Devo estar falando Português?

Richard Clayton

SHB
4th June 2012

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

NPL
National Physical Laboratory

Instant messaging “worms”

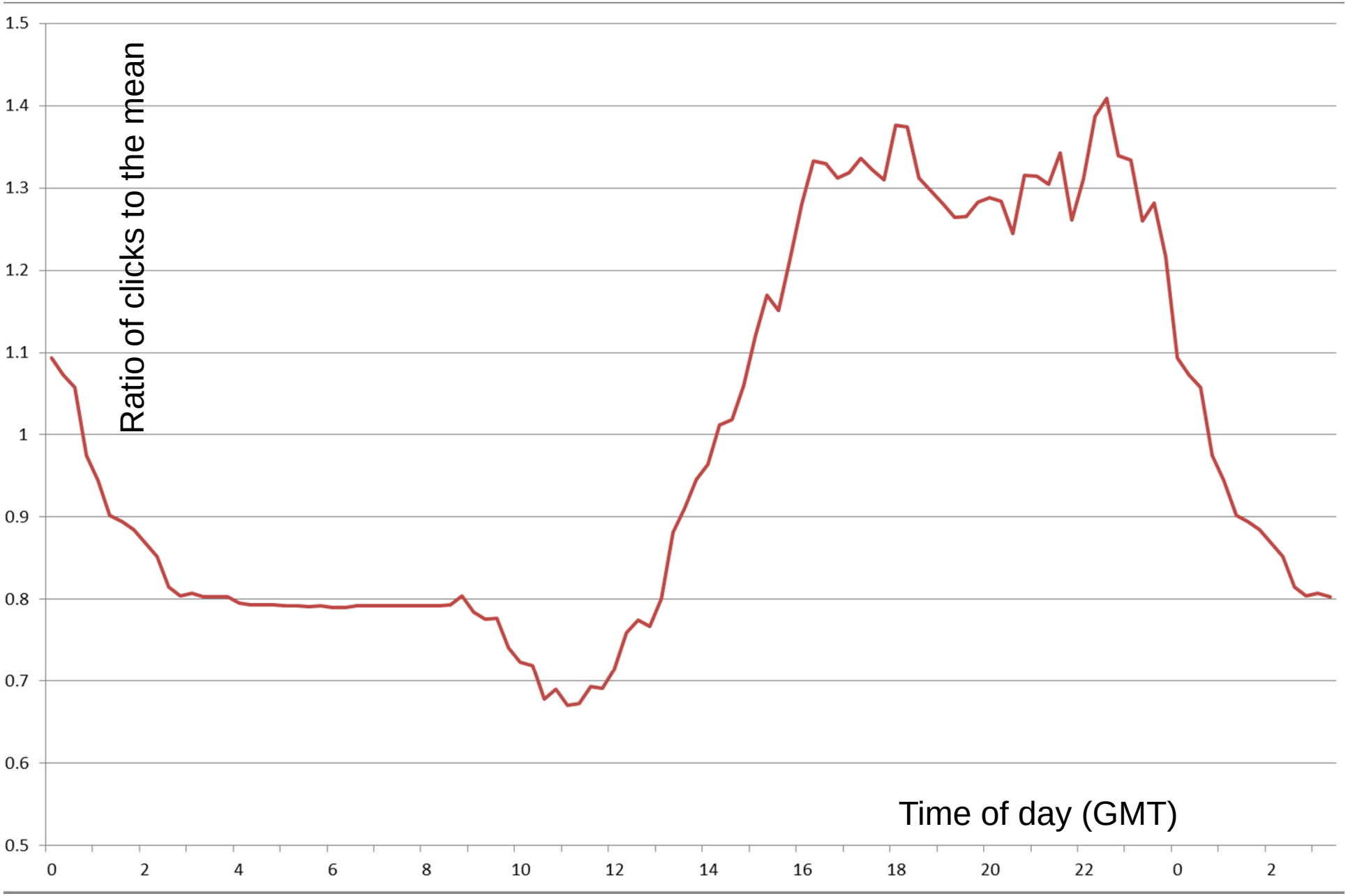
- Your IM buddy sends you a message

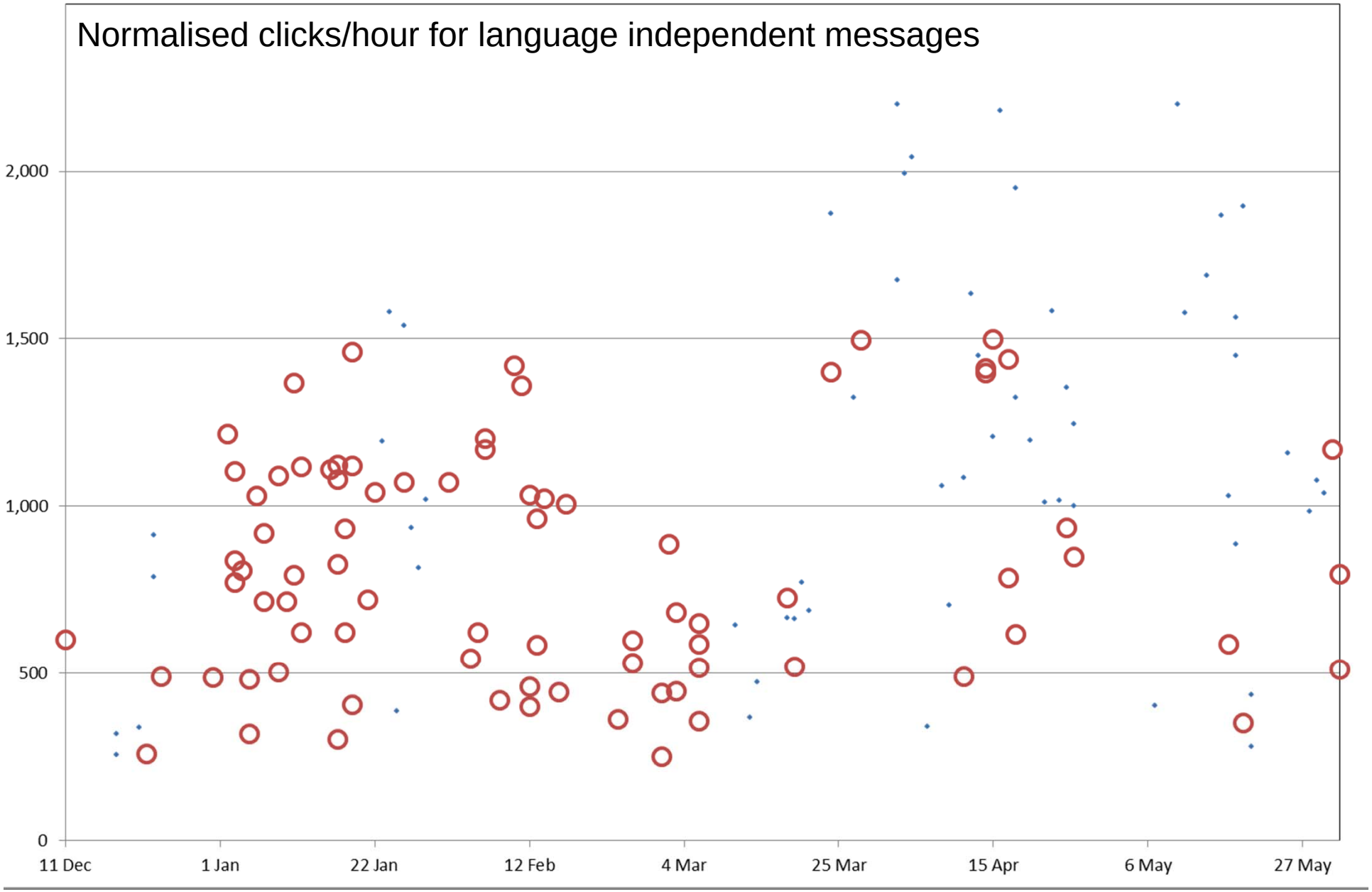
  `foto ☺ http://www.example.com/picfile.php?richard@ema.il`

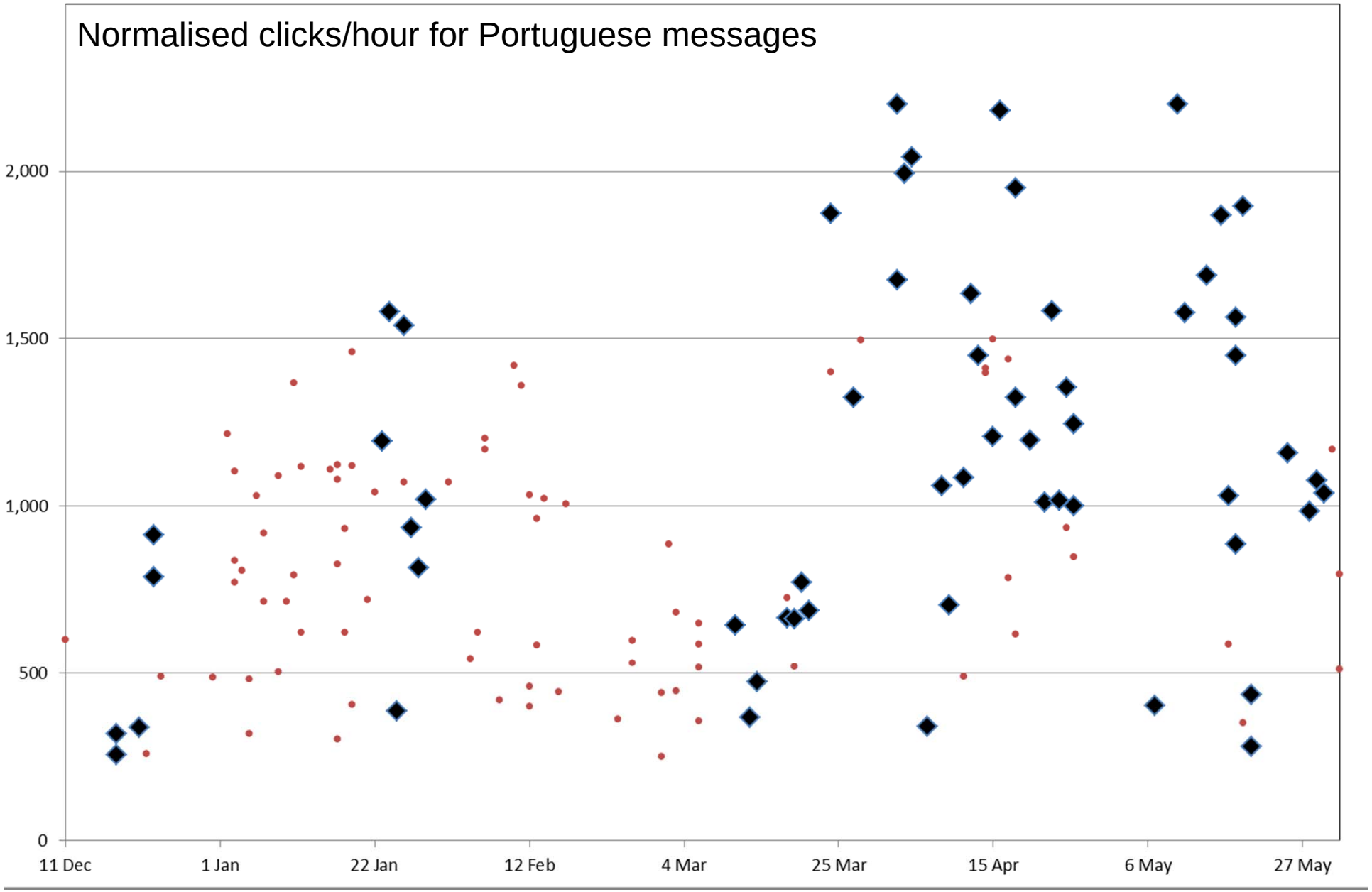
- You click on the link
- It’s an executable!
  - Microsoft dialog says “do you want to run an executable ?”
  - you read “do you want to see the picture your buddy sent ?”
  - what happens next we can only guess at…
- Once you are running the executable, it will IM all of your buddies saying **`Foto ☺ etc…`**
- Over past 2+ years this style of malware has infected millions on Yahoo! Facebook AOL Skype & Microsoft Messenger

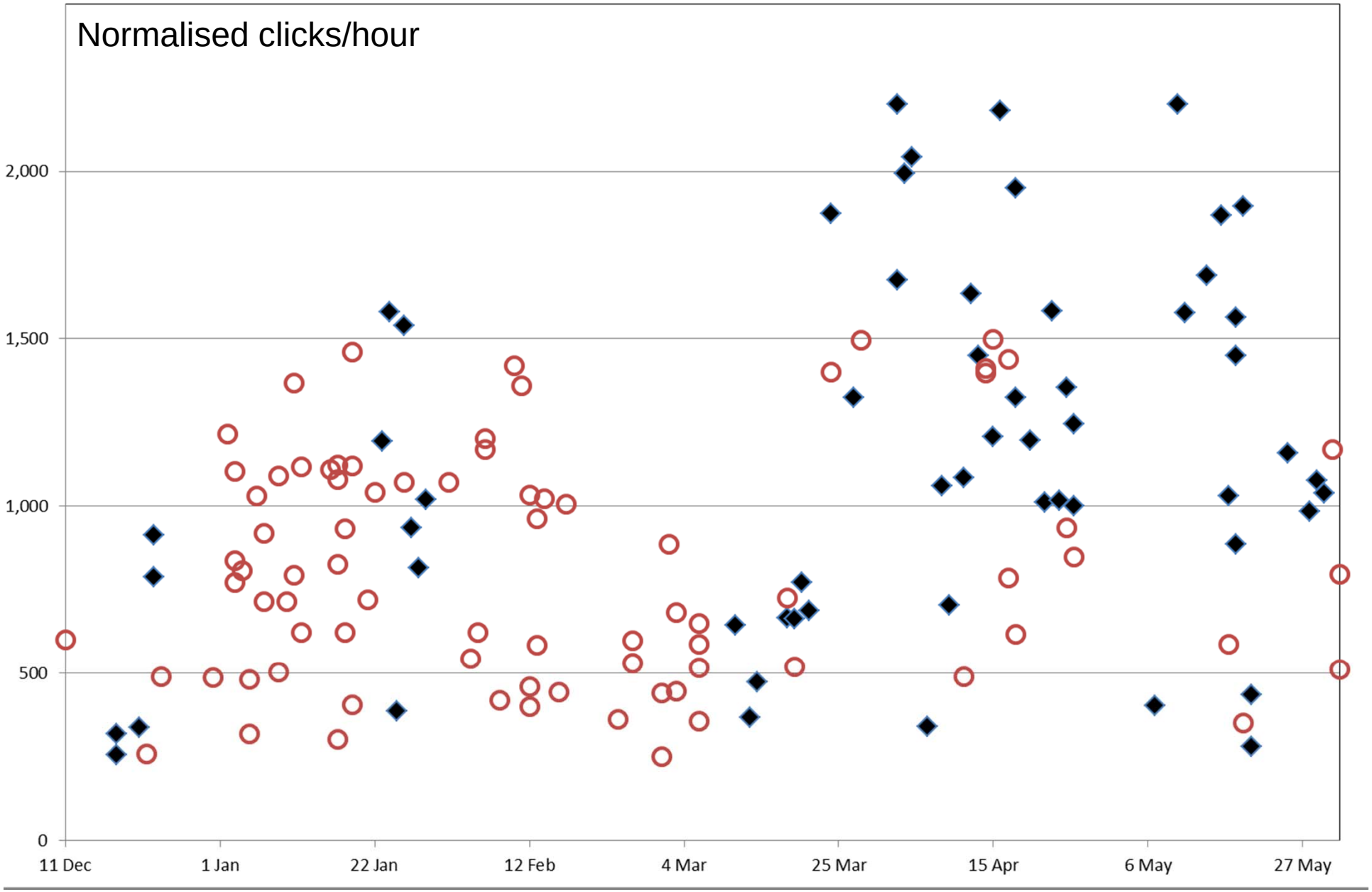
Tracking IM worms

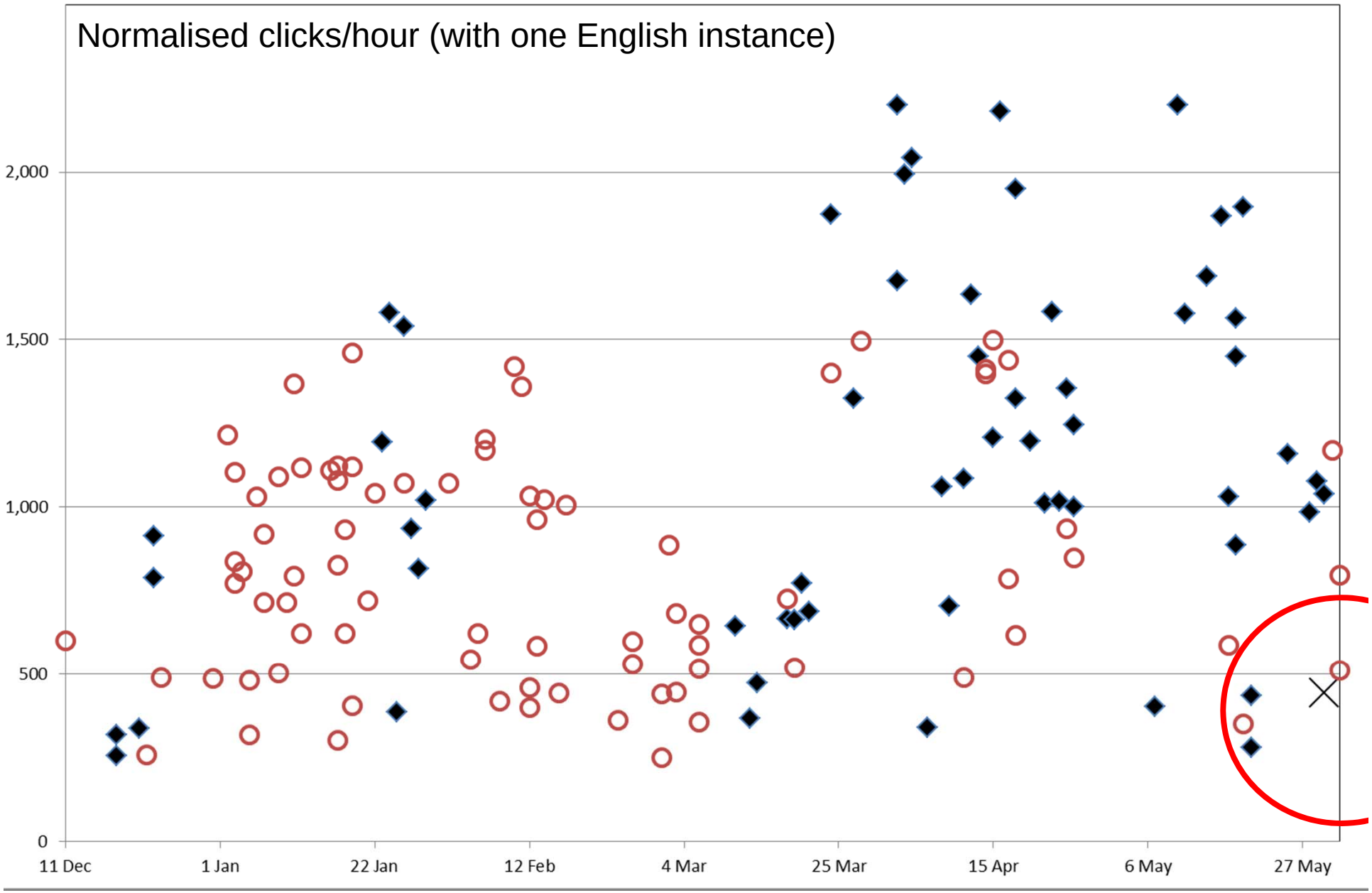
- I have been logging traffic on the C&C infrastructure
  - hence my 2011 talk about whether the domain name matters?
  - some evidence that URL shorteners decrease traffic
- Since Dec 2011 they have been using http://goo.gl/ URL shorteners pretty consistently
- That means it is possible to determine whether the message matters…
- Most infections now in Brazil:
  - Foto haha :D http://goo.gl/56uBH?richard@ema.il
  - haha foto http://goo.gl/56uBH?richard@ema.il
  - Mira esta foto .. :D http://goo.gl/56uBH?richard@ema.il
  - eu acho que é você na foto http://goo.gl/56uBH?richard@ema.il
- What works best ???


Ratio of clicks to the mean
1.5
1.4
1.3
1.2
1.1
1
0.9
0.8
0.7
0.6
0.5
0
2
4
6
8
10
12
14
16
18
20
22
0
2
Time of day (GMT)


Normalised clicks/hour for language independent messages
2,000
1,500
1,000
500
0
11 Dec
1 Jan
22 Jan
12 Feb
4 Mar
25 Mar
15 Apr
6 May
27 May


Normalised clicks/hour for Portuguese messages
2,000
1,500
1,000
500
0
11 Dec
1 Jan
22 Jan
12 Feb
4 Mar
25 Mar
15 Apr
6 May
27 May


Normalised clicks/hour
2,000
1,500
1,000
500
0
11 Dec
1 Jan
22 Jan
12 Feb
4 Mar
25 Mar
15 Apr
6 May
27 May


Normalised clicks/hour (with one English instance)
2,000
1,500
1,000
500
0
11 Dec
1 Jan
22 Jan
12 Feb
4 Mar
25 Mar
15 Apr
6 May
27 May

Conclusions

- Criminals don’t listen to SHB talks
  - (otherwise they would not be using shorteners)

- When criminals communicate with Brazilians in Portuguese this increases the likelihood of foolish events occurring
  - take care how you analyse the cause and effect!

Devo estar falando Português?

http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

NPL
National Physical Laboratory