

GTS 2012

Efeitos do ataque LOIC.

Eduardo Bergmann



Roteiro

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



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/>





Low Orbit Ion Cannon



Praetox.com

1. Select your target

URL

IP

2. Ready?

IMMA CHARGIN MAH LAZER

Selected target

NONE!

3. Attack options

Timeout: HTTP Subsite: TCP / UDP message:

Port: Method: Threads: Wait for reply

<= faster Speed slower =>

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed



Funcionamento

Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.25

Manual Mode (Do it yourself) IRC Mode (HiveMind) IRC server Port Channel Disconnected.

1. Select your target

URL Lock on

IP Lock on

3. Ready?

IMMA CHARGIN MAH LAZER

Selected target

NONE!

2. Attack options

TCP / UDP message U dun goofed

HTTP Subsite /

Append random chars to the subsite / message

Method Port Threads Timeout

TCP 80 10 9001

Wait for reply Use Gzip (HTTP)

Attack status

Idle Connecting Requesting Downloading Downloaded Requested Failed

github.com/NewEraCracker/LOIC

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
```



Implementações

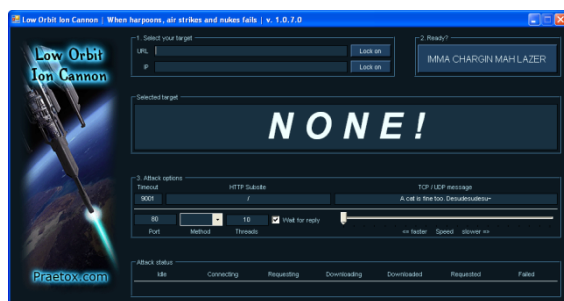
Windows

Linux

BSD

Android

Web
(JavaScript)



Participação consciente

- Downloads:

1. Estados Unidos

2. França

3. Brasil

4. Alemanha ...

👍 781 Recommendations

📄 10.491 Downloads (This Week)



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



Popular e acessível

The image shows a screenshot of a Facebook search results page for the query "low orbit ion". The page is divided into two columns. The left column displays a list of search results, each with a profile picture, name, description, and a "Curtir" (Like) button. The right column displays a list of search results, each with a profile picture, name, description, and either a "Curtir" button or an "Adicionar aos amigos" (Add friend) button.

facebook low orbit ion

Low Orbit Ion Cannon
Produto/Serviço · 572 curtiram
Curtir

LOIC = Low Orbit Ion Cannon
Eletrônicos · 107 curtiram
Curtir

Low Orbit Ion Cannon
Personagem fictício · 18 curtiram
Curtir

Low Orbit Ion Cannon
Eletrônicos · 5 curtiram
Curtir

LOIC (Low Orbit Ion Cannon)
Comunidade · 1 opção Curtir
Curtir

Friends of the Low Orbit Ion Cannon
Comunidade · 9 curtiram
Curtir

Low Orbit Ion Cannon
Adicionar aos amigos

Low Orbit Ion Cannon
Enviar mensagem
Adicionar aos amigos

Low Orbit Ion Cannon
Interesse · Página de comunidade · 4 curtiram
Curtir

low orbit ion canon
Interesse · Página de comunidade · 13 curtiram
Curtir

Low Orbit Ion Cannon
Enviar mensagem
Adicionar aos amigos

Low Orbit Ion Cannon RDoS
Adicionar aos amigos

Low Orbit Ion Cannon
Adicionar aos amigos

Low Orbit Ion Cannon
Organização · Página de comunidade · 3 curtiram
Curtir

Low Orbit Ion Cannon
Trabalha na empresa Anonymous
Estudou na instituição de ensino University of Oxford
Mora em Filadélfia
Assinar · Enviar mensagem
Adicionar aos amigos

Low-orbit Ion Cannon
Enviar mensagem
Adicionar aos amigos

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



Receberam ataques

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



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



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



Cenário dos testes

Ferramentas de ataque



PC

LOIC
JSLOIC



iPad 2

JSLOIC



Galaxy SII

JSLOIC
Android LOIC



Motorola Defy

JSLOIC
Android LOIC



Metodologia

- Ataques de trinta segundos por dispositivo.

- Dados coletados:

 - Pacotes por segundo

 - Bytes por segundo

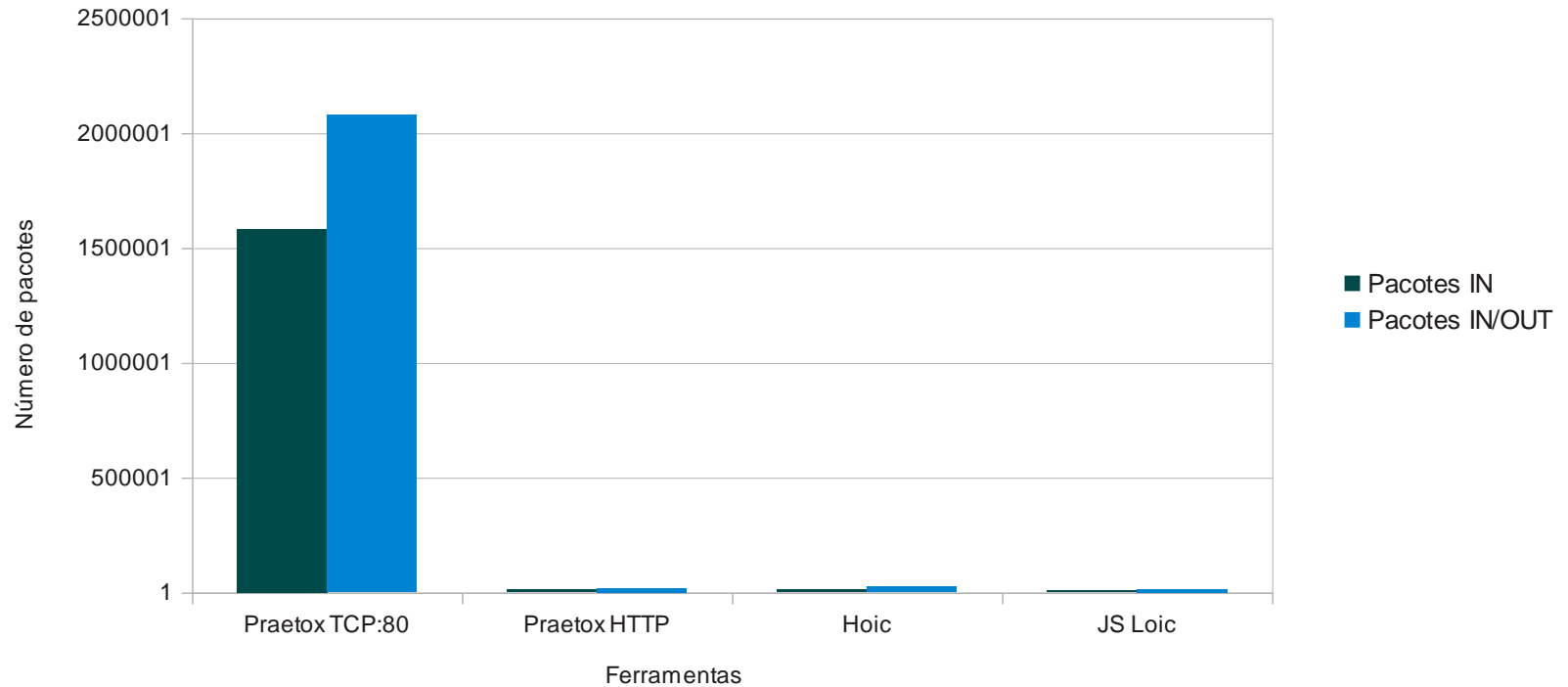
 - Consumo de CPU servidor

 - Consumo de memória do servidor



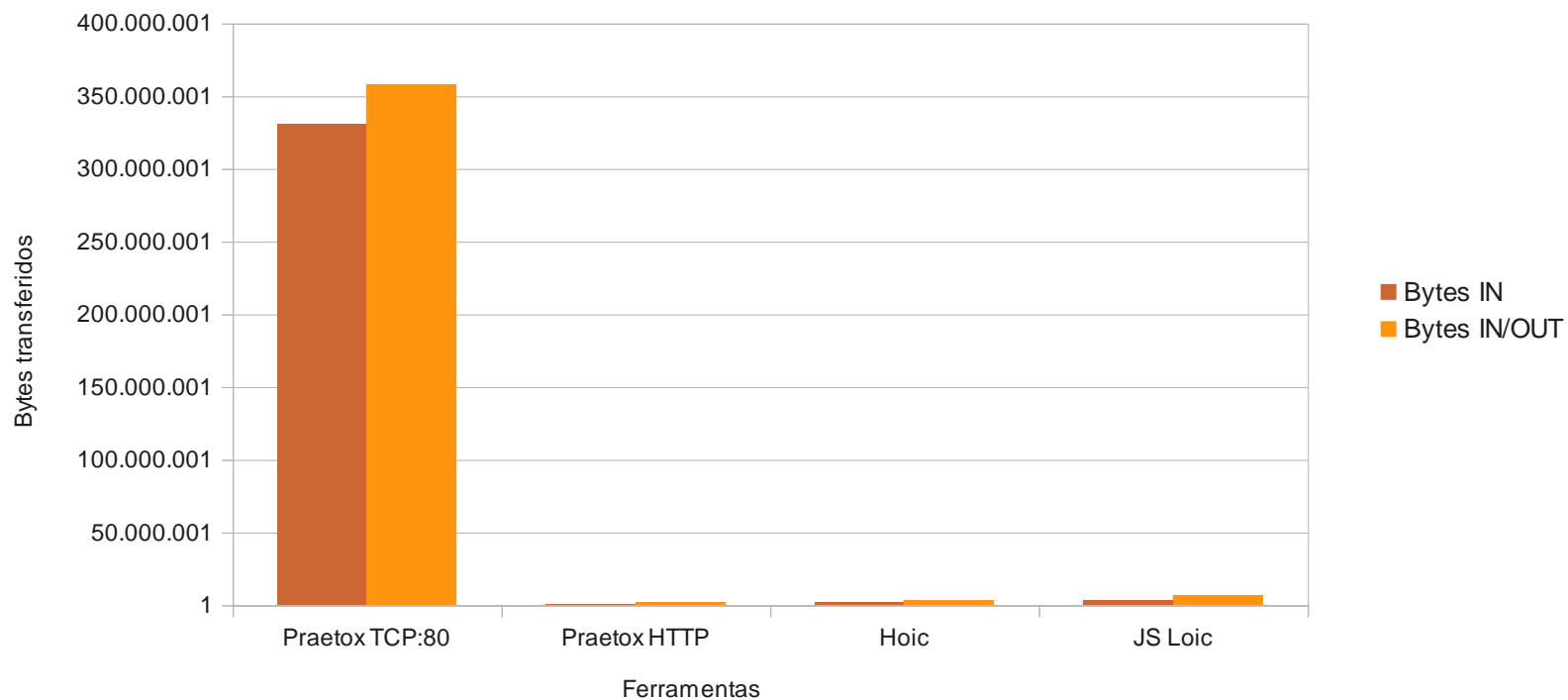
Resultado - PC

PC: Transferência de Pacotes



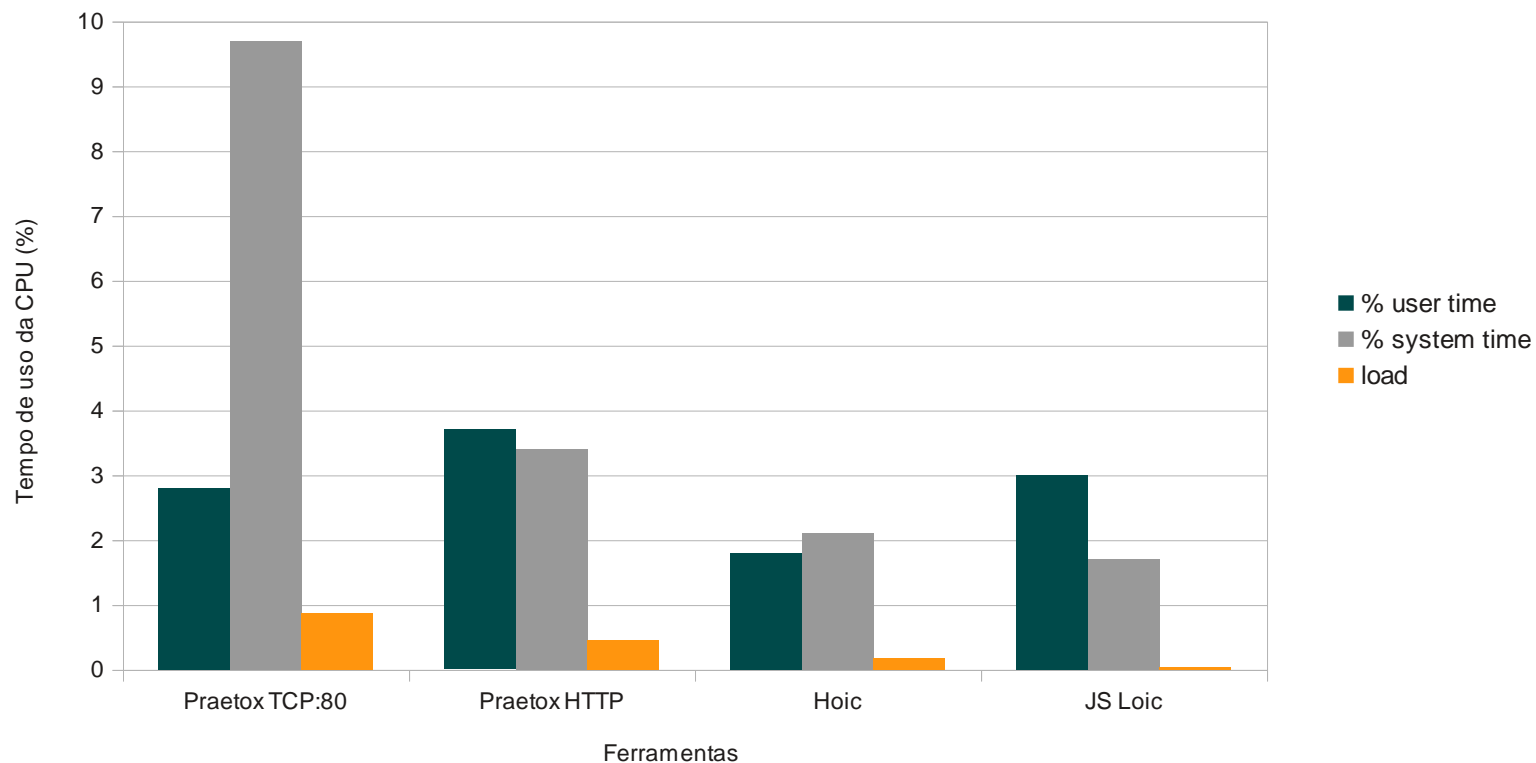
Resultado – PC

PC: Transferência de bytes



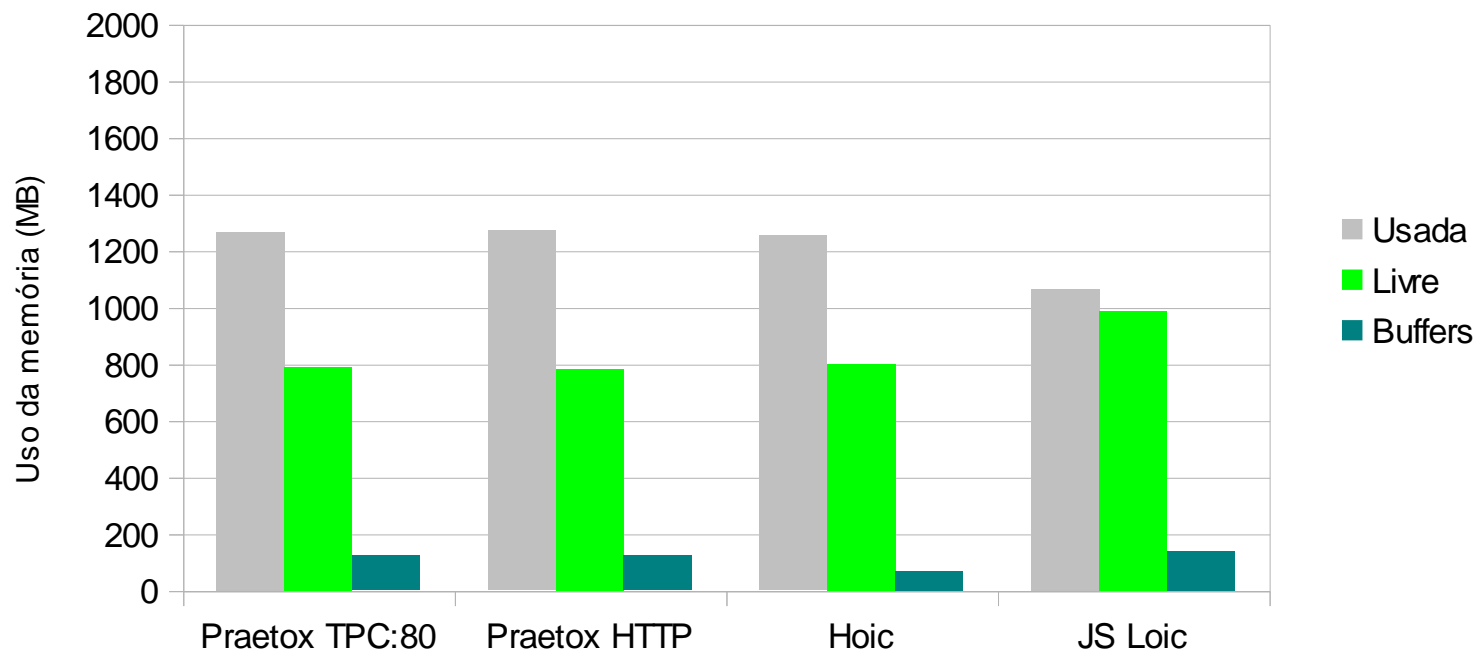
Resultado – PC

PC: Porcentagem de uso da CPU



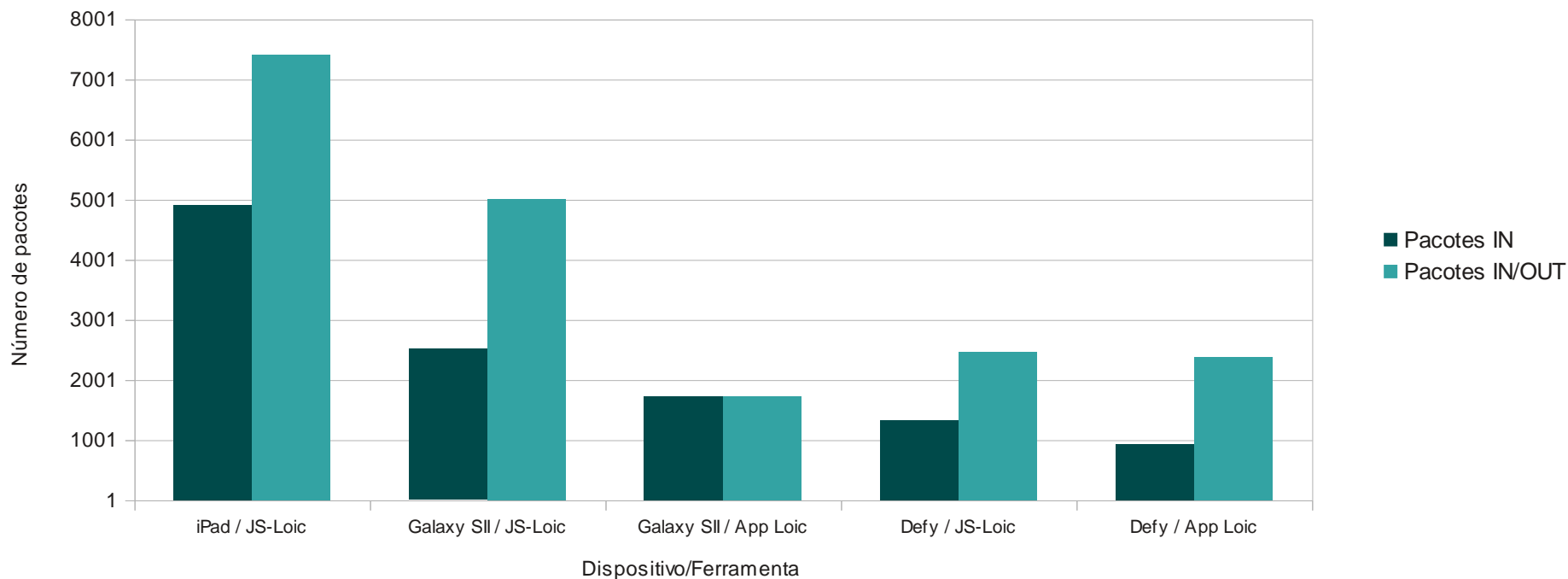
Resultado – PC

Uso da memória



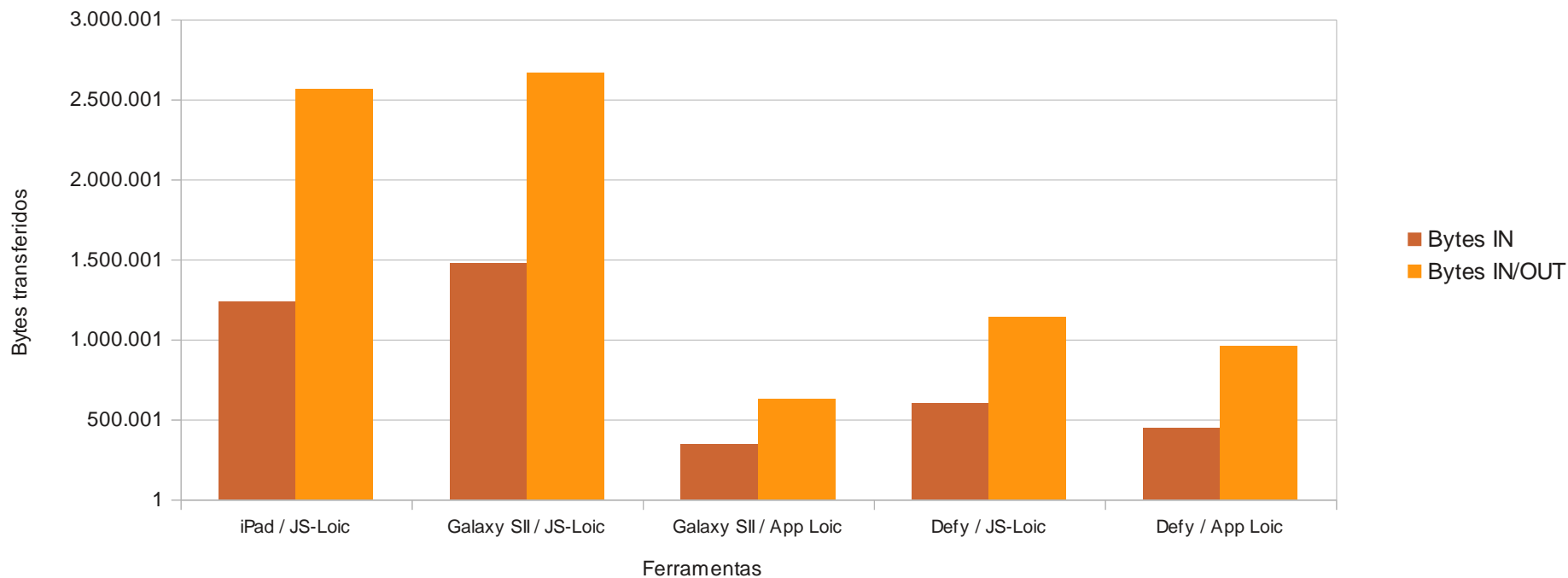
Resultado – Dispositivos móveis

Js Loic: Transferência de Pacotes



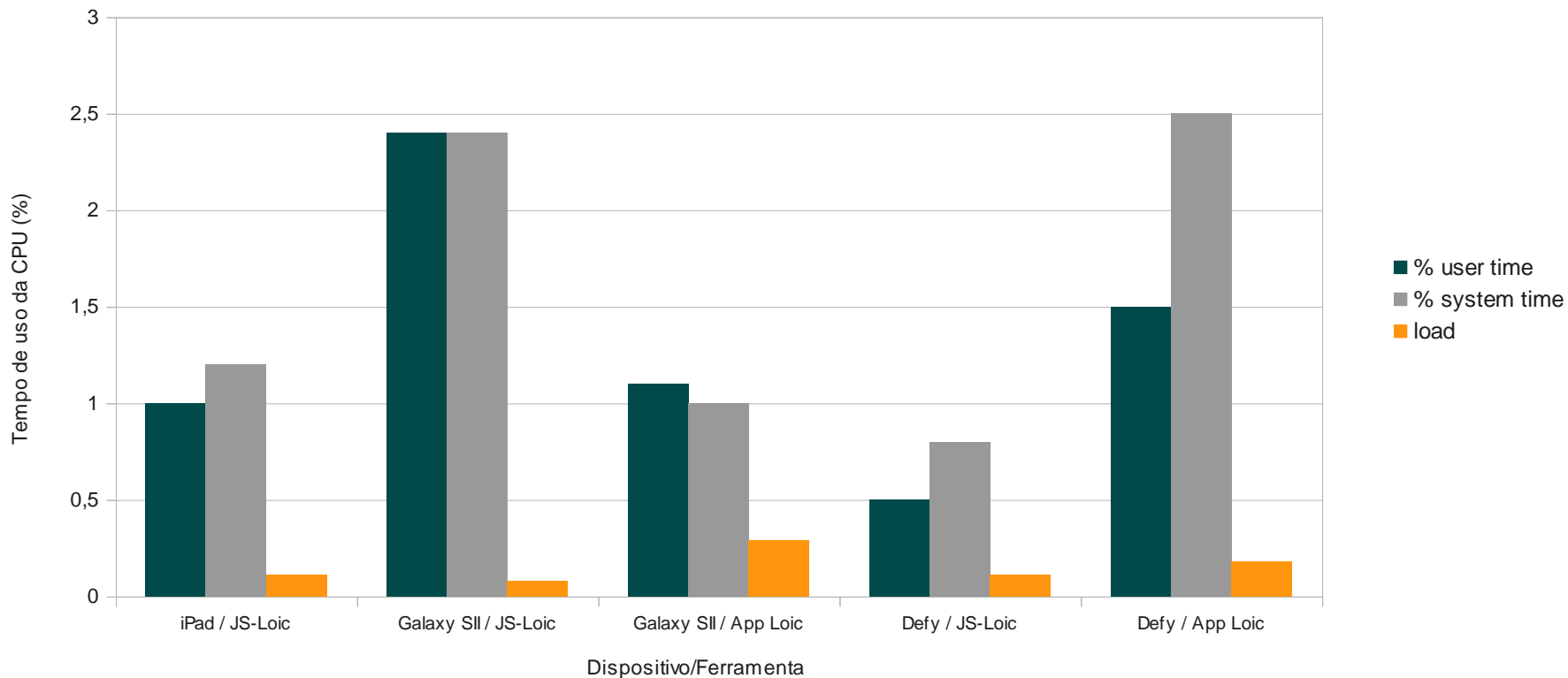
Resultado – Dispositivos móveis

Js Loic: Transferência de bytes



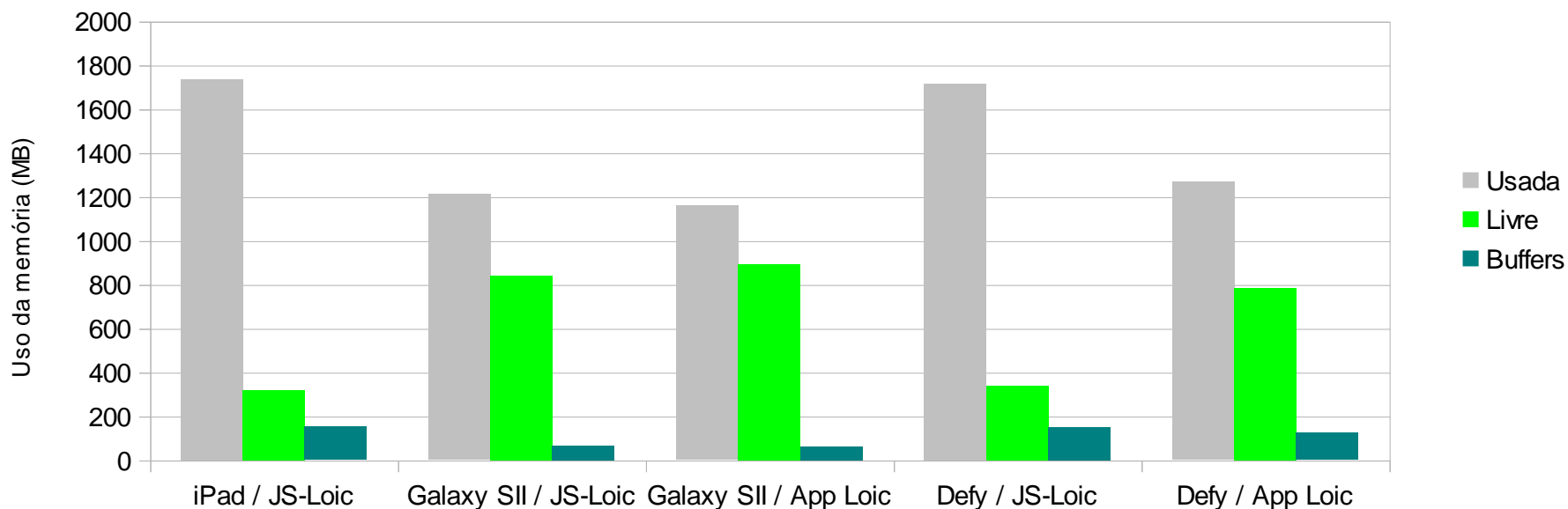
Resultado – Dispositivos móveis

Js Loic: Porcentagem de uso da CPU



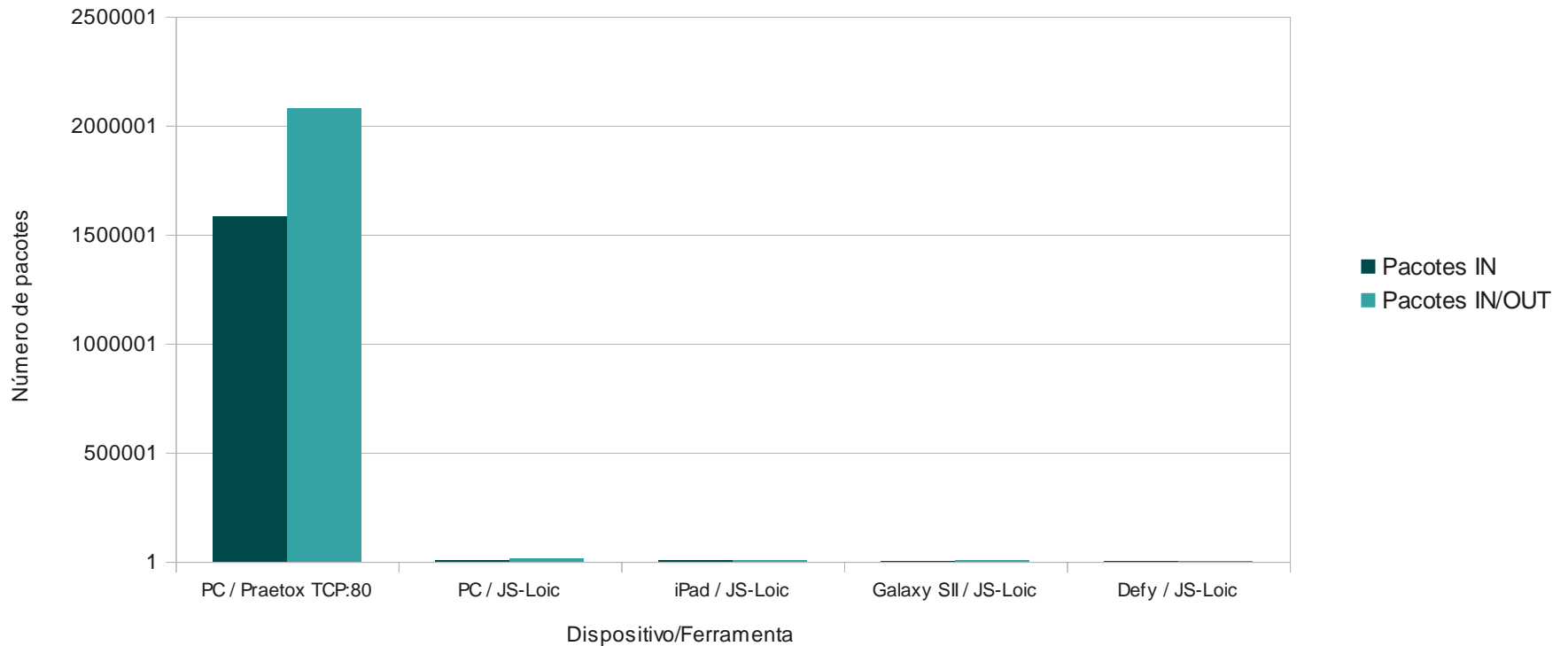
Resultado – Dispositivos móveis

Uso da memória



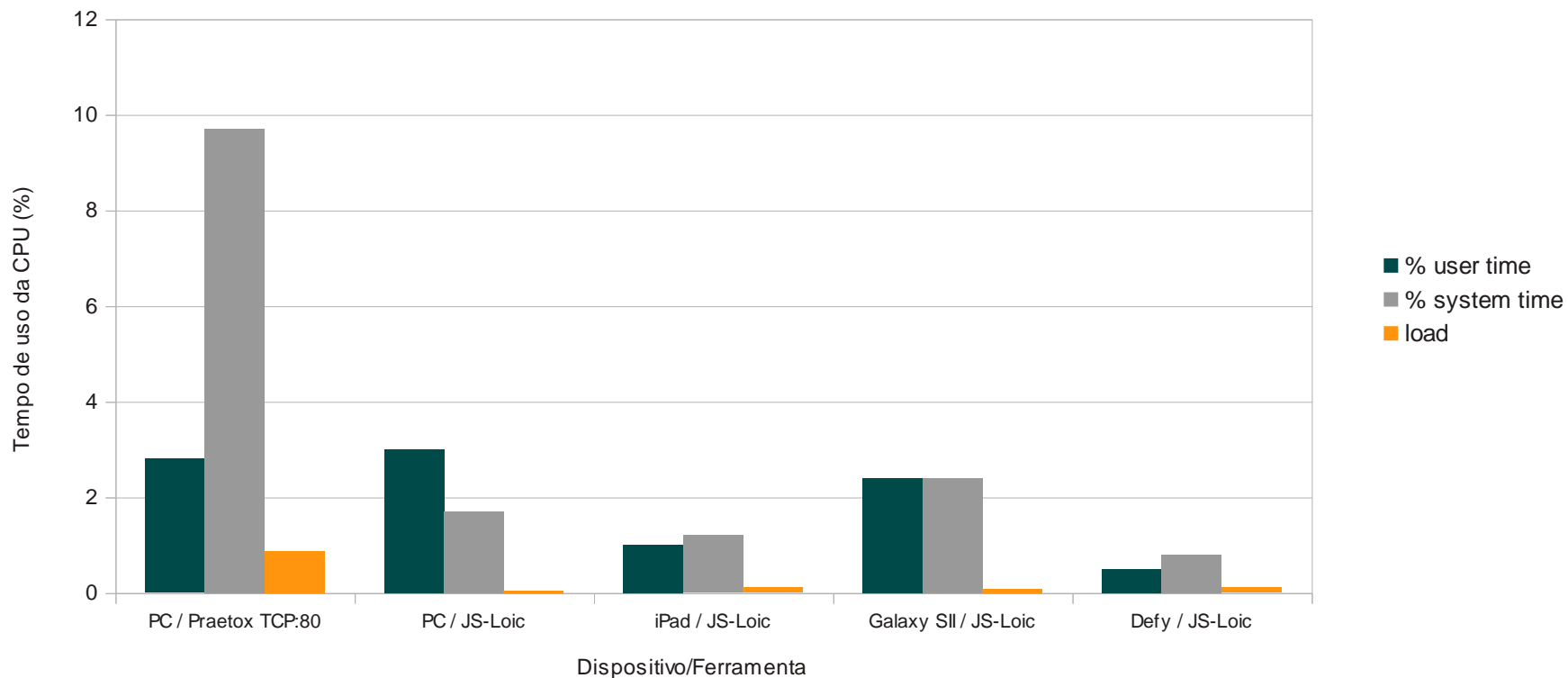
Resultado – Comparativo geral

Transferência de Pacotes



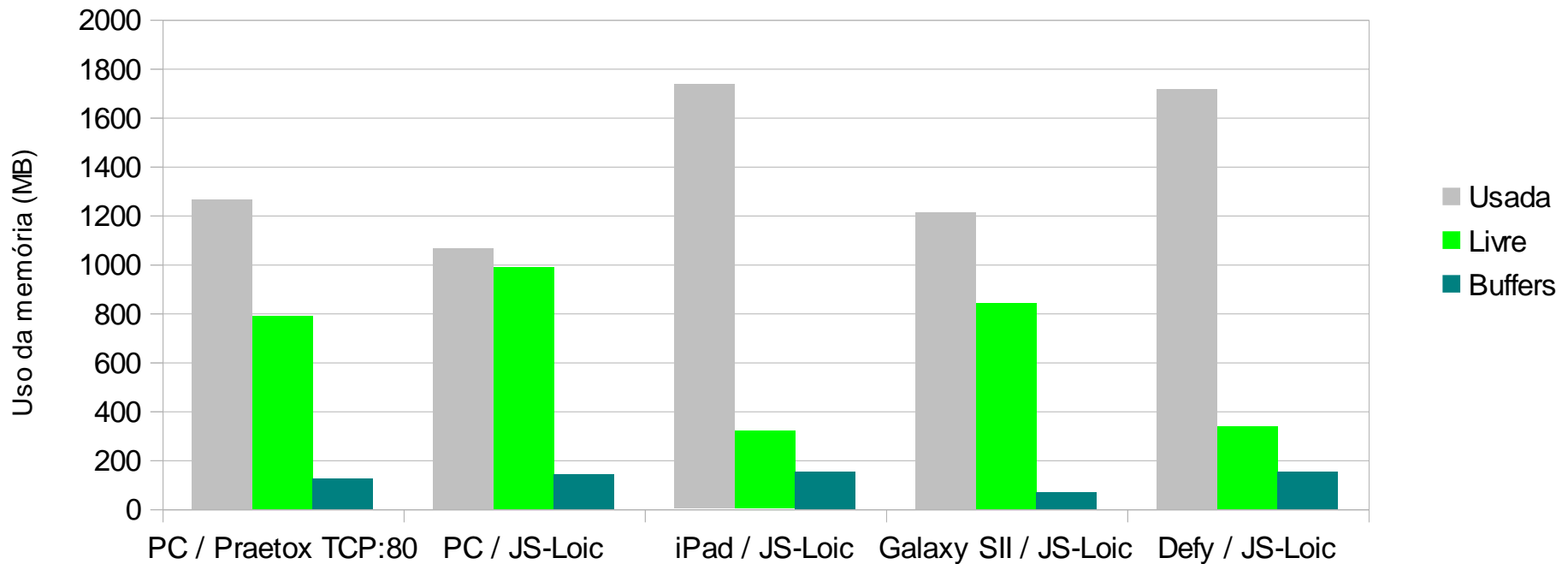
Resultado – Comparativo geral

Porcentagem de uso da CPU



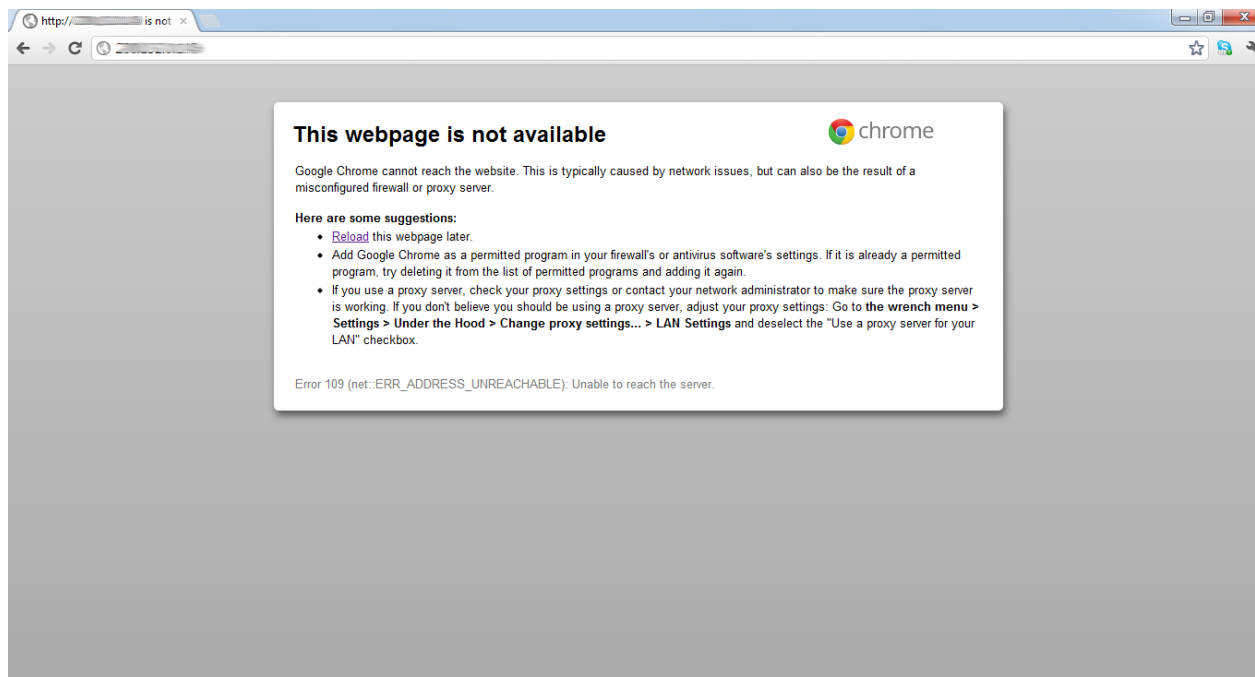
Resultado – Comparativo geral

Uso da memória

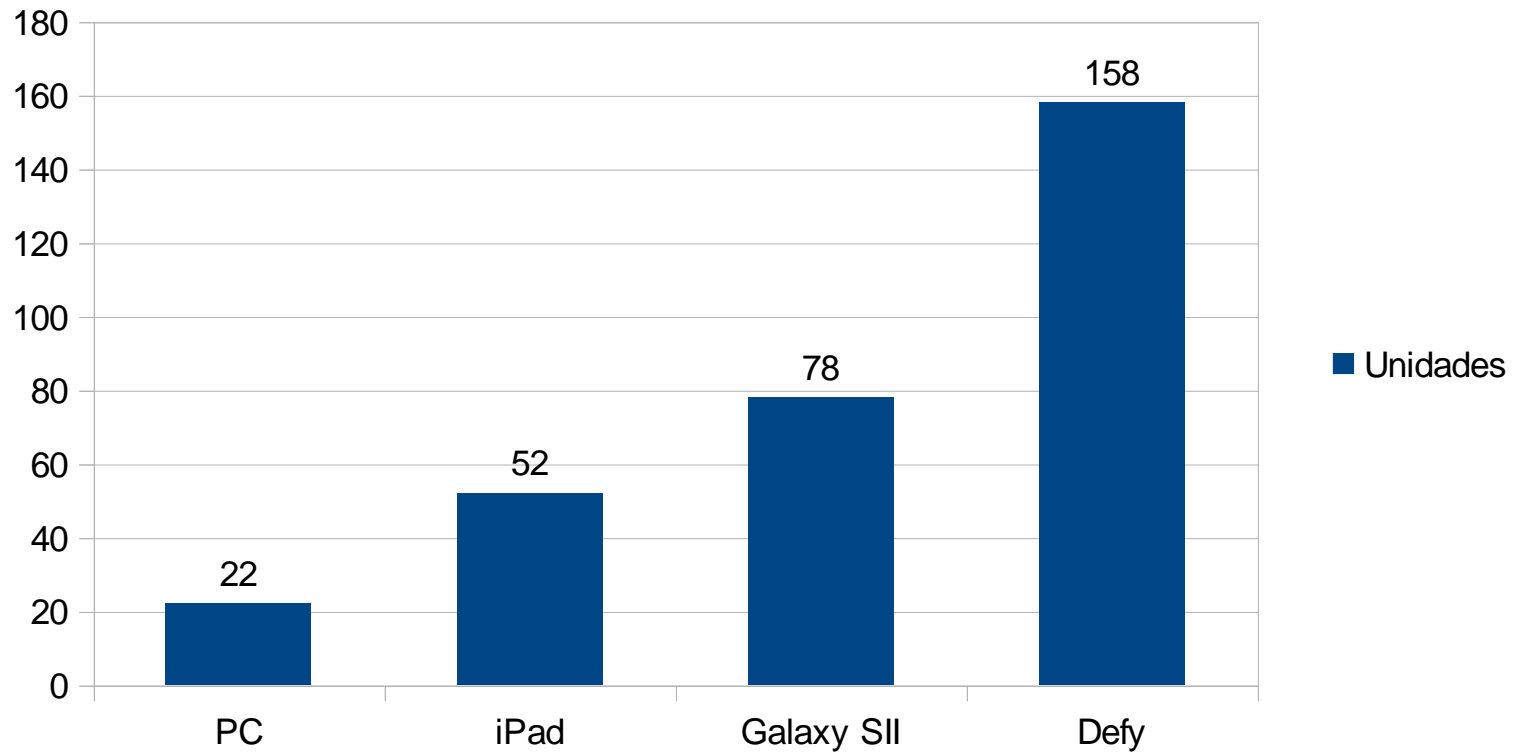


Resultado – Apache

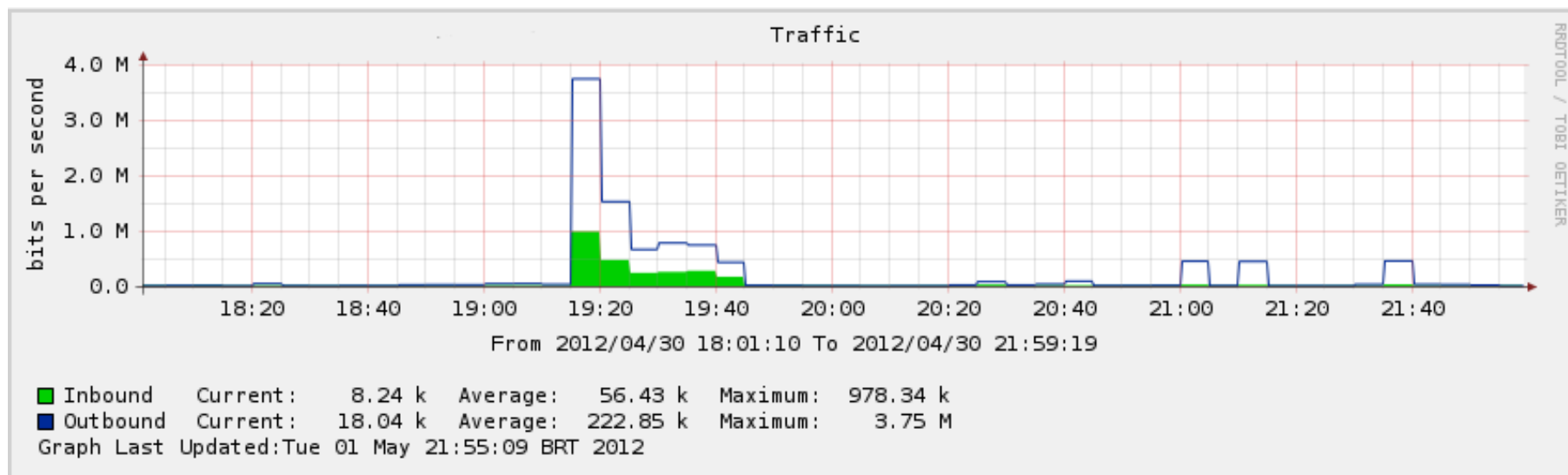
Tango Down



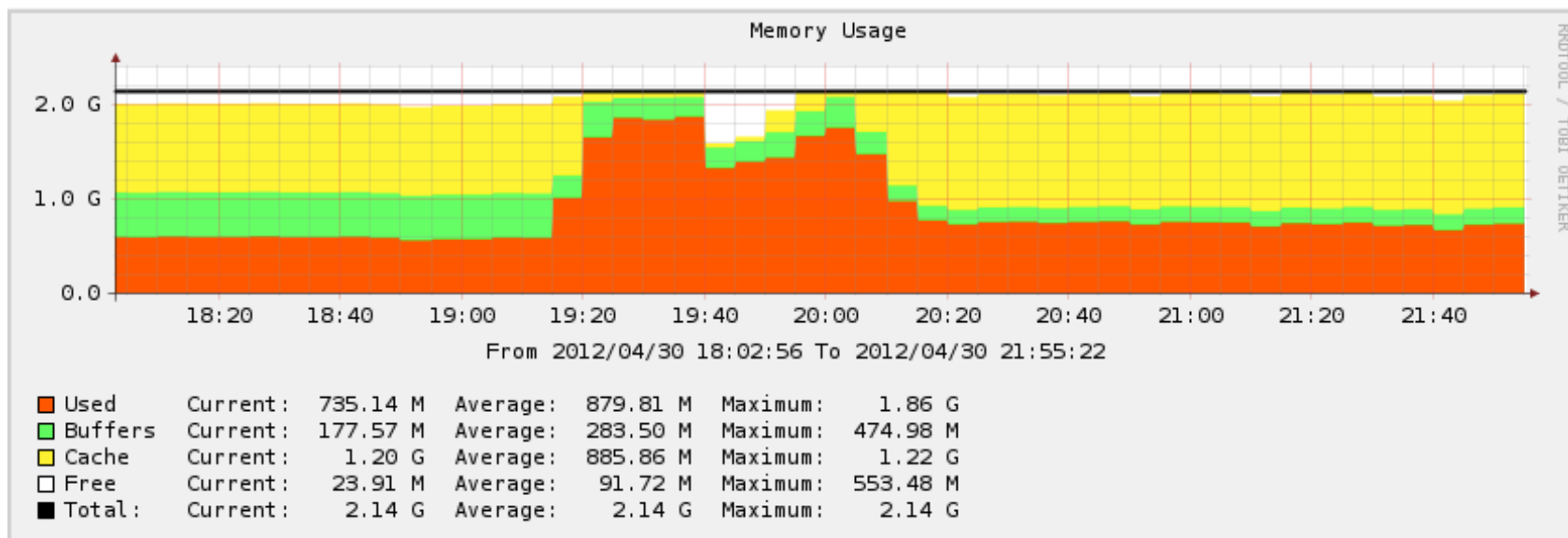
Resultado – Apache



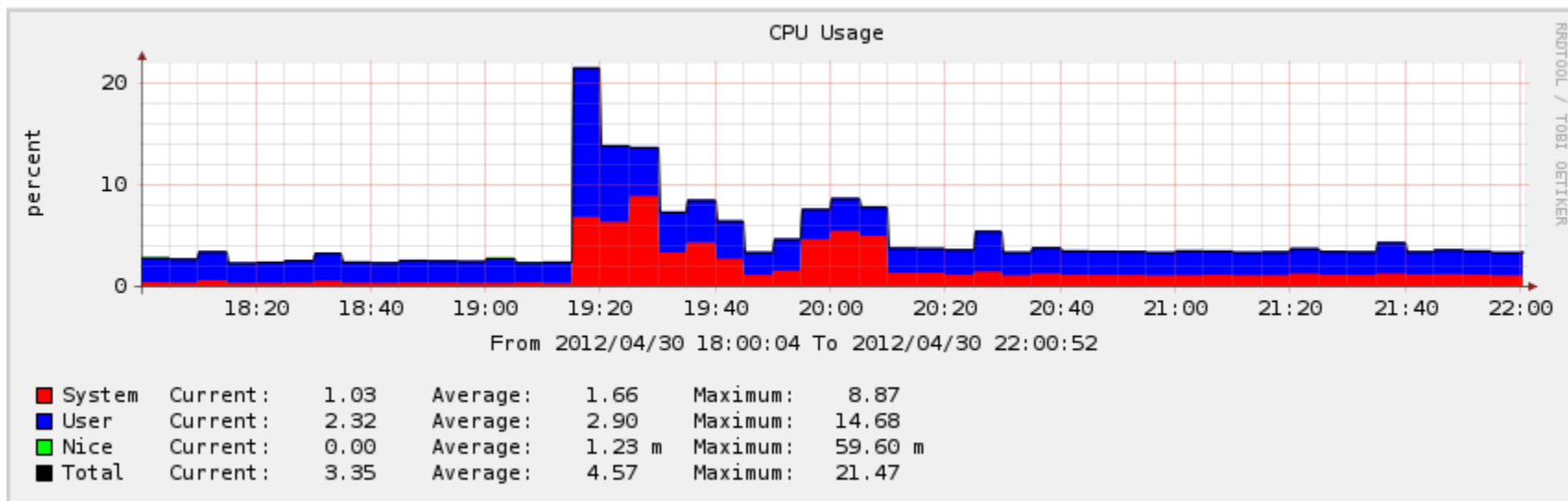
Resultado – Apache



Resultado – Apache



Resultado – Apache



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;
```



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;
```



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>



Colaboradores

Bruno Lorensi

César Loureiro

Douglas Ritter

Eduardo Bergmann

João Ceron (CERT-BR)

Leando Bertholdo

Liane Tarouco

Lucas Arbiza



Perguntas?

eduardo@pop-rs.rnp.br

