Which Malware Lures Work Best?
Measurements from a Large Instant Messaging Worm

Tyler Moore & Richard Clayton

Luxembourg
20th May 2015
Outline

• The “Yimfoca” instant messaging worm

• The impact of shorteners

• The impact of Portuguese
In the beginning (late April 2010)

- April 30: Reports of a new Instant Messenger worm start to circulate on Romanian web forums, 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 shipped to Symantec May 6th who name it “Yimfoca” and arrange for its detection
  - name from “Yahoo!” “IM” “infocard.exe”
  - probably a Rimekud variant (and rather boring)
- May 6: takedown of some (Symantec identified) C&C
Finding out how Yimfoca works

- Ran in VMware: DNS traffic and IRC traffic were captured.
  - resolved a hostname to locate IRC server
  - connected to this IRC server & joined channel #jakarta
  - topic of this channel was “foto 😊 http://malwareurl”
  - occasionally forced to join #mix or #!!! to download new code

- If connection to C&C failed backup hostnames were used

- Refreshing the channel topic caused malware to send out message to buddies (filling in the email address from the local machine’s IM address book)

- 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
- We could even identify the machine from which they were monitoring that the malware was still present
- Other activity from the same machine showed 5 different browser identification strings (some 32bit some 64bit) which may indicate size of the “gang”
- Logs also gave us a reliable measure of the click-through rate
- NB: not (quite) the infection rate
Also able to tell who was clicking

- 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
  - no email address assumed to be Yahoo! infecting Yahoo!
  - addresses of the form yahoo:email@yahoo.com were result of Microsoft customers whose Yahoo! IM buddies had clicked...

- Yahoo was blocking (failing to deliver) the worm messages
  - since URL rapidly changed, an automated system was used

- Charted numbers from the logging
  - clearly running riot on Microsoft platform
  - showed how effective Yahoo! blocking was
27 May, MS infections
Data from 30 May (@microsoft emails)
Data from 30 May (blank => yahoo)

no email (assume Y!)
Starting the take-down

• We now understood how to disable Yimfoca
  ▪ suspend ALL the hostnames used to locate IRC servers
  ▪ NB: knowledge of alternative names & “Plan B” crucial
  ▪ disable the IRC servers
  ▪ NB: both ought to be done “at the same time”

• So, we did !

• By June 17th all hostnames were suspended and all IRC servers
  (apparently hacked machines) were disabled (and the machines
  properly secured)
Meanwhile...

• Further analysis of our virus samples from May showed us not all of them were actually the “Yimfoca” we now understood.

• Also further analysis of the blocked message logs showed:
  ▪ various two year-old worms still broadcasting (fixed URLs and the malware was long gone)
  ▪ three Yimfoca variants

• So we decided to take down the three variants, since they had the same (ultra-effective) “foto 😊” lure, and because frankly they looked straightforward to tackle.

• They were straightforward and all were down by 22\textsuperscript{nd} June.

• So we won...
Similar worms start being deployed in Summer 2010
Yahoo’s blocking system works very well
Microsoft’s blocking system doesn’t
The new worm also spreads on the Facebook IM platform (they do moderately well…)
But in Spring 2011 the worms switched to using shorteners
Every 13 minutes they have a new URL
Yahoo’s blocking system fails to cope
Another round of takedowns June 2011 ….
… resurrected (again) in Brazil and drifts on into 2012
THE END (??)
Brazilian victims
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...
Number of clicks per user

Fraction of users clicking ≤ X times

- Overall
- Yahoo!
- Facebook
- Hotmail
Identifying infections

• Recall the #!! 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 :#!!!

21:01:04 [TUR|VIS]7412807!8824@A0EC43C1.9C986619.FA7C5148.IP JOIN :#!!!

21:01:04 [COL|XP]8048722!4192@0wn3d-37854CC6.dsl.intelnet.net.gt JOIN :#!!!

21:01:04 [FRA|XP]0325668!5702@0wn3d-12199A95.w90-56.abo.wanadoo.fr JOIN :#!!!

21:01:04 [USA|XP]8824866!8631@0wn3d-5B781FDF.dyn.optonline.net JOIN :#!!!

21:01:04 [FRA|XP]7843135!1927@1FC1DD4F.7CDF4AF6.BB45ABDE.IP JOIN :#!!

21:01:04 [DEU|XP]1690675!0013@0wn3d-1691EC12.dip.t-dialin.net JOIN :#!!

21:01:04 [BRA|XP]0026510!1847@DC4BA7FD.F279DEBE.5053F232.IP JOIN :#!!
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...
Phishing URLs (barclays is just an e.g.!)  

1. www.barklays.com/login.html  
Some special (ancient) cases

- http://www.barclays.com:security@www.kjakjas.info/login.html
  - disallowed by Microsoft (for HTTP) in Feb 2004

  - changes made to browser display c 2005
Does the bank name matter?

- Can be trivially obscured:
  
  `<a href="http://www.example.com">www.barclays.com</a>`

- Clearly the continued use of the bankname is thought to be useful – but it’s hard to measure, the widespread use of “kits” means that the kit builder makes the decision for the phisher.

- One datapoint is that online game phishing is heavily domain name based:

But 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
Another example

2011-02-14 21:51:04
2011-02-14 22:04:22
2011-02-14 23:01:41
justinloveis works better than fogz.eu
### Comparing domains (Feb-Apr 2011)

<table>
<thead>
<tr>
<th></th>
<th>Facebook</th>
<th>Myspace</th>
<th>Other</th>
<th>Shorteners</th>
</tr>
</thead>
<tbody>
<tr>
<td>#domains</td>
<td>13</td>
<td>1</td>
<td>65</td>
<td>18</td>
</tr>
<tr>
<td>#visitors (total)</td>
<td>144748</td>
<td>11373</td>
<td>956962</td>
<td>424039</td>
</tr>
<tr>
<td>#visitors/site (median)</td>
<td>11905</td>
<td>11373</td>
<td>11092</td>
<td>2851</td>
</tr>
<tr>
<td>#downloads /min (mean)</td>
<td>22</td>
<td>45</td>
<td>16</td>
<td>10</td>
</tr>
<tr>
<td>#download /min (median)</td>
<td>6</td>
<td>45</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Normalised rate (mean)</td>
<td>16</td>
<td>32</td>
<td>14</td>
<td>9</td>
</tr>
<tr>
<td>Normalised rate (median)</td>
<td>16</td>
<td>32</td>
<td>11</td>
<td>3</td>
</tr>
</tbody>
</table>
### Comparing domains (Aug-Oct 2011)

<table>
<thead>
<tr>
<th></th>
<th>Facebook</th>
<th>Orkut</th>
</tr>
</thead>
<tbody>
<tr>
<td>#domains</td>
<td>51</td>
<td>40</td>
</tr>
<tr>
<td>#visitors (total)</td>
<td>156823</td>
<td>140342</td>
</tr>
<tr>
<td>#visitors/site (median)</td>
<td>2991</td>
<td>3142</td>
</tr>
<tr>
<td>#downloads/min (mean)</td>
<td>7.4</td>
<td>6.8</td>
</tr>
<tr>
<td>#download/min (median)</td>
<td>3.9</td>
<td>3.9</td>
</tr>
<tr>
<td>Normalised rate (mean)</td>
<td>6.8</td>
<td>5.2</td>
</tr>
<tr>
<td>Normalised rate (median)</td>
<td>4.7</td>
<td>3.0</td>
</tr>
</tbody>
</table>
Language independent lures

- English 2.1%
  * is this you?*
- Portuguese 48.0%
  * eu acho que é você na*
- Language independent 49.9%
  * hahaha foto*
Time of day (GMT)

Ratio of clicks to the mean
Normalised clicks/hour for language independent messages
Normalised clicks/hour for Portuguese messages
Normalised clicks/hour
Normalised clicks/hour (with one English instance)
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