Child Sexual Abuse Image Website Takedown Times

Richard Clayton

richard.clayton@cl.cam.ac.uk

joint work with Tyler Moore

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

IWF Meeting, London
23 September 2008

Website take-down measurements

- Studying phishing website removal for almost 2 years
- Four major academic papers, more in the pipeline
  - Best Paper award at APWG meeting 2007
- Comparing performance gives key insights
  - Some banks faster than others
  - Some hosting mechanisms more long-lived than others
- Web logging data yields visitor counts and hence lo$$ statistics
- Multiple feeds of suspect URLs gives us one of the best views of the problem in the world (better than any individual company)
  - We can show if company/bank unaware of sites they stay up longer
- Specialist companies faster than “community efforts”

etc. etc.

Comparing website removal times

Phishing (where owner aware)		Sites	Mean	Median
Free web-hosting	Jan 2008	240	4.3	0.0
Compromised machines	Jan 2008	105	3.5	0.0
Rock-phish domains	Jan 2008	821	70.3	33.0
Fast-flux domains	Jan 2008	314	96.1	25.5

Fraudulent websites		Sites	Mean	Median
Escrow Agents	Oct-Dec 2007	696	222.2	24.5
Mule recruitment	Mar 07-Feb 08	67	308.2	188.0
Pharmacy	Oct-Dec 2007	82	1370.7	1404.5

Child sexual abuse image websites

- IWF provided anonymised list of Jan-Dec 2007 websites
- Excluded 8 domains with >100 reports (likely free webhosting)
    - 2585 domains, 54 sites still “up” on 3 Apr 2008 (dataset time)
- Calculated time from first appearance to first removal
- Unable to distinguish type of site or measure reappearances
- Median removal time = 264 hours (11.0 DAYS)
- Mean removal time = 562 hours (23.4 DAYS)
- If include the sites not yet removed (which makes figures comparable with previous slide)
    - Median removal time = 12 DAYS
    - Mean removal time = 30 DAYS (and growing)

Removal process for CSAI websites

- If in UK, check with CEOP (a few hours delay) then tell ISP

- If not in UK, report via CEOP
  - CEOP passes to Law Enforcement in foreign country
  - May need to passed to local officials from central contact point
  - Issue may not be a priority, and/or properly understood

- ALSO if not in UK, pass to country's INHOPE member (if any)
  - In US, this is NCMEC, who only pass on reports to "members"
  - Elsewhere, few hotlines have formal arrangements with ISPs

Removal process for other content

- Phishing websites
  - Bank usually uses specialist company (local language, 24 hour ops)
  - Removal company emails ISP
  - If no response within minutes/hours, company telephones ISP
  - If no response, involvement of CERTs, local police etc etc
- Mule recruitment (and other “volunteer” efforts)
  - Tend to use English and operate in spare time
  - Email sent to ISP
  - Follow up emails, phone calls etc if no reaction
  - Involvement of CERTs, local helpers, translation services etc as may thereafter may be needed
  - Much of the effort can involve explaining the scam
- Key difference is early (and repeated) contact with ISP

Why is CSAI done this way?

- “No authority” to tell Polish ISPs what to do
  - Nor has anyone else!
  - And no formal “authority” within the UK either!
- Might interfere with a police operation
  - Unusual for ISP not to be aware of such an operation
  - There may well be direct reporting anyway
- Some confusion of aims is apparent:
  - Is main aim to remove sites ?
  - or to catch the criminals ?
- Note that failure to make timely removal is incurring significant costs to ISPs in deployment of blocking solutions

Risks of more effective removal

- Faster removal of phishing websites has driven technology improvements by hosters (rock-phish proxies, fast-flux botnet hosting etc)

- But these developments are likely for CSAI sites anyway

- Note that many of these changes imply need to move to domain removal rather than website removal
    - Remarks by IWF about reappearance of websites (which we were unable to assess from the dataset we were provided with) suggest that domain removal should be being done anyway

Summary

- Phishing websites removed in hours
- Part time volunteers remove scam websites in 1-7 days
- Child Sexual Abuse Image websites removed in weeks
- Only thing removed slower is fake pharmacy websites
  - and they are not tackled by any group we can locate
- We were amazed to discover this, and consider it a scandal
- Main reason appears to be lack of prompt contact with ISPs
- IWF needs to decide if main policy aim is timely removal websites or to catch the criminals running them?
- If removal is important then need to revise procedures and perhaps seek donations “in kind” from take-down companies

Child Sexual Abuse Image Website Takedown Times

Paper: **http://www.cl.cam.ac.uk/~rnc1/takedown.pdf**

Blog: **http://www.lightbluetouchpaper.org**

UNIVERSITY OF CAMBRIDGE
Computer Laboratory