eCrime Research

Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Luxembourg
11th May 2010

Today’s talk

- Who am I?
- What I’ve been doing in Luxembourg
- Types of criminality
- Research challenges
- Infrastructure
- Recommendations

Malware

- “Malicious software” (worm/virus/trojan/drive-by-download)

CHALLENGES

- Behavioural analysis (how do we know it’s bad)
- All samples now unique, so hard to measure any trends
- Detection (Google’s scanning already a special case)
- New browser designs for security
- Hosting providers need detection systems
- Can we detect bad sites on the wire ?

Botnets

- Swiss-army knife: DDoS, spam, click fraud, fastflux hosting

CHALLENGES

- Identification/interdiction of rendezvous schemes
- Identification of activity (and C&C)
- Better counting
- Disruption/take-over: but complex ethical issues
- Well trodden area – but new systems all the time

Phishing

- Theft of credentials by impersonation

CHALLENGES

- Measurements of lifetimes, blacklist effectiveness &c
- Improvements to user interfaces/training
- Improvements to authentication (PassPet, PAKE)
- Measuring/detecting man-in-the-browser
- Measuring/detecting key logging

Spam

- Non-permission based mass messaging

CHALLENGES

- Email spam detection
- Image spam
- Reliable measurements
- Contact forms on websites
- Blog spam
- Fake blogs (Google groups etc)
- Human detection (CAPTCHAs &c)

“Hacking”

- Unauthorised access to computing resources

CHALLENGES

- How can we secure one machine?
- How can we secure millions of machines
- How can hosting providers secure thousands of machines
- How do criminals find vulnerable machines?
- How can we provide realistic measurements of activity?

DDoS

- Distributed (usually) Denial of Service

CHALLENGES

- Detection of DDoS (at endpoint, on networks, at IXPs)
- Traceback of attacks
- Analysis of targets/motivation/capabilities

Others

- Click Fraud - data hard to obtain
- HYIP - lots of data, trivial problem
- Fake escrow - limited data, victims secretive
- 419 scams - extensive data on early stages of scams
- Lottery scams - hardly studied
- Fake banks - associated with 419 scams
- Counterfeit goods - hardly studied

Infrastructure

- Spam mine
- Network telescope (darknet)
- Passive DNS
- Malware collector
- Blog spam collector
- Honeypot machines
- Underground economy monitoring
- Fuzzers

Recommendations

- Easy to get on the map
  - Malware, Botnets
- Well-trodden areas, needing new approaches
  - Spam, Phishing, Hacking
- Pattern recognition payoffs
  - DDoS, Malware/Botnet traffic analysis
- Virgin territory
  - Blog spam
- MSc projects
  - HYIP
  - Fake Escrow, etc etc

eCrime Research

BLOG:

http://www.lightbluetouchpaper.org/

PAPERS:

http://www.cl.cam.ac.uk/~rnc1/publications.html

UNIVERSITY OF CAMBRIDGE
Computer Laboratory