Which Malware Lures Work Best?

Measurements from a Large Instant Messaging Worm

Tyler Moore & **Richard Clayton**

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Barcelona
27th May 2015

Outline

- The “Yimfoca” instant messaging worm
- The impact of shorteners
- The impact of Portuguese

An instant messaging worm (Spring 2010)

- Instant messaging ‘worm’ affects Yahoo Instant Messenger and (the interconnected) Windows Live Messenger
- Message from buddy says:
  - foto ☺ http://example.com/image.php?user@email.example.com
- The recipient clicks and (if OKs a pop-up) is infected
  - sees a generic MySpace page to reduce suspicion
- Malware resolves a hostname to locate IRC server
  - connected to this IRC server & joined channel #jakarta
  - refreshed topic of this channel was “foto ☺ http://malwareurl”
  - occasionally forced to join #mix or #!l! to download new code
- To monitor what was going on I created a Perl “bot” to emulate compromised machine, to camp on channel(s) of the multiple IRC servers and record traffic...

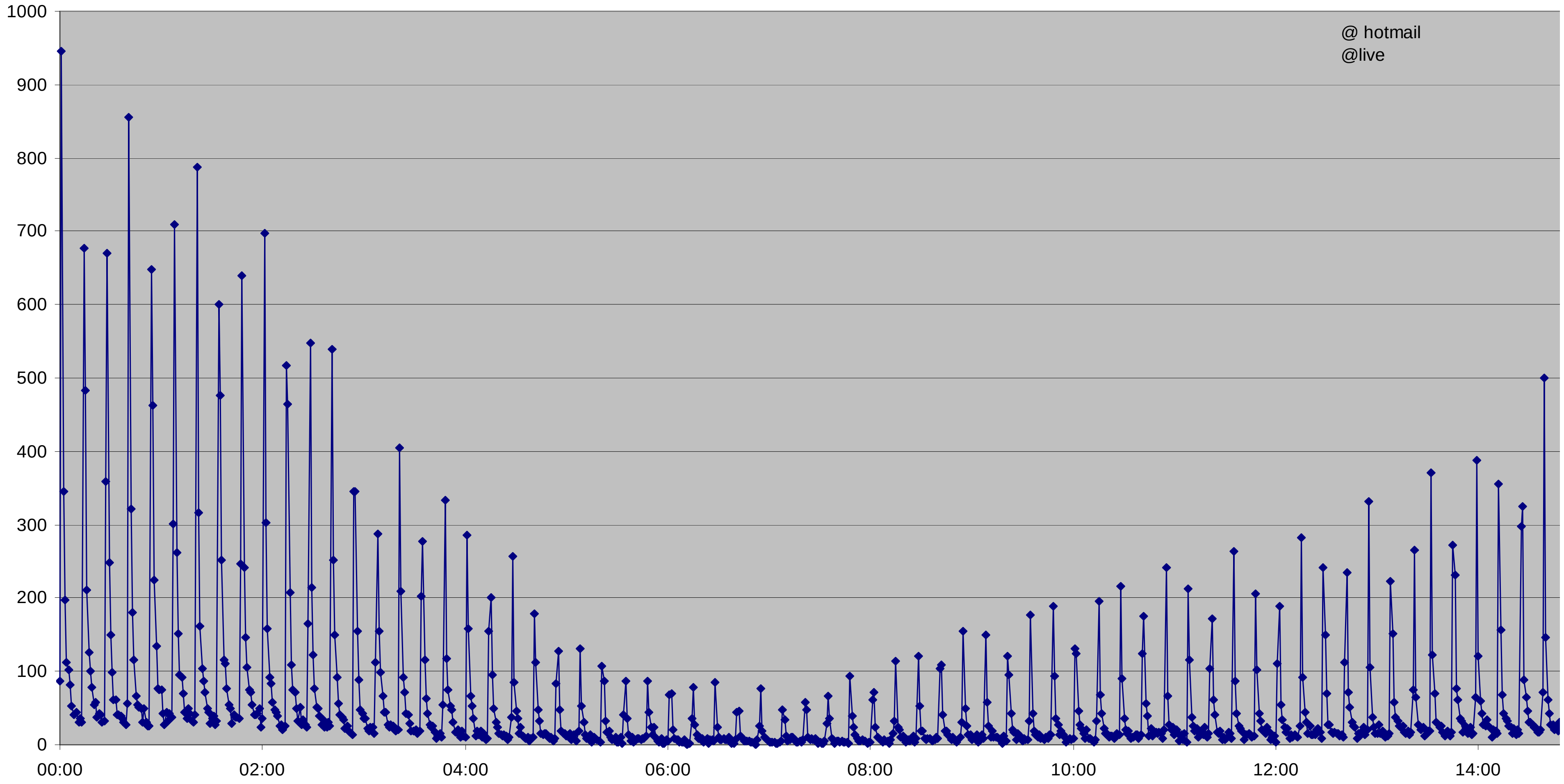
Example IRC traffic (26 May: farqebook)

```
13:51:06 wd74!wd74@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
14:04:25 wd74!wd74@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
14:17:46 wd74!wd74@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
14:31:06 wd74!wd74@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
14:44:26 wd74!wd74@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
14:57:46 wd74!wd74@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
15:04:59 irc.priv8net.com MODE #jakarta +o msg
15:11:06 wd74!wd74@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
15:24:28 wd74!wd74@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
16:17:26 wd56!wd56@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
16:30:46 wd56!wd56@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
16:44:08 wd56!wd56@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
16:57:28 wd56!wd56@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
17:10:48 wd56!wd56@uNkn0wn.eu TOPIC #jakarta :.m.s|.m.e foto :D http://farqebook.com/photos.php?=
```

Apache logs

- Turned out the criminals were, more often than not, hosting the malware at a hosting site with world-readable weblogs
- So we were able to inspect logs and determine activity
  - logs also gave us a reliable measure of the click-through rate
  - NB: not (quite) the infection rate
- The URL was (by this time) generally of the form
  - http://example.com/photo.php?your.email@hotmail.com
- Email addresses being extracted from Microsoft IM client
  - hence could count Microsoft customer infections
- Yahoo was blocking (failing to deliver) the worm messages
  - since URL rapidly changed, an automated system was used
- Charted numbers from the logging

Data from 30 May (@microsoft emails)



Instant messenger worms (Part II)

- Initial worm taken down in Spring 2010
- Similar worms start being deployed in Summer 2010
  - Yahoo blocks the URLs
- The new worm also spreads on the Facebook IM platform
- But in Spring 2011 the worms switched to using shorteners
- Every 13 minutes they have a new URL
  - a challenge for blocking systems to keep up
- Another round of takedowns June 2011 ....
- ... resurrected (again) in Brazil and drifts on into 2012
- THE END (??)

Estimating how many infected

- We have extensive web server logs
- We exclude AV vendors, Yahoo, Facebook etc.
  - Facebook is downloading in parallel to assess nature of URL
- We also exclude multiple clicks by same IP
  - analysis of this shows Facebook's protection had some impact
- For all worms (to Aug 2012) this gave us 14 million "real" clicks
  - from original dataset of 63 million downloads
- BUT this is click rates, maybe people didn't click OK or had AV…
  - but AV generally didn't detect this at the time of download
  - and we think most people would click through the warning…

Identifying infections

- Recall the #!l! channel for software update. My Perl bot joined this channel on each new IRC server
  - turned out that I was first to join the channel on some new servers and so I was chanop
- So I have a record of activity!

```
20:49:37 wd63!wd63@uNkn0wn.eu TOPIC #jakarta :.s|.m.s|.m.e Foto :D http://f-myspace.net/profile.php?=
21:01:03 [TUR|XP]2643895!6505@AECBF337.60FB0797.B0379ED3.IP JOIN :#!l!
21:01:04 [TUR|VIS]7412807!8824@A0EC43C1.9C986619.FA7C5148.IP JOIN :#!l!
21:01:04 [COL|XP]8048722!4192@0wn3d-37854CC6.dsl.intelnet.net.gt JOIN :#!l!
21:01:04 [FRA|XP]0325668!5702@0wn3d-12199A95.w90-56.abo.wanadoo.fr JOIN :#!l!
21:01:04 n[USA|XP]8824866!8631@0wn3d-5B781FDF.dyn.optonline.net JOIN :#!l!
21:01:04 [FRA|XP]7843135!1927@1FC1DD4F.7CDF4AF6.BB45ADBE.IP JOIN :#!l!
21:01:04 [DEU|XP]1690675!0013@0wn3d-1691EC12.dip.t-dialin.netJOIN :#!l!
21:01:04 [BRA|XP]0026510!1847@DC4BA7FD.F279DEBE.5053F232.IP JOIN :#!l!
```

Estimating the infection rate

- 2010-06-04 04:54:27 to 15:15:44 UTC
  - Perl program was chanop : and 17779 machines joined the channel

- For the same period we have web logs
  - 18720 unique downloads of the malware

- Hence infection rate is 95.0%
  - that is – people ARE clicking through the warning

Total infection numbers

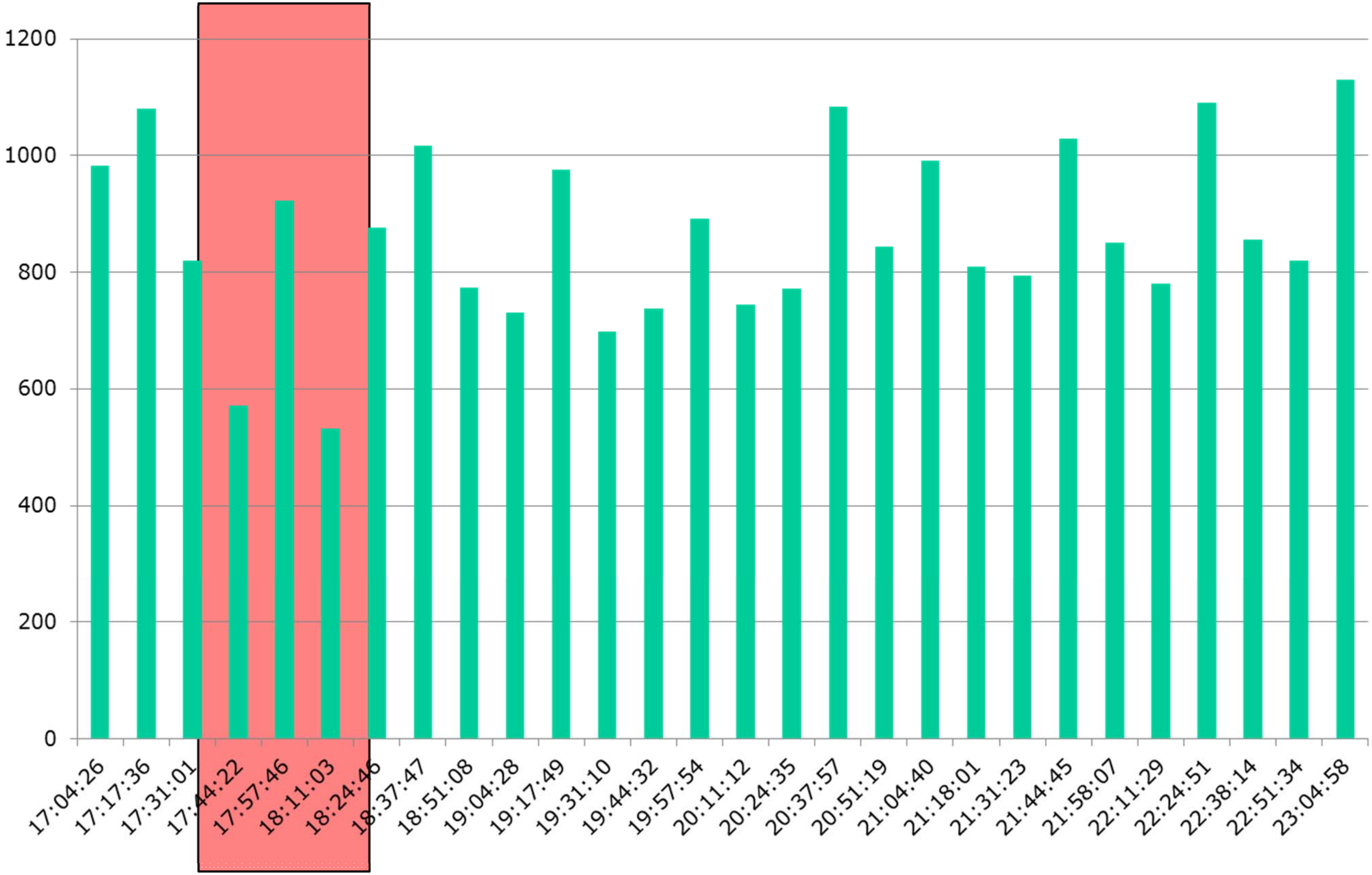
- Estimates from daily rates, and messages ...
  - 27 May – 22 Jun = 36000 minutes
  - we have web log data from 40.7% of this time
- The de-duplicated number of clicks is 717 083
- Hence 1.67 million infected machines
  - perhaps 20% -- 80% higher because no diurnal adjustment
- Recall that when we were chanop we saw 1717/hour
- The overall rate is 2577/hour
- But worms grow exponentially (at least for a while) and note that we have no data for late April to end of May
  - so 1717:2577 disparity not implausible
- We estimate more than 3 million machines infected

Now some human factors research...

Sometimes URL shorteners are used

```
2011-02-17 17:04:26 is this you on pic? http://kunfacebook.net/album.php?=
2011-02-17 17:17:36 is this you on pic? http://kunfacebook.net/album.php?=
2011-02-17 17:31:01 is this you? http://kunfacebook.net/album.php?=
2011-02-17 17:44:22 is this you? http://linkmenow.org/images555?=
2011-02-17 17:57:46 is this you? http://linkmenow.org/images555?=
2011-02-17 18:11:03 is this you? http://linkmenow.org/images555?=
2011-02-17 18:24:46 is this you? http://linkmenow.org/images555?=
2011-02-17 18:37:47 is this you? http://kunfacebook.net/album.php?=
2011-02-17 18:51:08 is this you? http://kunfacebook.net/album.php?=
2011-02-17 19:04:28 is this you? http://kunfacebook.net/album.php?=
2011-02-17 19:17:49 is this you? http://kunfacebook.net/album.php?=
2011-02-17 19:31:10 is this you? http://kunfacebook.net/album.php?=
2011-02-17 19:44:32 is this you? http://kunfacebook.net/album.php?=
2011-02-17 19:57:54 is this you? http://kunfacebook.net/album.php?=
2011-02-17 20:11:12 is this you? http://kunfacebook.net/album.php?=
```

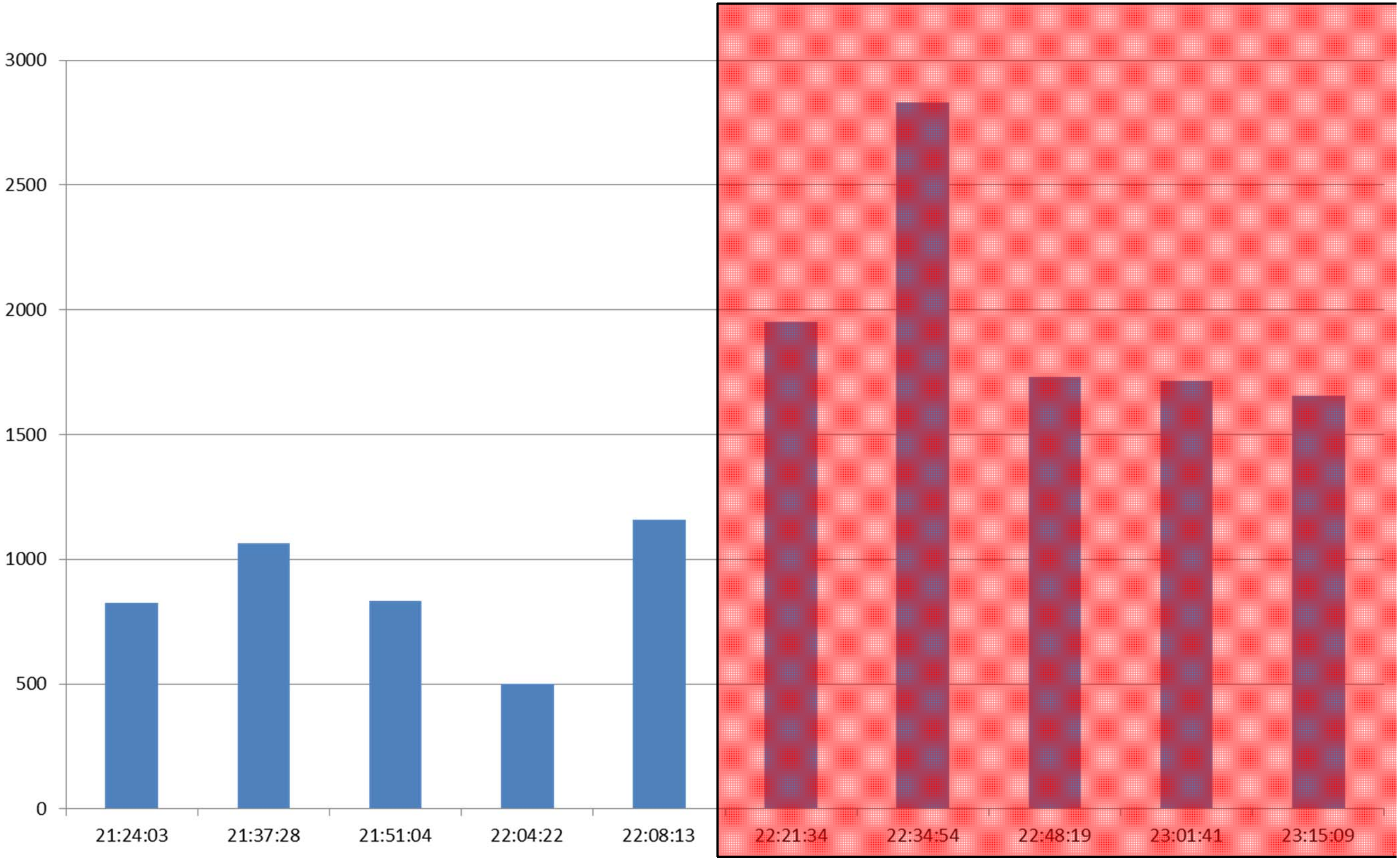
Some impact on clicks: lower if shortener



Another example

```
2011-02-14 21:24:03 Foto :D http://fogz.eu/images886?=
2011-02-14 21:37:28 Foto :D http://fogz.eu/images886?=
2011-02-14 21:51:04
2011-02-14 22:04:22
2011-02-14 22:08:13 Foto :D http://fogz.eu/images91?=
2011-02-14 22:21:34 Foto :D http://justinloveis.net/album.php?=
2011-02-14 22:34:54 Foto :D http://justinloveis.net/album.php?=
2011-02-14 22:48:19 Foto :D http://justinloveis.net/album.php?=
2011-02-14 23:01:41
2011-02-14 23:15:09 Foto :D http://justinloveis.net/album.php?=
2011-02-14 23:28:27 Foto :D http://justinloveis.net/album.php?=
```

justinloveis works better than fogz.eu



Comparing domains (Feb-Apr 2011)

	Facebook	Myspace	Other	Shorteners
#domains	13	1	65	18
#visitors (total)	144748	11373	956962	424039
#visitors/site (median)	11905	11373	11092	2851
#downloads /min (mean)	22	45	16	10
#download /min (median)	6	45	11	3
Normalised rate (mean)	16	32	14	9
Normalised rate (median)	16	32	11	3

Language independent lures

- English 2.1%

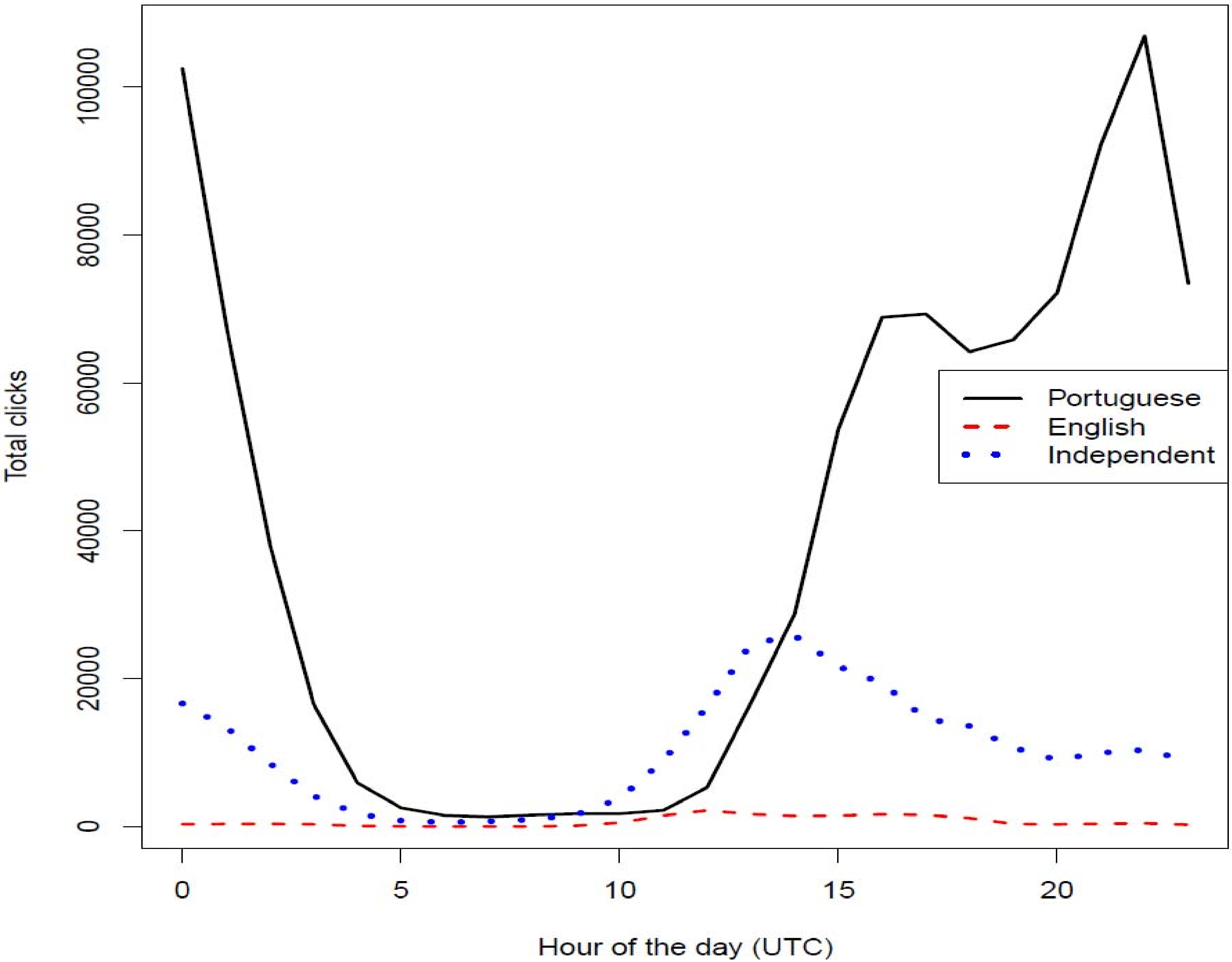
  `is this you?`

- Portuguese 48.0%

  `eu acho que  é você na`

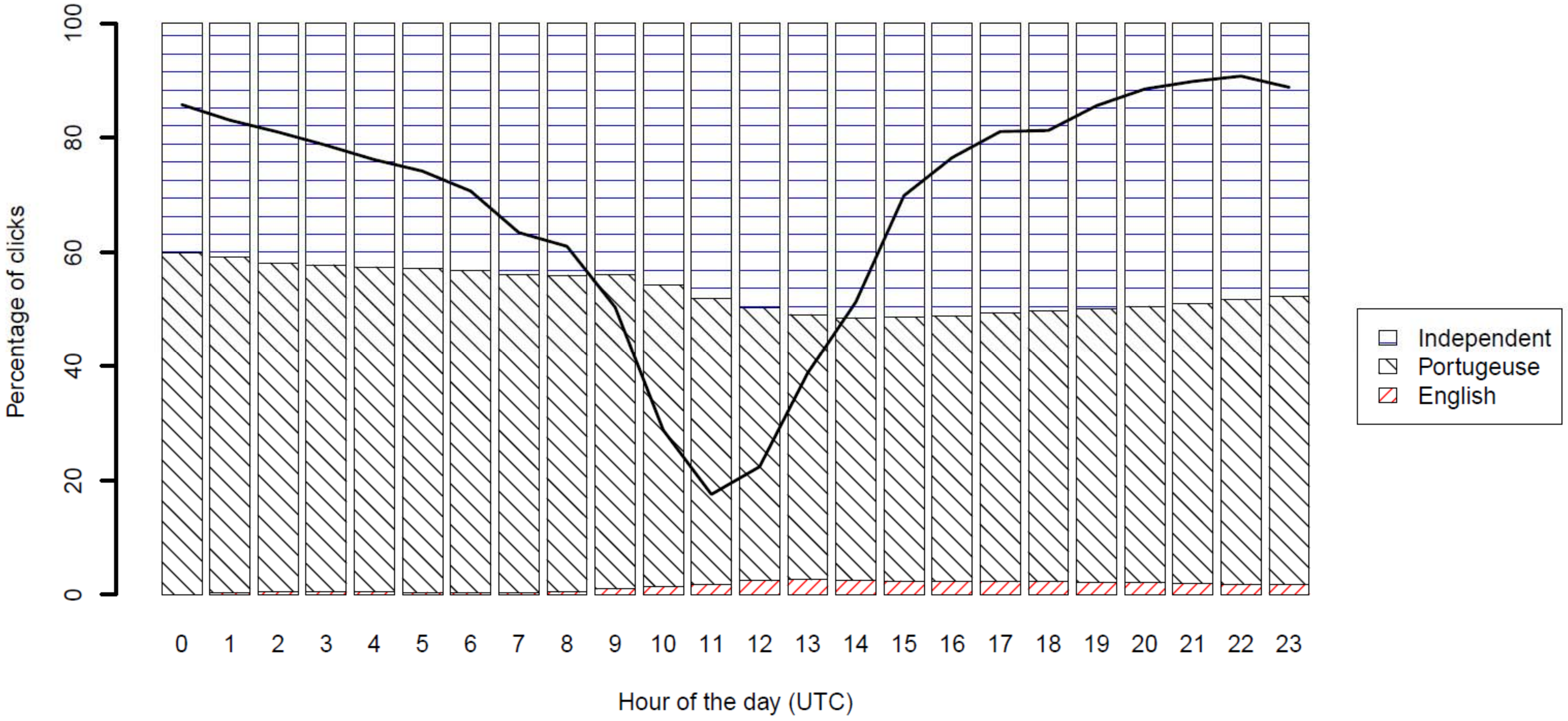
- Language independent 49.9%

  `hahha foto`



Total clicks
0
20000
40000
60000
80000
100000
0
5
10
15
20
Hour of the day (UTC)
Portuguese
English
Independent

The effect is real !



Superimposed line is clicks on Portuguese lures

Conclusions

- Some fairly simple lures and some low-tech IRC servers will allow you to build a multi-million machine botnet
- People really do click OK without reading what the warning message says
- Shorteners are not as attractive as domain names and are clicked rather less
- When criminals communicate with Brazilians in Portuguese this increases the likelihood of foolish events occurring

http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory