cais Inteligência em Cibersegurança RNP

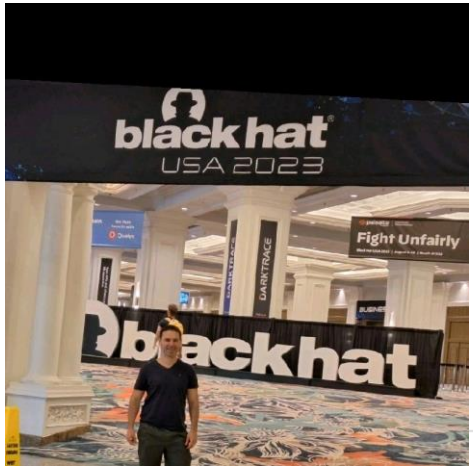
2° Hackathon do Hackers do Bem

Rildo Souza

Coordenador de Segurança da Informação

Quem sou

- Rildo Souza
- Pai da Mariana
- Coordenador do Red e Blue Team
- Ex aluno da Unicamp e SENAC
- Cursando Mestrado, algumas especializações e certificações
- Na área de segurança da informação formalmente desde 2009



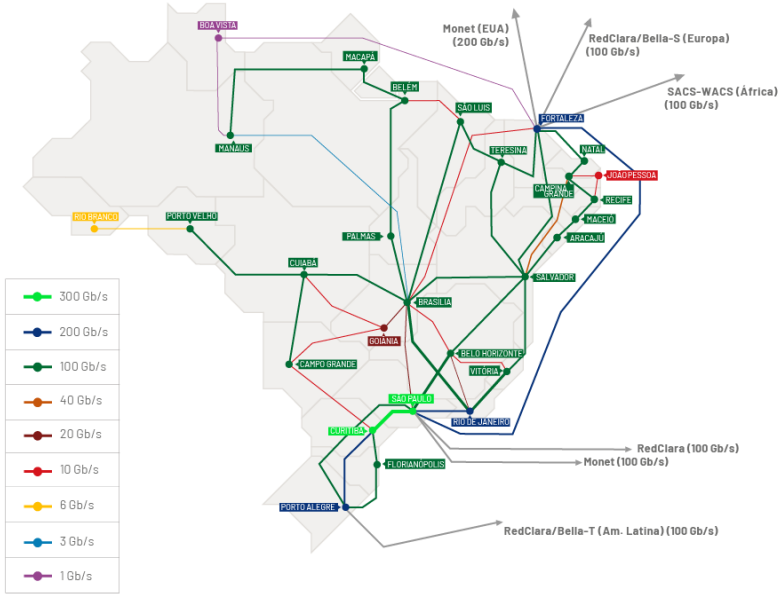
RNP

TLP: CLEAR

RNP – Rede Nacional de Ensino e Pesquisa

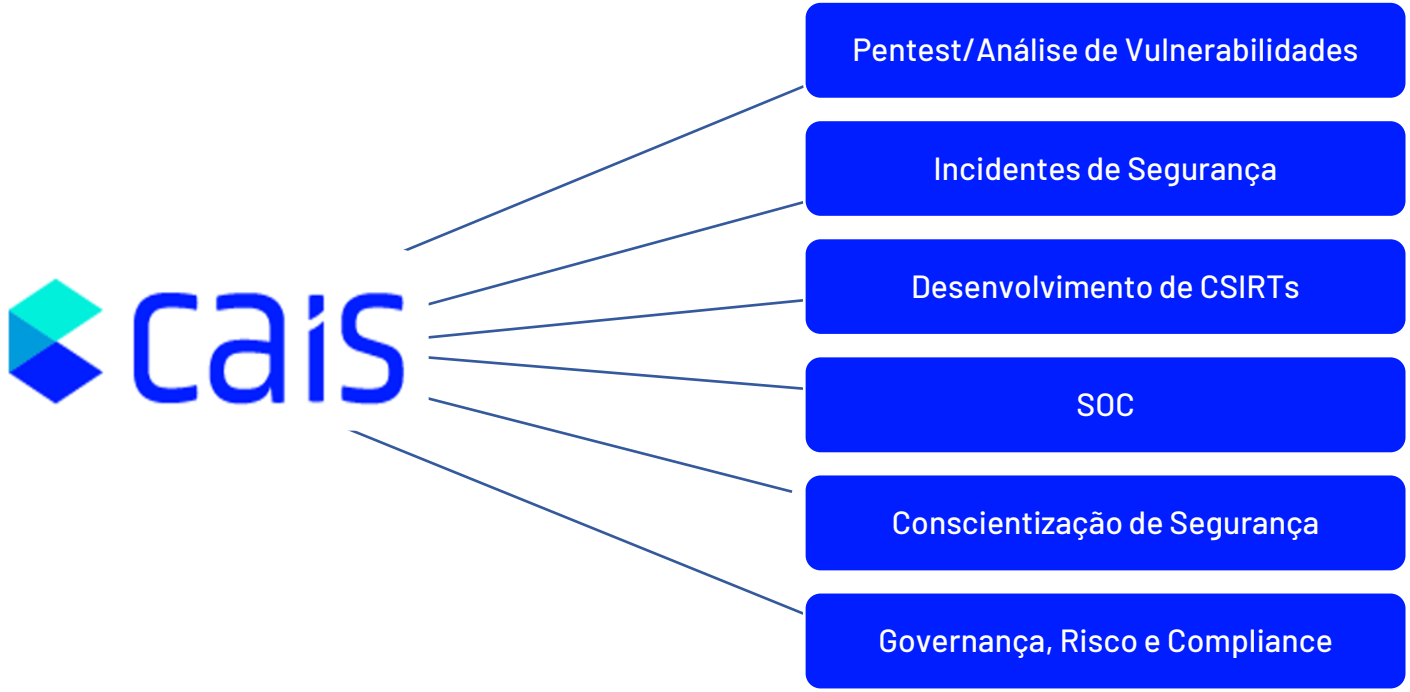
CONEXÃO | DEZEMBRO/23 | Capacidade agregada 3,82 Tb/s | Capacidade internacional 600 Gb/s

- Internet de alta capacidade, serviços personalizados e promoção de projetos de inovação.
- Beneficiamos 4 milhões de alunos, professores e pesquisadores brasileiros.
- Pioneiros, ao trazer a internet para o Brasil e a primeira rede de fibra ótica na América Latina em 2005.
- Apoiamos com tecnologia e serviços mais de 1500 universidades, institutos educacionais e culturais, agências de pesquisa, hospitais de ensino, parques e polos tecnológicos.



TLP: CLEAR

CAIS – Inteligência em Cibersegurança



RNP

TLP: CLEAR

Contexto

~1850 Instituições clientes

Sistema Gerenciamento de notificações de segurança

1116 Usuários (gestores, analistas e estagiários)

Aproximadamente 100.000 Notificações de Vulnerabilidades anualmente

Dados de Julho 2023 até Julho 2024
Fonte: CAIS/RNP

RNP

TLP: CLEAR

O problema

- CAIS é CSIRT de coordenação responsável por notificar vulnerabilidades e incidentes de segurança na Rede Ipê;
- Clientes do Sistema RNP não possuem pessoas, ferramentas e conhecimento técnico para atuarem nas notificações;
- Número alto de vulnerabilidades **não corrigidas** pelos clientes;
- Ausência de uma solução centralizada para validação de vulnerabilidades pelos clientes.

Estatísticas

Vulnerabilidades

Hosts com o serviço NTP vulneráveis que podem ser utilizados em ataques DDoS	7,670
Servidores Web vulneráveis ao ataque Poodle	5,003
Host com o serviço SMB vulnerável	3,499
Hosts com o serviço PortMapper vulneráveis que podem ser utilizados em ataques DDoS	2,242
Hosts com o serviço NetBios vulneráveis que podem ser utilizados em ataques DDoS	1,864
Host com o serviço de DNS Recursivo Aberto	1,028
Host com o protocolo IPP vulnerável	975
Hosts com o serviço TFTP vulneráveis que podem ser utilizados em ataques DDoS	936
Servidores Web vulneráveis ao ataque Freak	809

Percentual Vulnerabilidades

TOP 10: Vulnerabilidades Estados

Dados de Julho 2023 até Julho 2024
Fonte: CAIS/RNP

TLP: CLEAR

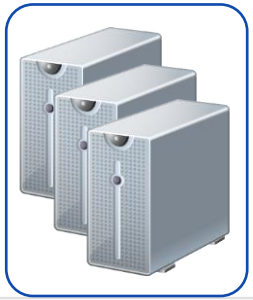
Como as vulnerabilidades afetam os clientes ?

Ataques de Negação de serviço

Pacote NTP: 100bytes

Pacote NTP: 58 Kbytes

Sua instituição



Vítima

RNP

TLP: CLEAR

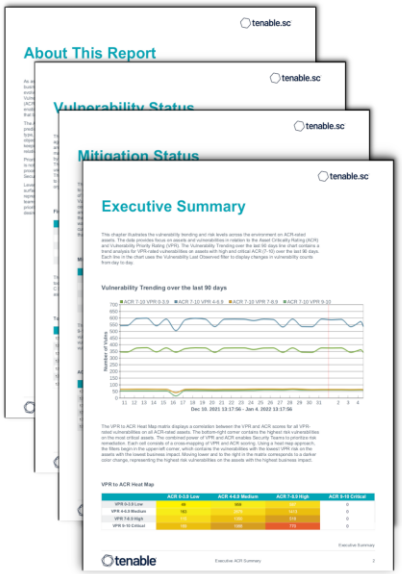
Como as vulnerabilidades afetam os clientes ?

Fontes: https://www.thesslstore.com/blog/facebook-data-leak-cambridge-analytica/
https://www.watchguard.com/br/wgrd-news/blog/o-ransomware-e-implacavel-o-que-voce-pode-fazer-para-se-proteger-contra-ele

RNP

TLP: CLEAR

Processo atual utilizado pelos clientes para validar vulnerabilidades




```
Prezados,

Foram identificados servidores NTP vulneráveis que podem ser utilizados em ataques de negação de serviço (DDoS).

Os servidores abaixo estão respondendo consultas NTP Mode 6 para READVAR, consultas desse tipo podem retornar
dados como: Versão do NTP, Versão do sistema operacional entre outros.
O CAIS recomenda que ao menos uma das soluções abaixo sejam executadas para proteger seu servidor NTP contra ataques desse tipo.

• Seguir as recomendações de Hardening do Team-Cymru para evitar consultas públicas do tipo READVAR
  https://www.team-cymru.com/secure-ntp-template.html


Para verificar se o seu servidor está vulnerável, execute as rotinas abaixo:

1 - Instalar o NTPQ em uma máquina fora da sua rede
  - Executar a consulta READVAR
    # ntpq -c rv  "IP"

2 - Instalar o NMAP
 - Executar o comando abaixo:
sudo nmap -sU -p 123 --script ntp-info "IP"
```

```
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       https://www.cais.rnp.br/             #
# Tel. 019-37873300      Fax. 019-37873301                    #
# Chave PGP disponivel   https://www.cais.rnp.br/cais-pgp.key #
#############################################################

-------------------------------------------------------------------------------
Data e hora UTC(+0),IP Vulnerável,Porta Origem,Protocolo,Hostname Origem,ASN, Sistema Operacional,Versao NTP, RefID
2024-08-10 14:34:26, [redacted] 123, udp,-, 1916, -, -,-
```

RNP

TLP: CLEAR

Expectativa sobre o novo processo

- Desenvolver uma plataforma integrada que agregue e permita a execução de testes de vulnerabilidades para os clientes;

- Simplificar as tarefas do analista de segurança, reduzindo o tempo de busca por ferramentas de segurança;

- Apoiar o encerramento dos tickets de notificação de vulnerabilidades pelas instituições;

- Tornar o ambiente dos clientes do sistema RNP mais seguros.

RNP

Ambiente

Ambiente **Vulnerável**

- 200.130.38.132

Sala no Discord

Ambiente **Estável**

- 200.130.38.130

Rede Wi-Fi

RNP

TLP: CLEAR

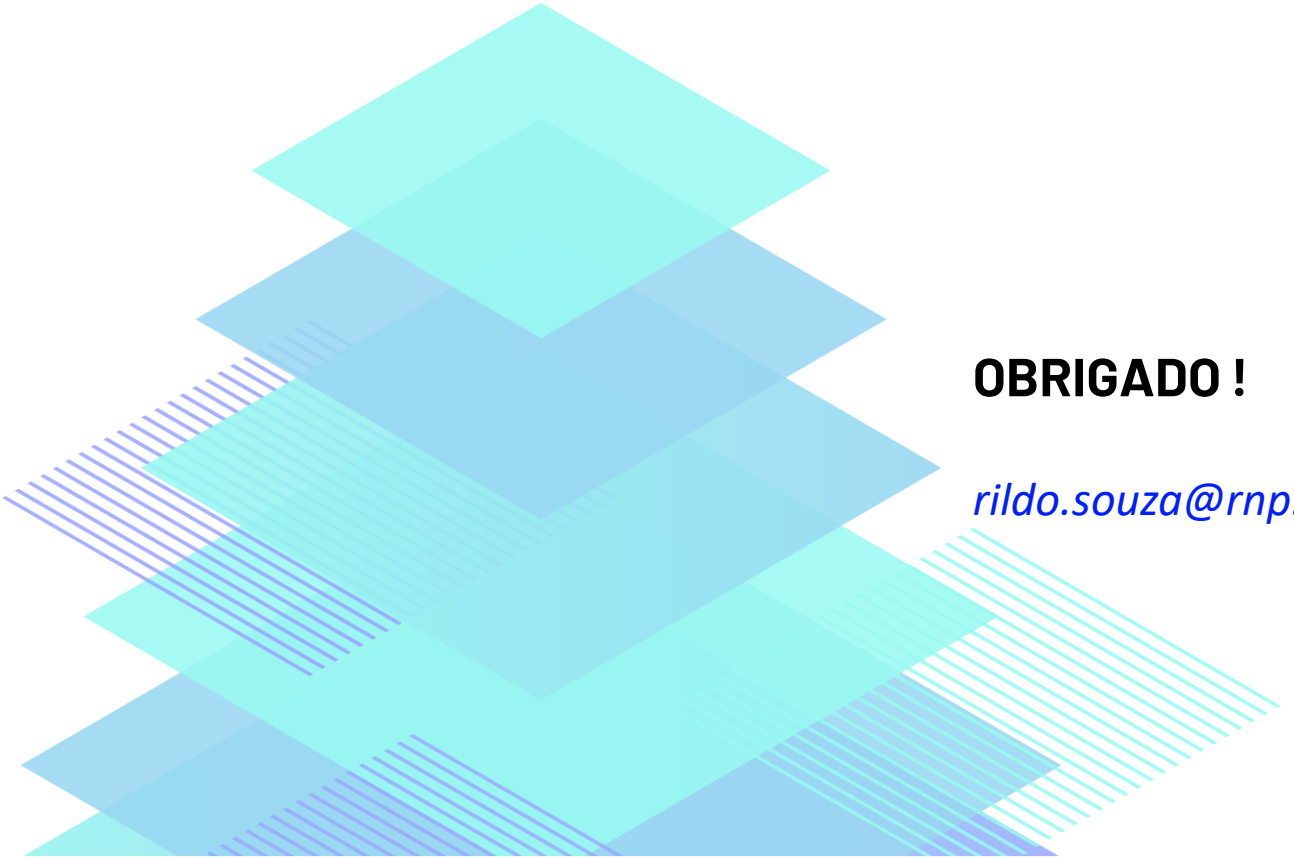
Ambiente: Portas Abertas e Serviços

- 53 UDP – DNS
- 123 UDP – NTP
- 137 UDP – NetBIOS
- 161 UDP – SNMP
- 445 TCP – SMB
- 3306 TCP - MySQL
- 6379 TCP – Redis
- 1900 UDP – SSDP
- 11211 TCP/UDP – Memcached
- 427 TCP/UDP - SLP

RNP

Fonte:https://www.linkedin.com/pulse/art-asking-questions-bala-pitchandi

TLP: CLEAR



OBRIGADO !

rildo.souza@rnp.br