Eficácia de *honeypots* no combate a *worms* em instituições

Luiz Otávio Duarte[1]
André Ricardo Abed Grégio[1]
Antonio Montes[1,2]
Adriano Mauro Cansian[3]

[1] LAC - Laboratório Associado de Computação e Matemática Aplicada
INPE - Instituto Nacional de Pesquisas Espaciais

[2] CenPRA - Centro de Pesquisas Renato Archer
MCT - Ministério da Ciência e Tecnologia

[3] ACME - Advanced Counter-Measures Environment
UNESP - Universidade Estadual Paulista

Roteiro

- Quem somos;
- Motivação;
- Cenário Atual;
- Definições;
- As Instituições;

Roteiro

- Abordagens;
- Exemplos;
- Trabalhos Futuros;

Apresentação

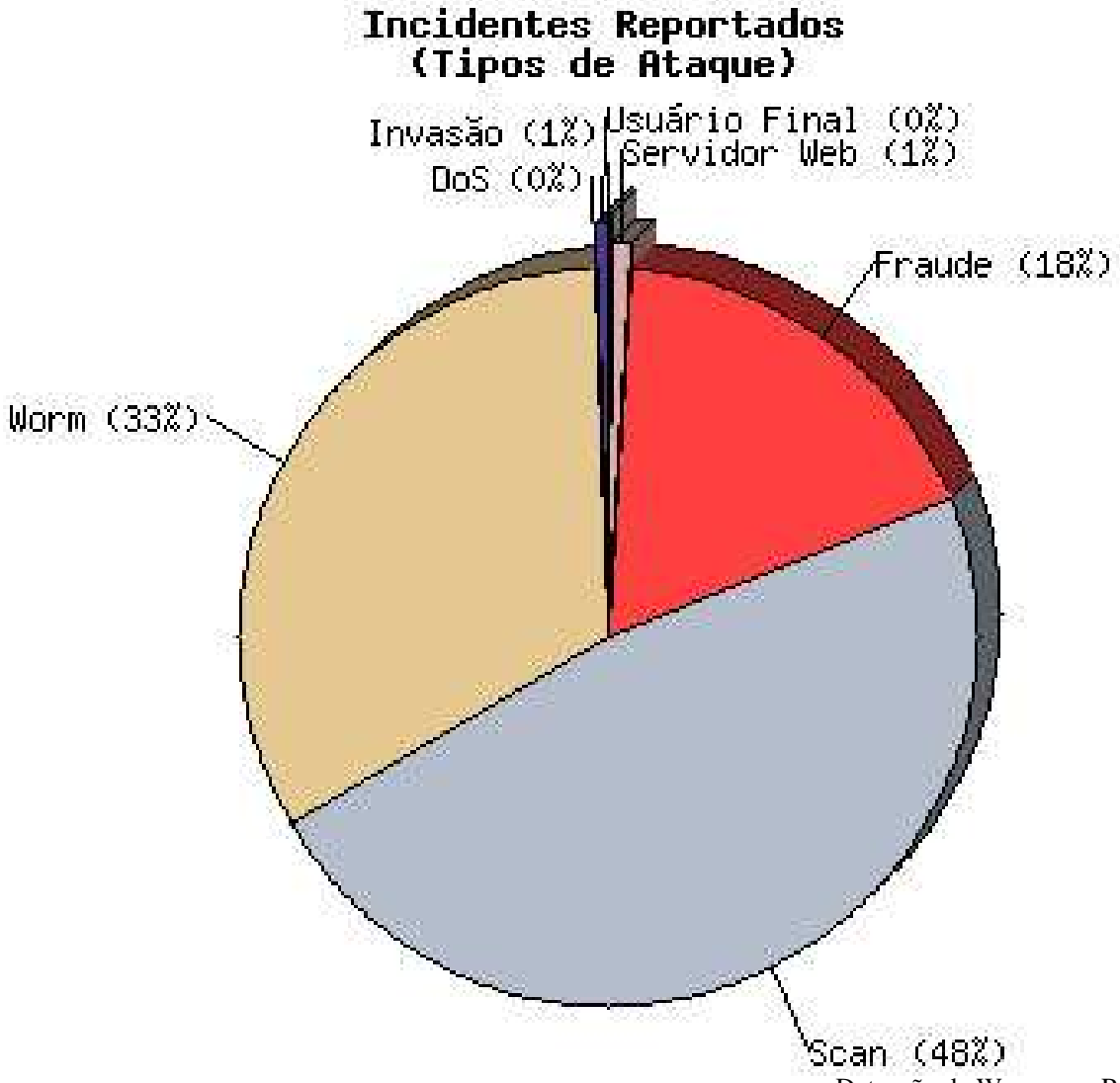
- Quem somos?
  - Pesquisadores de segurança de sistemas e redes de computadores.
- Quais as linhas de pesquisas em segurança?
  - SDI, ICP, *forensics*, *Honeynet*, *Honeypots*, Segurança de software...
- Onde obter maiores informações?
  - `http://www.lac.inpe.br/security`
  - `http://www.acmesecurity.org`

Introdução

- As redes de computadores são especialmente vulneráveis à indisponibilidade de serviços devido aos *worms*.
- As redes de alta conectividade são um mecanismo clássico para aumentar a disponibilidade e confiabilidade, entretanto, também aumentam a sobrevivência dos *worms*.

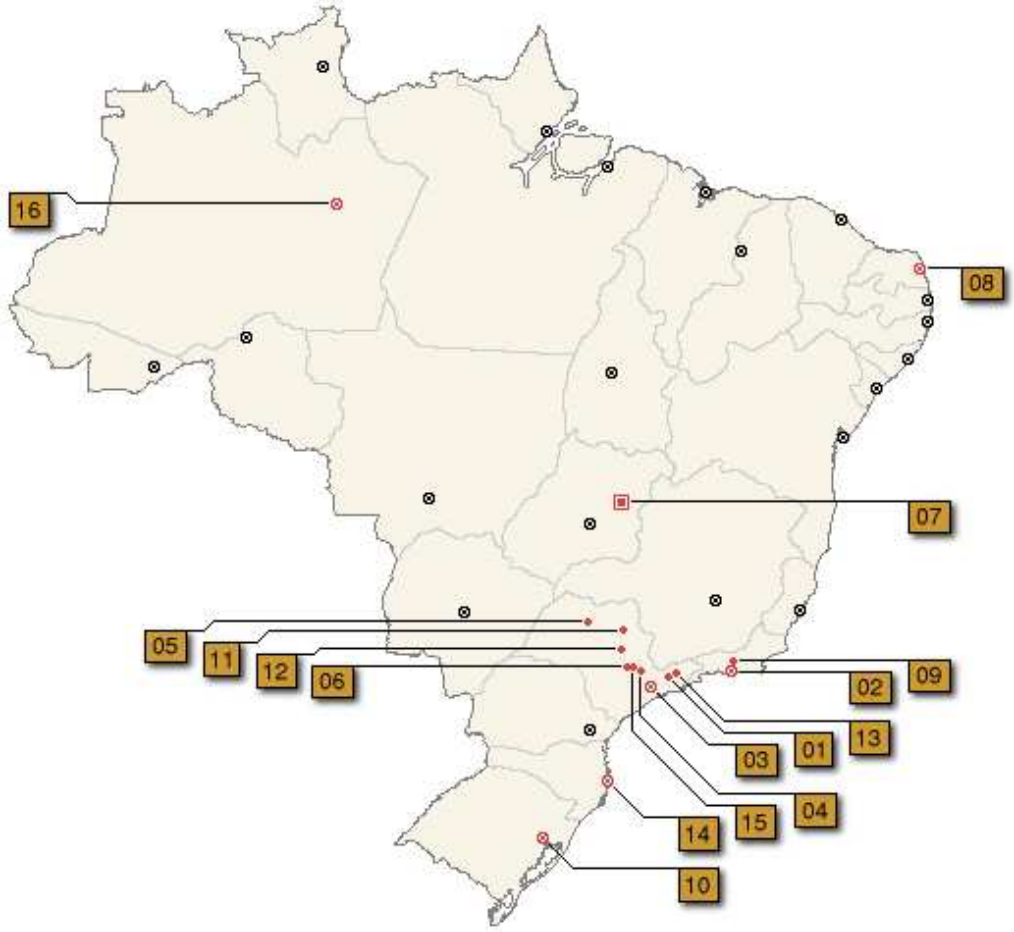
Motivação I

CERT.br (`http://www.cert.br`) Janeiro à março de 2005.



Motivação II

Projeto *Honeypots* Distribuídos - Aliança Brasileira.



Motivação III

- O controle de *worms* é realizado geralmente por meio de anti-vírus e atualizações, mas em grandes instituições, este controle costuma ser frágil e precário.
- Um dos grandes problemas das redes hoje em dia, além do SPAM, é o ataque via *worms*, diversificado constantemente.
- As instituições comumente realizam filtragens nos dispositivos na borda da rede, e não entre as sub-redes $\Longrightarrow$ *modems, notebooks*.

Cenário Atual

- Os *worms* não mais se resumem a consumir banda e recursos computacionais $\Longrightarrow$ *payload* destrutivo.
- Instituições de ensino $\Longrightarrow$ diversidade de sistemas operacionais.
- Muitos sistemas apresentam reincidência de ataques (*worms* revisitados - CERT/CC - `http://www.cert.org`).

Objetivo

- Mostrar que um *honeypot* de baixa interação é também uma ferramenta de auxílio para:
  - Os administradores de redes, na identificação de atividades maliciosas;
  - A verificação do comportamento do tráfego na rede interna.

Abordagem utilizada

- A abordagem utilizada neste trabalho:
  - Reduz drasticamente falsos alertas, dado que quase toda interação com o *honeypot* é, por definição, não autorizada.
- É possível identificar:
  - *worms*;
  - usuários mal intencionados;
  - máquinas mal configuradas.

Definição: *Worm*

- Um programa independente que se replica entre máquinas através de conexões de rede, geralmente congestionando-as, bem como os sistemas de informação assim que ele se espalha.
- Programa de computador que pode executar independentemente, propagando uma versão de si mesmo para outros *hosts* em uma rede, consumindo recursos computacionais.
- FONTE: Glossary of Vulnerability Testing Terminology

  `http://www.ee.oulu.fi/research/ouspg/sage/glossary/`

Formas de propagação

- Vetor de propagação em ataques de *buffer overflow*;
- Através do compartilhamento de binários infectados (P2P);
- ...

Definição: *Honeypots*

- *A honeypot is an information system resource whose value lies in unauthorized or ilicit use of that resource.*
- Um *honeypot* é um sistema projetado para ser sondado, atacado e/ou comprometido.
- FONTE: The Honeynet Project

  `http://www.honeynet.org/`

Honeypots x Worms

- Um *honeypot* pode ser utilizado para monitorar a atividade maliciosa em uma rede, pois captura toda a interação proveniente de máquinas internas;
- Se um *worm* infectar um *host* interno e tentar se propagar através da rede, quando interagir com o *honeypot* ele será detectado.

As Instituições

- Instituições de pesquisa e ensino;
- Possuidoras de mais de 1000 *hosts* ativos;
- Com mais de 100 redes “/24” ativas.

Instituição 1

- De grande porte e distribuída;
- Topologia em estrela;
- Cerca de 14000 *hosts* ligados em rede.

Instituição 2

- Dividida em poucas unidades, próximas geograficamente;
- Topologia em estrela;
- Cerca de 1500 *hosts* conectados na rede.

Instituição 1 vs. Instituição 2 I

- Instituição 1:
  - Raras reuniões entre os responsáveis pela administração e segurança da rede de cada unidade;
  - Sobrecarga de funções $\Longrightarrow$ Cada unidade possui pouco mais de um analista, geralmente sem o preparo adequado;

Instituição 1 vs. Instituição 2 II

- Instituição 2
  - Reuniões freqüentes com os administradores de redes e/ou responsáveis pela segurança dos sistemas das unidades;
  - Nas unidades, cada um dos departamentos possui analistas e técnicos responsáveis;
  - Grupo de Resposta a Incidentes reconhecido pelo CERT/CC.

Arquivo de logs do honeypot

- Honeyd.log

data hora protocolo [E|S|-] IP_Origem Porta_Origem IP_Destino Porta_Destino: Bytes [Flags|0] [S.O.]

Abordagens I

- Manual
  - `grep -e '[E|S|-] <IP-rede-instituicao>' honeyd-log > blah.txt`

```
2005-05-14-01:02:17.2762 tcp(6) S 10.0.11.56 2960 10.0.0.119
139 [Windows XP SP1]
2005-05-14-01:02:20.8843 tcp(6) E 10.0.11.56 2960 10.0.0.119
139: 0 0
2005-05-14-01:02:31.7337 tcp(6) S 10.0.11.56 1288 10.0.0.119
139 [Windows XP SP1]
2005-05-14-01:02:41.9174 tcp(6) E 10.0.11.56 1288 10.0.0.119
139: 72 0
```

Abordagens II

- *Script*
  - Analisa os *logs* do *pflog* e envia os dados para `security@instituicao.bla` $\Longrightarrow$ Não é possível observar a evolução de ataques, o histórico dos ocorridos, o que aconteceu em relação a um determinado período.

Abordagens III

- As abordagens, manual e via *script*, não permitiam comparar as atividades geradas a partir da rede interna com as da rede externa;
- Muito trabalho para identificar se os alertas enviados estavam ou não surtindo efeito;
- Dificuldade em se manter um histórico dos fenômenos ocorridos.

Gráficos

- Para que se fosse possível comparar atividades, identificar tentativas de acesso a serviços, diferenciar acessos oriundos da rede interna e externa, bem como manter um histórico, um conjunto de gráficos e arquivos htm foram gerados.
- Utilização do software ORCA.

ORCA

- Basicamente gera gráficos de arquivos que possuam algum campo de *timestamp* e dados a serem *plotados*;
- Pode gerar gráficos representados em áreas ou linhas, entre outros;
- Legenda configurável.

Utilização do ORCA

1. Arquivos de *log* do *honeyd* são utilizados para gerar arquivos de entrada para o ORCA, chamados `orca_data`;
2. Estes arquivos são então utilizados pelo ORCA para gerar os gráficos, segundo um arquivo de configuração do ORCA.
3. Estes gráficos então são armazenados segundo suas datas para posteriormente serem visualizados.

Exemplo `orca_data`

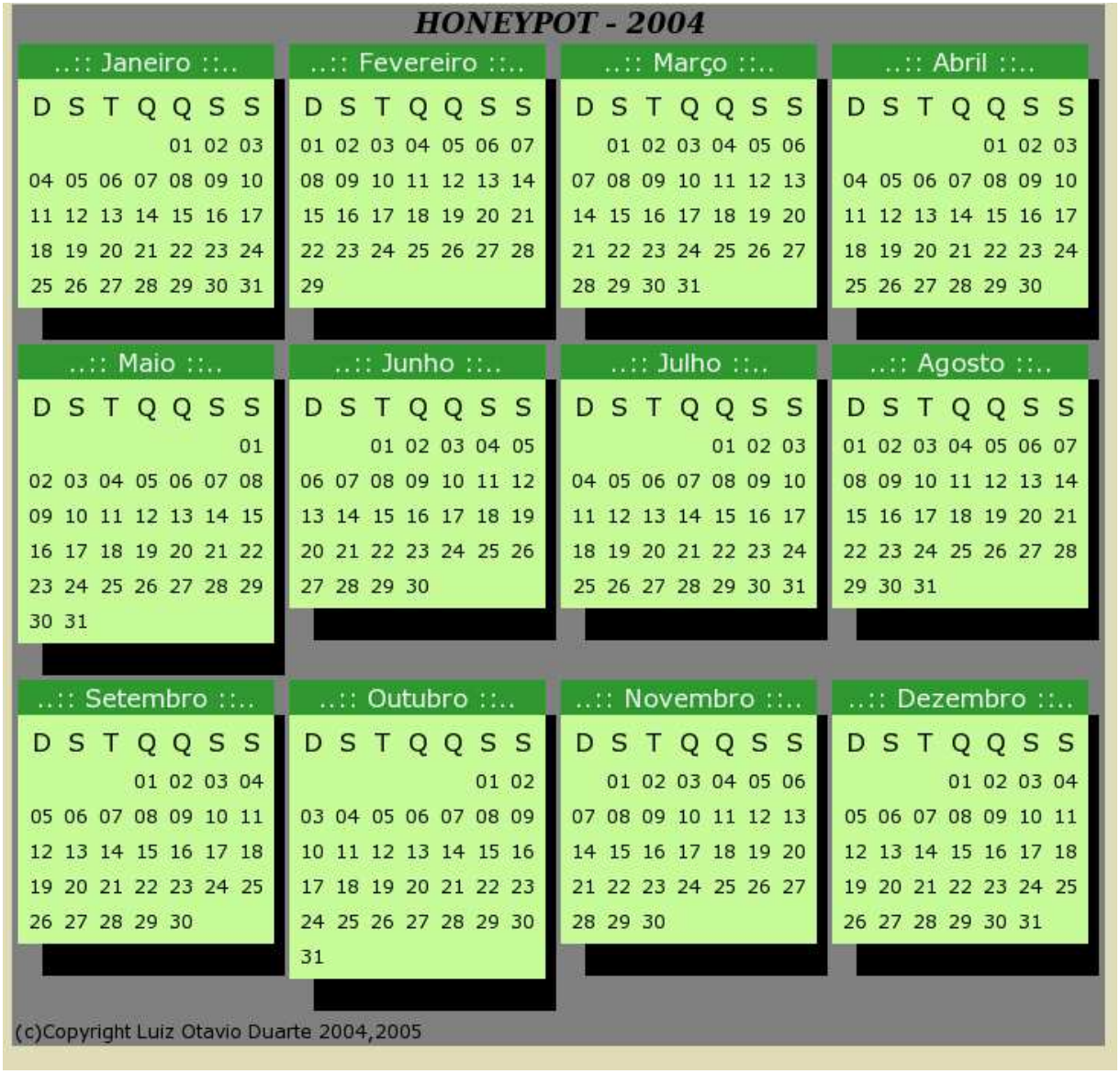
- **byintorext.2004-07-19**

```
1090195200 5 0 .69897000433601880478
1090195500 2 0 .30102999566398119521
1090195800 3 0 .47712125471966243729
1090196100 158 0 2.19865708695442262321
1090196400 11 0 1.04139268515822504075
1090196700 6 0 .77815125038364363251
1090197000 30 0 1.47712125471966243729
1090197300 4 0 .60205999132796239042
1090197600 4 0 .60205999132796239042
1090197900 11 0 1.04139268515822504075
1090198200 8 0 .90308998699194358564
(...)
```

Manipulação dos Gráficos

- Para melhor localizar e visualizar os gráficos, páginas HTML foram geradas.
- Estas páginas permitem que, tanto os gráficos gerados, quanto as saídas geradas pelo *script* `honeydsum`(`http://www.honeynet.org.br`) e o próprio `honeyd.log` sejam visualizados.
- Para melhor manusear os dados, um calendário é gerado utilizando o *script* `makecal.pl` (`http://www.lac.inpe.br/~lgbarbato`).

Exemplos



HONEYPOT - 2004

..:: Janeiro ::..

D	S	T	Q	Q	S	S
				01	02	03
04	05	06	07	08	09	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

..:: Fevereiro ::..

D	S	T	Q	Q	S	S
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29						

..:: Março ::..

D	S	T	Q	Q	S	S
	01	02	03	04	05	06
07	08	09	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

..:: Abril ::..

D	S	T	Q	Q	S	S
				01	02	03
04	05	06	07	08	09	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

..:: Maio ::..

D	S	T	Q	Q	S	S
						01
02	03	04	05	06	07	08
09	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

..:: Junho ::..

D	S	T	Q	Q	S	S
		01	02	03	04	05
06	07	08	09	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

..:: Julho ::..

D	S	T	Q	Q	S	S
			01	02	03	
04	05	06	07	08	09	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

..:: Agosto ::..

D	S	T	Q	Q	S	S
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

..:: Setembro ::..

D	S	T	Q	Q	S	S
			01	02	03	04
05	06	07	08	09	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

..:: Outubro ::..

D	S	T	Q	Q	S	S
					01	02
03	04	05	06	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

..:: Novembro ::..

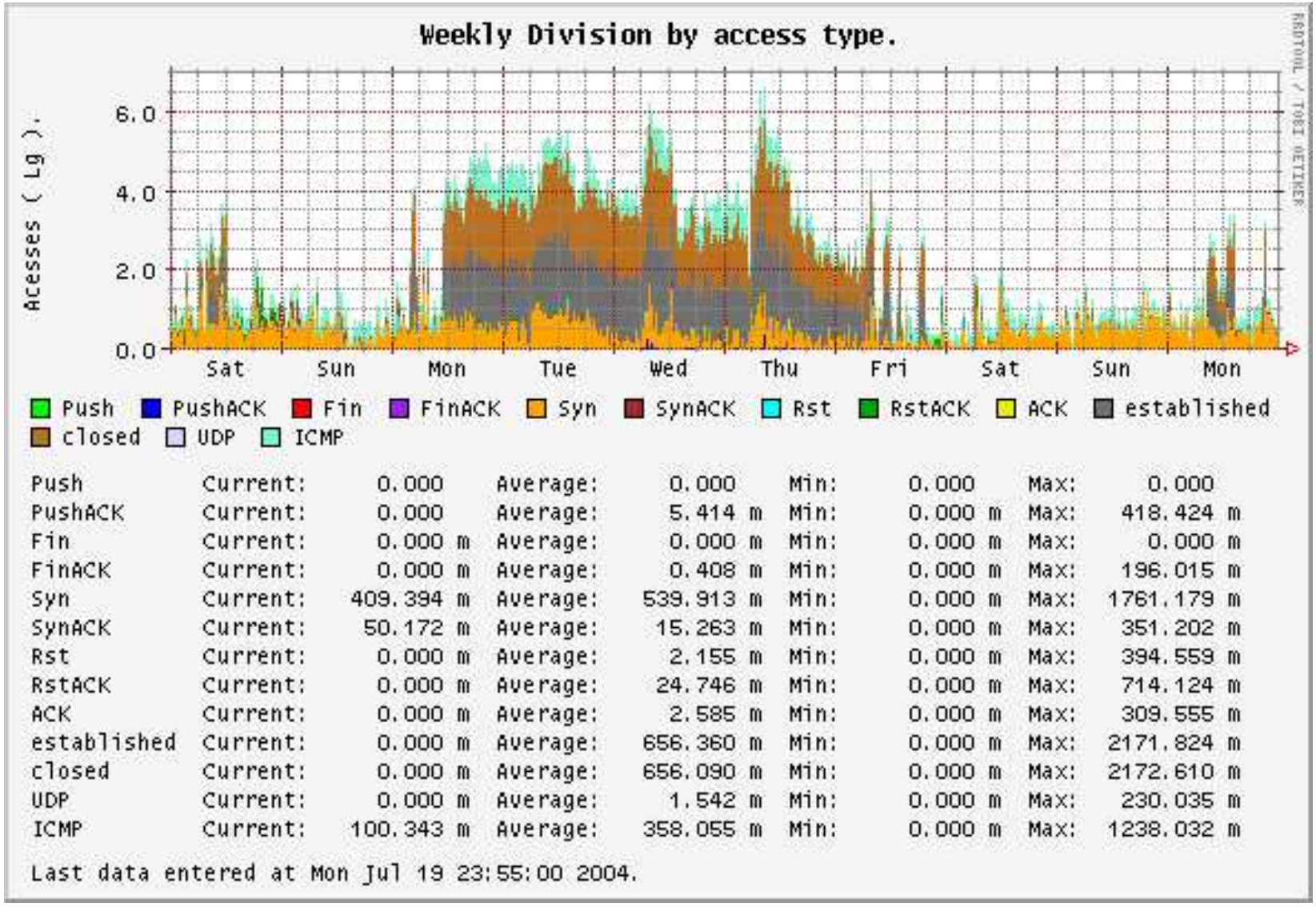
D	S	T	Q	Q	S	S
	01	02	03	04	05	06
07	08	09	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

..:: Dezembro ::..

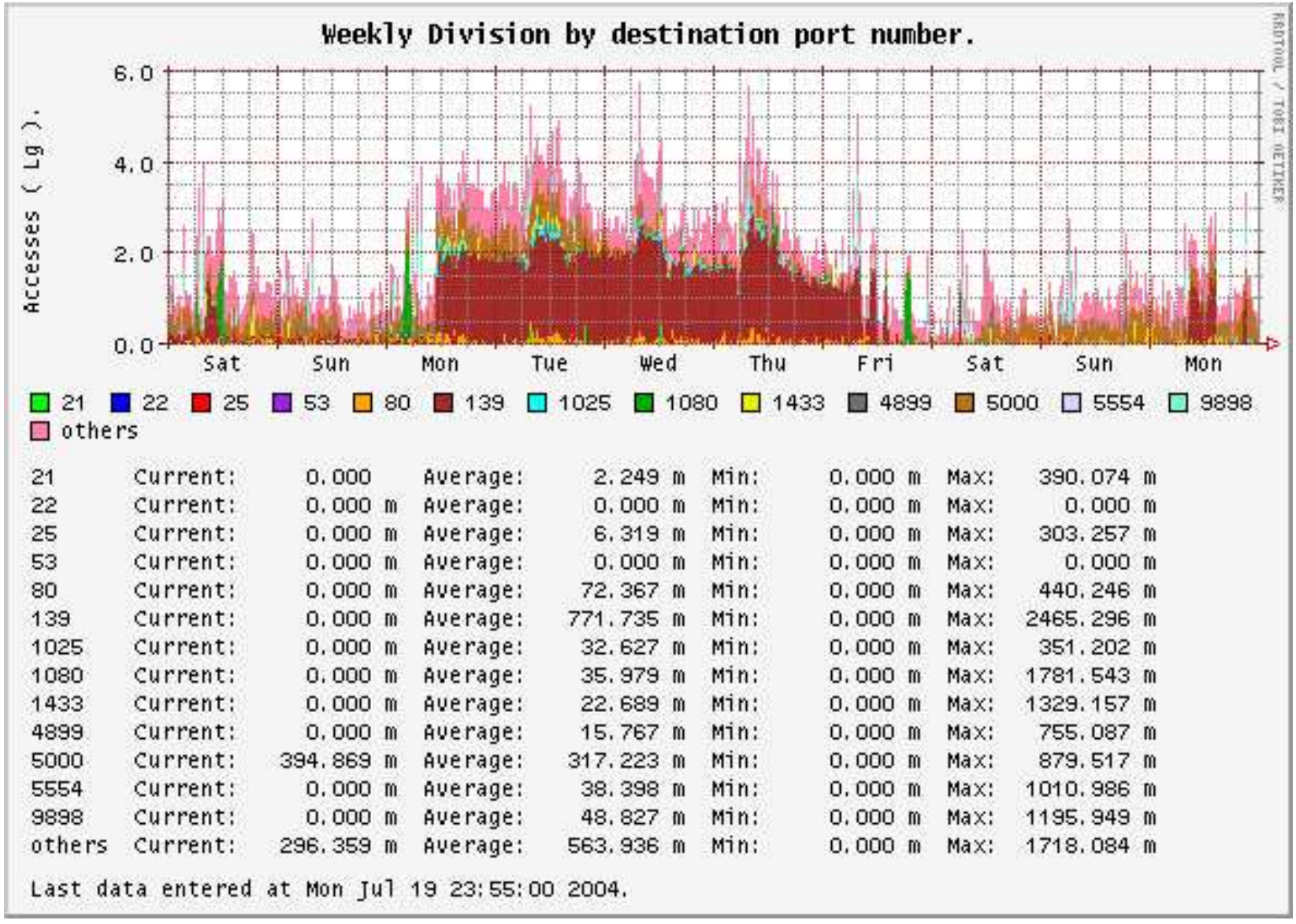
D	S	T	Q	Q	S	S
			01	02	03	04
05	06	07	08	09	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

(c)Copyright Luiz Otavio Duarte 2004,2005

byflag.weekly.2004-07-19.png



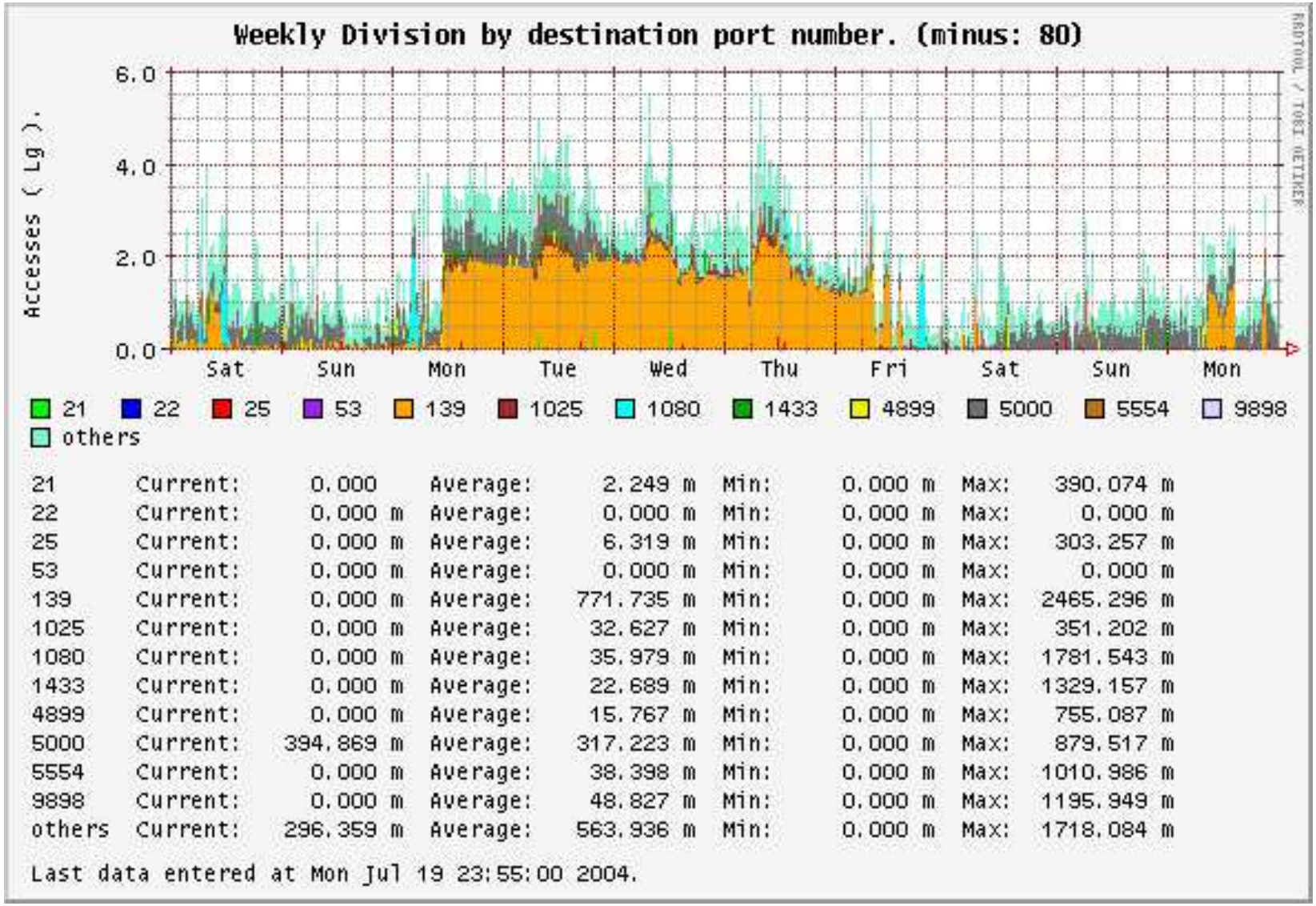
bydstport.weekly.2004-07-19.png



21	Current:	0.000	Average:	2.249 m	Min:	0.000 m	Max:	390.074 m
22	Current:	0.000 m	Average:	0.000 m	Min:	0.000 m	Max:	0.000 m
25	Current:	0.000 m	Average:	6.319 m	Min:	0.000 m	Max:	303.257 m
53	Current:	0.000 m	Average:	0.000 m	Min:	0.000 m	Max:	0.000 m
80	Current:	0.000 m	Average:	72.367 m	Min:	0.000 m	Max:	440.246 m
139	Current:	0.000 m	Average:	771.735 m	Min:	0.000 m	Max:	2465.296 m
1025	Current:	0.000 m	Average:	32.627 m	Min:	0.000 m	Max:	351.202 m
1080	Current:	0.000 m	Average:	35.979 m	Min:	0.000 m	Max:	1781.543 m
1433	Current:	0.000 m	Average:	22.689 m	Min:	0.000 m	Max:	1329.157 m
4899	Current:	0.000 m	Average:	15.767 m	Min:	0.000 m	Max:	755.087 m
5000	Current:	394.869 m	Average:	317.223 m	Min:	0.000 m	Max:	879.517 m
5554	Current:	0.000 m	Average:	38.398 m	Min:	0.000 m	Max:	1010.986 m
9898	Current:	0.000 m	Average:	48.827 m	Min:	0.000 m	Max:	1195.949 m
others	Current:	296.359 m	Average:	563.936 m	Min:	0.000 m	Max:	1718.084 m

Last data entered at Mon Jul 19 23:55:00 2004.

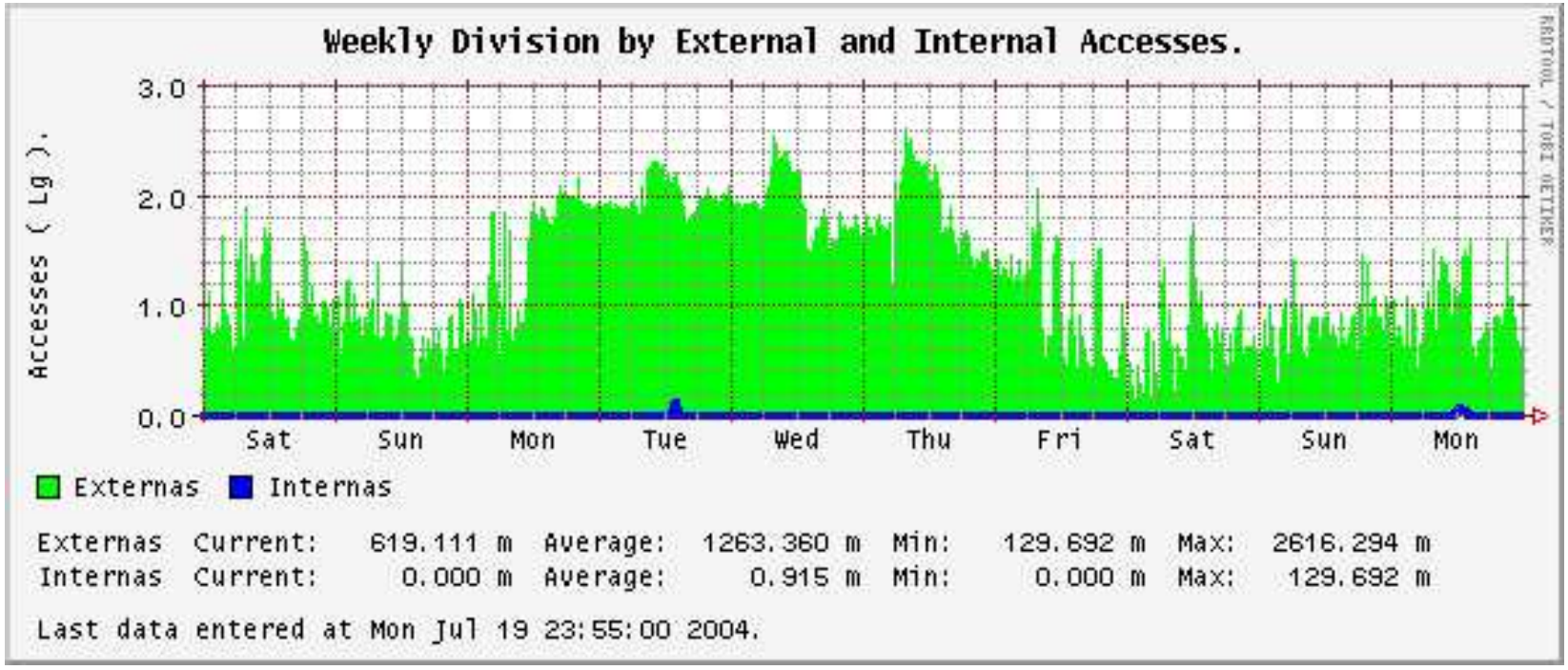
bydstport80.weekly.2004-07-19.png



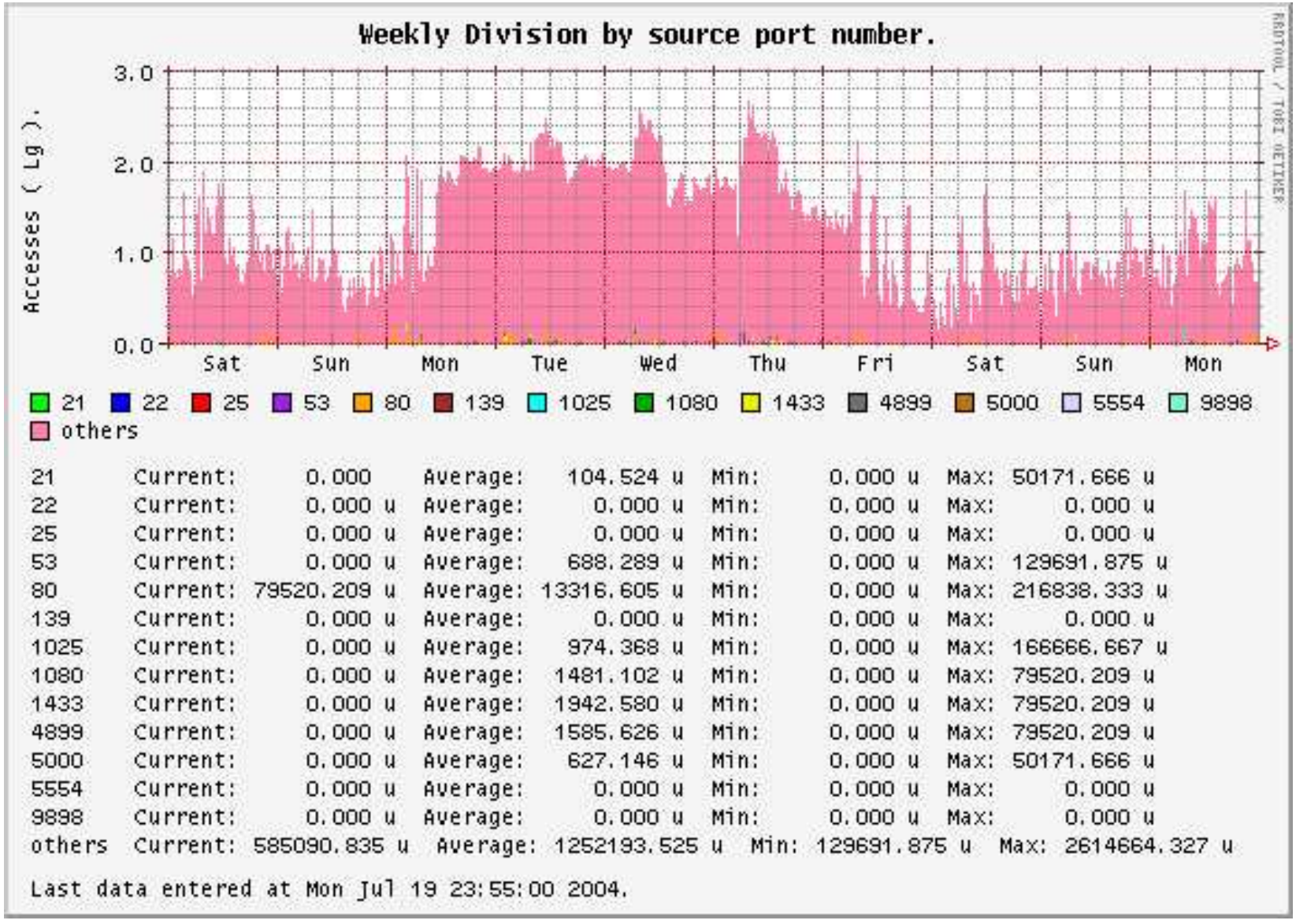
21	Current:	0.000	Average:	2.249 m	Min:	0.000 m	Max:	390.074 m
22	Current:	0.000 m	Average:	0.000 m	Min:	0.000 m	Max:	0.000 m
25	Current:	0.000 m	Average:	6.319 m	Min:	0.000 m	Max:	303.257 m
53	Current:	0.000 m	Average:	0.000 m	Min:	0.000 m	Max:	0.000 m
139	Current:	0.000 m	Average:	771.735 m	Min:	0.000 m	Max:	2465.296 m
1025	Current:	0.000 m	Average:	32.627 m	Min:	0.000 m	Max:	351.202 m
1080	Current:	0.000 m	Average:	35.979 m	Min:	0.000 m	Max:	1781.543 m
1433	Current:	0.000 m	Average:	22.689 m	Min:	0.000 m	Max:	1329.157 m
4899	Current:	0.000 m	Average:	15.767 m	Min:	0.000 m	Max:	755.087 m
5000	Current:	394.869 m	Average:	317.223 m	Min:	0.000 m	Max:	879.517 m
5554	Current:	0.000 m	Average:	38.398 m	Min:	0.000 m	Max:	1010.986 m
9898	Current:	0.000 m	Average:	48.827 m	Min:	0.000 m	Max:	1195.949 m
others	Current:	296.359 m	Average:	563.936 m	Min:	0.000 m	Max:	1718.084 m

Last data entered at Mon Jul 19 23:55:00 2004.

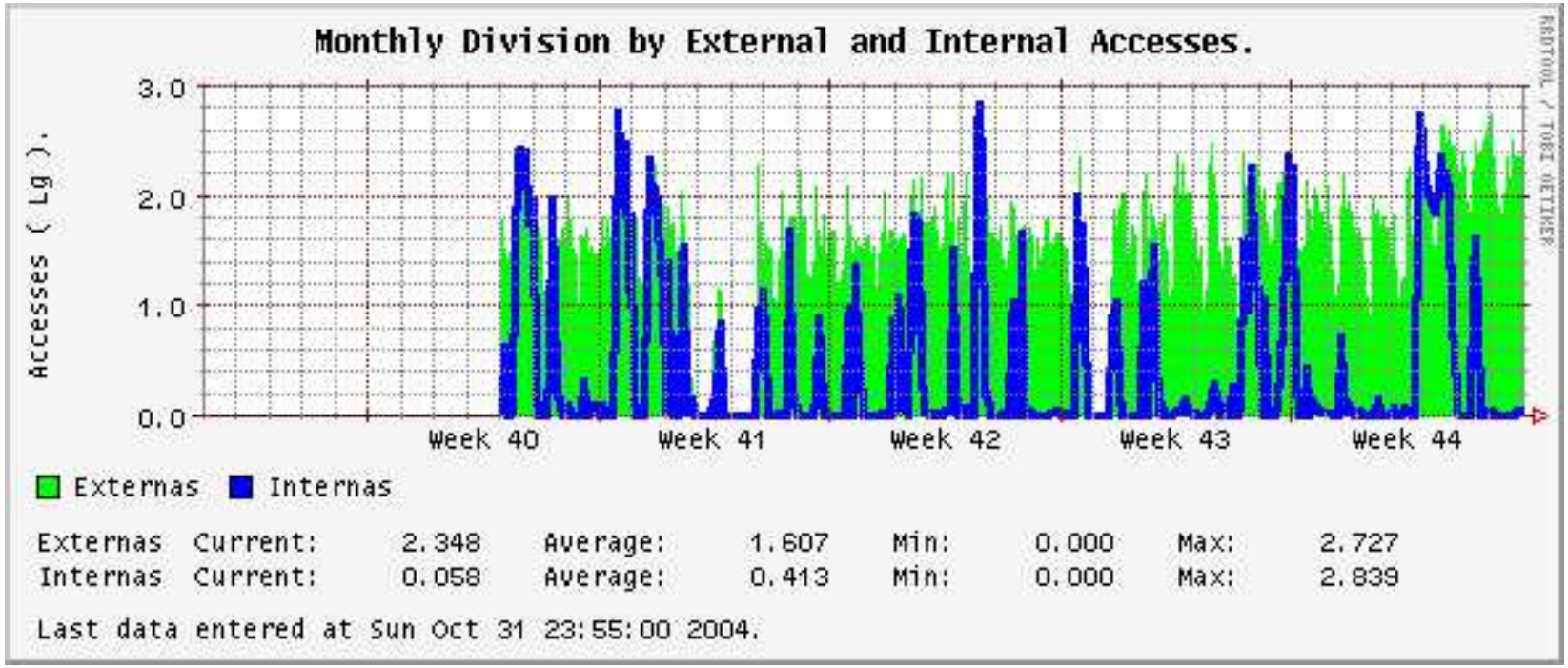
byintorext.weekly.2004-07-19.png

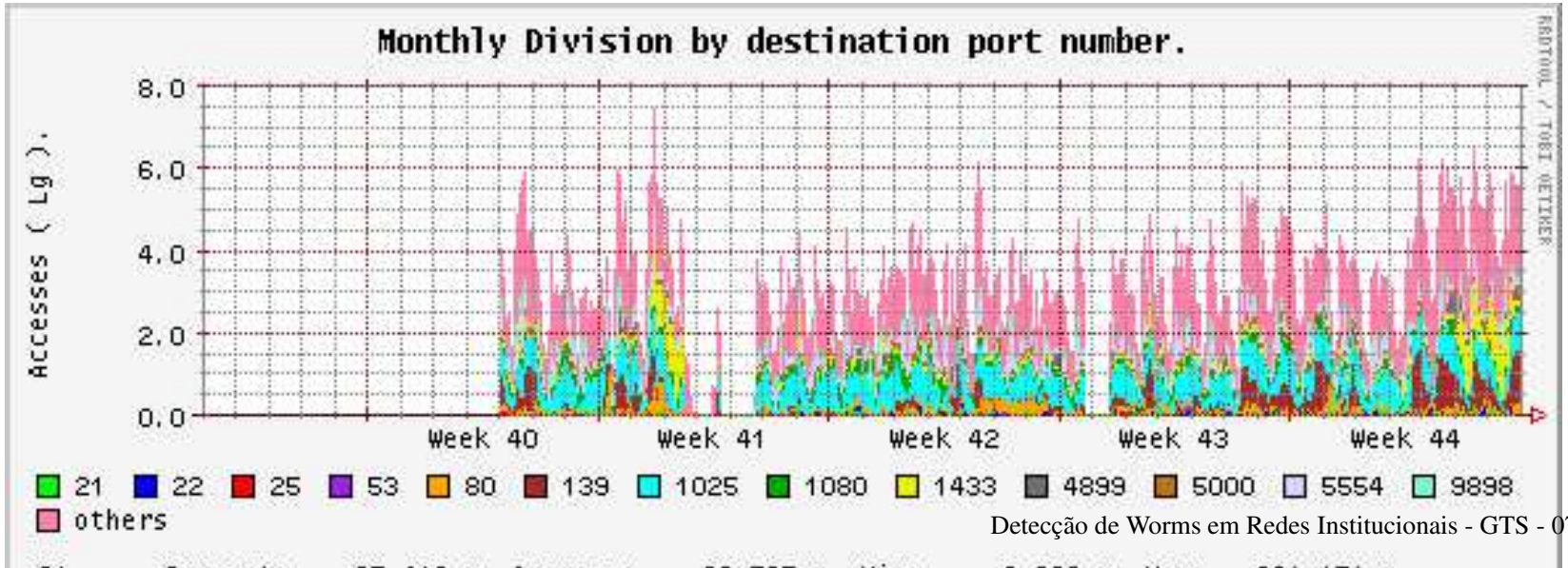


bysrcport.weekly.2004-07-19.png

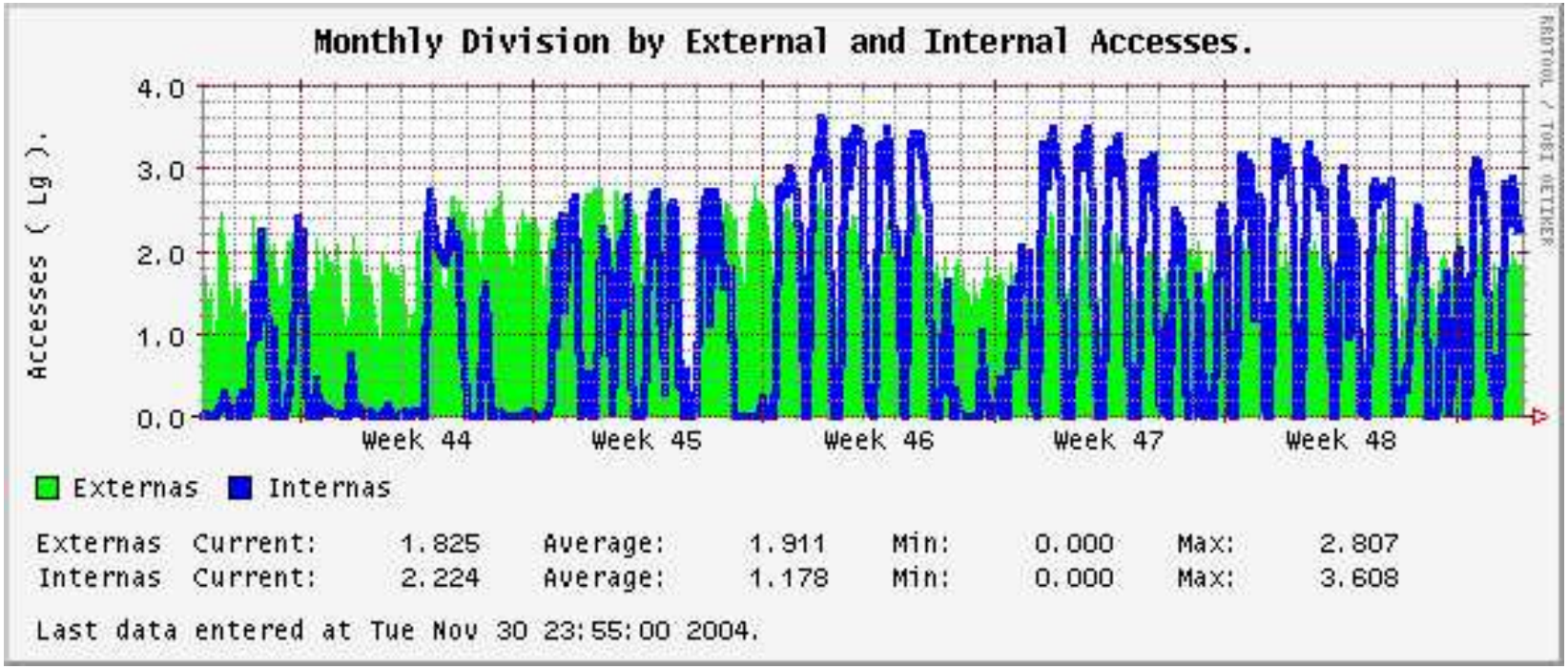


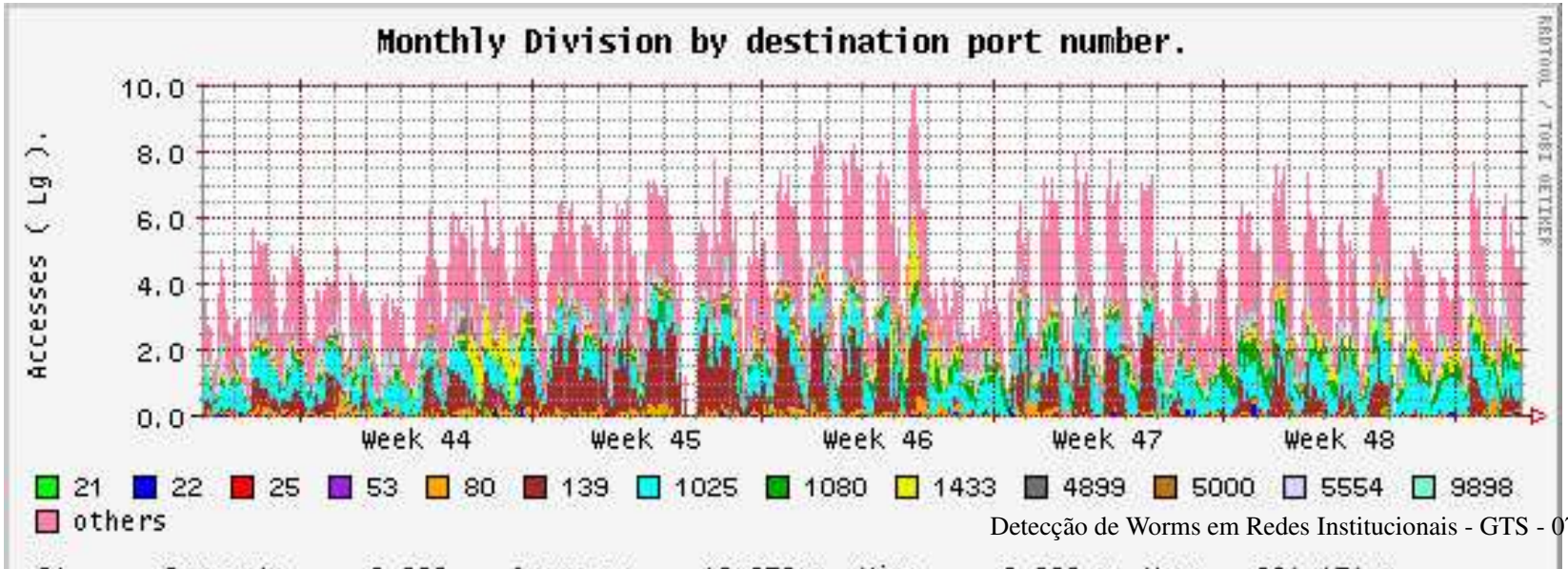
Estudo de caso: Instituição 1 (10/2004)



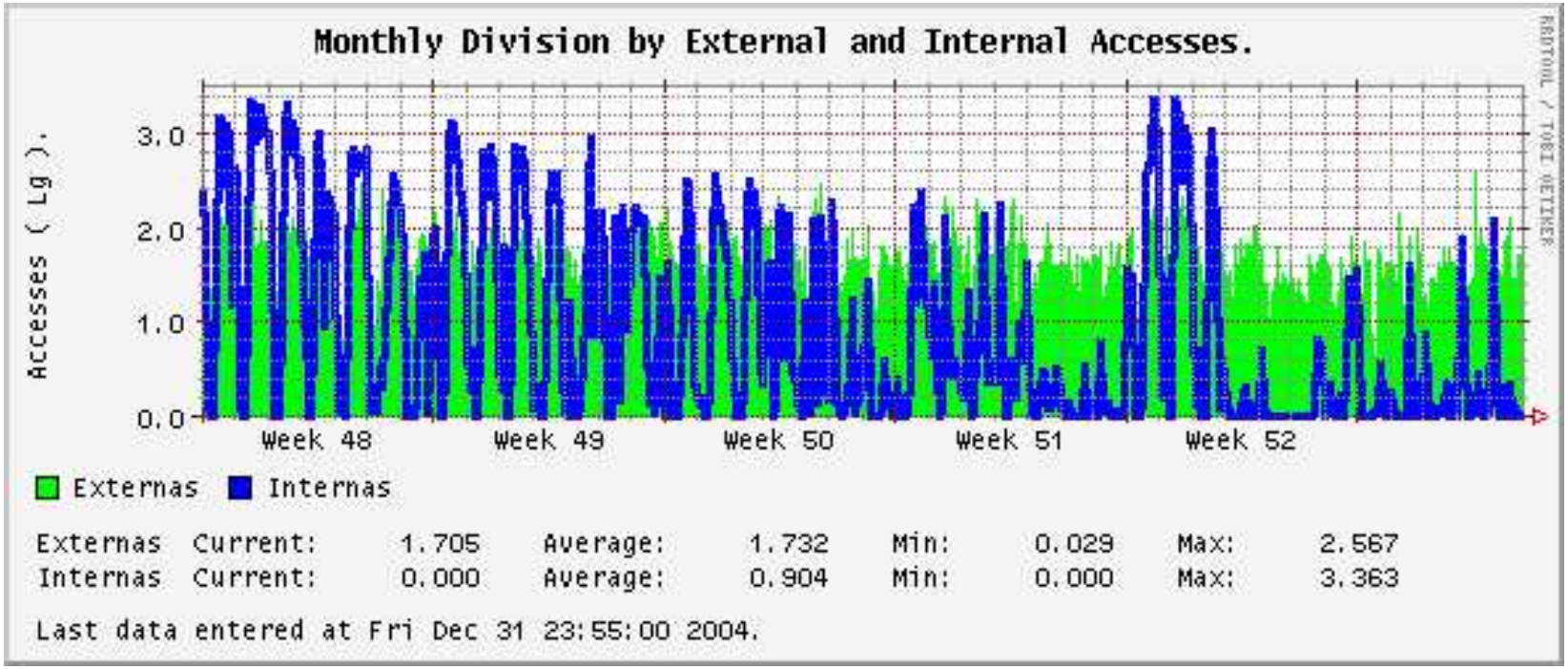


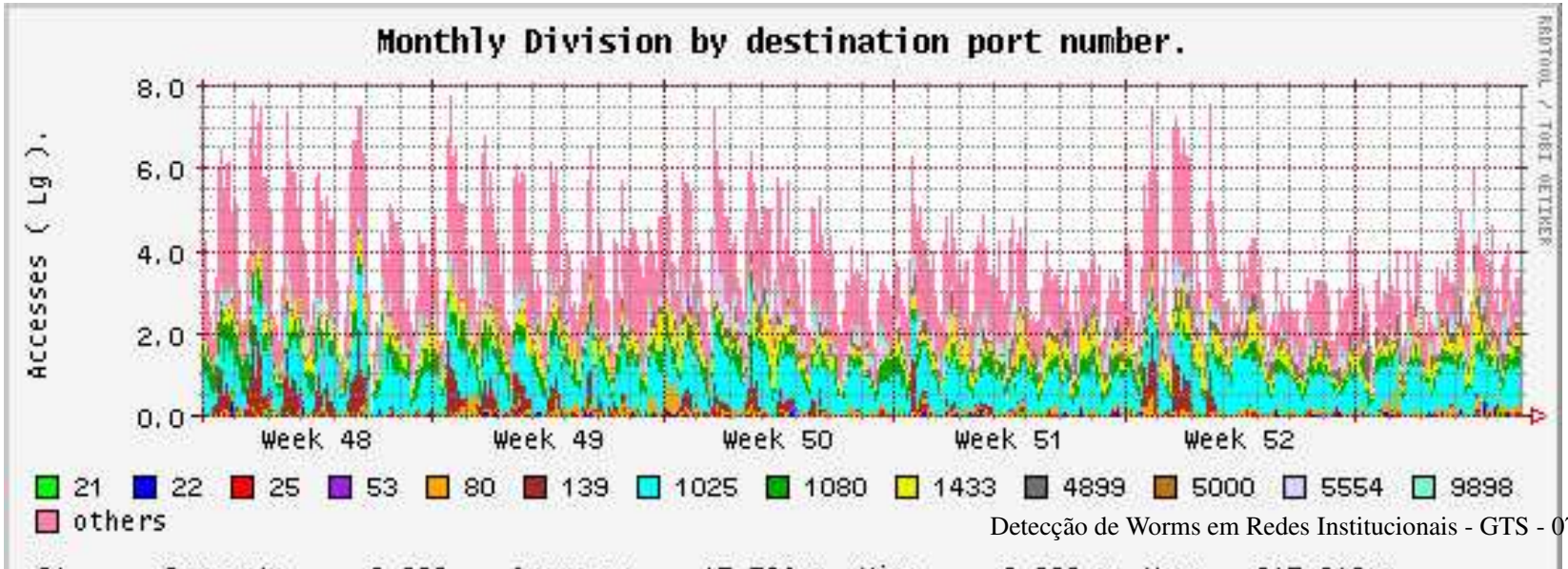
Estudo de caso: Instituição 1 (11/2004)



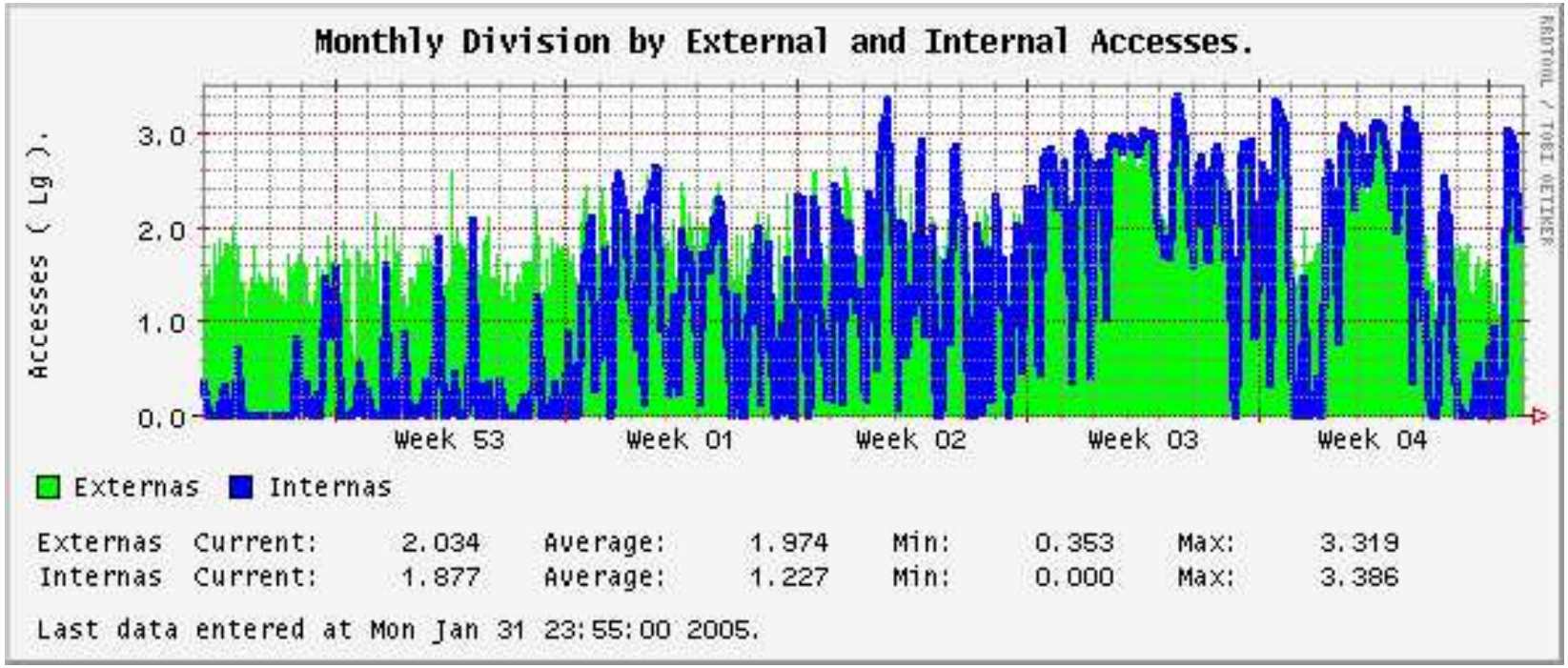


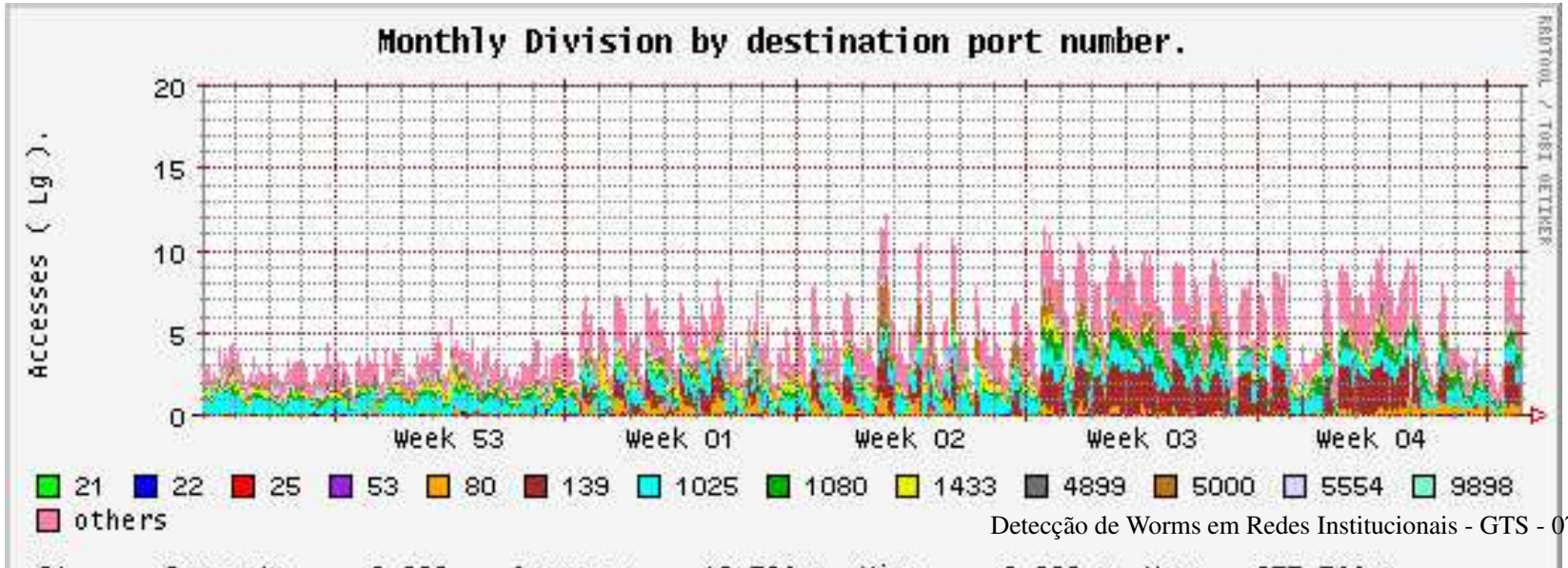
Estudo de caso: Instituição 1 (12/2004)



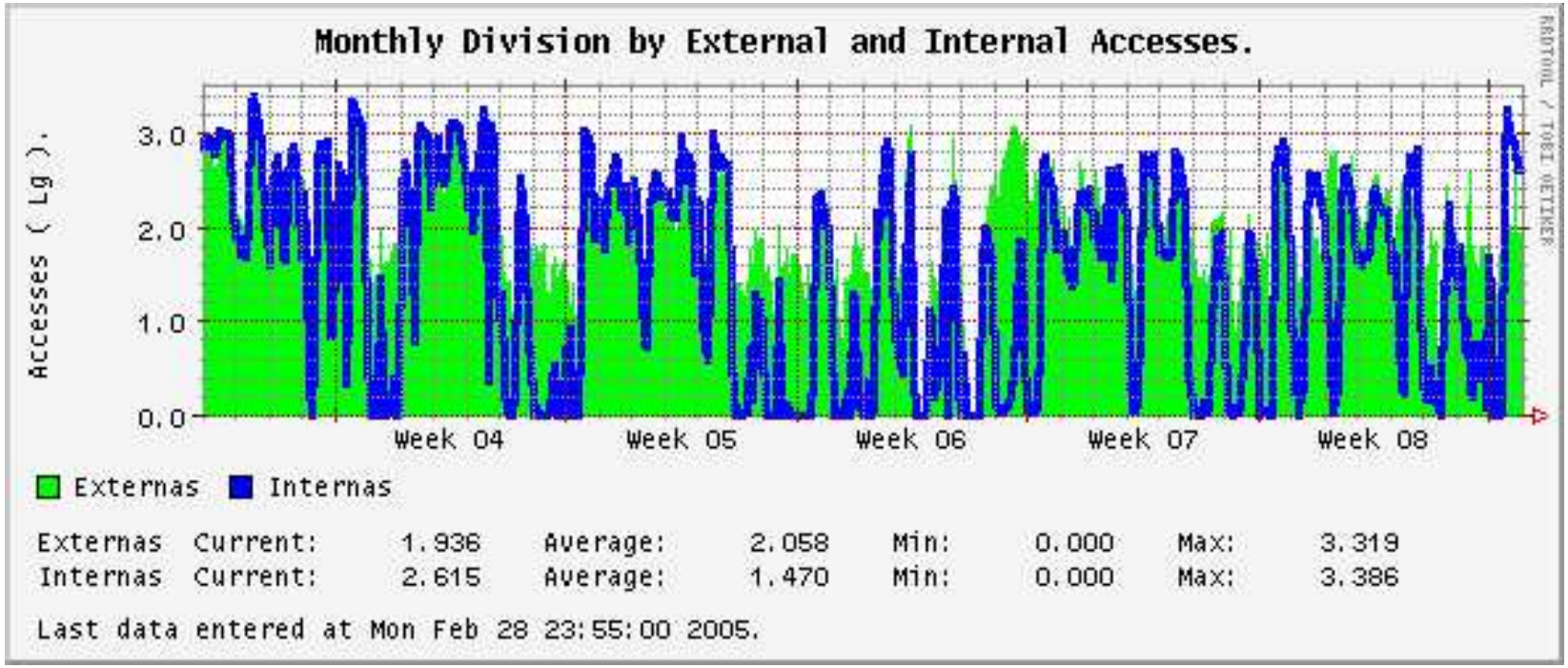


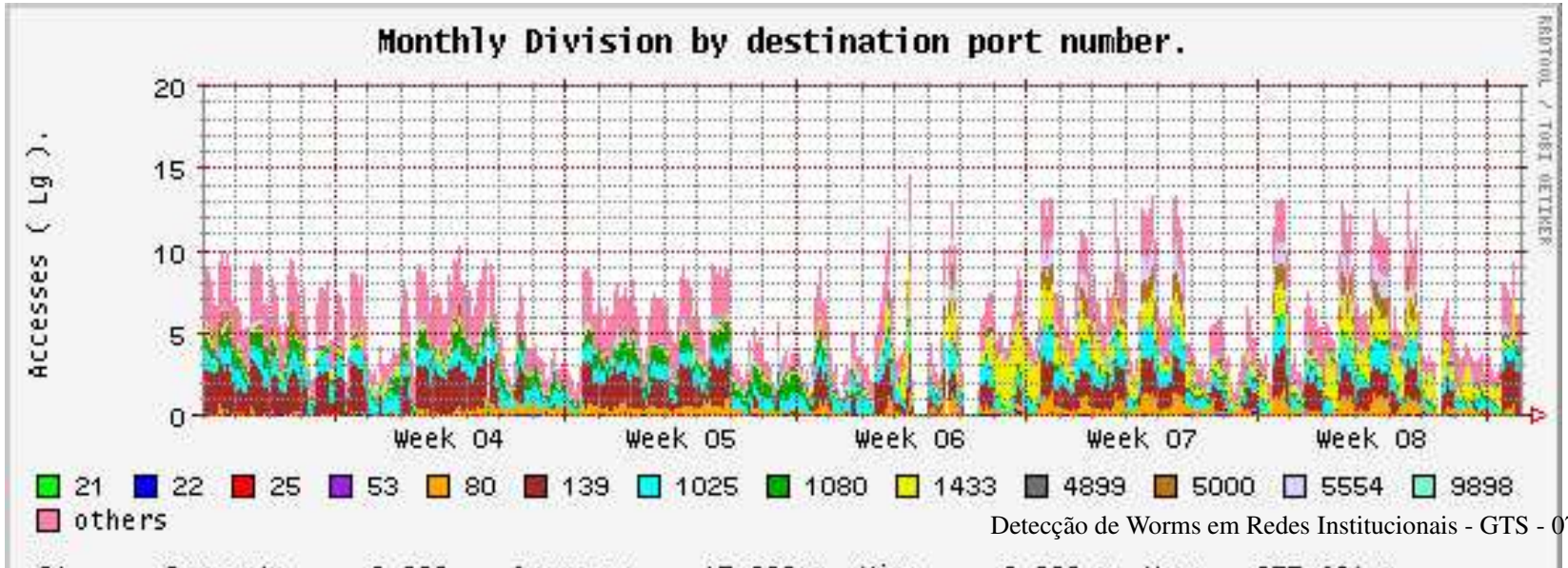
Estudo de caso: Instituição 1 (01/2005)



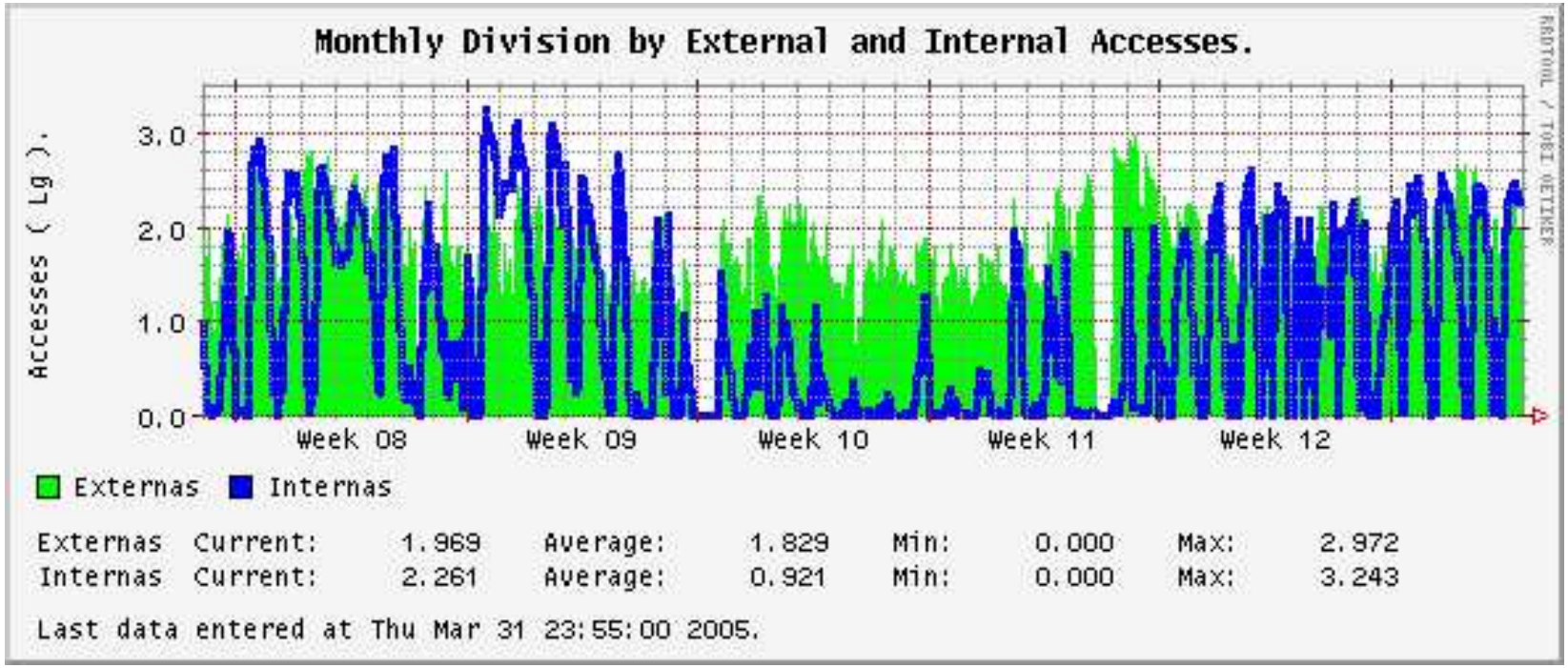


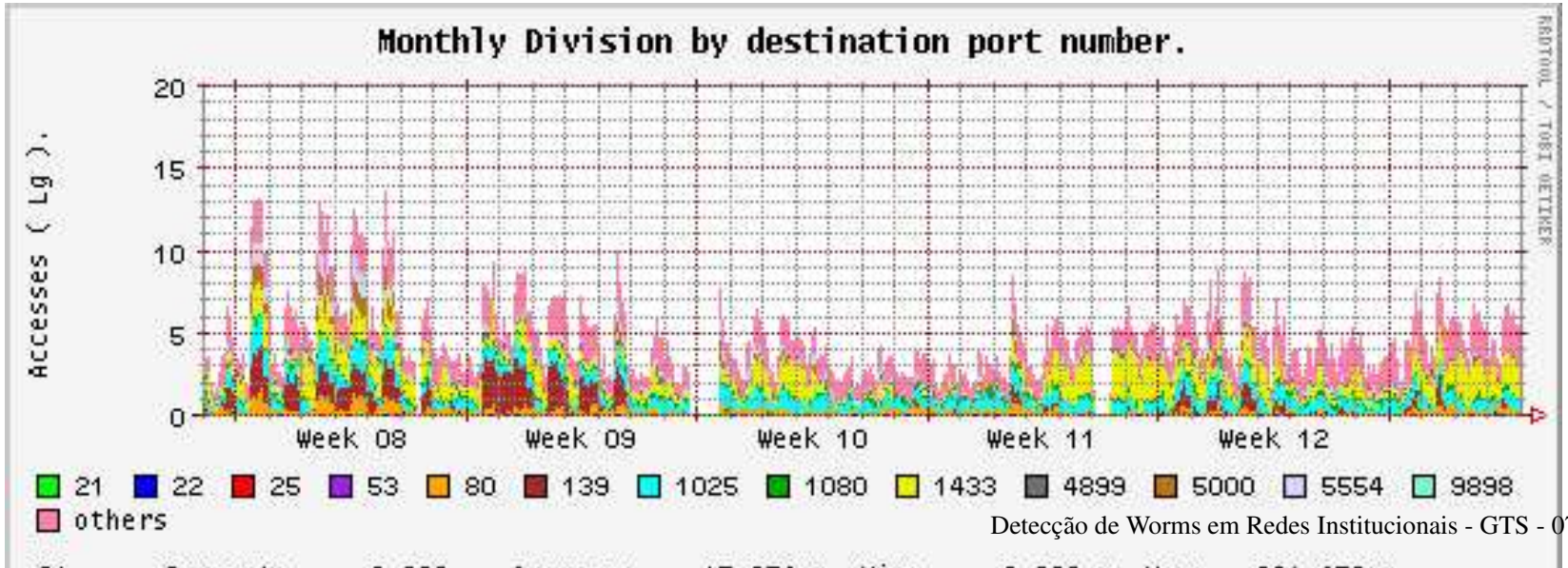
Estudo de caso: Instituição 1 (02/2005)





Estudo de caso: Instituição 1 (03/2005)

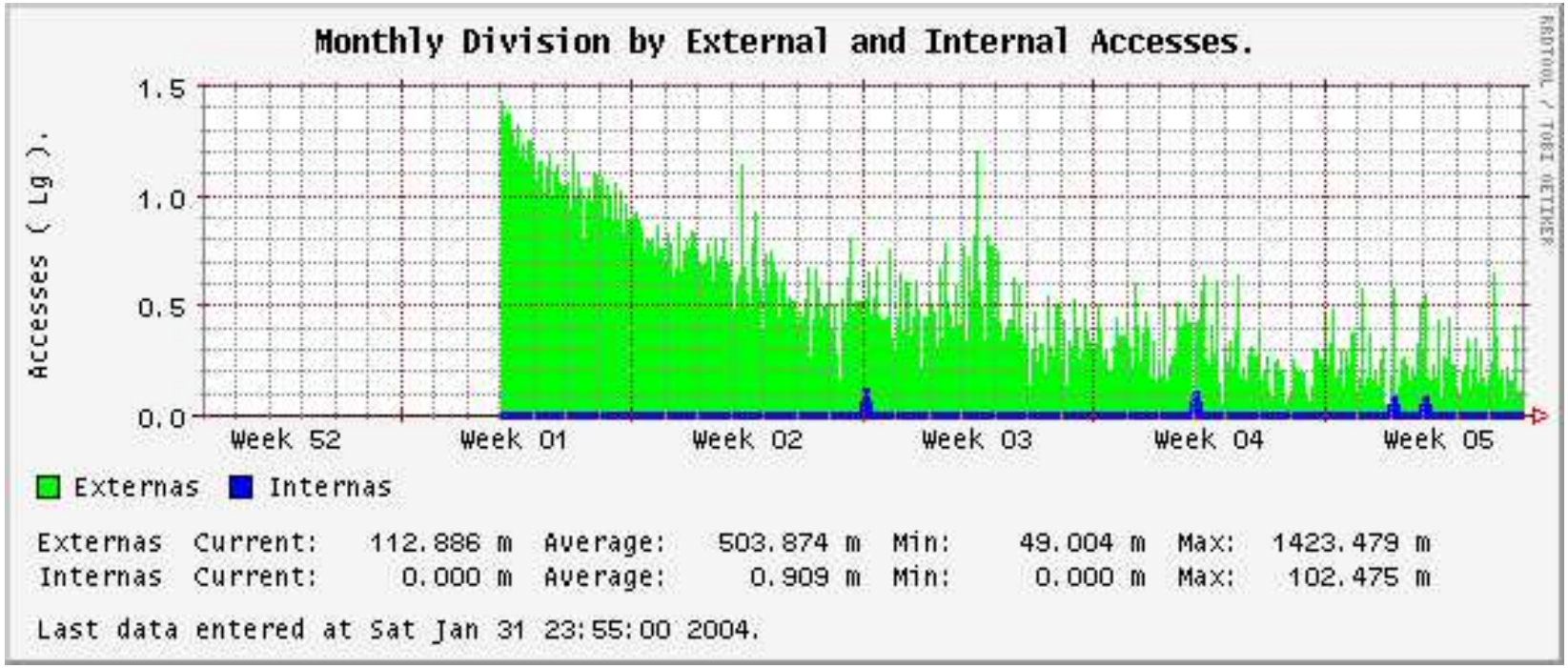


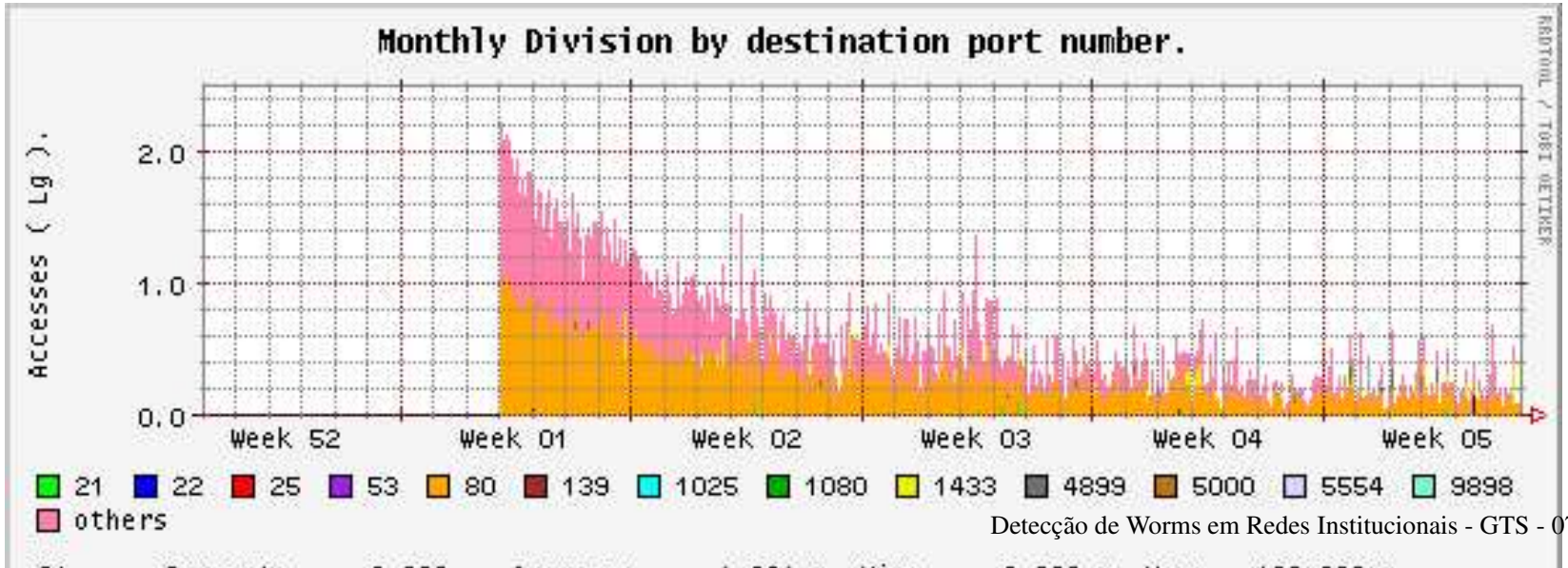


Como identificar *worms*? I

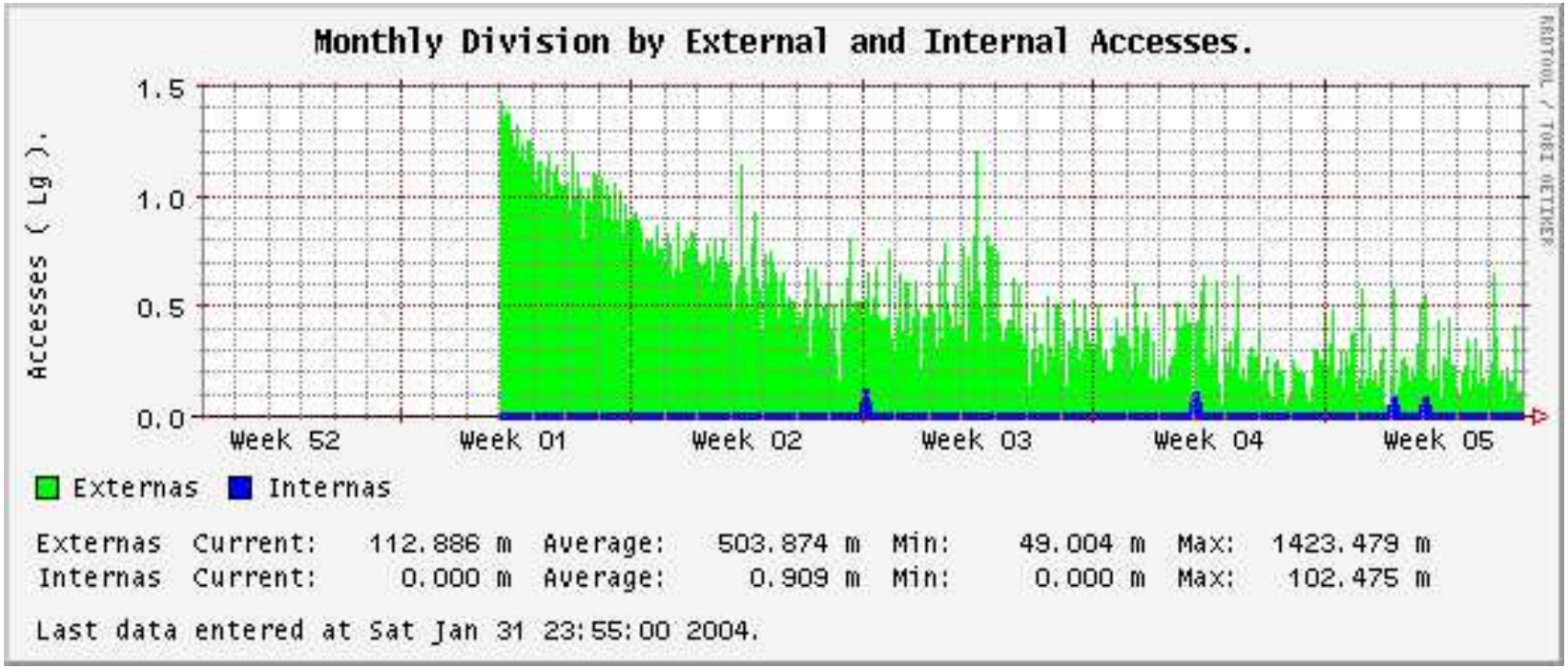
- **SASSER**: TCP 445, 5554, 9996;
- **DABBER**: TCP 5554, 8967, 9898;
- **SLAMMER**: UDP 1433, 1434;
- **BOBAX**: TCP 445, 5000;
- **KIBUV**: TCP 135, 445, ...

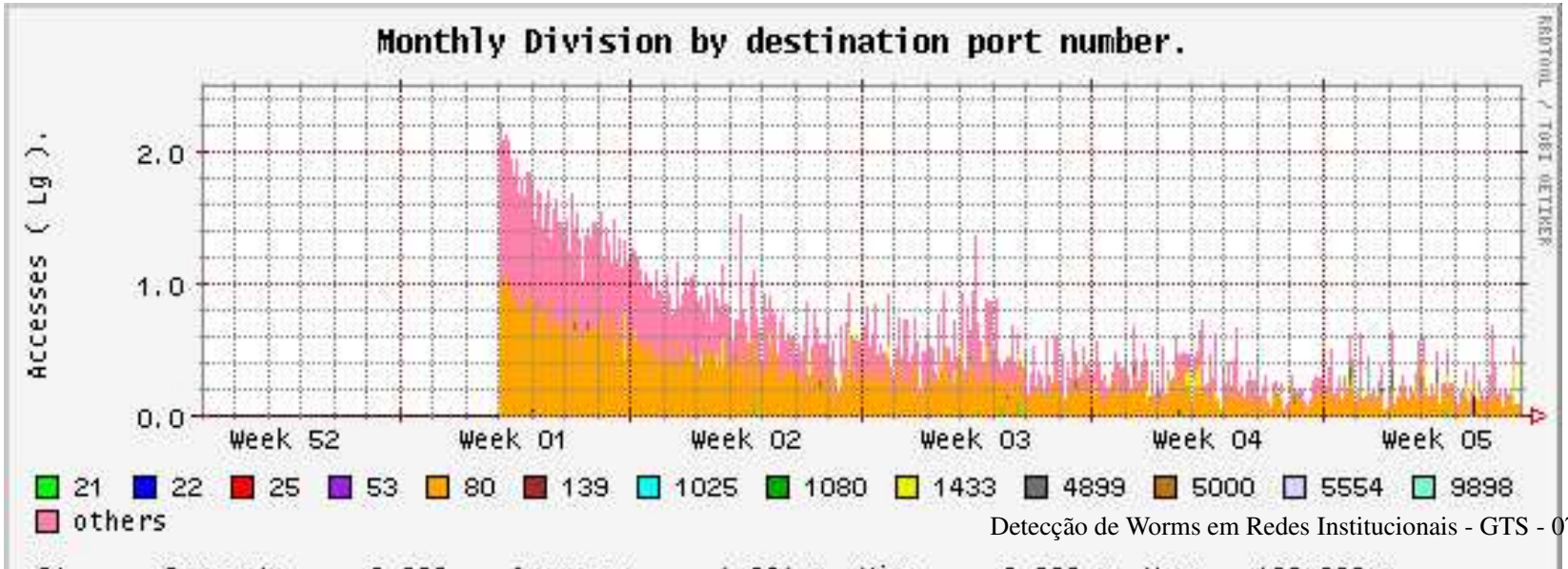
Estudo de caso: Instituição 2 (01/2004)



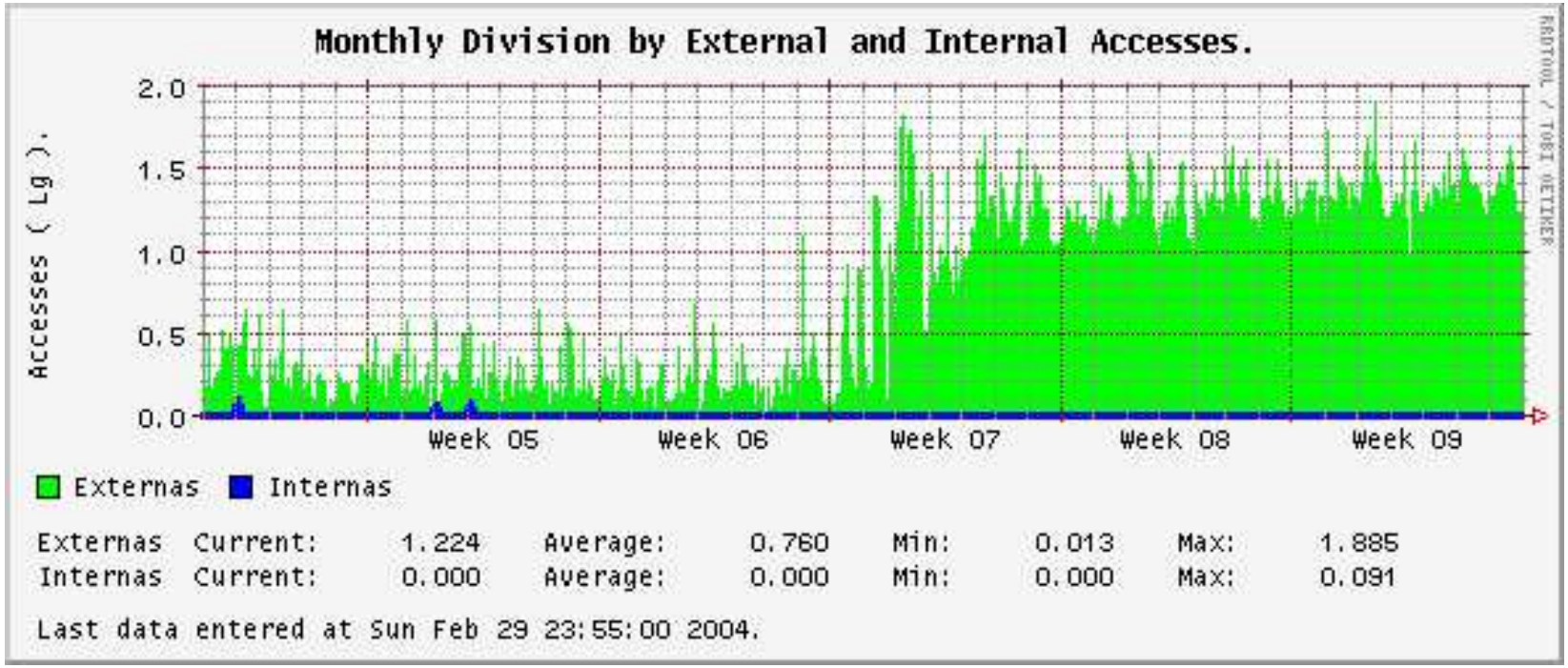


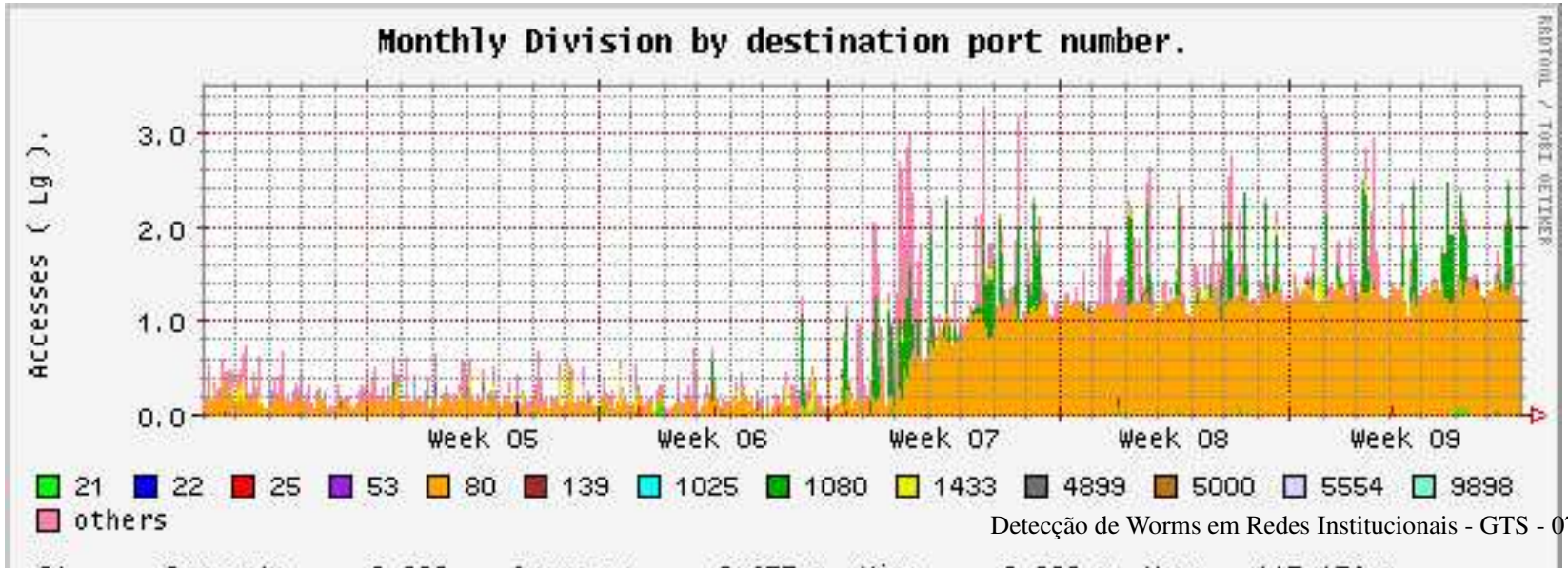
Estudo de caso: Instituição 2 (01/2004)



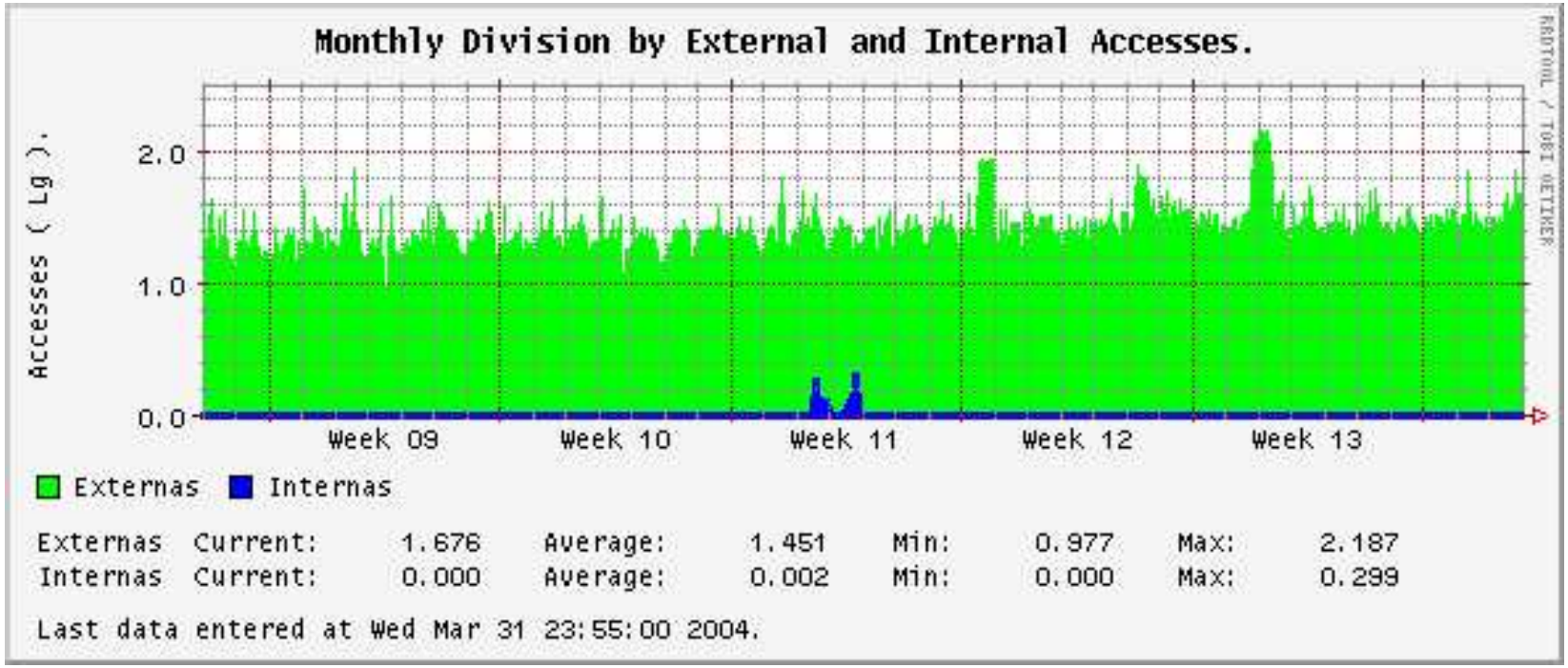


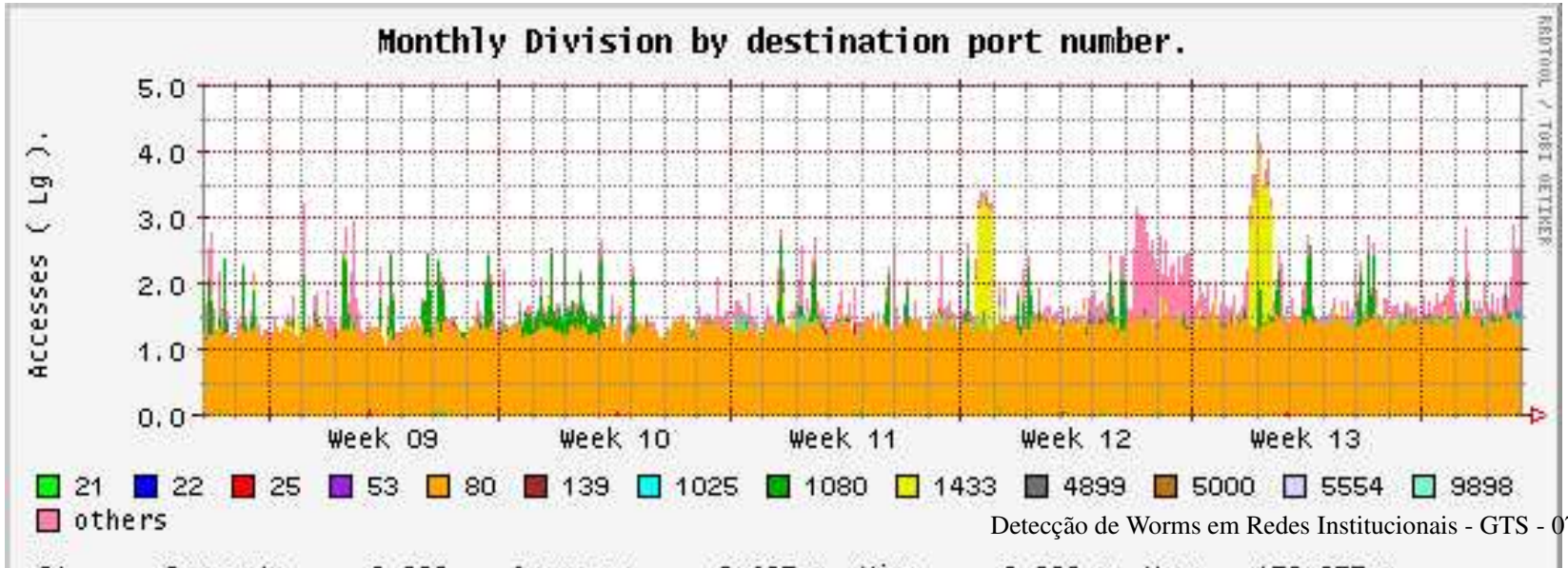
Estudo de caso: Instituição 2 (02/2004)



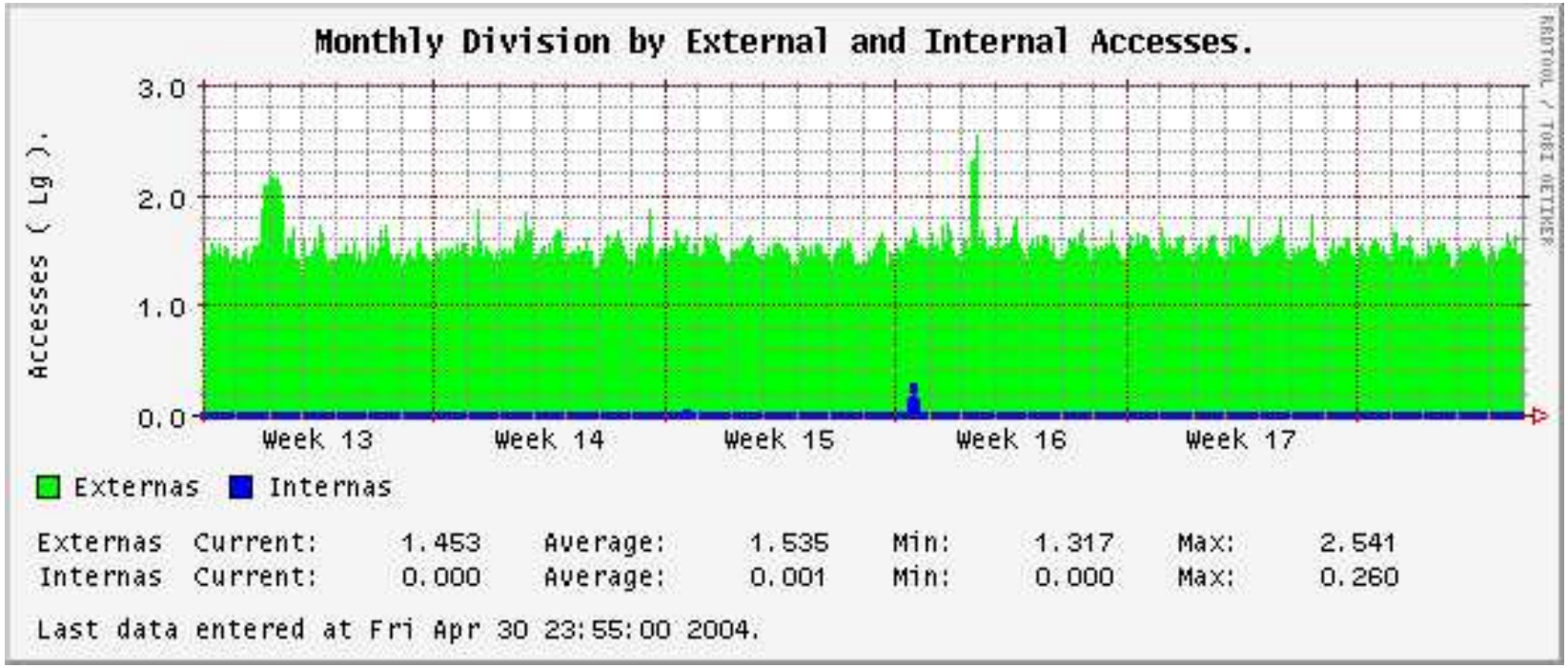


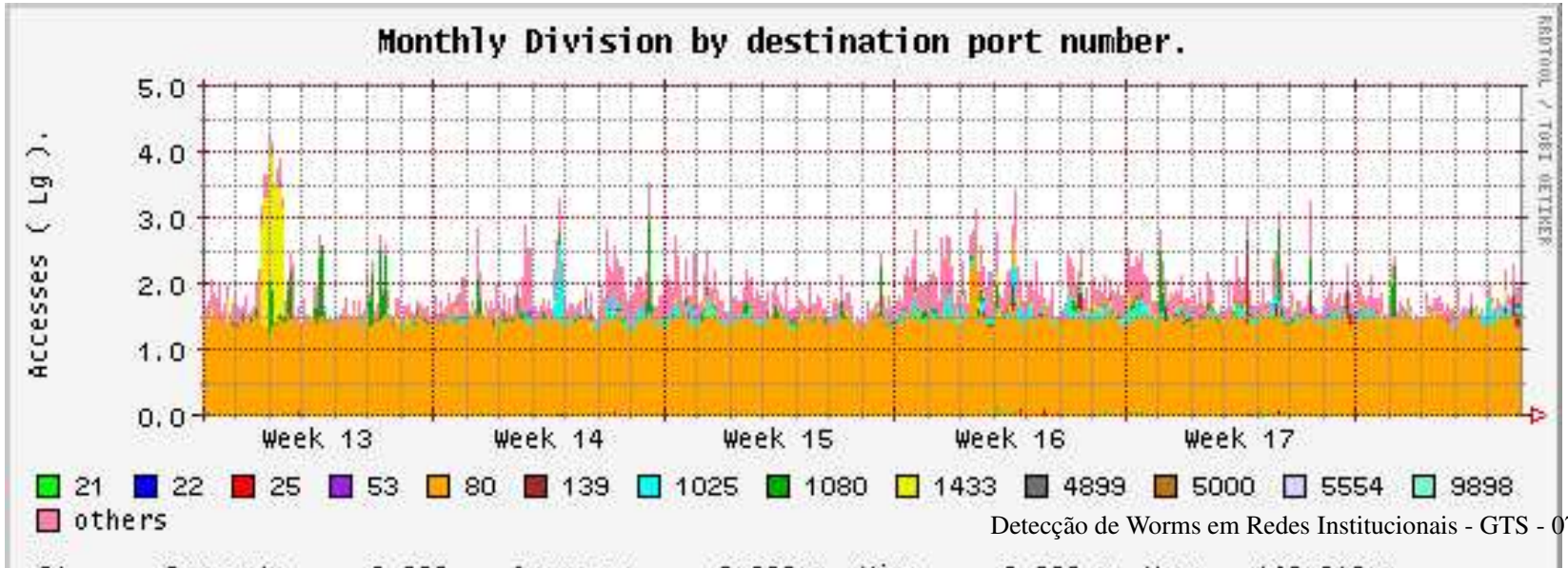
Estudo de caso: Instituição 2 (03/2004)



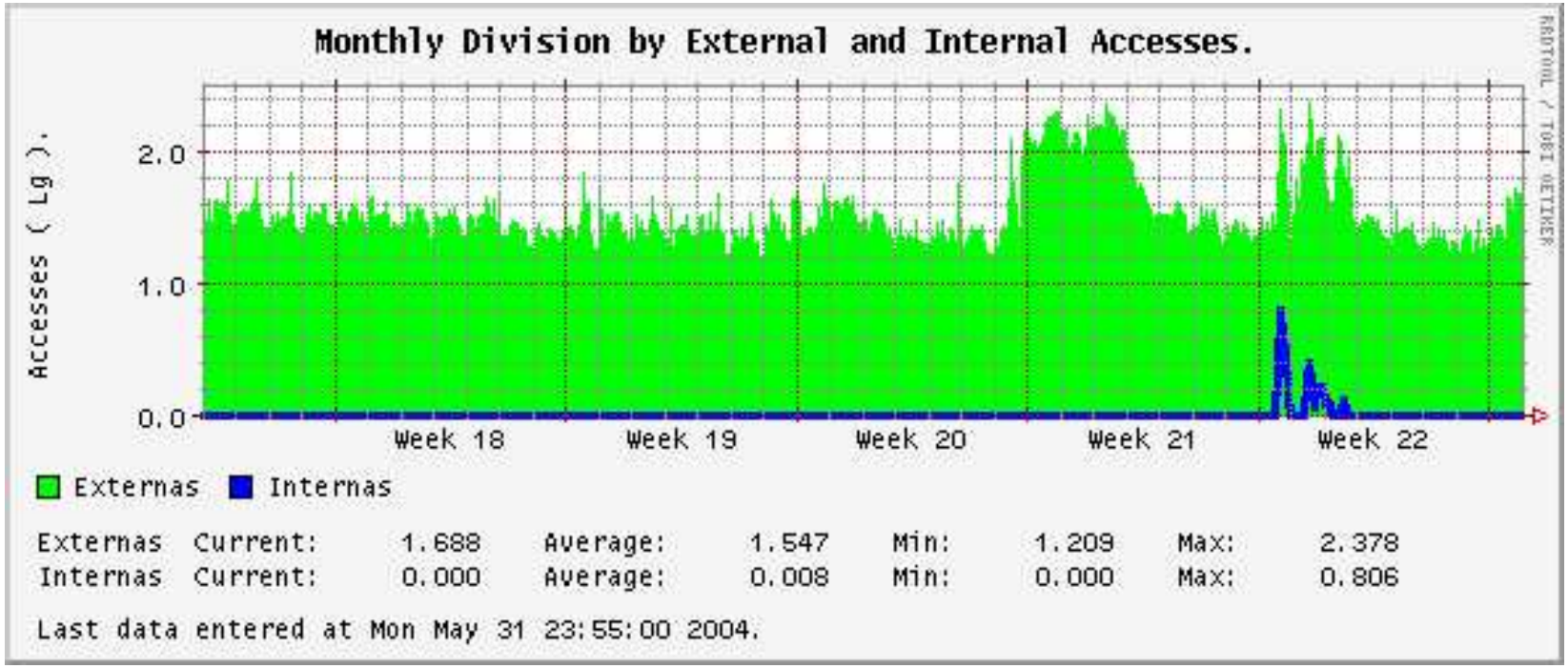


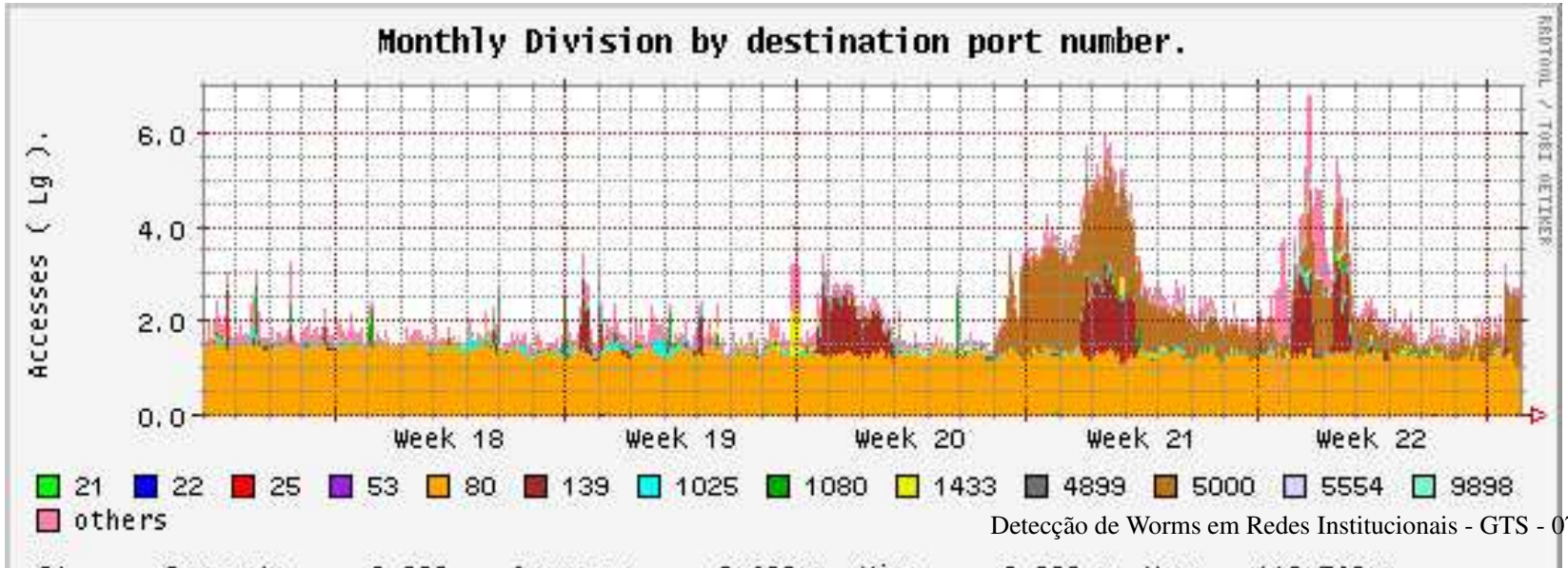
Estudo de caso: Instituição 2 (04/2004)



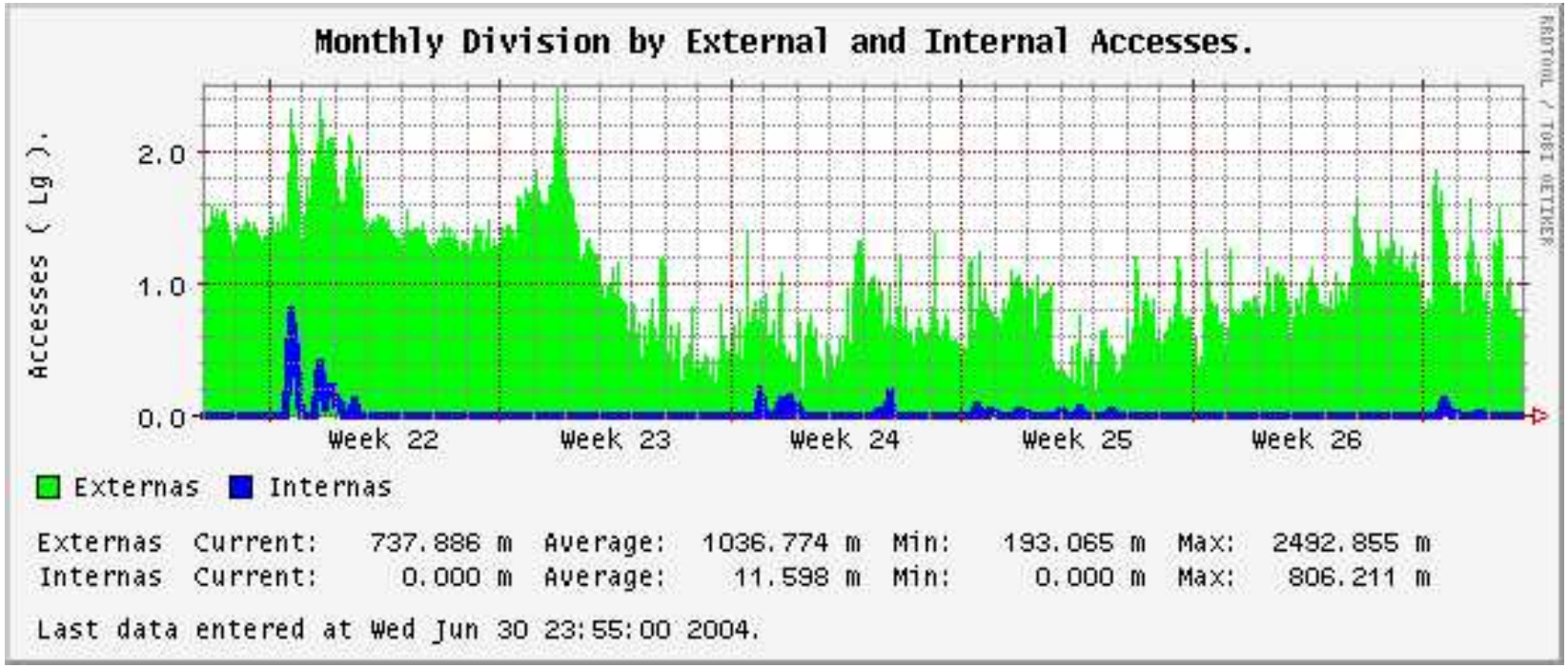


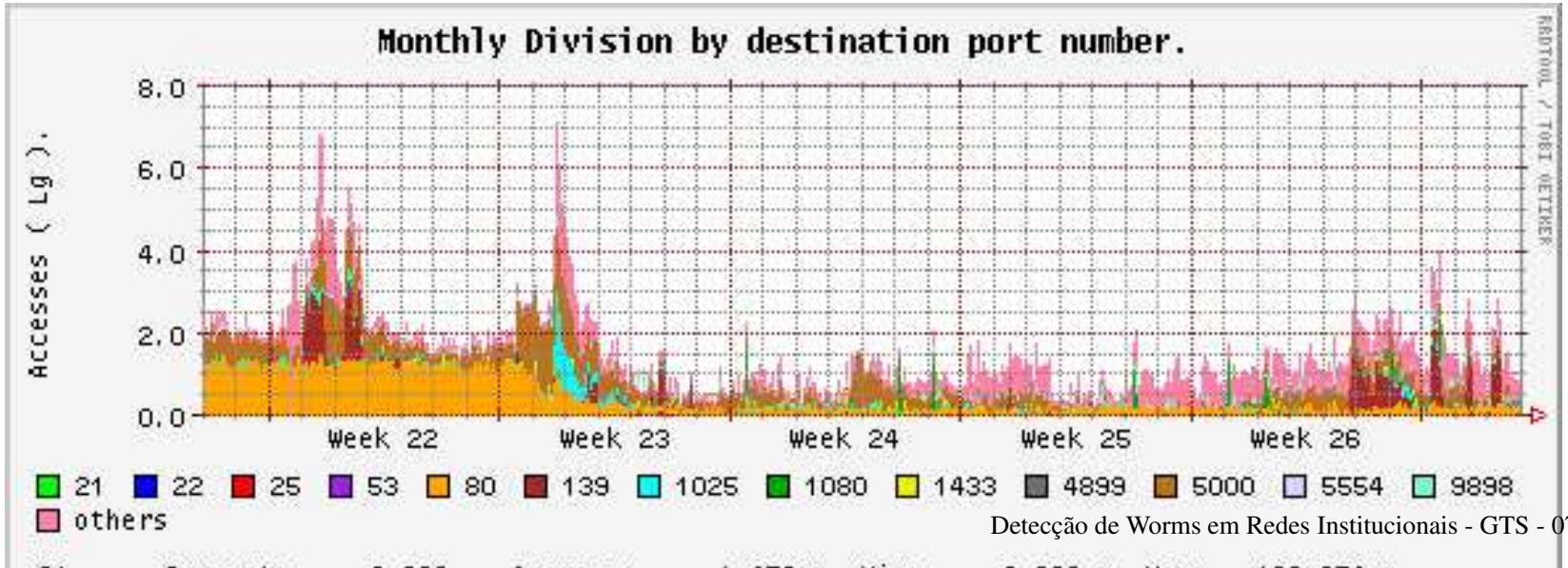
Estudo de caso: Instituição 2 (05/2004)



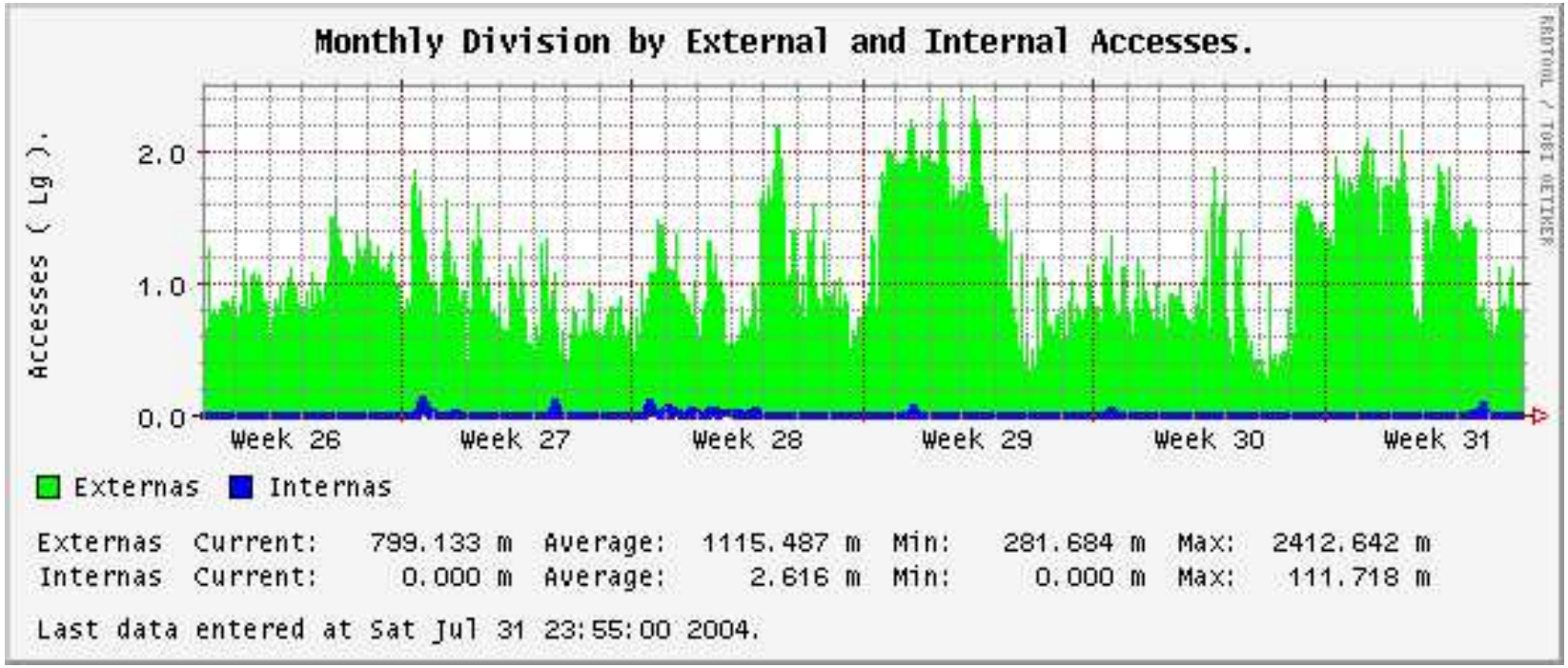


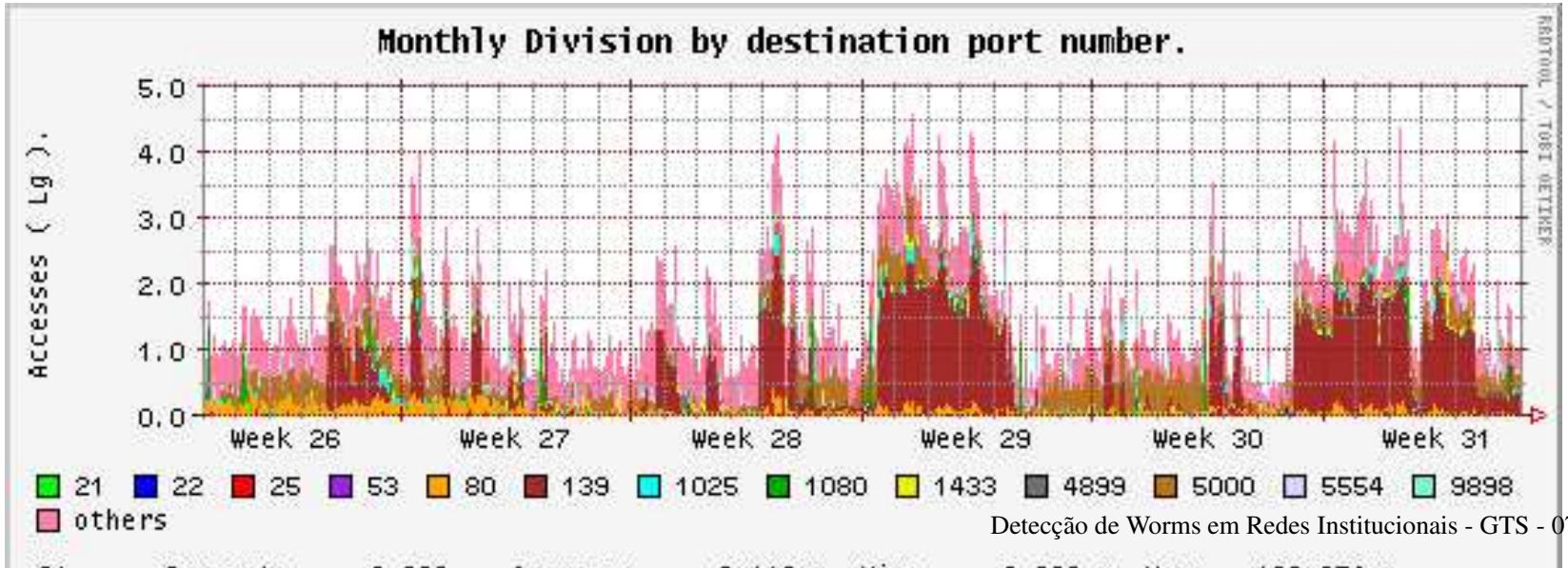
Estudo de caso: Instituição 2 (06/2004)



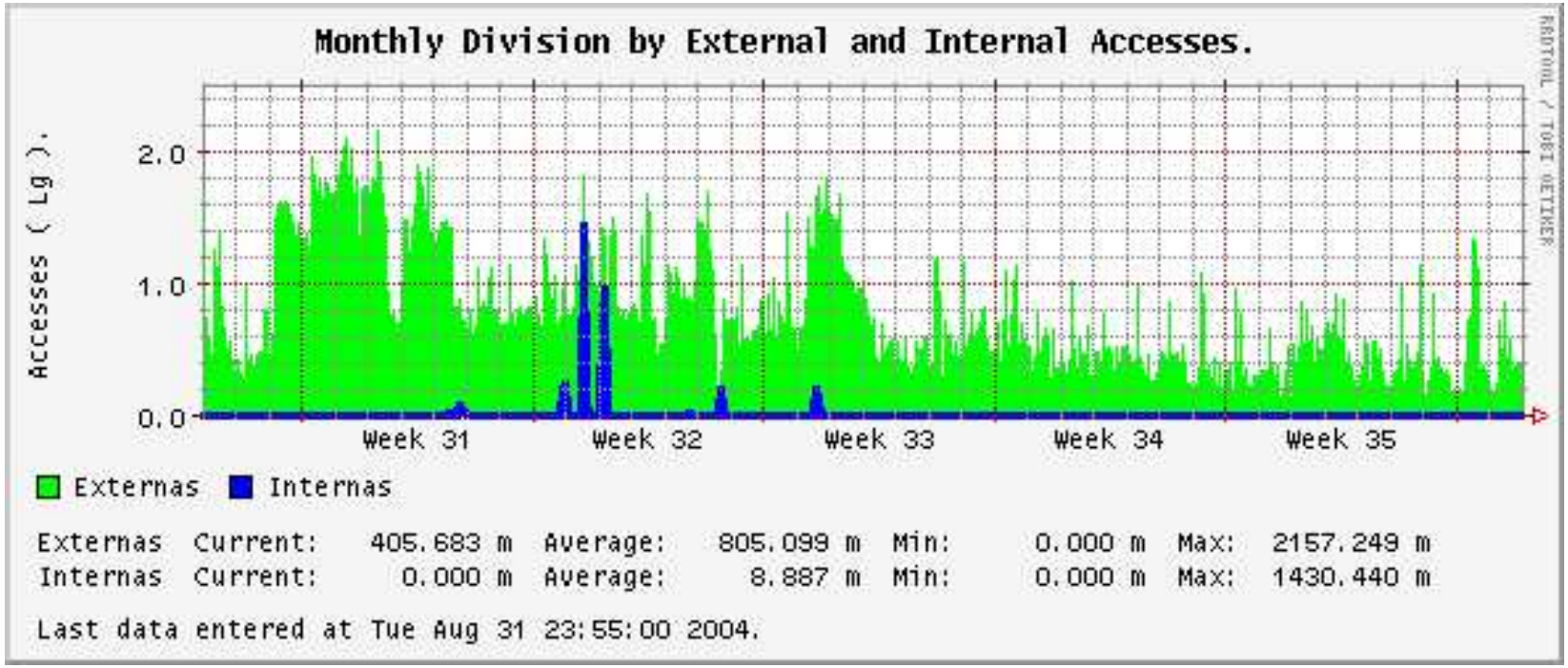


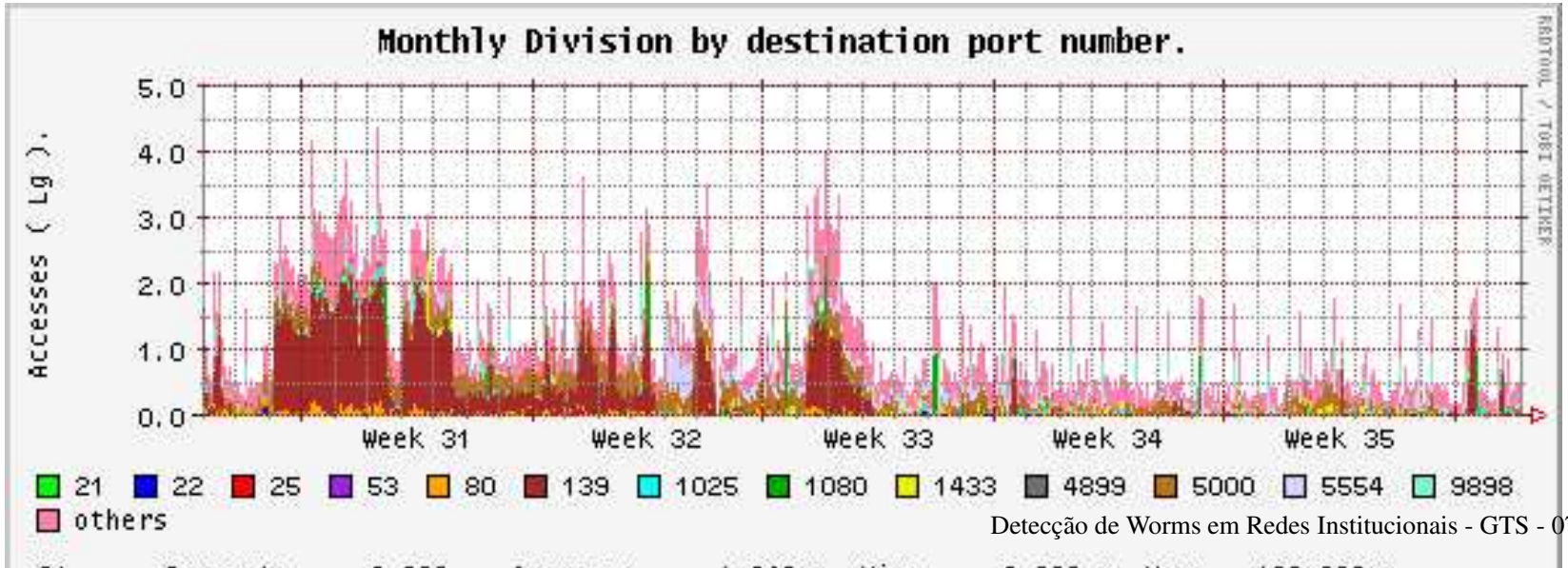
Estudo de caso: Instituição 2 (07/2004)



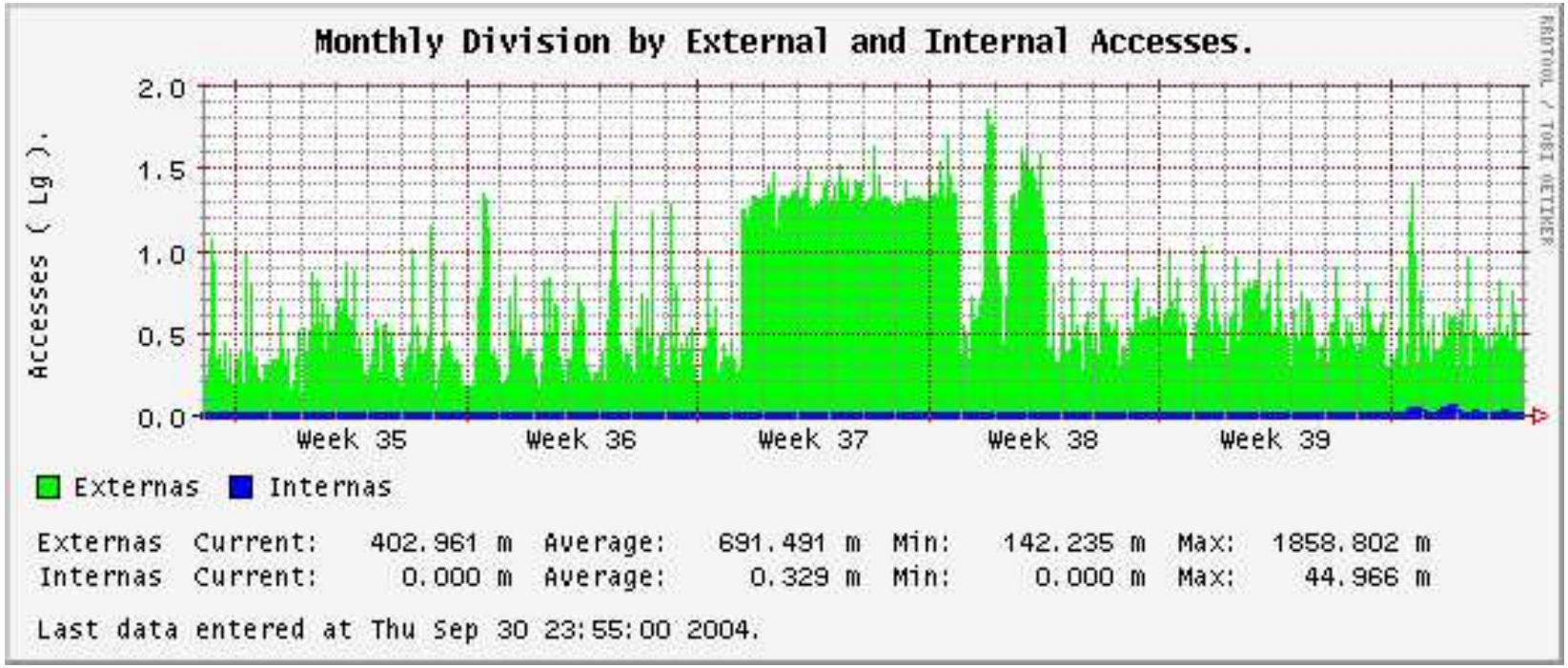


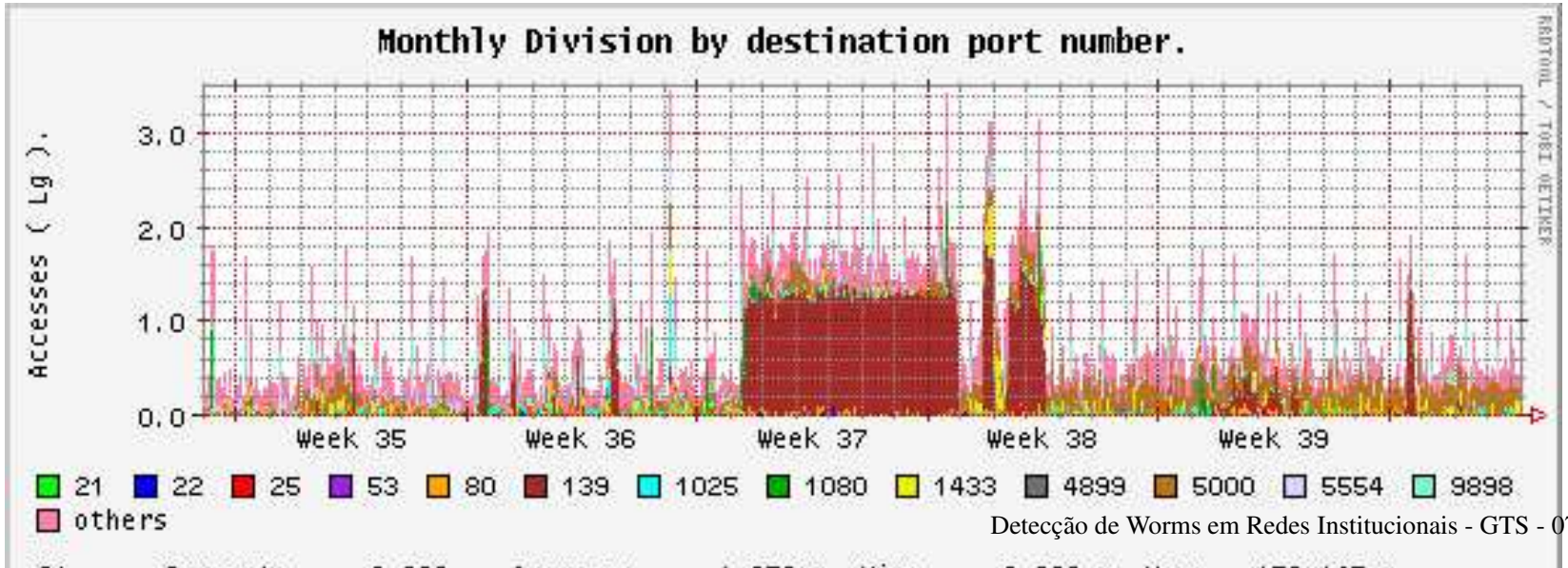
Estudo de caso: Instituição 2 (08/2004)



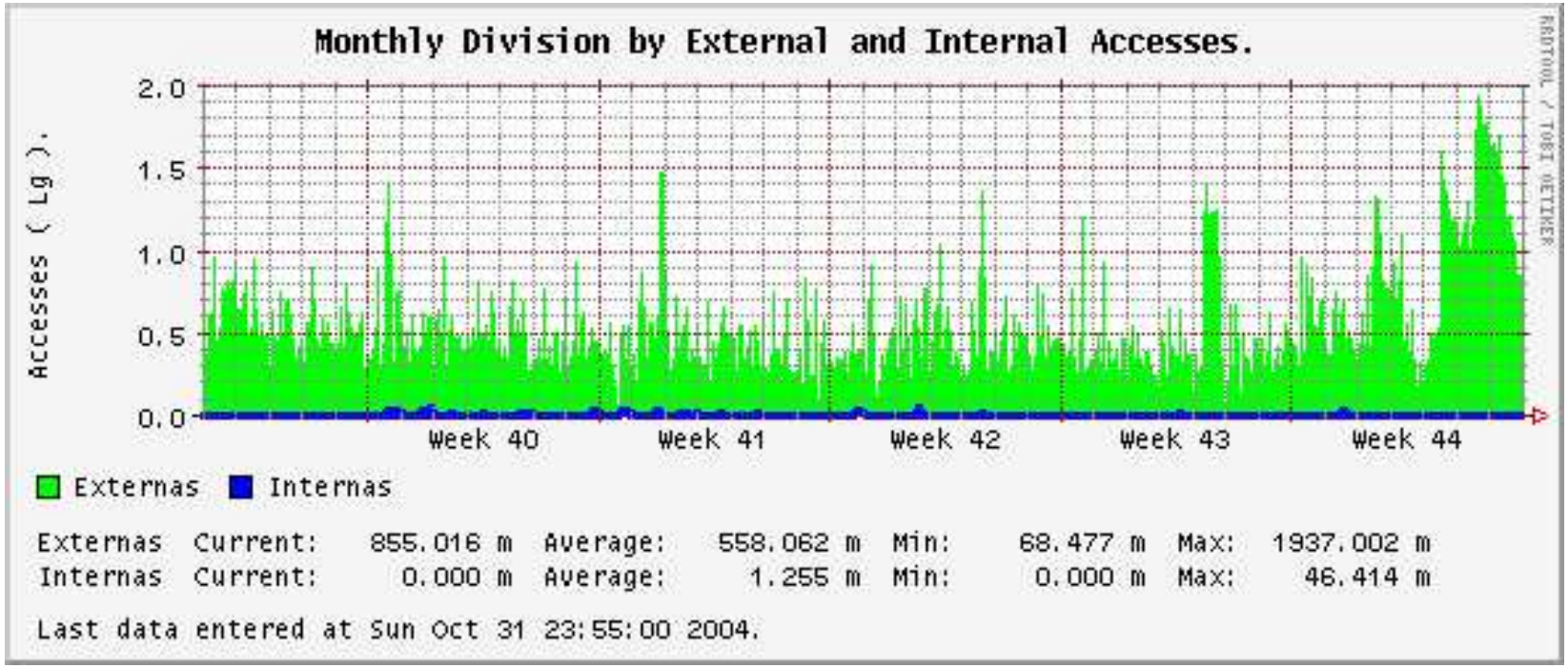


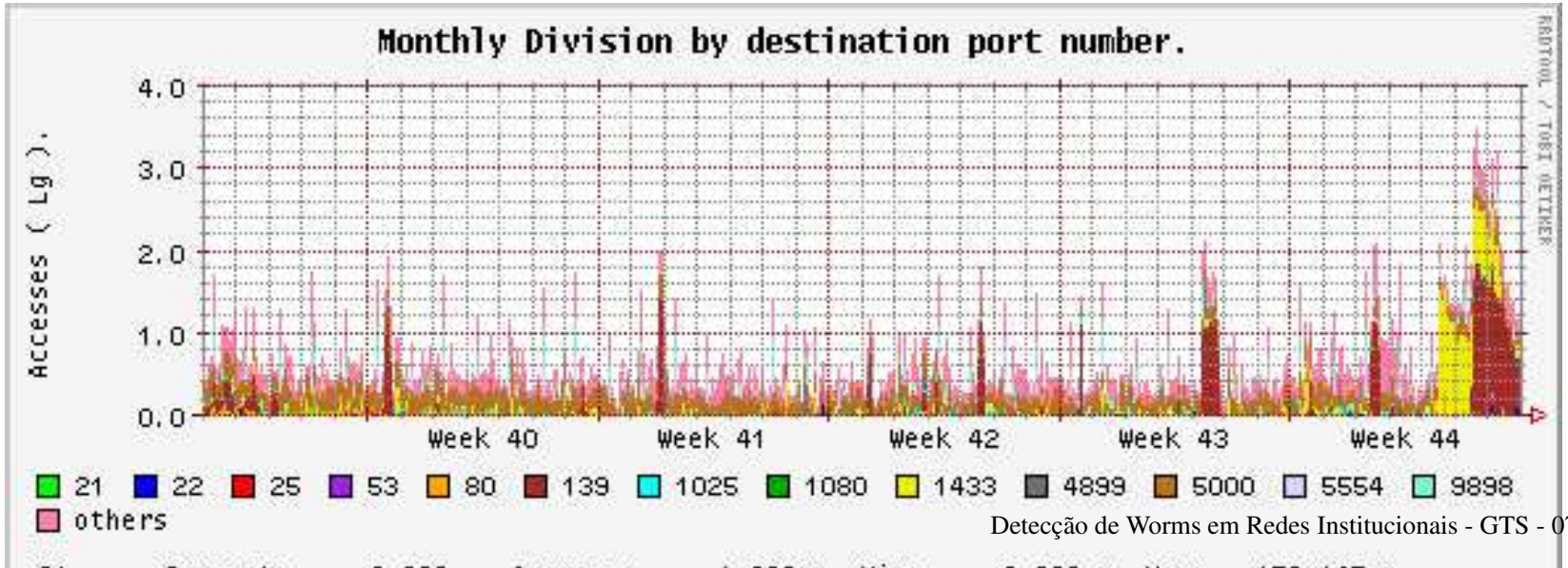
Estudo de caso: Instituição 2 (09/2004)



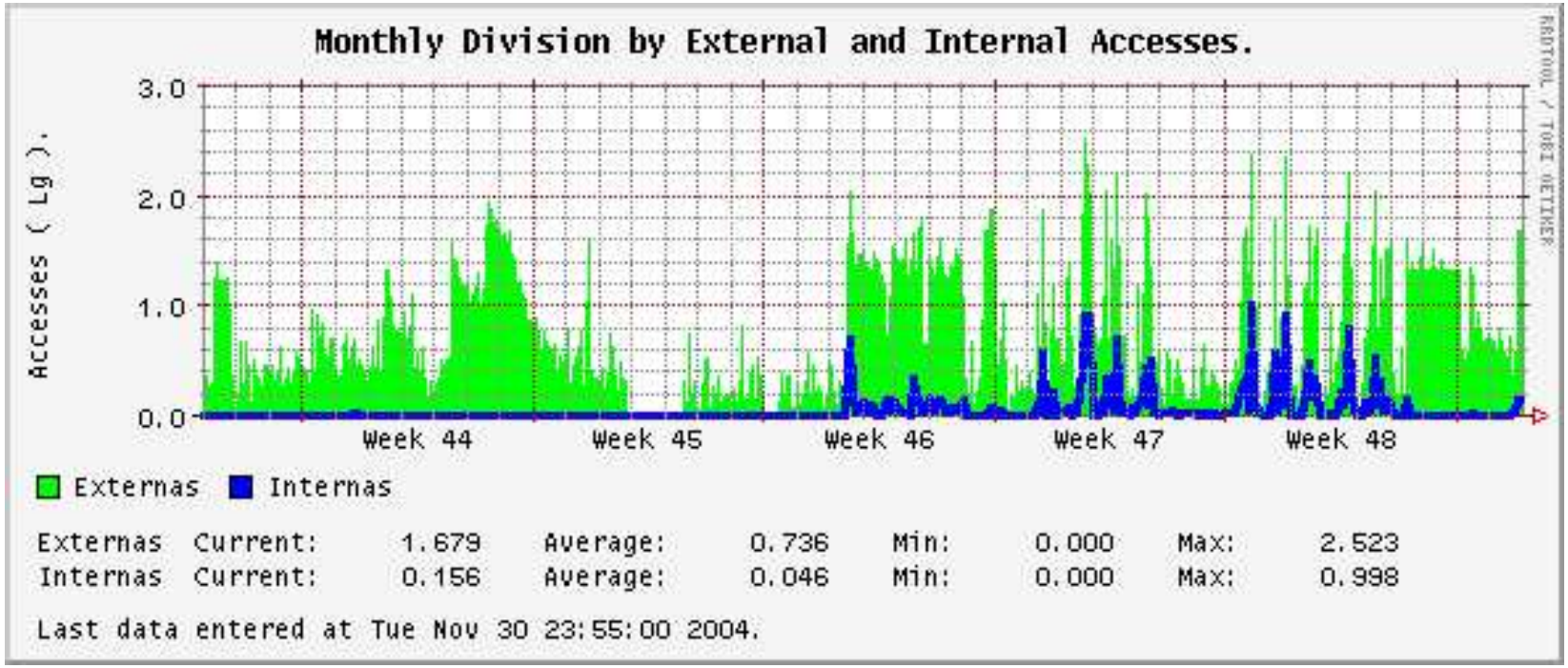


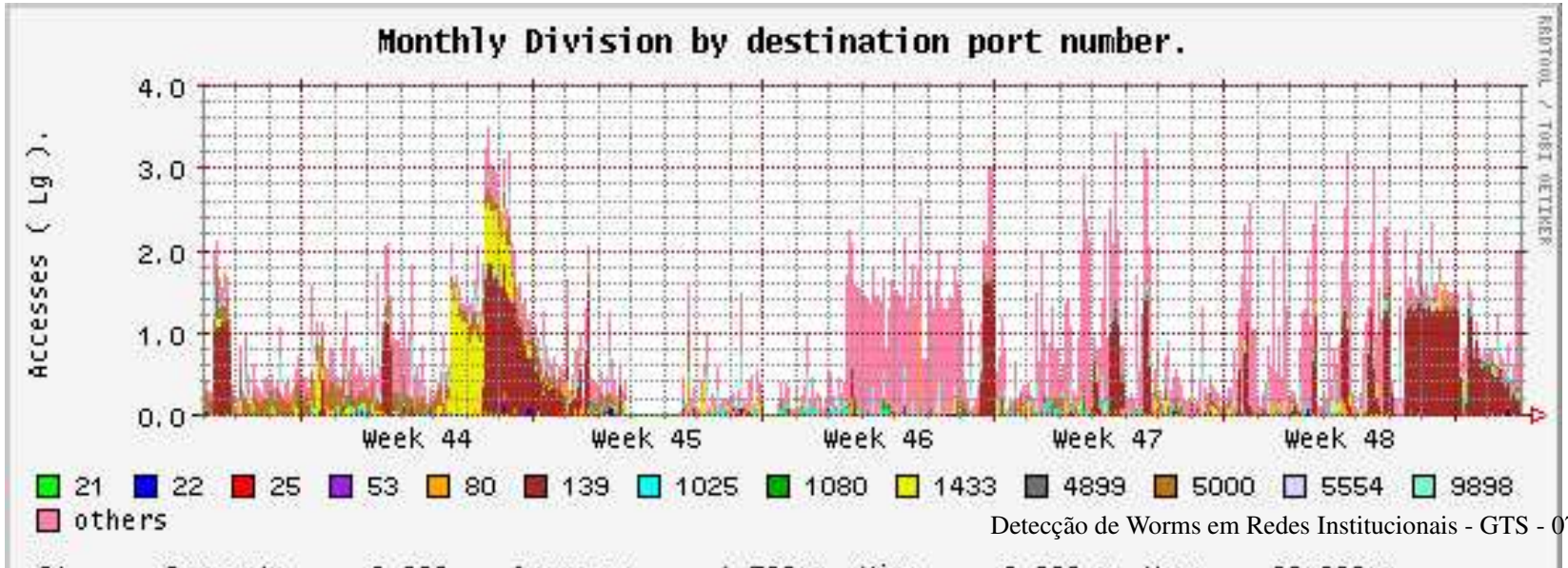
Estudo de caso: Instituição 2 (10/2004)



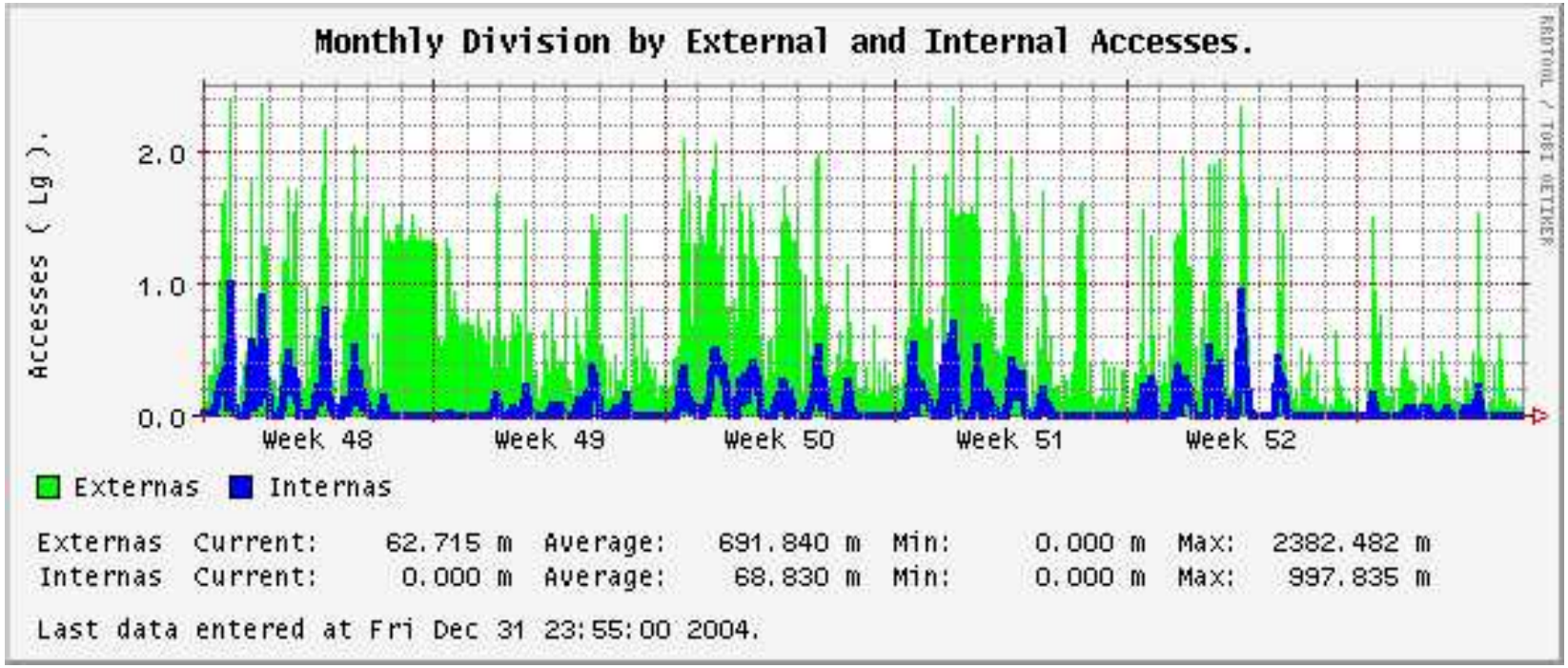


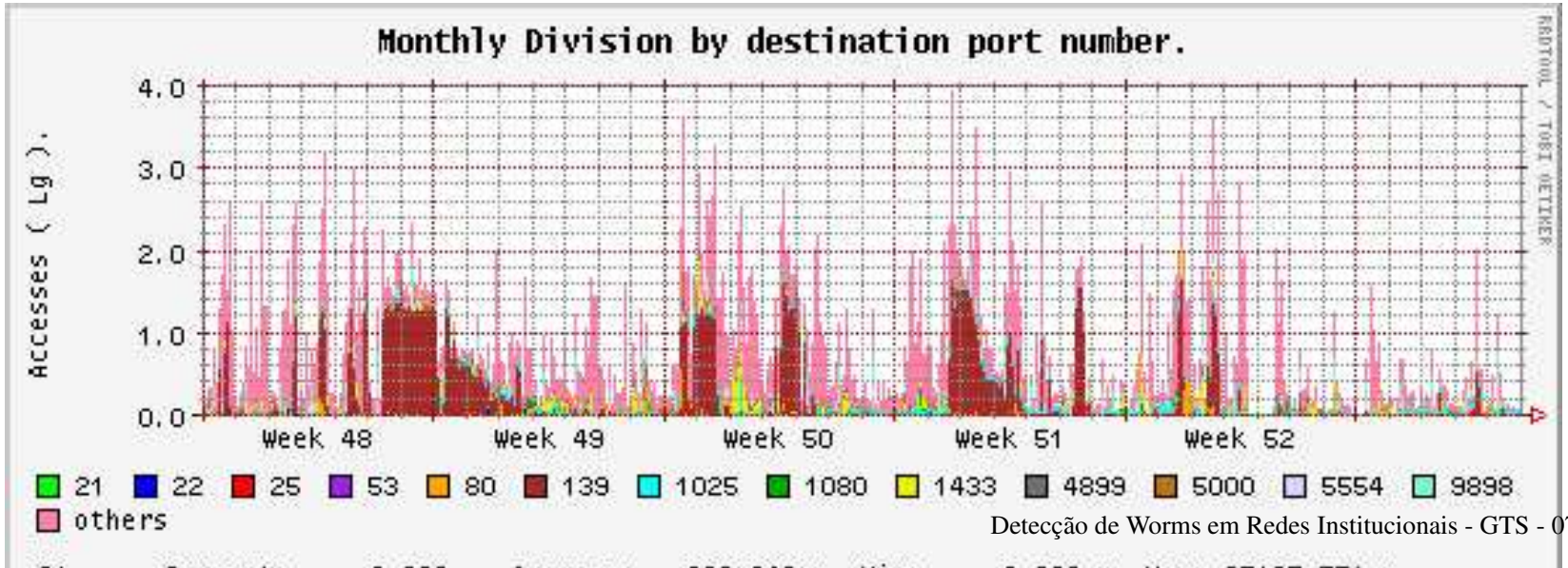
Estudo de caso: Instituição 2 (11/2004)





Estudo de caso: Instituição 2 (12/2004)





Conclusões I

- Na Instituição 1, a abordagem via *script*, serviu para ter-se uma idéia mais precisa da ordem de grandeza das infecções, permitindo melhor rapidez no tratamento dos casos de *worms*;
- Auxiliou os administradores a correr atrás do problema, mas os administradores são em número pequeno e a disseminação dos *worms* é mais rápida que as ações que devem ser tomadas.

Conclusões II

- **FALTA:** Sistematizar práticas eficientes de desinfecção na Instituição 1.
- Em ambos os casos, foi possível detectar atividades que não atendem às políticas de segurança das organizações.

Trabalhos Futuros

- Utilizar *logs* de capturas de pacotes para identificar assinaturas de *worms*;
- Aprimorar e implantar o sistema de geração de gráficos.

Obrigado!

Luiz Otávio Duarte
<duarte@lac.inpe.br>
PGPi KeyID: 4CF4CB68

André Ricardo Abed Grégio
<andre.gregio@lac.inpe.br>
PGPi KeyID: 00940DC6

Adriano Mauro Cansian
<adriano@acmesecurity.org>
PGPi KeyID: 3893CD2B

Antonio Montes
<antonio.montes@cenpra.gov.br>
PGPi KeyID: AB2FF611