

Studying the CSAI eco-system

Dr Richard Clayton



**UNIVERSITY OF
CAMBRIDGE**

Computer Laboratory

IWF, London
20th March 2012

Background

- I am one of the few academics with published work on blocking systems for CSAI and(or!) on website take-down effectiveness
 - my skill, such as it is, has been to construct lawful experiments
 - for “take-down” the IWF contributed data (thank you), though the conclusions that we drew from it were perhaps unexpected
 - I like measuring things – even when we know what the answer “must be”, we always learn more when we do measurements
 - I work in “security economics”; the economics is more significant than the tech, when it comes to ensuring that systems are secure
- I was asked by the IWF to make suggestions about what types of academic research might be encouraged going forward
- I discussed this with Susie Hargreaves in January (I was abroad when the bigger meeting was held)...
- ... and here I am to make similar points again

How do people consume CSAI ?

- Do we understand how CSAI is consumed ?
- Do people join sites and stay members for a long period ?
 - hoping for new material ?
 - not daring to keep copies on their own machine ?
 - or do they join, slurp everything and disappear forever ?
- Is there any pattern to when new members arrive ?
 - Friday night drunken experimentation ?
 - do they join in the middle of the night or the afternoon ?
- Theories about this are used to justify easy-to-avoid blocking and they show what the trade-off is between taking down a site and using it as a honeypot... but currently they're just theories
- Processing the logs from websites that are taken down (with ISP or police cooperation) would start to answer these questions !

How do people find CSAI ?

- Some sites are taken down and are then resurrected
- How do people find the new locations ?
 - mailing lists ? (that's how Al Qadea does it)
 - web forums ?
 - search engines ?
 - re-use of the same domain name ?
 - perhaps they don't ?
- HTTP referrers tell you where people came from (and in the case of search engines, what search terms they used)
- If you don't want to play "whack-a-mole" forever then you either need to arrest every webmaster (no argument there, but it's going to take a while) or you need to disrupt the system so that websites have to start again from scratch every time

How is the eco-system evolving ?

- Material is moving to torrents and to cyber-lockers
 - everyone likes a techie story; so is there compelling data for this ? or merely a number of thrillingly complex anecdotes ?
- The number of websites has reduced – has that reduced the number of page views ? Or the overall number of consumers ?
- How does “trust” work as the eco-systems change ? Are there (criminal) experts who can tell you how the new technologies work, and what not to waste your time on ?
- Are there “how to host” or “how to view” tutorials for the new technologies ? Is it possible to disrupt the availability of advice that is specifically CSAI oriented ?

Summary

- Providing and viewing CSAI is an eco-system
 - for ~20 years we've been pulling up weeds and shooting foragers...
 - ... but are we getting rid of the roots of those weeds ?
 - ... are forager numbers static, or is the population growing/shrinking ?
- Analysing the weblogs of CSAI sites will provide statistical data
 - if websites are indeed becoming extinct, we should be mining this rich vein information before it is gone for good
- Are there knowledge sharing communities in web forums ?
- The key question for me is "how do people find this material" ?
 - I rather suspect the answer is much, much, more complicated than "they use Google" or "they came across it by accident and liked it"
- So what are the answers ? And do some matter more than others ? We should be doing smarter disruption than lip service to blocking and scaring people they might be arrested !

<http://www.lightbluetouchpaper.org>

Dr Richard Clayton



**UNIVERSITY OF
CAMBRIDGE**

Computer Laboratory