Might Governments Clean-up Malware?

Dr Richard Clayton
`richard.clayton@cl.cam.ac.uk`

MAAWG
4th October 2010

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

SnT
securityandtrust.lu

NPL
National Physical Laboratory

Technical stuff

- Malware (“malicious software”) aka virus, worm, trojan
- Software running on end user machine under criminal control
- Machine ends up in botnet and sends spam, participates in DDoS, commits click fraud etc, etc; and usually runs a keylogger (stealing user credentials for banks, webmail etc, etc)
- Fix by stopping all malware processes, fixing up registry removing all executables, restoring AV etc. Can be really easy; or it may be simpler/safer to rebuild the system from scratch
- Malware detected by remote sites (monitoring spam etc, or monitoring the botnet C&C systems)
- Reports have to go to the ISP, because only they can translate IPaddr/port/time into identity of compromised customer

What do ISPs do with reports?

Pass to customer

- Customer then has to clean up malware

Internet	free scanners (if reachable, and genuine!)	
friends/family	may do more harm than good	$
computer shop	specialist support	$$$
“Geek Squad”	generic support	$$
new machine	8% in 2006 survey	$$$$$$$

- ISP technical support not capable or willing to assist
  - remote diagnosis problematic
  - liability issues if make things worse

Ignore

- Cost of talking to customer equivalent to a whole year of profits
  - not quite true (see footnote!) but more true than false

How a government scheme would work

- ISP delivers report to customer (perhaps under duress?)
- Customer fixes it themselves, or uses Official Scheme
- Scheme uses a contractor, but Government subsidises cost
- Customer still pays $20-$30 (to avoid a “moral hazard”)
- Contractor cleans up machine
- Everyone happy

- So what tender price should the contractor put in ?
- And what is the scheme going to cost the taxpayer ?

Calculating the tender price

- Cost of clean-up is currently $52 (Tango LU), $90 (Comcast US)
  - because of source of reports, likely to be economies of scale
  - assume $70/clean-up and customer pays $30, hence $40 tender
- BUT opportunity to sell the user some anti-virus software
  - list price $70, trade discount 60% => $42 profit
  - assume 50% take up, and can reduce tender price by $21!
  - if do deal with AV vendor may do even better!
- BUT some people will buy new machine
  - assume $100 profit, but only 5% take up, reduce tender by $5
- BUT you get an relationship with a customer for future sales
  - Google Adwords cost of “new laptop” is $1 to $4, assume $4 !
- Modelling this all correctly (the categories overlap!) an organisation confident in its sales ability would tender $11.05

What is the cost to the taxpayer?

- Infection rates not really known, 1% too low, 10% too high!
- Figures from Microsoft Malicious Software Removal Tool (MSRT) suggest that about 1% of machines need cleaning per month
- Assume that half of all problems dealt with by customer (or by the IT department in a corporation)
- Hence about 0.5% population would use service each month
- With a government subsidy of $11.05 that means annual cost to the exchequer per computer is a mere 66 cents
- Low price for an effective “public health” policy
- For comparison: fluoridisation of water costs 92 cents per person per annum

Should the government be involved?

- Not unreasonable for government to care about “public health”
- Should make scheme more trustworthy for end-users
  - and of course the subsidy makes it cheaper!
- May make it easier to pressure ISPs to act
- But governments can be inefficient
  - albeit their role limited to choosing contractor
- ISPs already self-organising
  - initiatives in Germany, The Netherlands and Australia (trying to prevent the cost affecting price competition)
  - Comcast has gone it alone (so far) in the USA
- Your politics will determine if it is either ‘obvious’ or anathema!

Summary

- Malware is bad!
- Much is spotted by its effect on the wider Internet
- Only ISPs know who was using the IP address
- Incentives act to discourage ISPs passing reports to end-users
- Paper outlines a Government subsidy to clean-up malware

  `http://www.cl.cam.ac.uk/~rnc1/malware.pdf`
- Subsidy would be less than might be naively expected
- Just such a scheme is “being evaluated” by Luxembourg Ministry of Economics ☺ but to no effect so far ☹
- Discuss !

Might Governments Clean-up Malware?

PAPER: http://www.cl.cam.ac.uk/~rnc1/malware.pdf

BLOG: http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

SnT
securityandtrust.lu

NPL
National Physical Laboratory