Devo estar falando Português?

Richard Clayton

SHB
4th June 2012
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 ???
Normalised clicks/hour for language independent messages
Normalised clicks/hour for Portuguese messages
Normalised clicks/hour
Normalised clicks/hour (with one English instance)
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