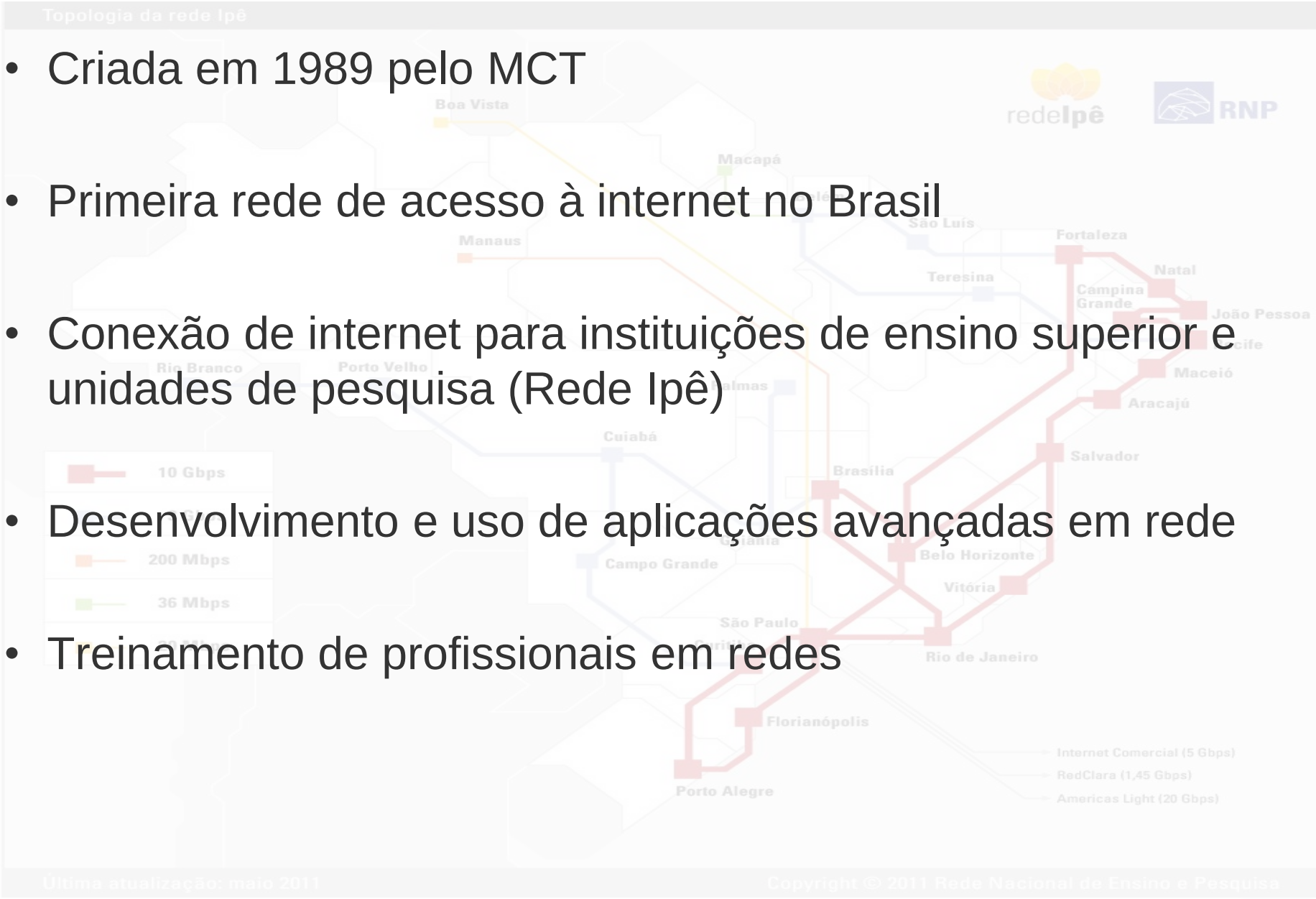
BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Agenda

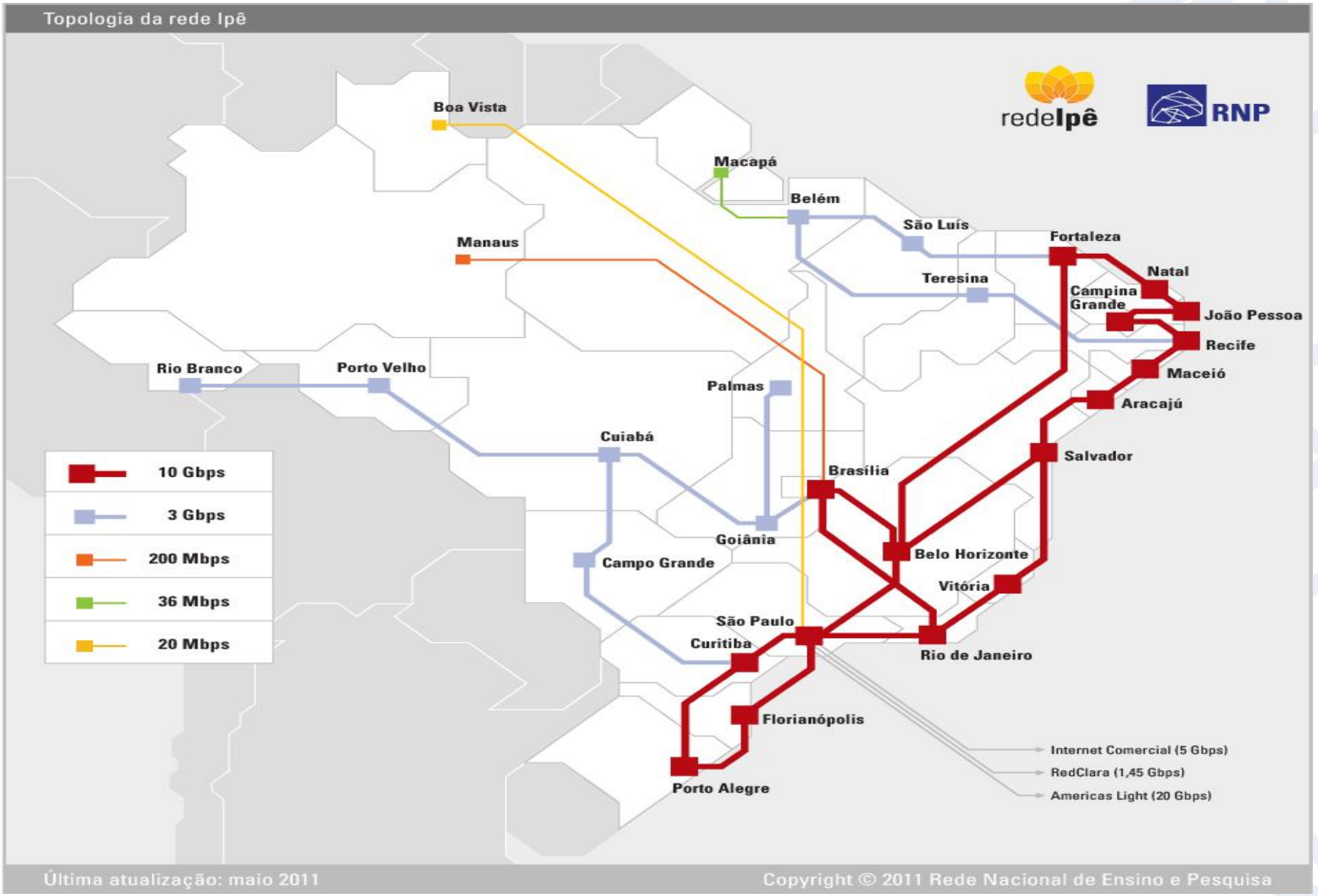
- Rede Nacional de Ensino e Pesquisa – RNP
- Centro de Atendimento a Incidentes de Segurança – CAIS
- Tratamento de Incidentes de Segurança
- Histórico e incidentes em 2011
- Incidentes por estado
- Código malicioso
- Conteúdo abusivo
- Fraude
- Tentativas de intrusão
- Demais categorias

Rede Nacional de Ensino e Pesquisa - RNP

- Criada em 1989 pelo MCT
- Primeira rede de acesso à internet no Brasil
- Conexão de internet para instituições de ensino superior e unidades de pesquisa (Rede Ipê)
- Desenvolvimento e uso de aplicações avançadas em rede
- Treinamento de profissionais em redes



Rede Nacional de Ensino e Pesquisa - RNP



- **Rede Ipê: sexta geração**
  - Mais de 800 instituições conectadas
  - 3,5 milhões de usuários estimados
  - 27.500 grupos de pesquisa beneficiados
  - Universidades federais, escolas agrotécnicas, centros federais de educação tecnológica, centros de pesquisa, hospitais, museus, outros.

"A RNP está na ponta de lança da construção de uma sociedade do conhecimento. Depende do Plano Nacional de Banda Larga e da RNP dar suporte às instituições brasileiras de formação de capital humano."

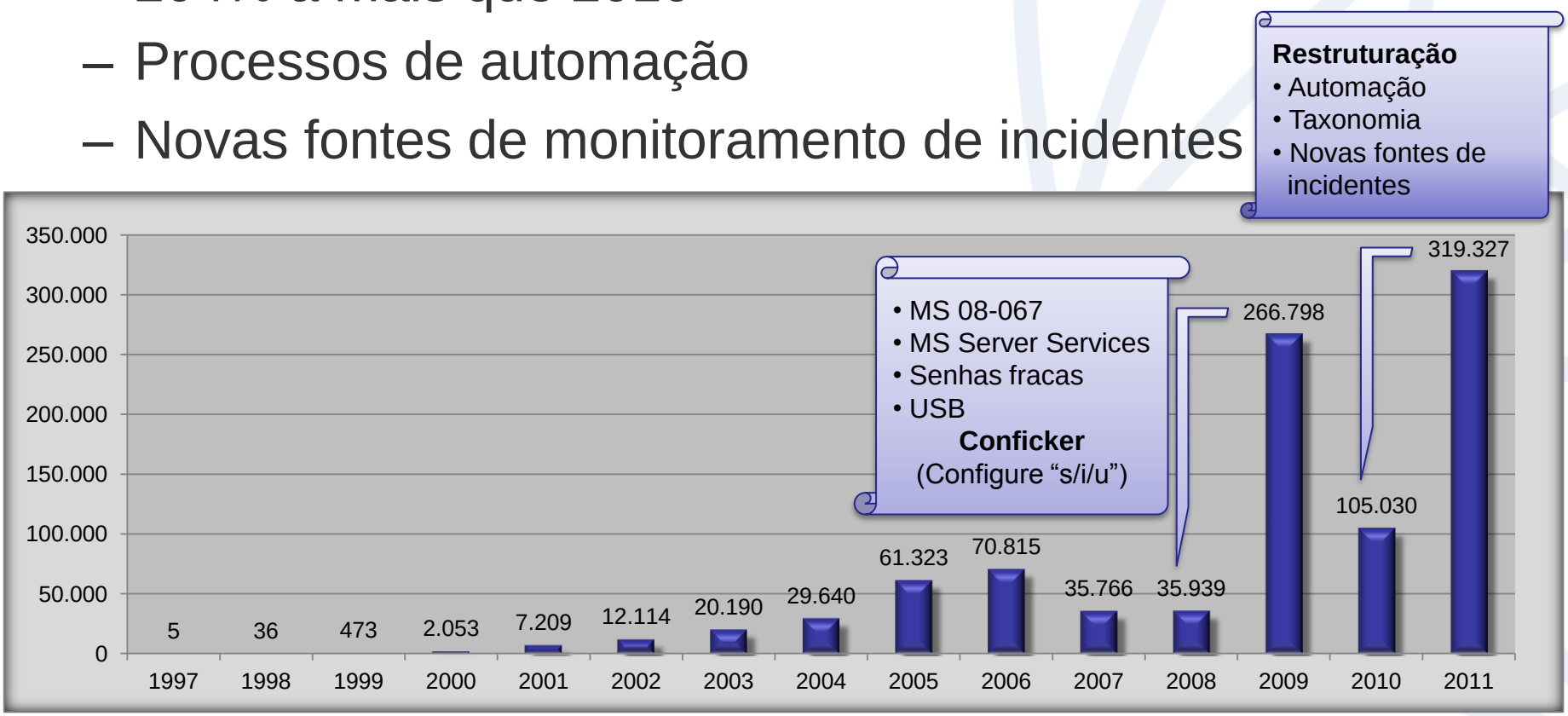
Aluízio Mercadante – MCTI – 13/07/2011

- **CAIS**
  - Área criada em 1997 na RNP
  - Detecção, resolução e prevenção de incidentes de segurança
  - Divulgação de informações e alertas de segurança
  - Quatro sub-áreas
    - Disseminação da Cultura de Segurança (DCS)
    - Gestão de Riscos e Segurança da Informação (GRSI)
    - Infraestrutura e Serviços à Comunidade Acadêmica (SERV)
    - Gestão de Incidentes de Segurança (GIS)

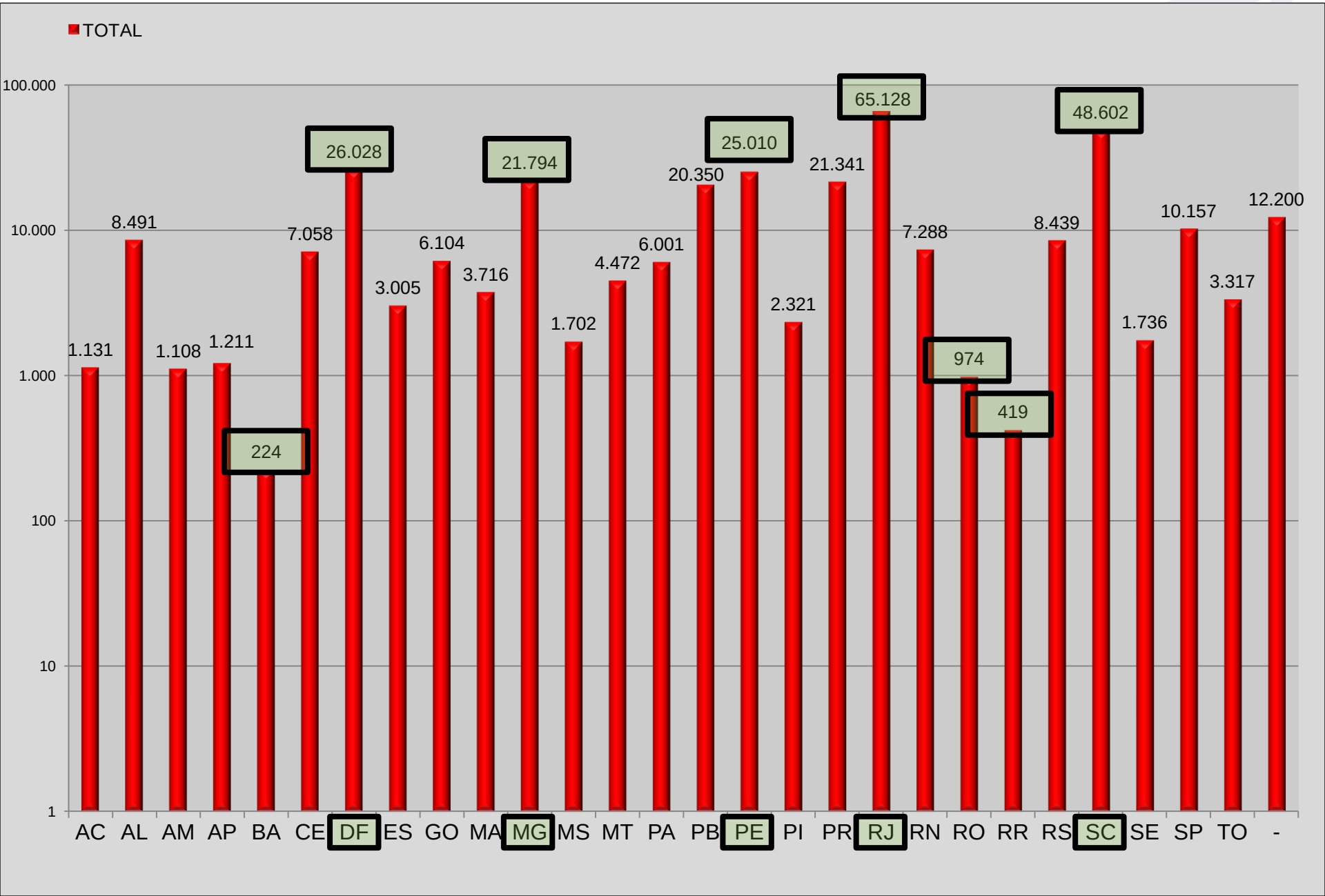
- **Gestão de incidentes de segurança (GIS)**
  - Papel de coordenação e suporte aos clientes
  - Atuação nos núcleos da RNP e no backbone
  - 2 analistas dedicados ao T.I.

Histórico e incidentes em 2011.

- **Em 2011:**
  - Total de 319.327 incidentes tratados
  - 20% a mais incidentes que 2009
  - 204% a mais que 2010
  - Processos de automação
  - Novas fontes de monitoramento de incidentes



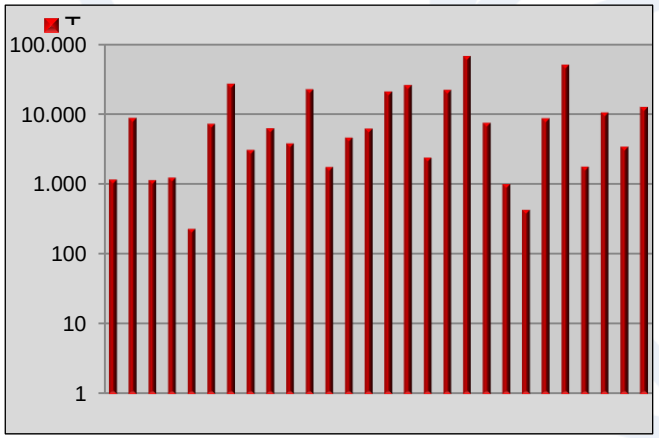
Incidentes por estado



Incidentes por estado

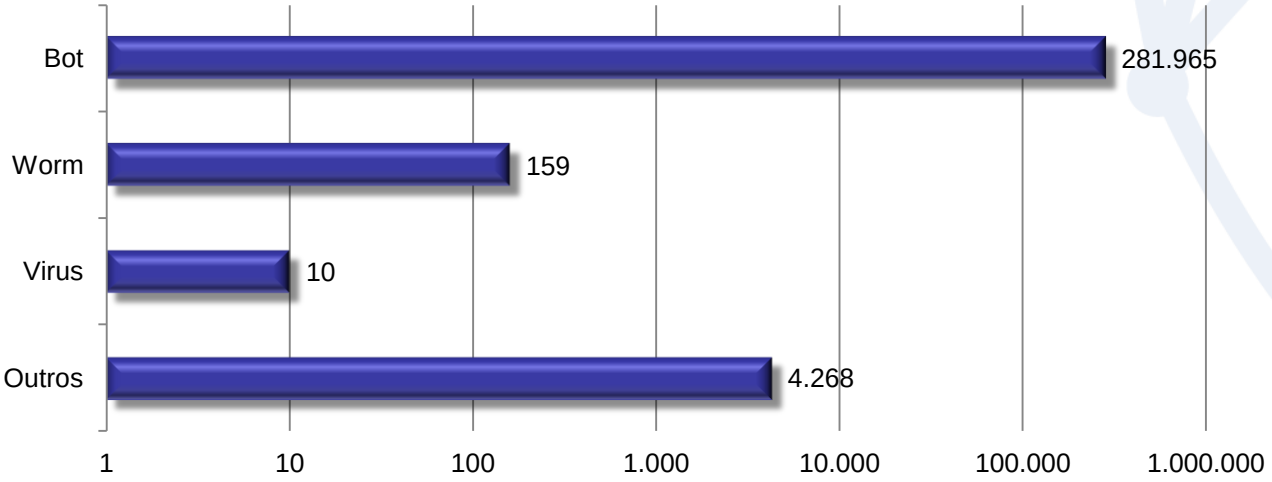
- 23 estados possuem índice de fechamento de incidentes menor que 1%
  - Incluindo RJ, SC, DF, PE, MG, PR e PB (> 20K incidentes)

- Estados com melhores índices no combate a incidentes de segurança
  - BA: ~9%
  - RS: ~4,5%; AM: ~3,2 % ; SP: ~1,4%



Código malicioso

- Vírus, worms, trojans, bots, spywares, scripts, outros
- Representam 90% do total de incidentes na Rede Ipê (286.397 incidentes)
- Botnets: 98% das infecções



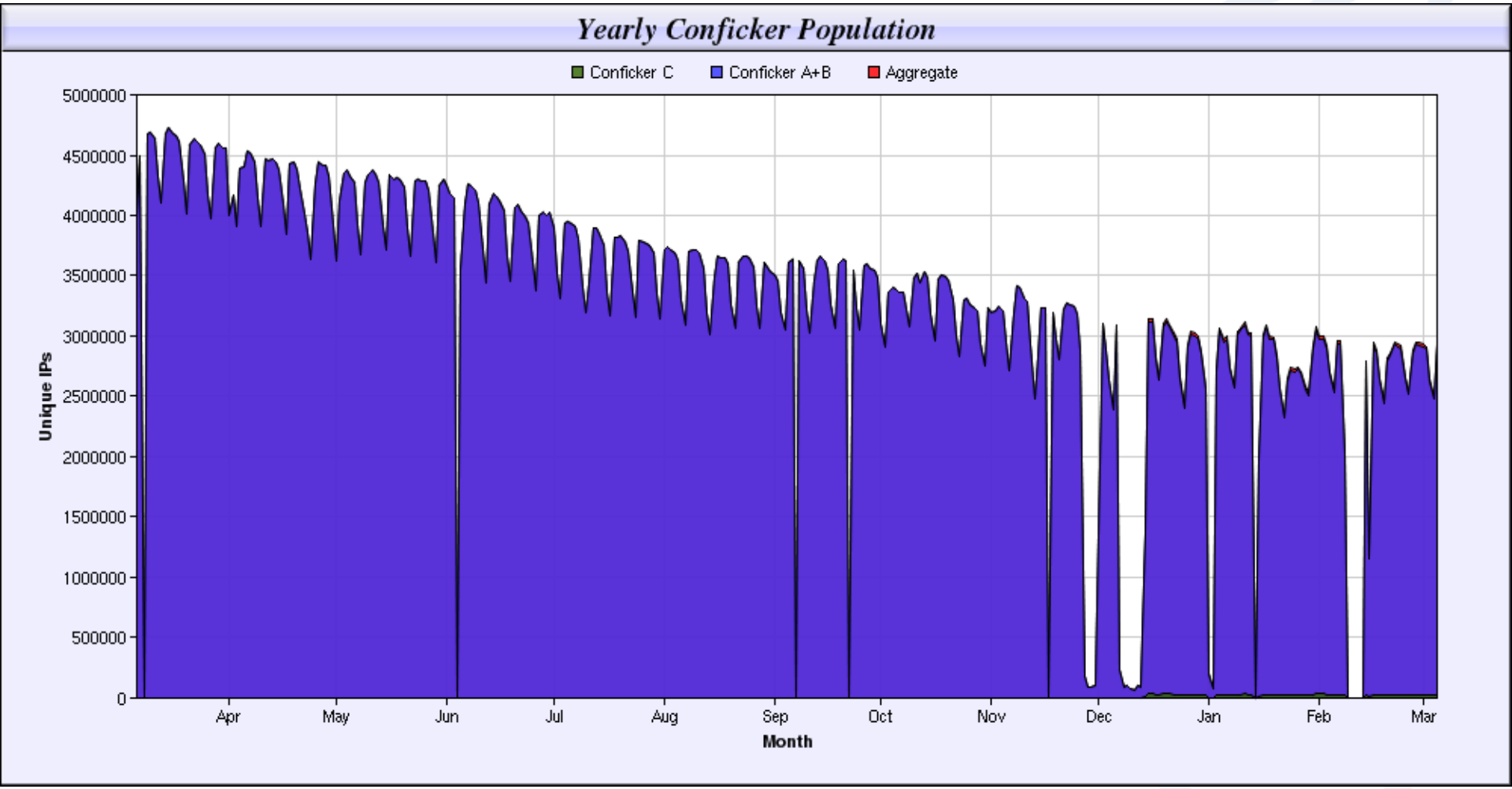
Código malicioso

- **Conficker na RNP (2011):**
  - 154.890 incidentes (~ 48% dos incidentes)
  - 9.822 ips únicos
  - 1.472 redes /24 únicas

- **Conficker no mundo:**
  - Conficker A+B+C (2012-03-07)
    Total hits HTTP: 672.627.608
    IP's únicos: 2.931.401
    ASN's únicos: 14.439
    GEO's únicas: 226

http://www.confickerworkinggroup.org

Código malicioso

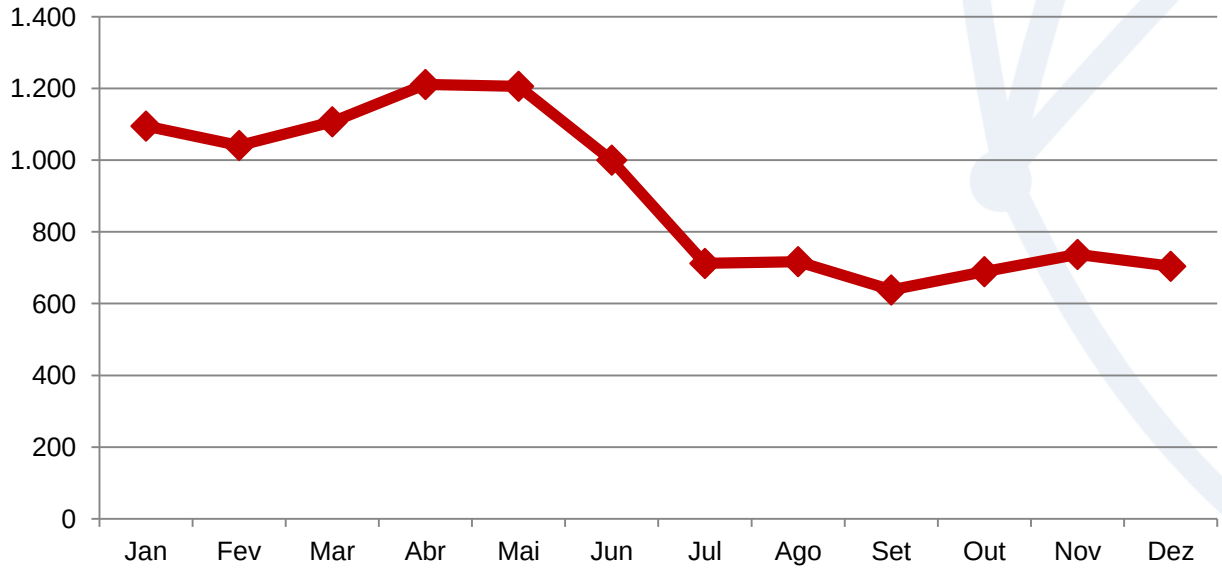


http://www.confickerworkinggroup.org

Conteúdo abusivo

- Envio de spam, casos de difamação, assédio, discriminação, outros.

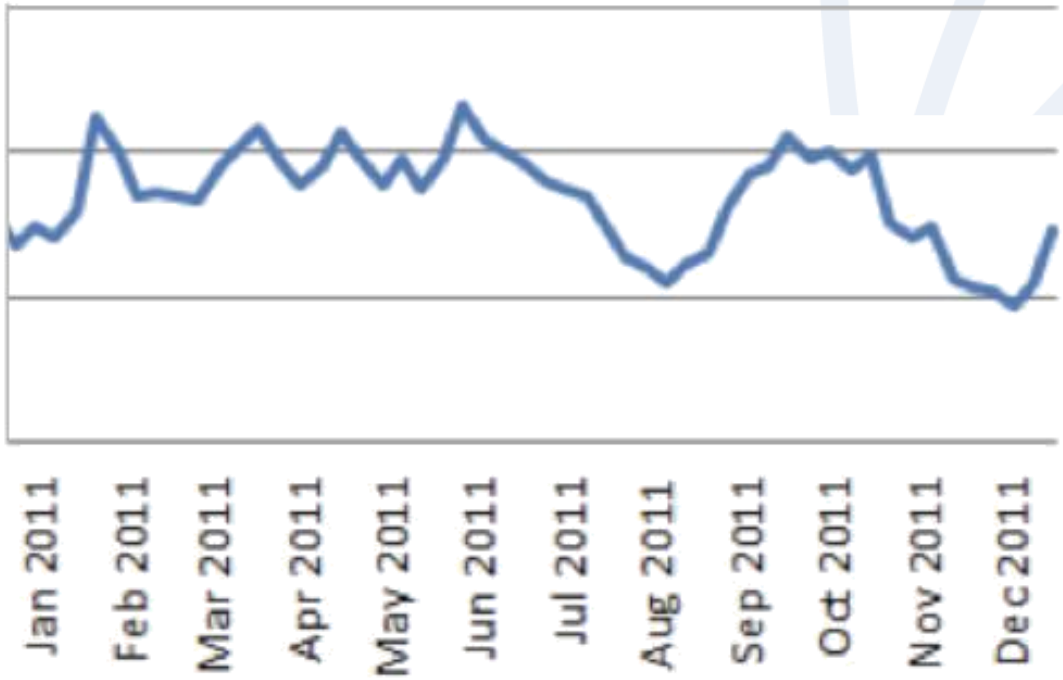
- 10.857 notificações em 2011 (3,34% do total anual)



Conteúdo abusivo

– Envio de spam, casos de difamação, assédio, discriminação, outros.

– 10.857 notificações em 2011 (3,34% do total anual)

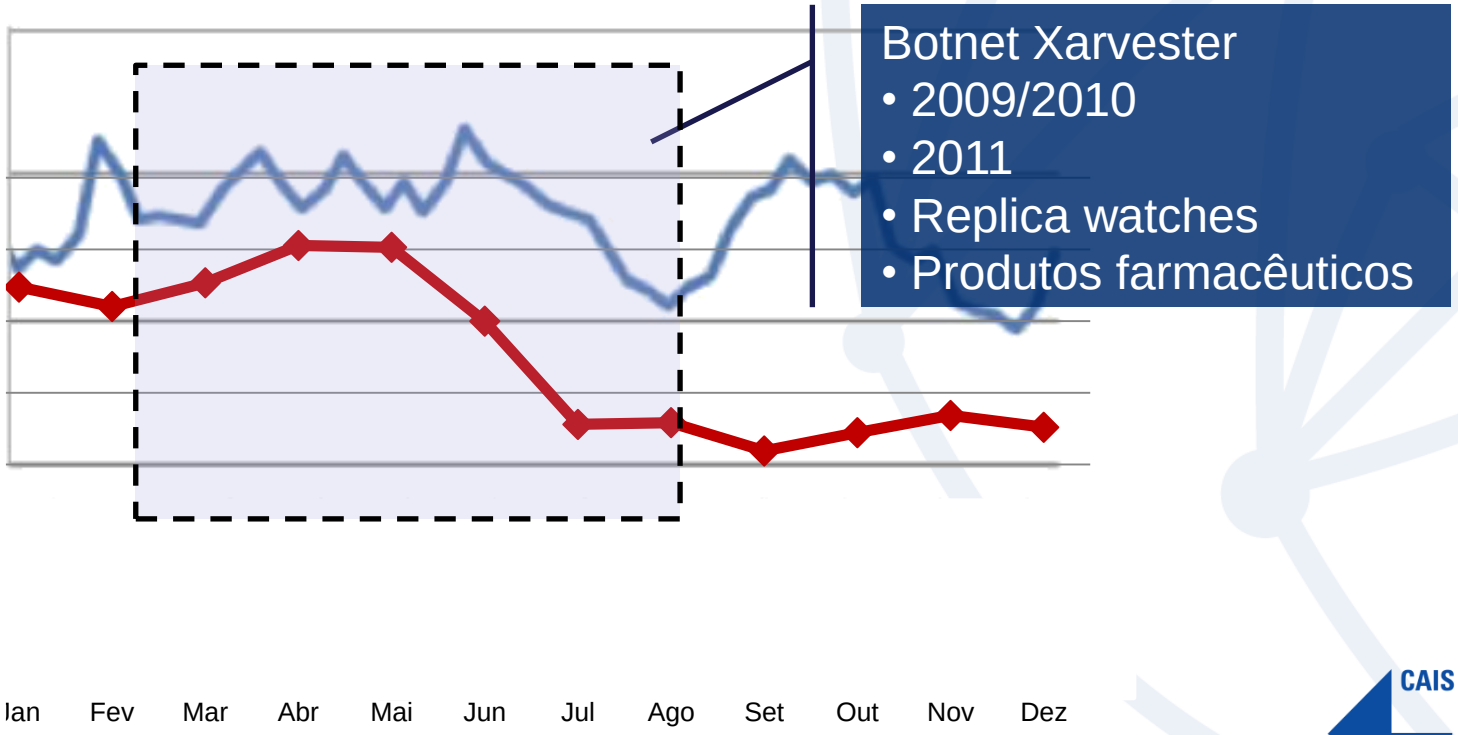


m86_security_labs_report_2h2011.pdf

Conteúdo abusivo

– Envio de spam, casos de difamação, assédio, discriminação, outros.

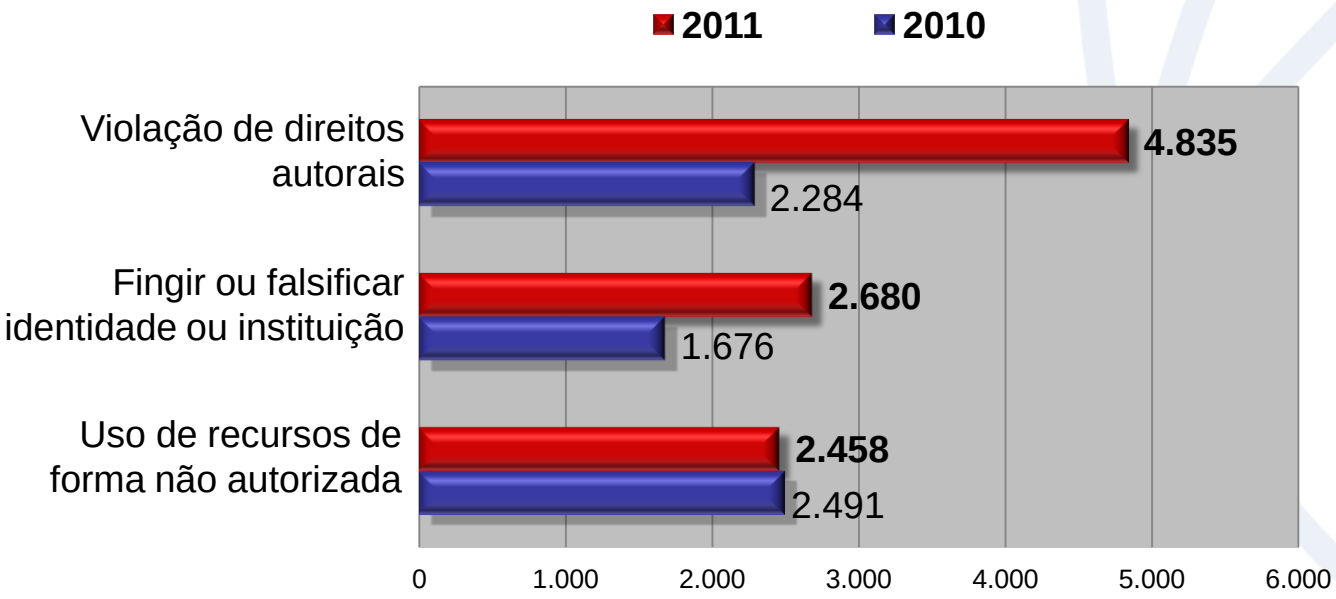
– 10.857 notificações em 2011 (3,34% do total anual)



m86_security_labs_report_2h2011.pdf

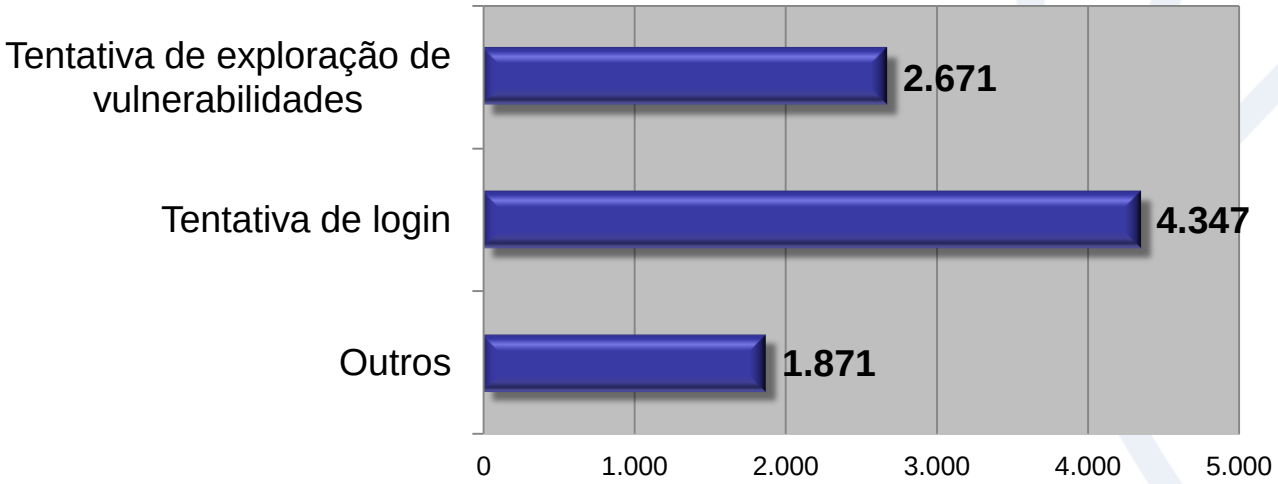
Fraude

- Violam direitos autoriais
- Entidade assume de forma ilegítima a identidade de outra
- Utilização de recursos de forma não autorizada
- 9.973 notificações em 2011 (3,12% do total anual)

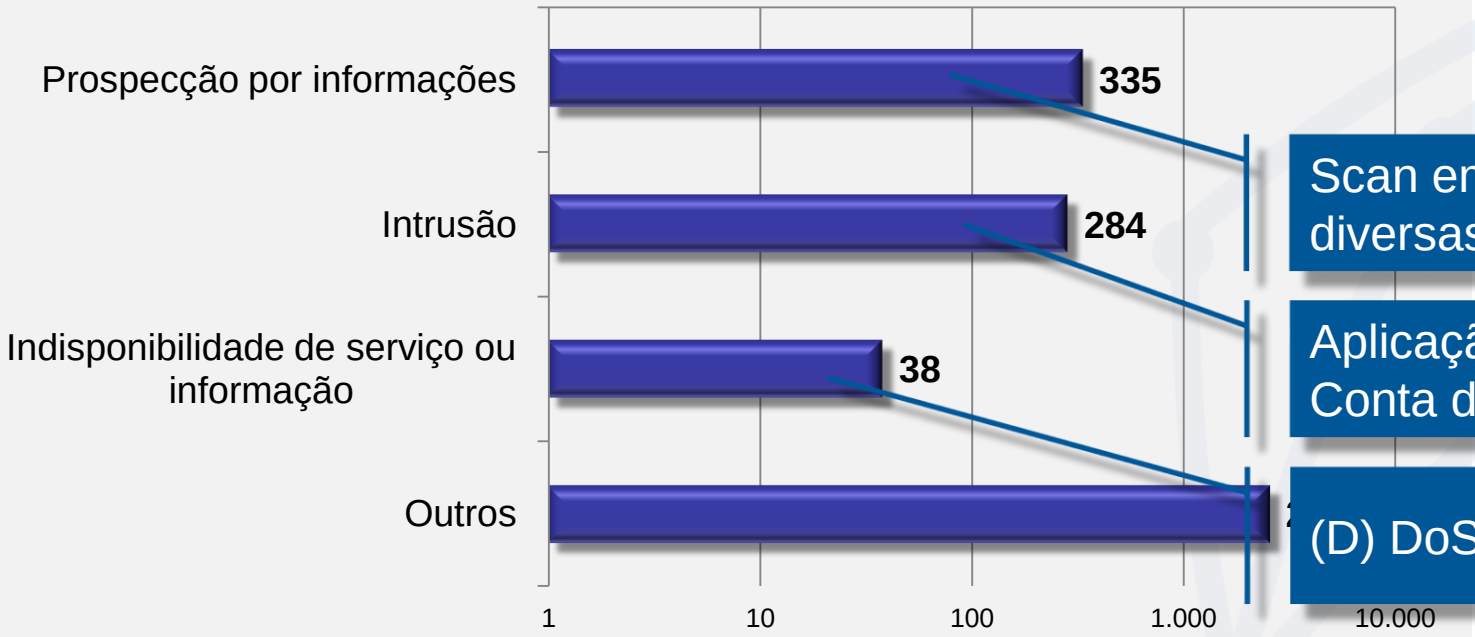


Tentativas de intrusão

- XSS, SQL Injection
- SSH, Mail, FTP
- 8.889 notificações em 2011 (2,78% do total anual)



Demais categorias



Scan em portas diversas, icmp, etc

Aplicação: 265
Conta de usuário: 19

(D) DoS

Centro de Atendimento a Incidentes de Segurança – CAIS/RNP

http://www.rnp.br/cais/

 @cais_rnp

Atanaí Sousa Ticianelli <atanai at cais.rnp.br>

Notificação de Incidentes

Para encaminhar incidentes de segurança envolvendo redes conectadas à RNP:

1. E-mail: cais@cais.rnp.br

Para envio de informações criptografadas use a chave PGP pública do CAIS: http://www.rnp.br/cais/cais-pgp.key

2. Formulário para Notificação de Incidentes de Segurança: http://www.rnp.br/cais/atendimento_form.html

Hotline INOC-DBA (Inter-NOC Dial-By-ASN): 1916*800

Atendimento Emergencial: Para contato fora do horário comercial (09:00 - 18:00 - Horário de Brasília) por favor utilize o telefone (61) 226-9465.

Alertas do CAIS: O CAIS mantém a lista rnp-alerta@cais.rnp.br. Assinatura aberta à comunidade de segurança. Inscrição através do formulário em:

http://www.rnp.br/cais/alertas/