GTS 2012

Efeitos do ataque LOIC.

Eduardo Bergmann

Roteiro

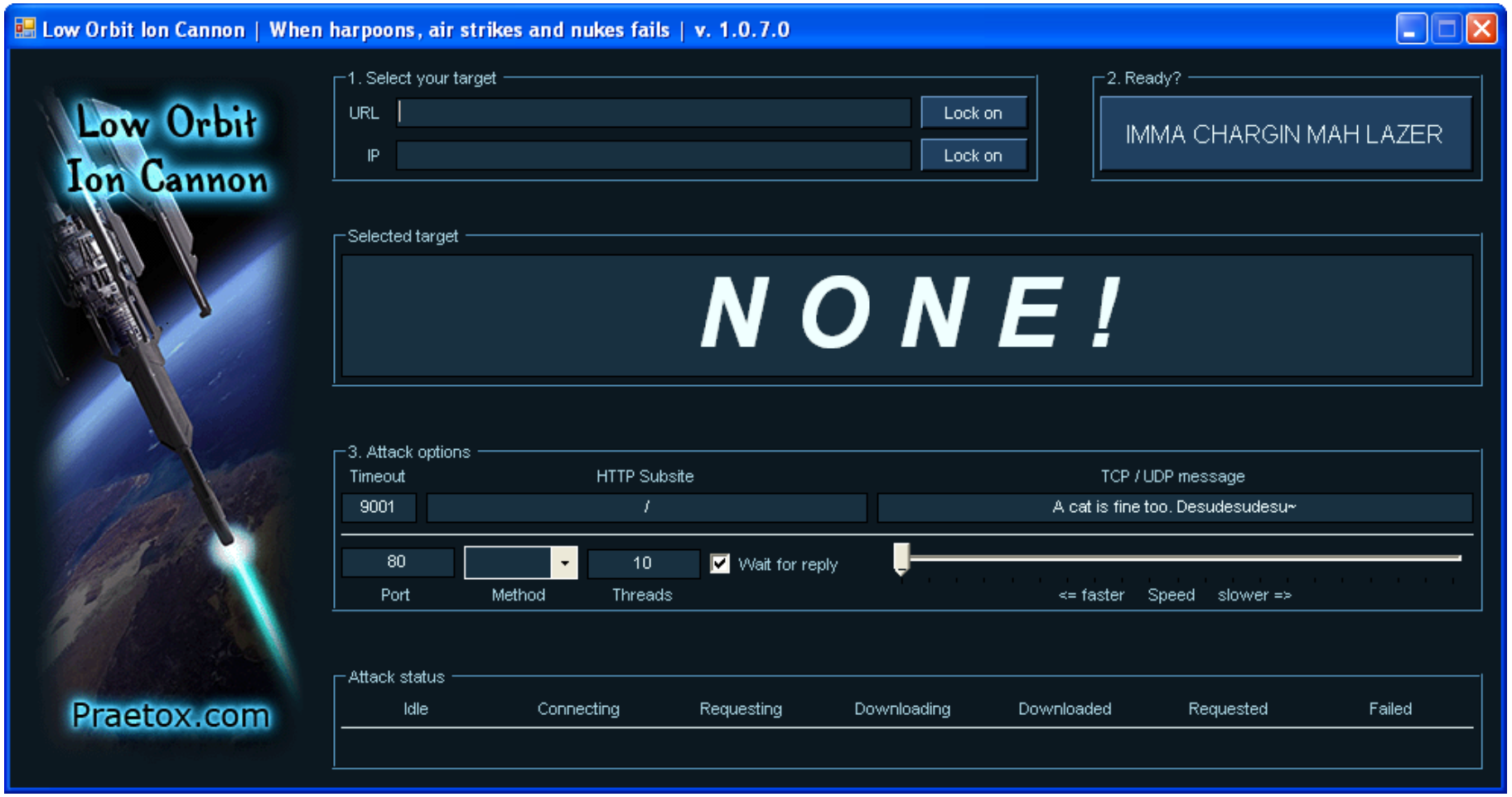
- LOIC: Definição, participação e ferramentas
- Cenário de testes
- Metodologia
- Resultados
- Prevenção
- Conclusão

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

LOIC: Low Orbit Ion Cannon

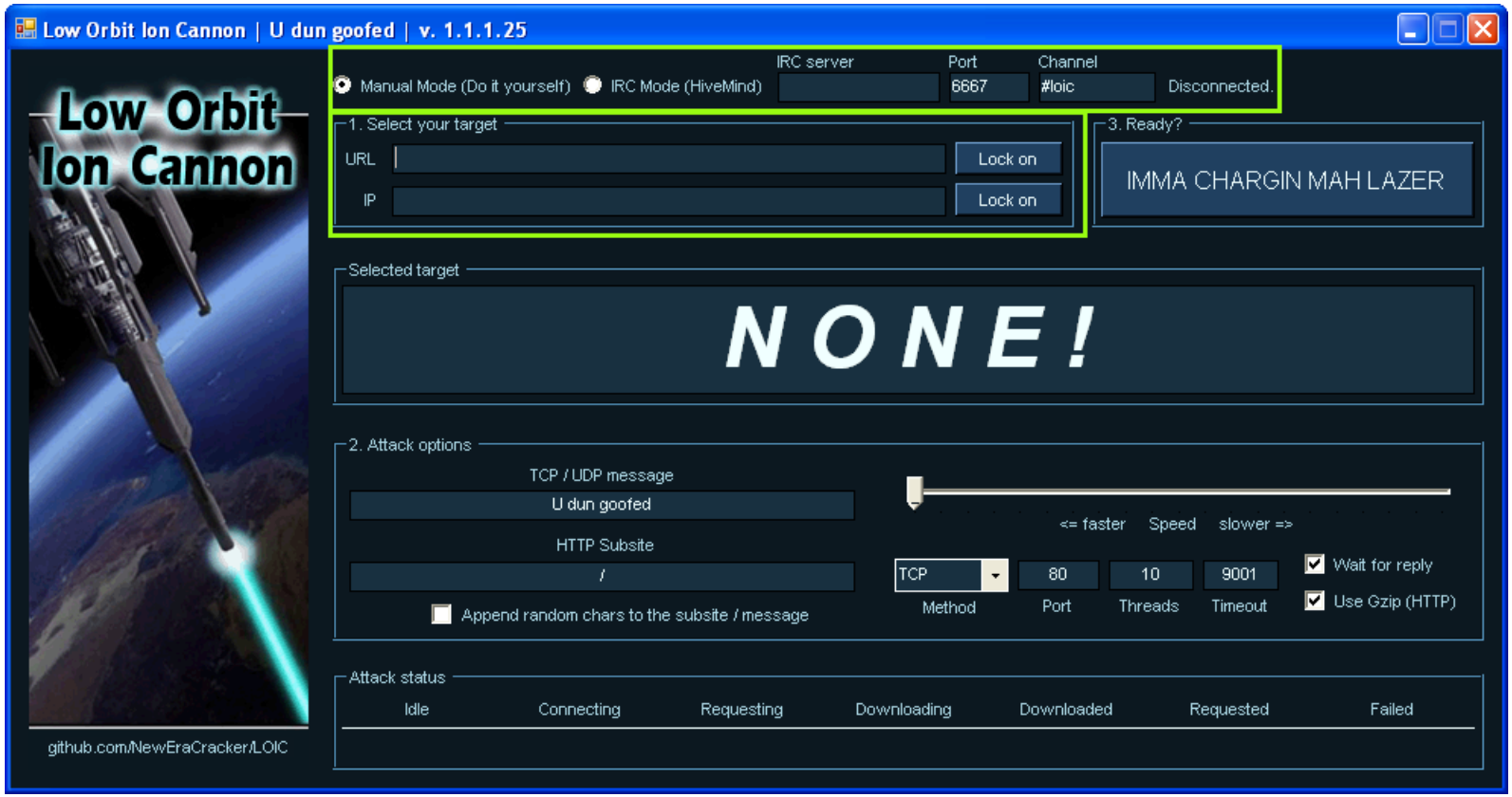
- Desenvolvida pela Praetox Technologies
- Ferramenta de teste de carga
- TCP(Transmission Control Protocol),
- UDP (User Datagram Protocol)
- HTTP (HyperText Transfer Protocol)
- Disponível em: http://sourceforge.net/projects/loic/



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERTRS
Computer Emergency Team - Rio Grande do Sul

Funcionamento



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT.RS
Computer Emergency Team - Rio Grande do Sul

Funcionamento via canal IRC

- Iniciar ataque:

!lazor targetip=<IRC_server> message=<texto> port=80 method=http wait=false threads=15 method=tcp random=true start

- Finalizar ataque:

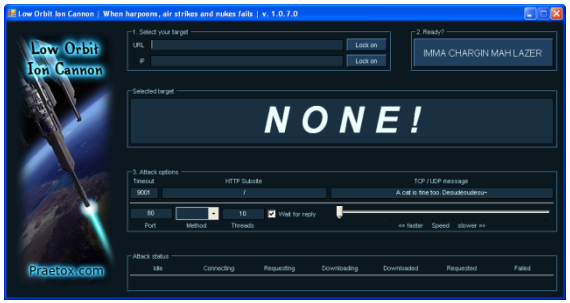
!lazor stop

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

Implementações

Windows
Linux
BSD



Android

Web
(JavaScript)

PoP-RS
Ponto de Presença da
RNP no Rio Grande do Sul

CERTRS
Computer Emergency Team - Rio Grande do Sul

Participação consciente

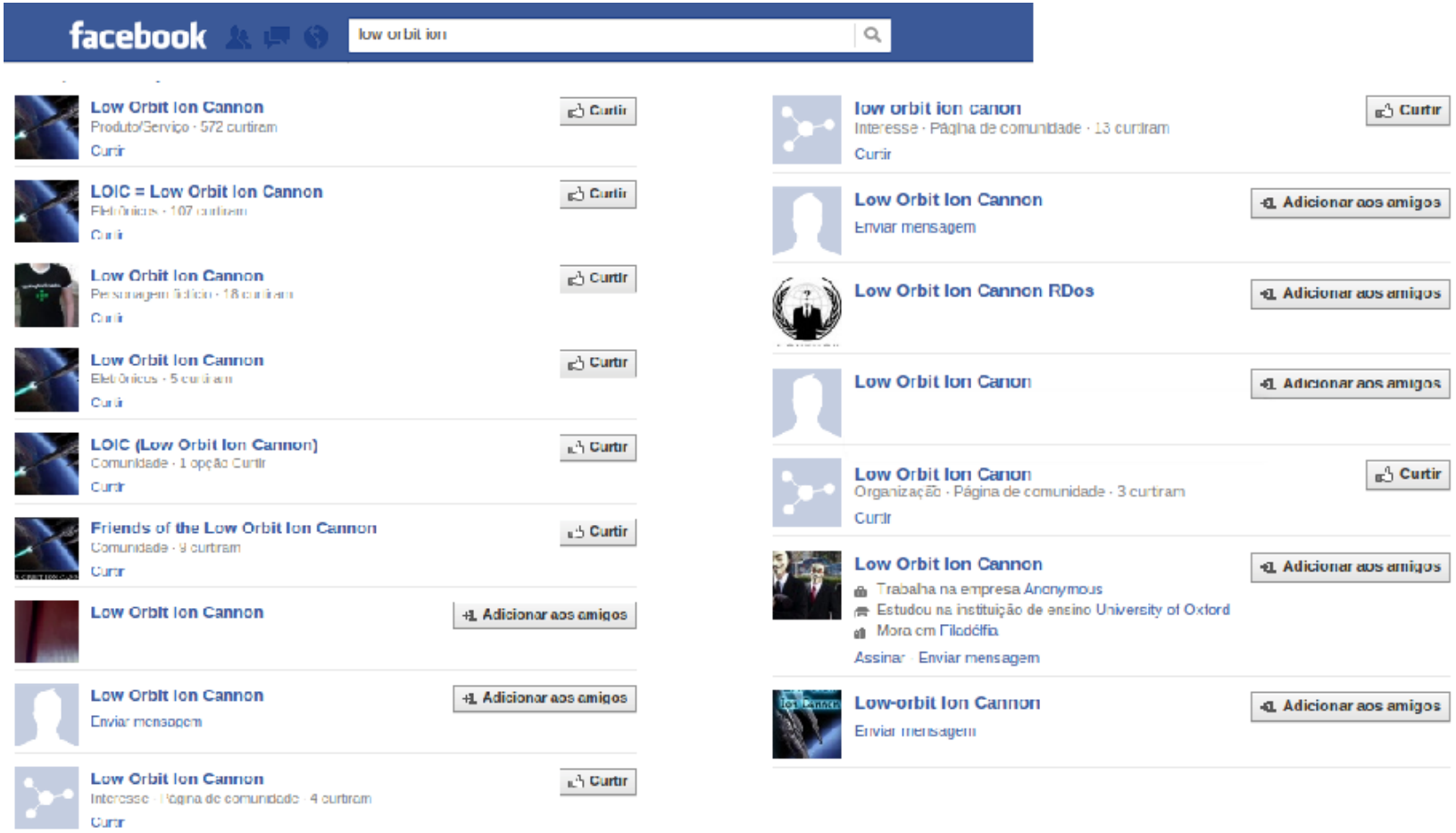
- Downloads:
  1. Estados Unidos
  2. França
  3. Brasil
  4. Alemanha ...

http://sourceforge.net/projects/loic/ em 26 de abril de 2012

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERTRS
Computer Emergency Team - Rio Grande do Sul

Popular e acessível



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

Agendamento de ataque

```
1.  Twitter - @AnonymousWiki
2.
3.
4.  January 19th, 2012
5.
6.  Popular file-sharing website megaupload.com gets shutdown by U.S Justice - FBI and charged its founder
    with violating piracy laws. Four Megaupload members were also arrested. The FBI released a press release
    on its website which you can view here:
7.  http://www.fbi.gov/news/pressrel/press-releases/justice-department-charges-leaders-of-megaupload-
    with-widespread-online-copyright-infringement
8.
9.  We Anonymous are launching our largest attack ever on government and music industry sites. Lulz. The FBI
    didn't think they would get away with this did they? They should have expected us.
10.
11.
12.
13. #OpMegaupload
14. The following sites were taken down in response to the FBI shutting down megaupload.com
15. :) TANGO DOWN
```

http://pastebin.com/WEydcBVV em 26 de abril de 2012

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

Receberam ataques

- FBI
- MPAA – Motion Picture Association of America
- Departament of Justice
- RIAA – Recording Industry Association of America
- Sony
- Visa
- MasterCard
- Paypal

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

Cenário dos testes

Servidor atacado:

- Core 2 Duo 2.2 Ghz
- 2 Gb RAM
- Ubuntu 10.04
- Apache 2.2
- Conectado a um switch ethernet 100 Mbps

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

Cenário dos testes

PC

Core 2 Duo 2.2 Ghz

2 GB RAM

iPad 2

Dual-core Apple A5X

512 MB RAM

Galaxy SII

Dual-core 1.2 GHz Cortex-A9

1 GB RAM

Motorola Defy

800 MHz Cortex-A8

512 MB RAM

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERTRS
Computer Emergency Team - Rio Grande do Sul

Cenário dos testes

Ferramentas de ataque

PC

LOIC
JSLOIC

iPad 2

JSLOIC

Galaxy SII

JSLOIC
Android LOIC

Motorola Defy

JSLOIC
Android LOIC

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

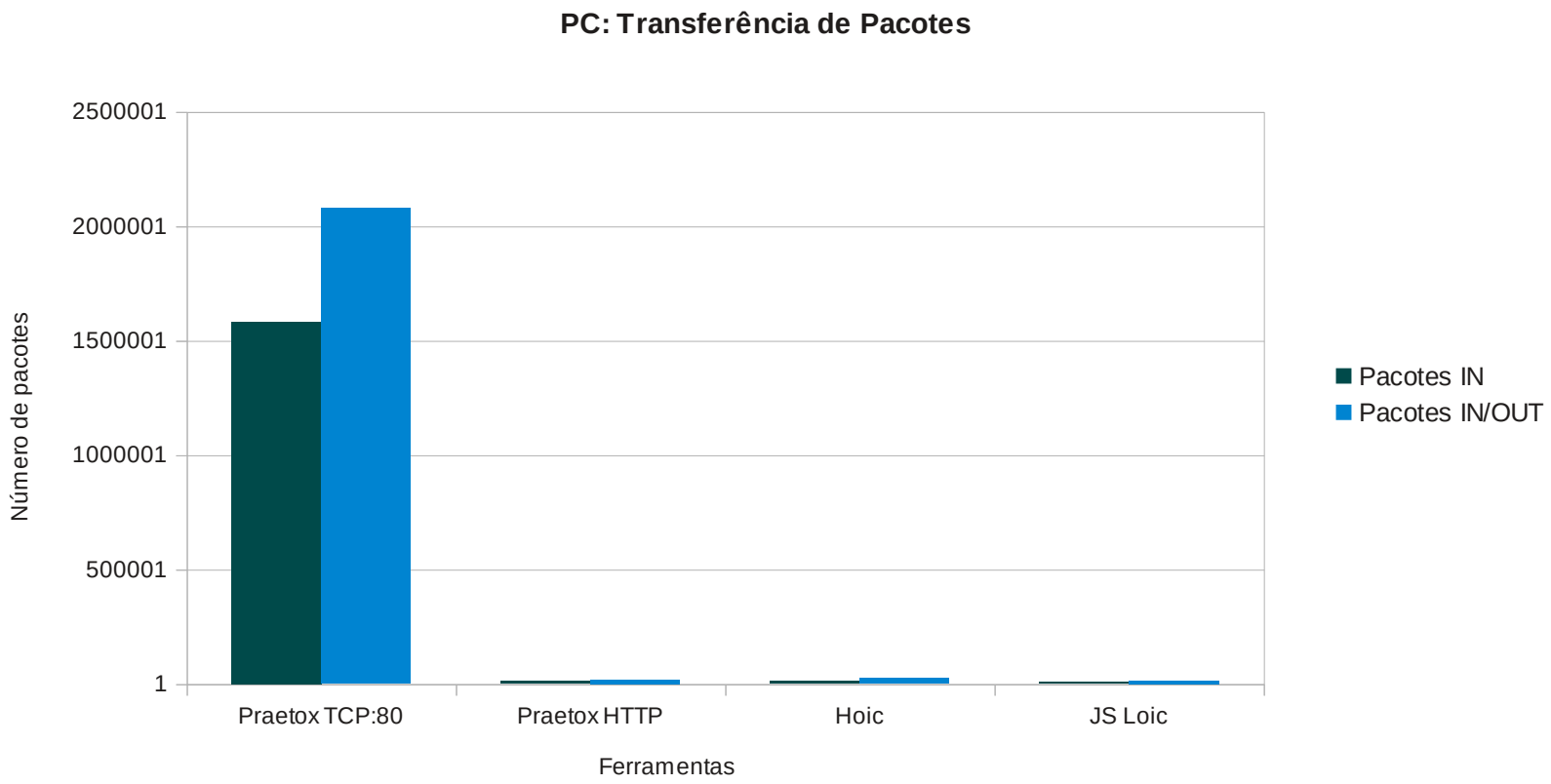
Metodologia

- Ataques de trinta segundos por dispositivo.
- Dados coletados:
  - Pacotes por segundo
  - Bytes por segundo
  - Consumo de CPU servidor
  - Consumo de memória do servidor

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

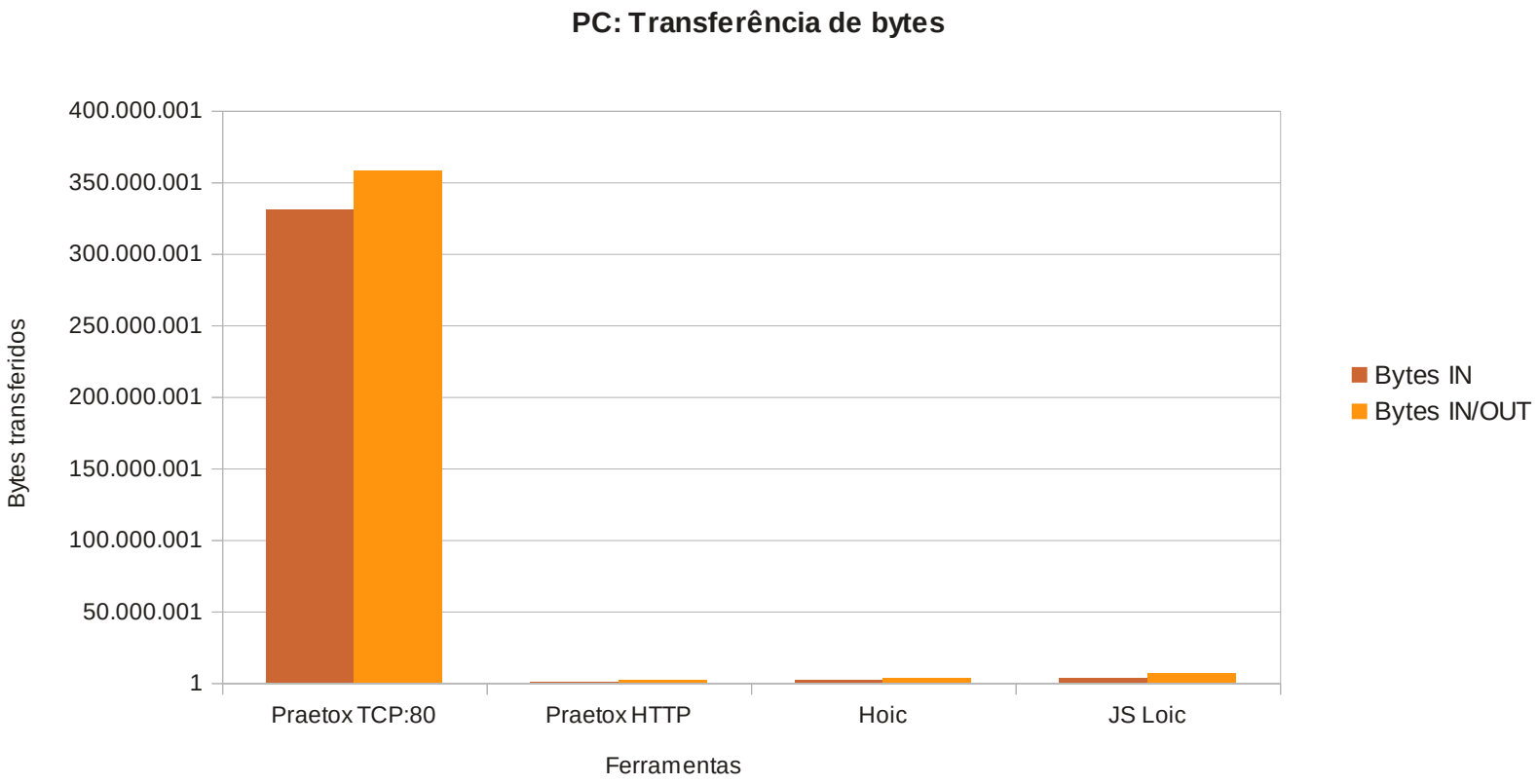
Resultado - PC



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

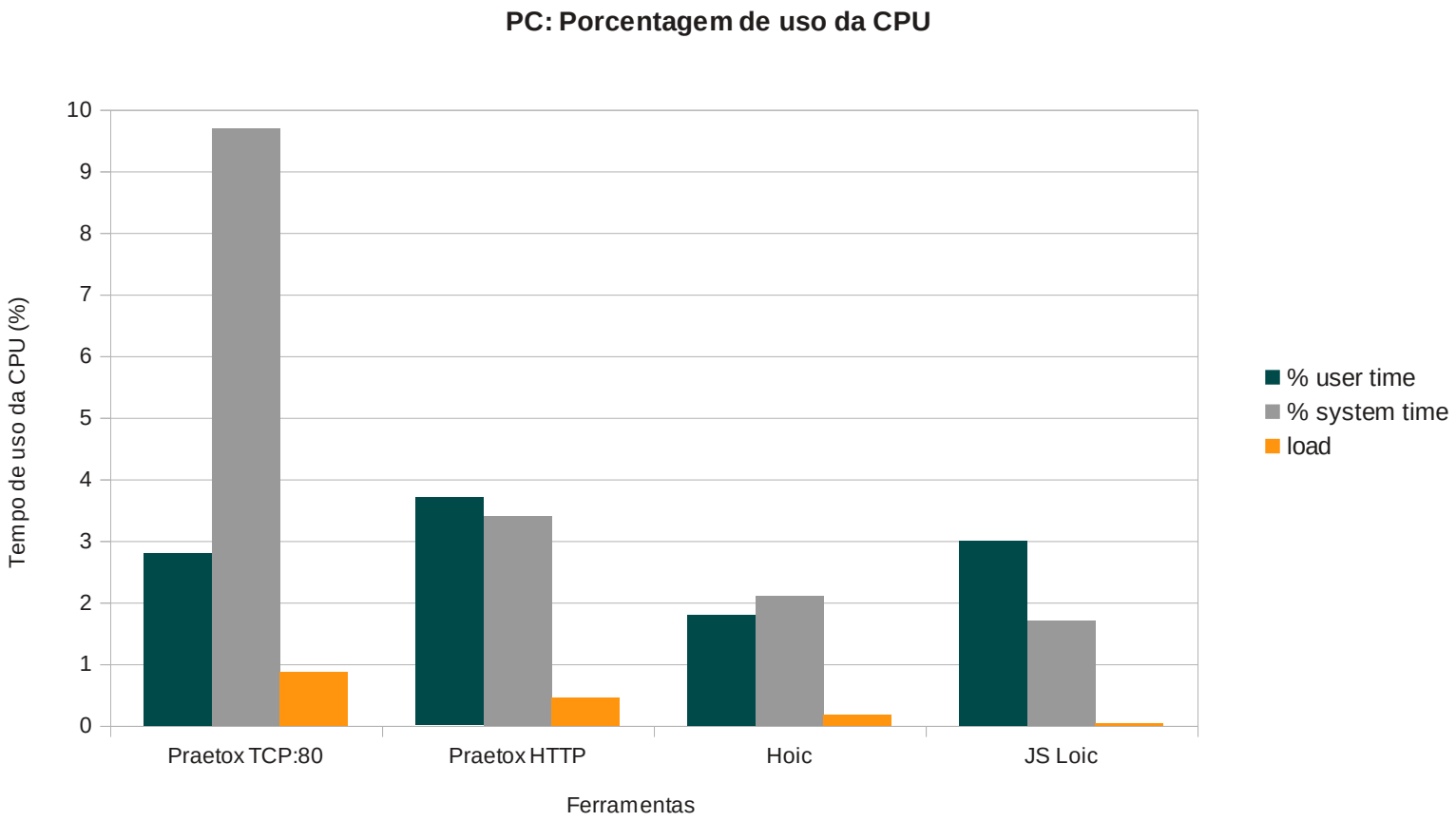
Resultado – PC



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

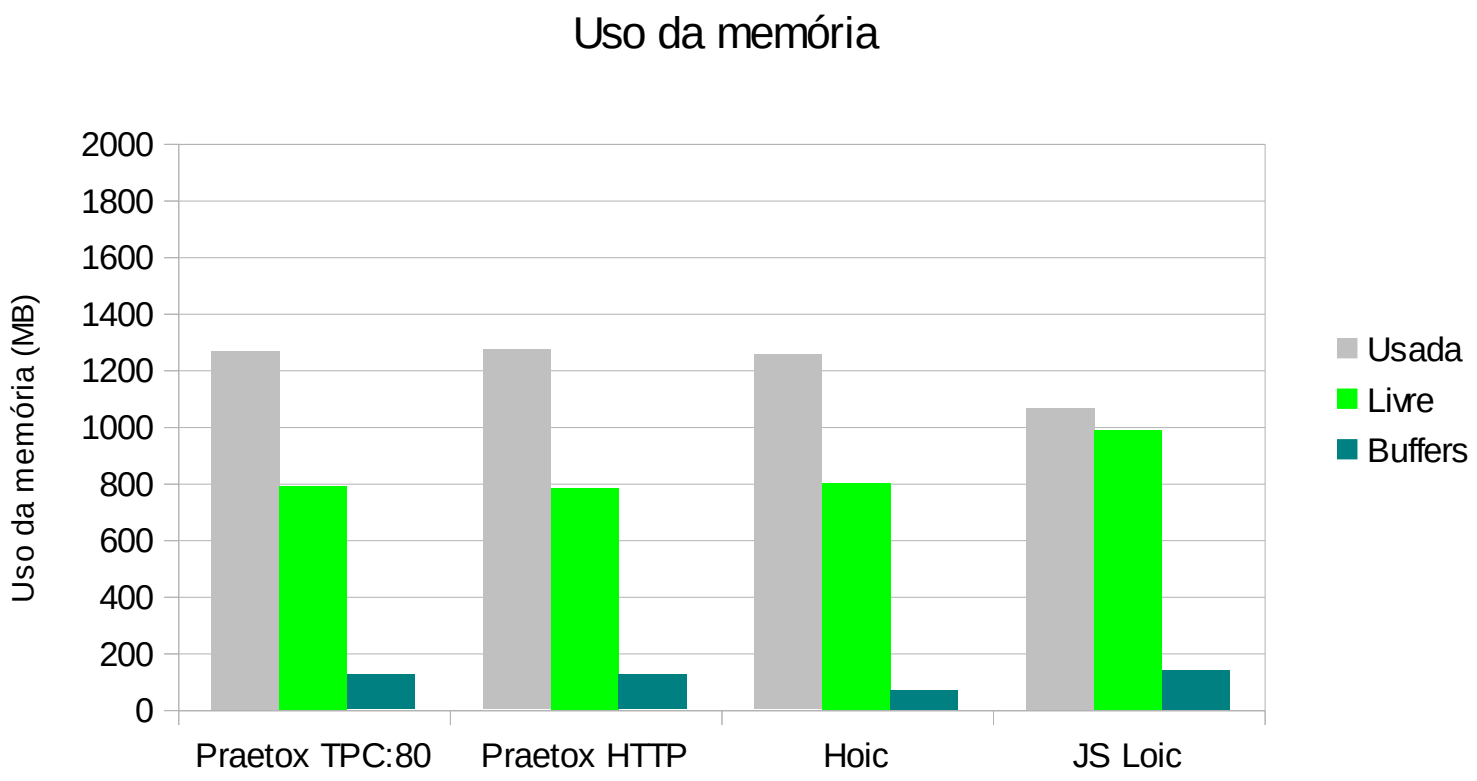
Resultado – PC



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

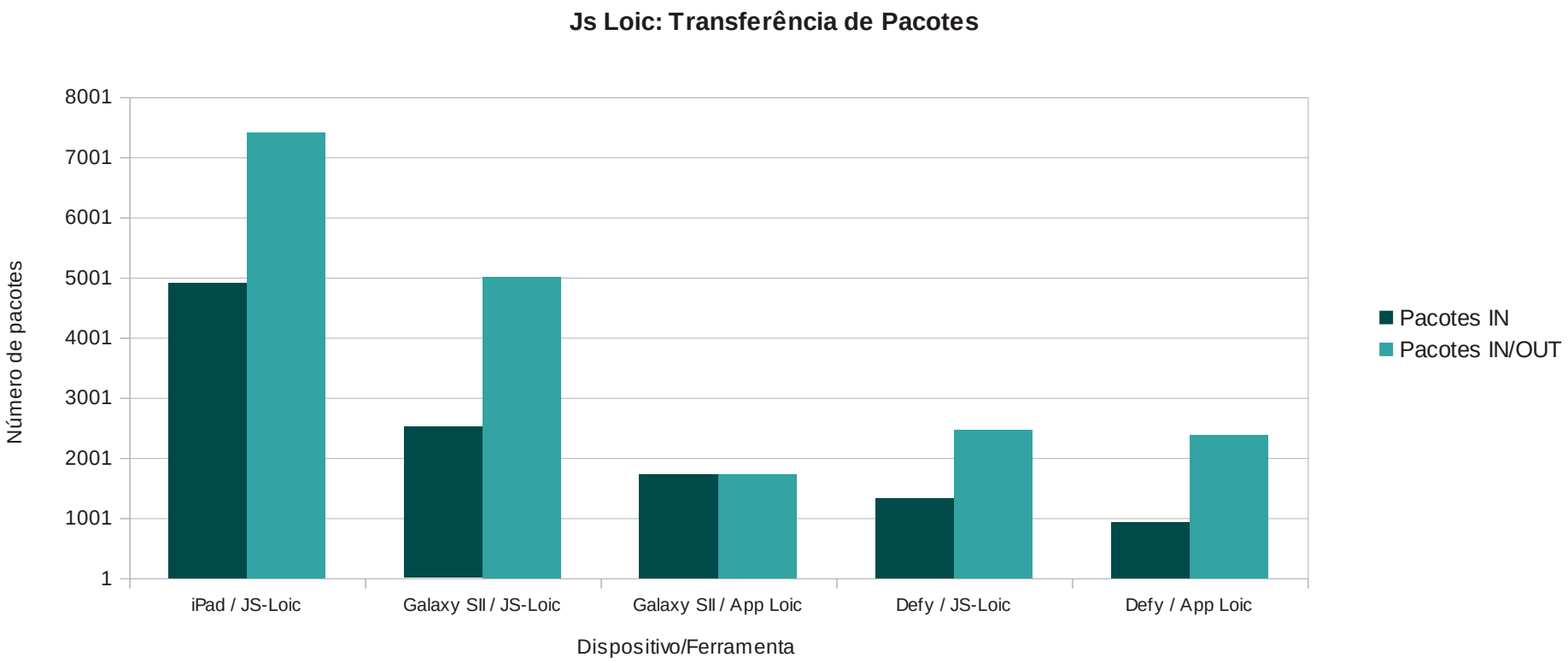
Resultado – PC



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

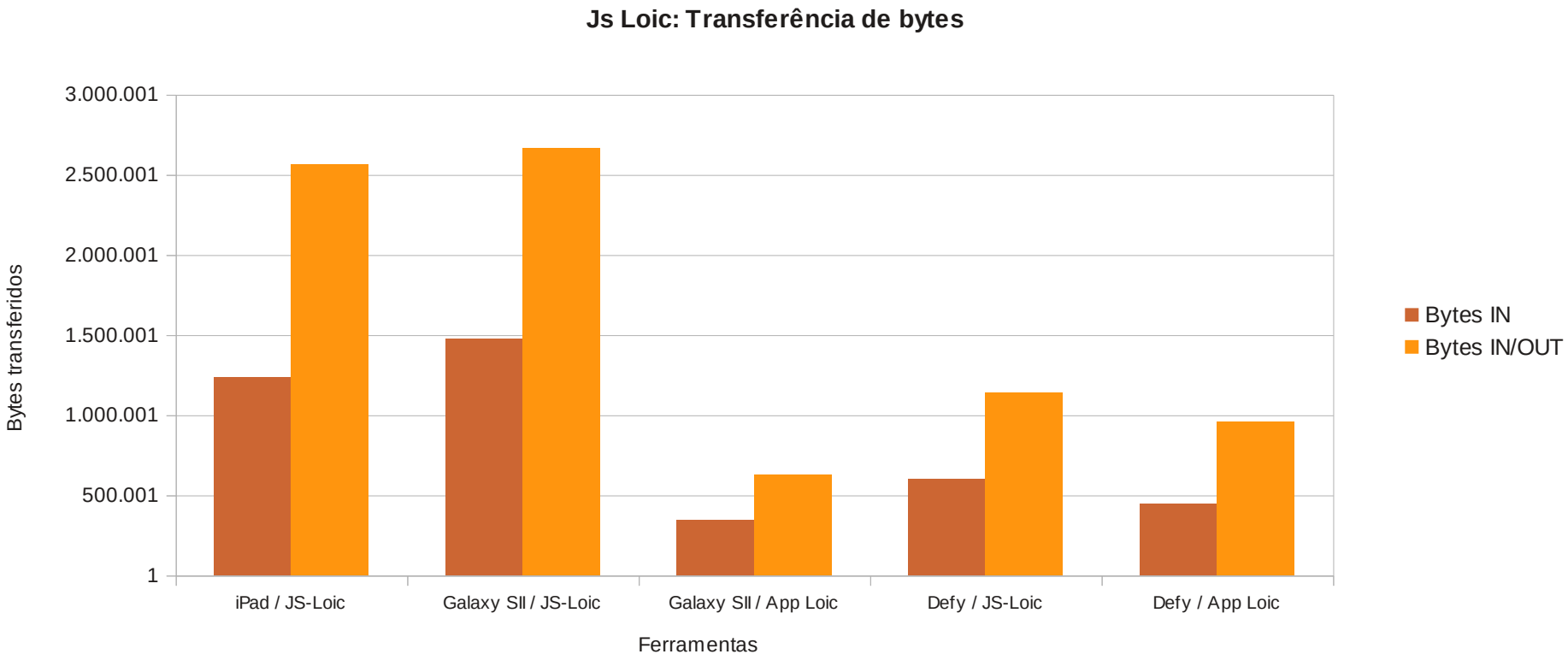
Resultado – Dispositivos móveis



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

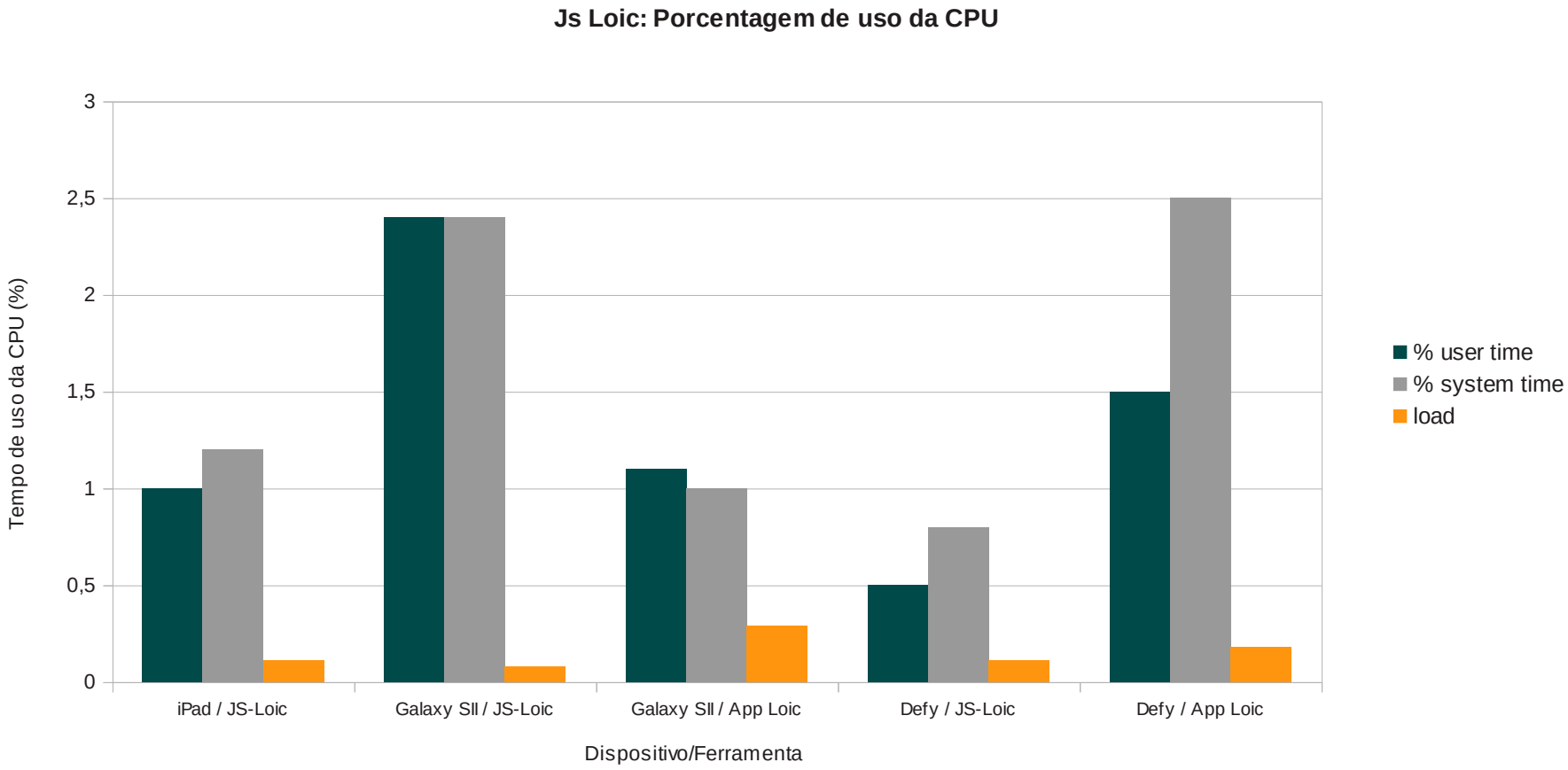
Resultado – Dispositivos móveis



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

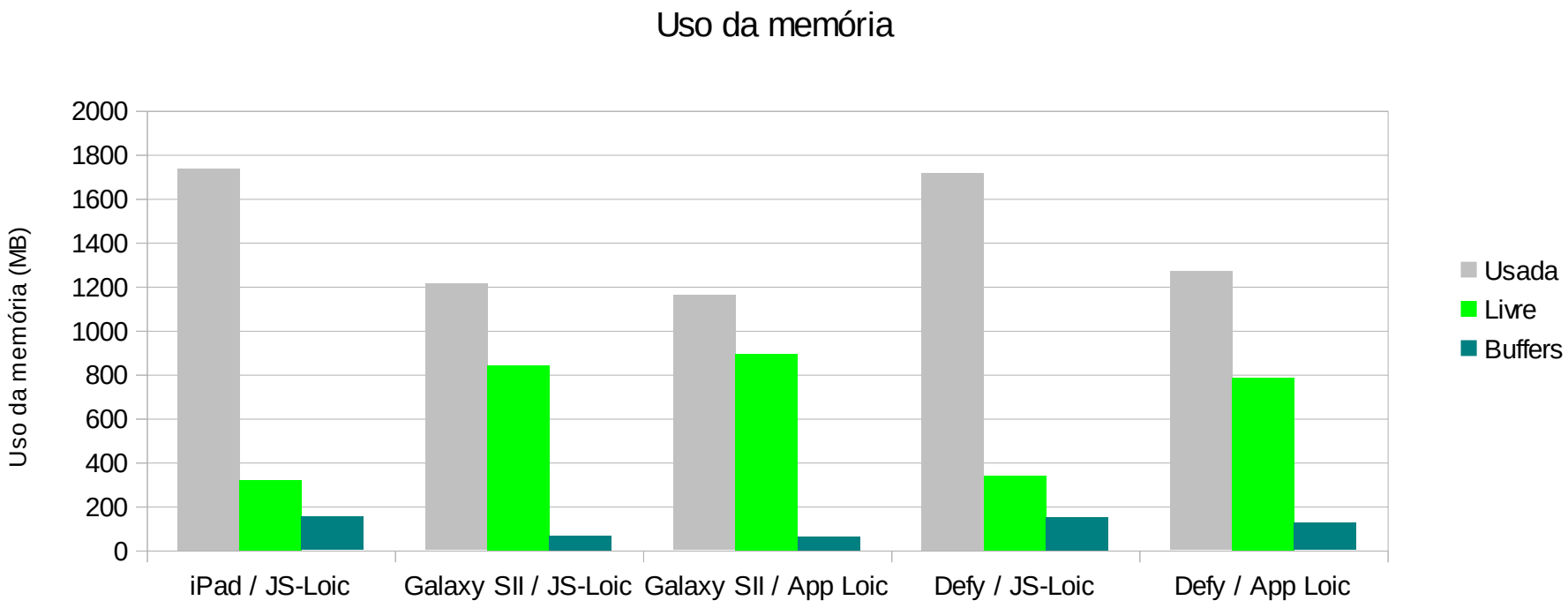
Resultado – Dispositivos móveis



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

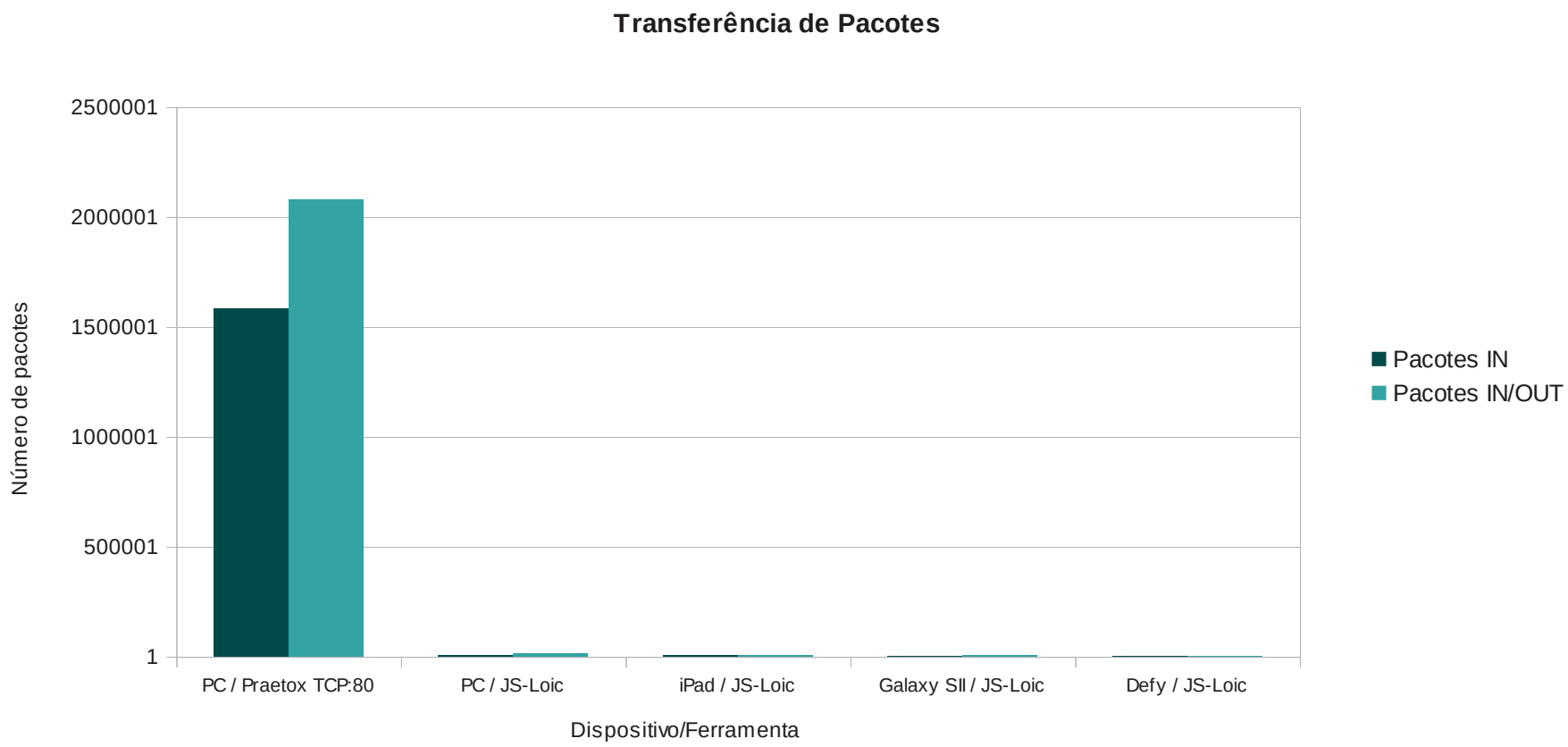
Resultado – Dispositivos móveis



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

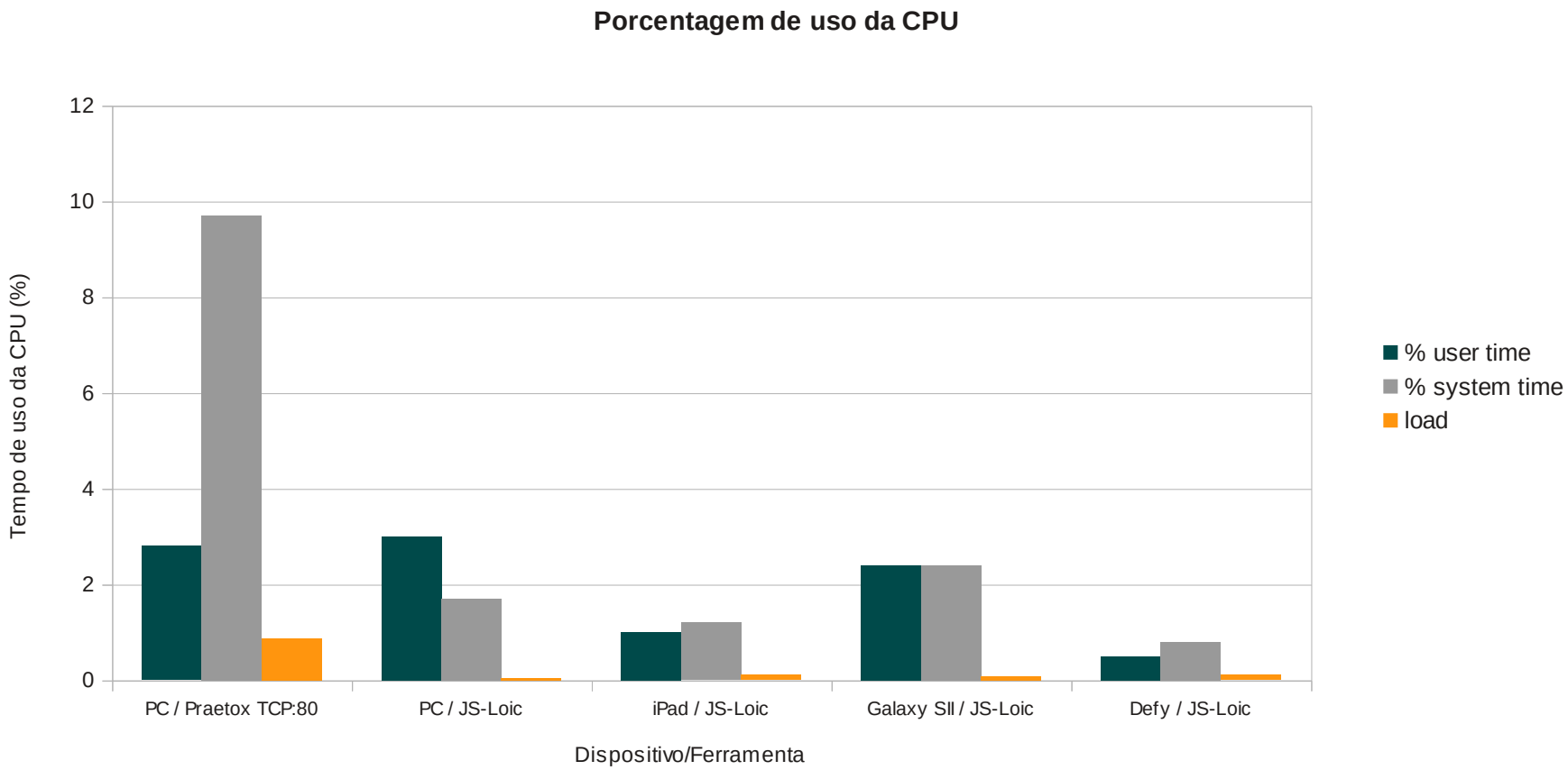
Resultado – Comparativo geral



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

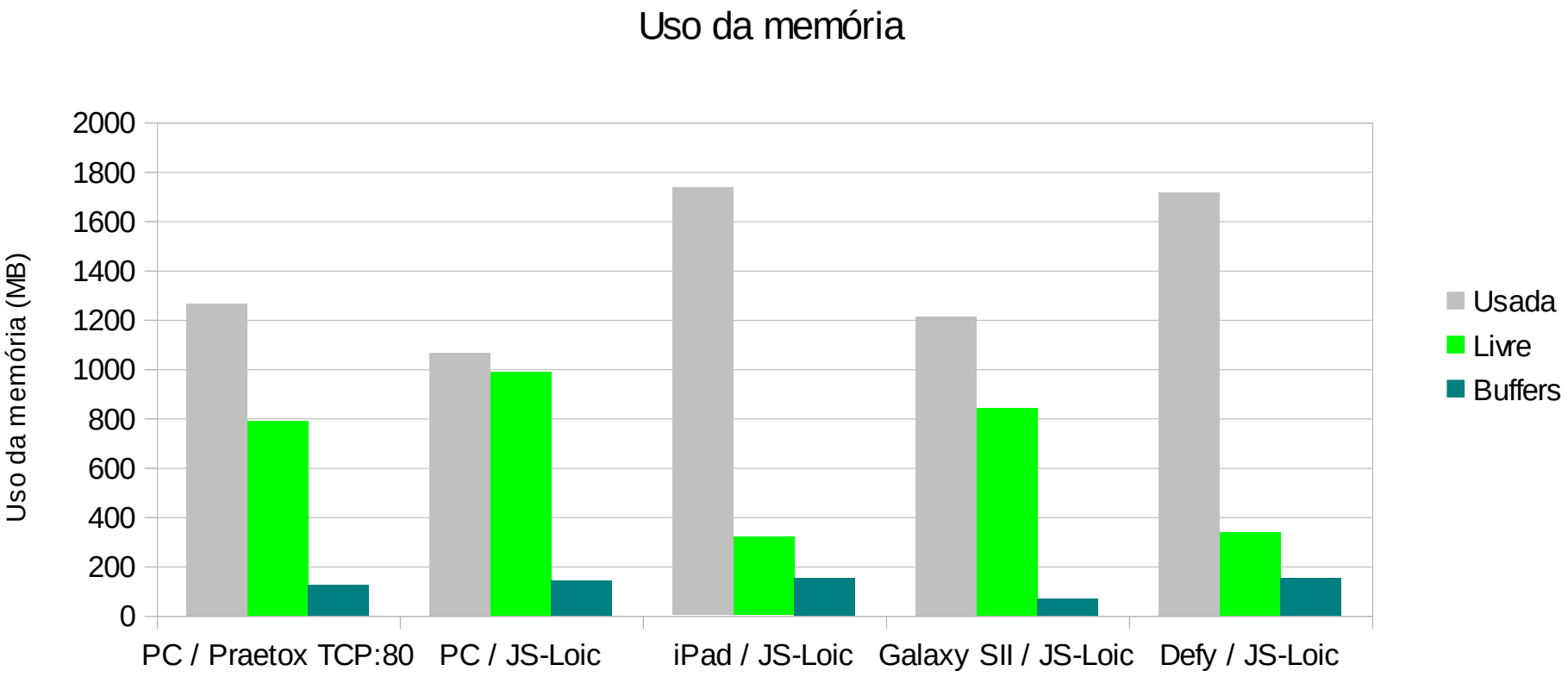
Resultado – Comparativo geral



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

Resultado – Comparativo geral

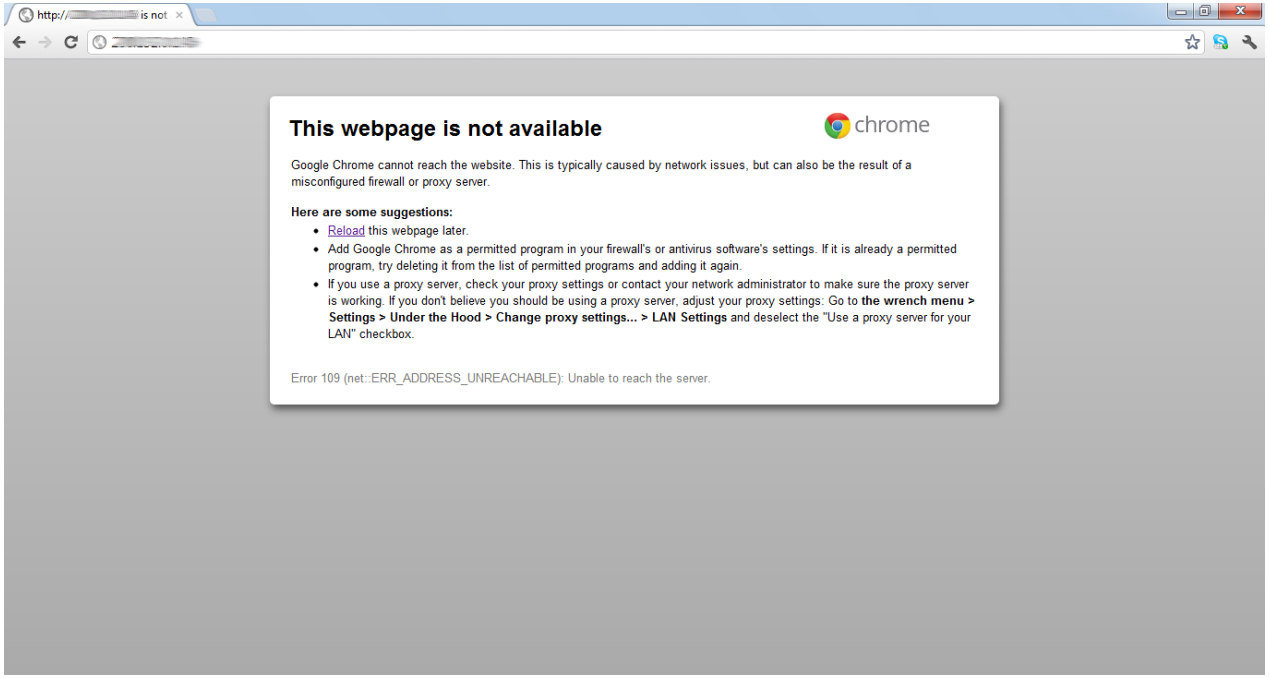


PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

Resultado – Apache

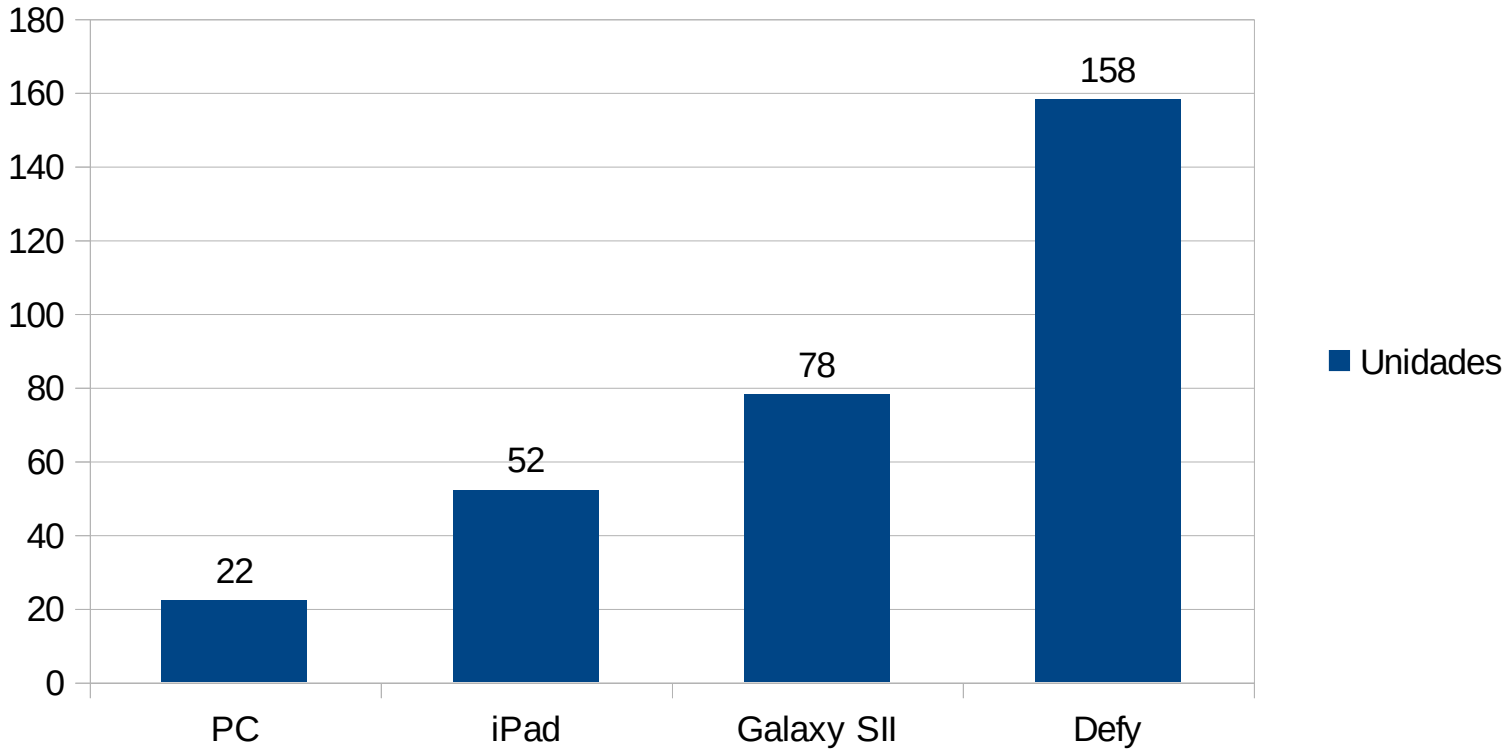
Tango Down



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERTRS
Computer Emergency Team - Rio Grande do Sul

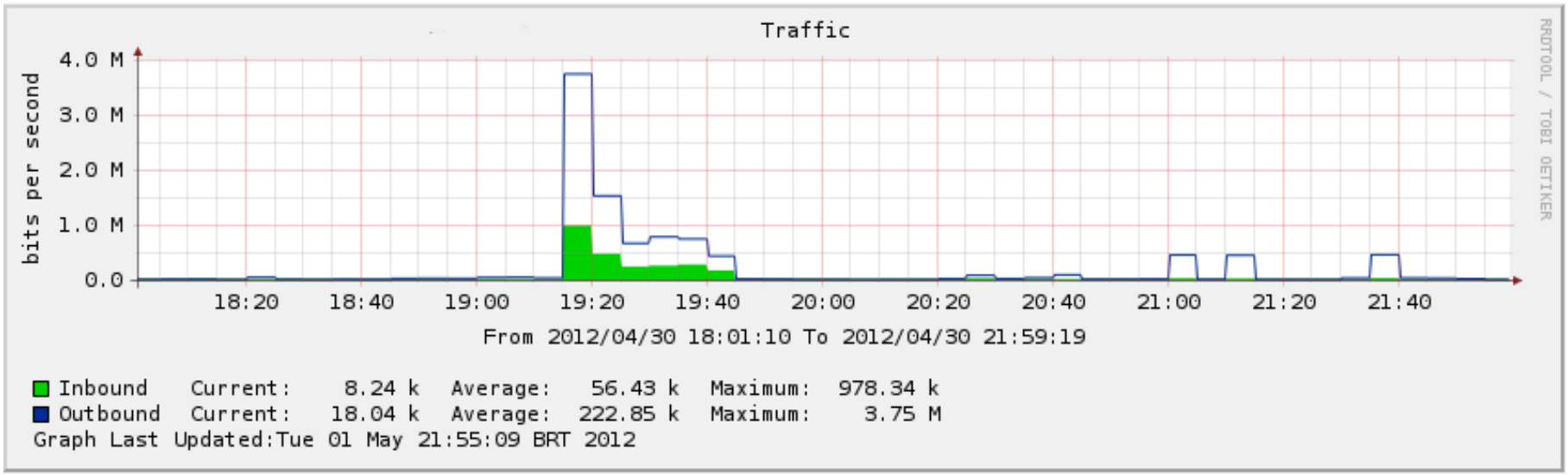
Resultado – Apache



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

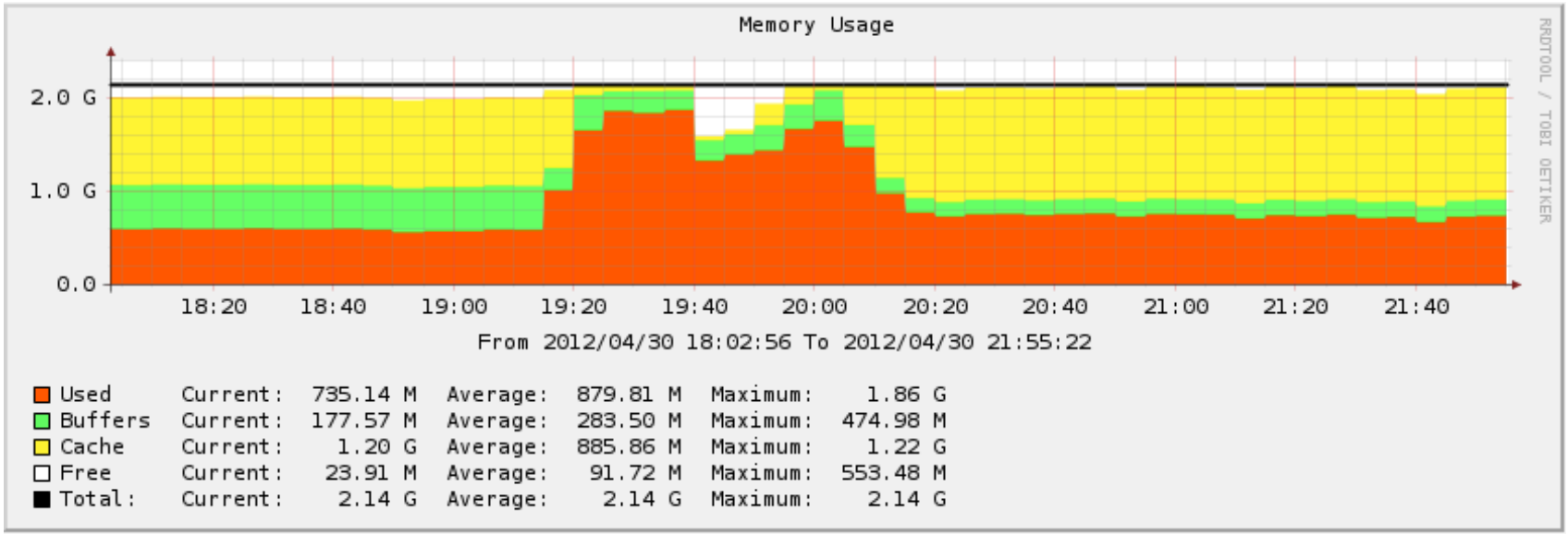
Resultado – Apache



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT.RS
Computer Emergency Team - Rio Grande do Sul

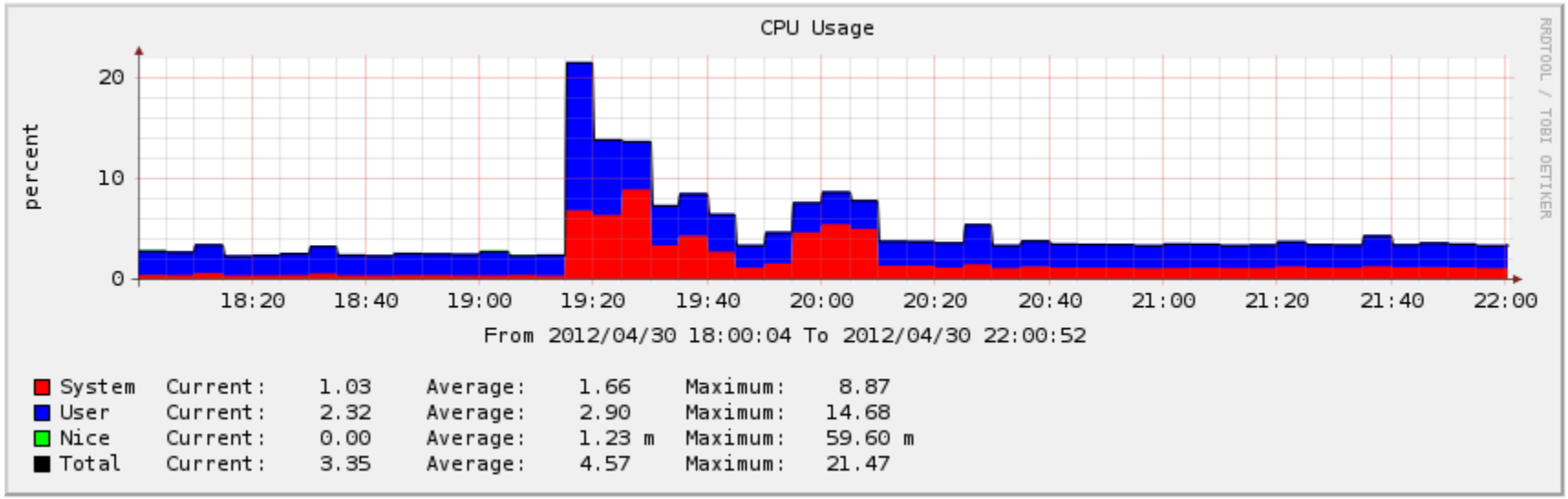
Resultado – Apache



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

Resultado – Apache



PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

Prevenção

- Snort como NIDS (Network Intrusion and Detection System)

TCP

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"SLR - LOIC DoS Tool(TCP Mode) - Behavior Rule (tracking/threshold)";
flow: established,to_server;
flags:A;
dsize:1448<>1448;
threshold: type threshold, track by_src, count 10 , seconds 10;
```

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

Prevenção

HTTP

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"SLR - LOIC DoS Tool (HTTP Mode)";
flow: established,to_server;
content:"|A cat is fine too. Desudesudesu~|";
threshold: type threshold, track by_src, count 10 , seconds 10;
```

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

Referências

Attacks by “Anonymous” WikiLeaks Proponents
not Anonymous. http://eprints.eemcs.utwente.nl/19151/01/2010-12-CTIT-TR.pdf

Effectiveness of Defense Methods Against DDoS Attacks by Anonymous
http://referaat.cs.utwente.nl/TSConIT/download.php?id=1085

DDoS: threats and mitigation
http://www.sciencedirect.com/science/article/pii/S1353485811701283

PoP-RS
Ponto de Presença da
RNP no Rio Grande do Sul

CERT RS
Computer Emergency Team - Rio Grande do Sul

Colaboradores

Bruno Lorensi
César Loureiro
Douglas Ritter
Eduardo Bergmann
João Ceron (CERT-BR)
Leando Bertholdo
Liane Tarouco
Lucas Arbiza

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

CERT-RS
Computer Emergency Team - Rio Grande do Sul

Perguntas?

eduardo@pop-rs.rnp.br