The impact of website take-down on phishing

Richard Clayton

(joint work with Tyler Moore)

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

San Francisco
31st July 2007

Academics & phishing

- Everyone can play! Display instant expertise!!
  - examine psychology, attempt to block spam, detection of websites, browser enhancements, password mangling, reputation systems etc
- Our approach : Security Economics
  - phishing will continue, because humans involved!
  - so we measure the impact, assess the effectiveness of countermeasures, aim to work out how to change incentives so that problem tends to fix itself…

Data collection

- Used `http://www.phishtank.com` database
- Fetch webpages for all submissions
  - **caveat**: not currently following all indirections
  - **caveat**: site may already be removed
- Add entries for IP address and Reverse-DNS
- Determine when page is removed
- Calculate elapsed time
  - remove duplicates by ignoring last path element

Types of phishing website

- Insecure end user

  http://www.example.com/~user/www.bankname.com/

- Insecure machine

  http://www.example.com/bankname/login/

  http://49320.0401/bankname/login/

- Free web hosting

  http://www.bank.com.freespacesitename.com/

- Misleading domain name

  http://www.banckname.com/

  http://www.bankname.xtrasecuresite.com/

Rock-phish is different!

- Compromised machines run a proxy
- Domains do not infringe trademarks
  - name servers usually done in similar style
- Distinctive URL style

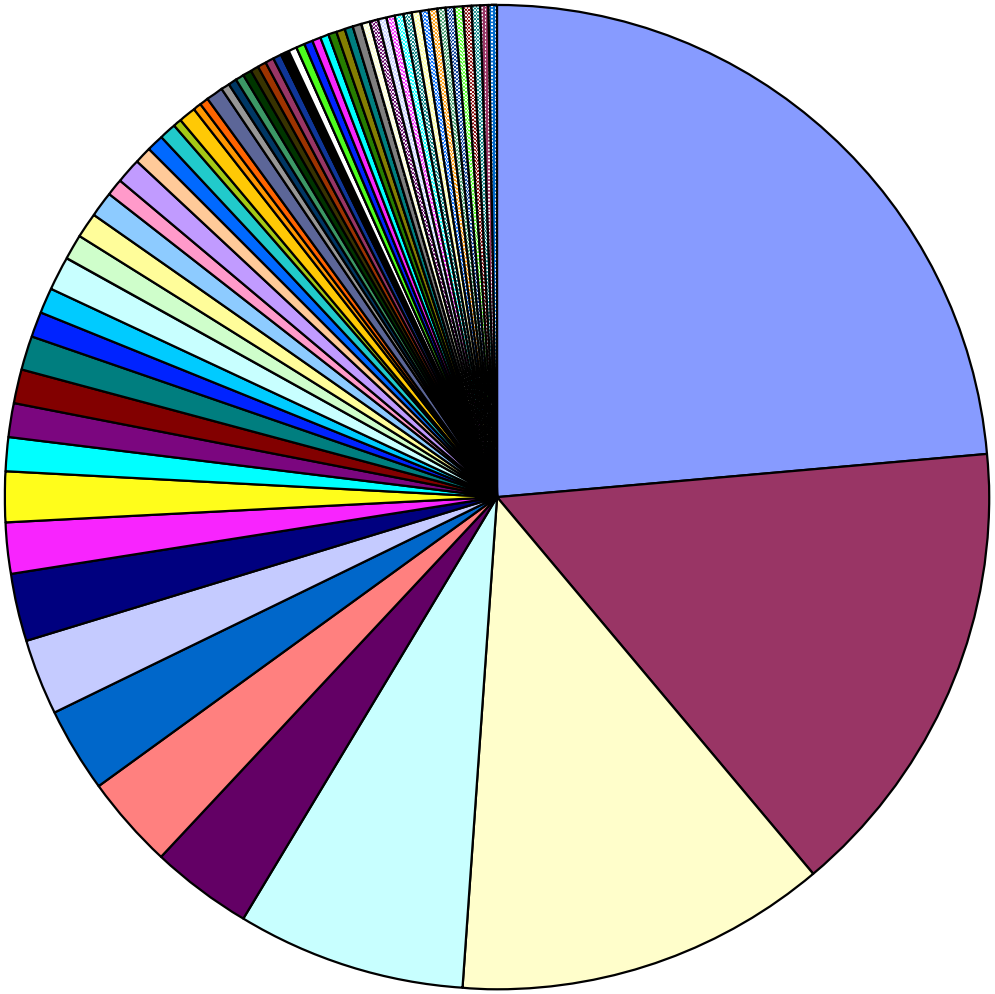
  `http://session9999.bank.com.lof80.info/signon/`
- We track domains & IP addresses generically
- Some usage of “fast-flux” from Feb’07 onwards
  - viz: resolving to 5 (or 10…) IP addresses at once

Phishing website lifetimes (hours)	# sites (8 weeks)	Mean lifetime	Median lifetime
Non-rock	1707	58.4	20
Rock-phish domains	419	94.3	55
Rock-phish IP addresses	122	124.9	25
Fast-flux rock-phish domains	67	454.4	202
Fast-flux rock-phish IP addresses	2995	124.6	20

The numbers game

- We saw 1,707 phishing websites, 419 rock-phish domains and 67 fast-flux domains…
- PhishTank has 18,260 rock-phish reports, 1,803 fast-flux reports and 15,030 non-rock reports (alive at first inspection)
- Large numbers suit the security industry, community activists, law enforcement seeking excuses to ignore the problem…

Banks attacked



- PAYPAL (23.6%)
- EBAY (15.3%)
- BOA (12.1%)
- WACHOVIA (7.6%)
- WELLS FARGO (3.3%)
- HALIFAX (2.9%)
- HSBC (2.9%)
- POSTEITIALIANE (2.5%)
- NATIONWIDE (2.1%)
- LLOYDS (1.7%)
- CHASE (1.6%)
- RBC (1.3%)
- US BANK (1.1%)
- DESJARDINS (1.0%)
- NCUA (1.0%)
- CITIBANK (0.9%)
- EGOLD (0.9%)
- FNB SA (0.9%)
- HAWAIIUSA FCU (0.9%)
- AMAZON (0.8%)
- EGG (0.8%)
- WESTPAC (0.7%)
- CAPITAL ONE (0.7%)
- WESTUNION (0.7%)
- BARCLAYS (0.5%)
- NATWEST (0.5%)
- TCF (0.5%)
- GERMANAMERICAN (0.4%)

ck-phish sites)

23.8%

15.3%

erica 12.1%

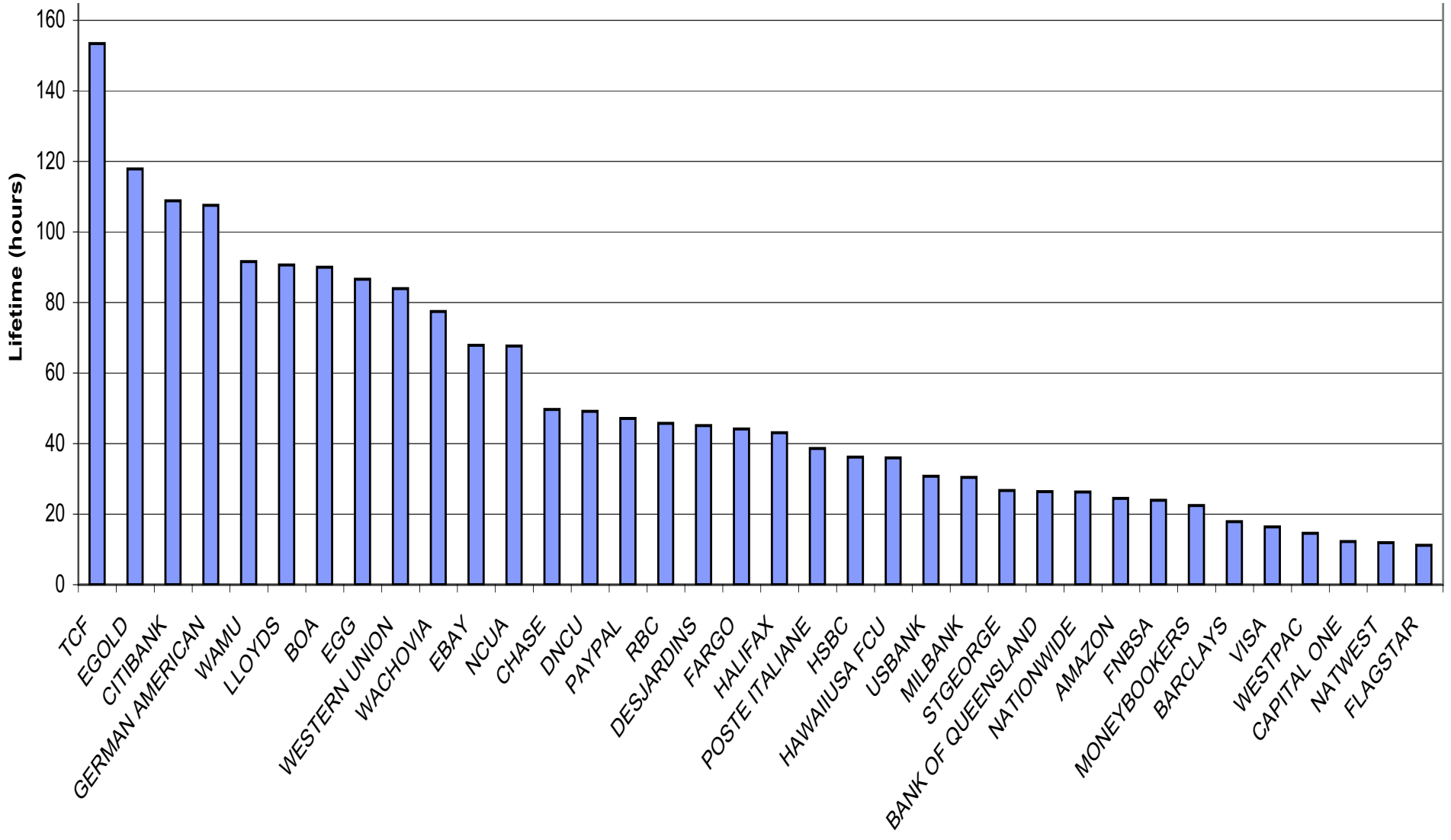
7.6%

3.3%

c etc

ed in total

st one attack


Lifetime (hours)
160
140
120
100
80
60
40
20
0
TCF
EGOLD
CITIBANK
GERMAN AMERICAN
WAMU
LLOYDS
BOA
EGG
WESTERN UNION
WACHOVIA
EBAY
NCUA
CHASE
DNCU
PAYPAL
RBC
DESJARDINS
FARGO
HALIFAX
POSTE ITALIANE
HSBC
HAWAIIUSA FCU
USBANK
MILBANK
STGEORGE
BANK OF QUEENSLAND
NATIONWIDE
AMAZON
FNBSA
MONEYBOOKERS
BARCLAYS
VISA
WESTPAC
CAPITAL ONE
NATWEST
FLAGSTAR

Free web-hosting take-down data

Lifetime (in hours)	# sites	Mean	Median
`yahoo.com`	59	11.27	5
`pochta.ru`	67	82.24	31

BUT: all but one `pochta.ru` site was eBay & values are similar to other eBay removal times

How many visitors?

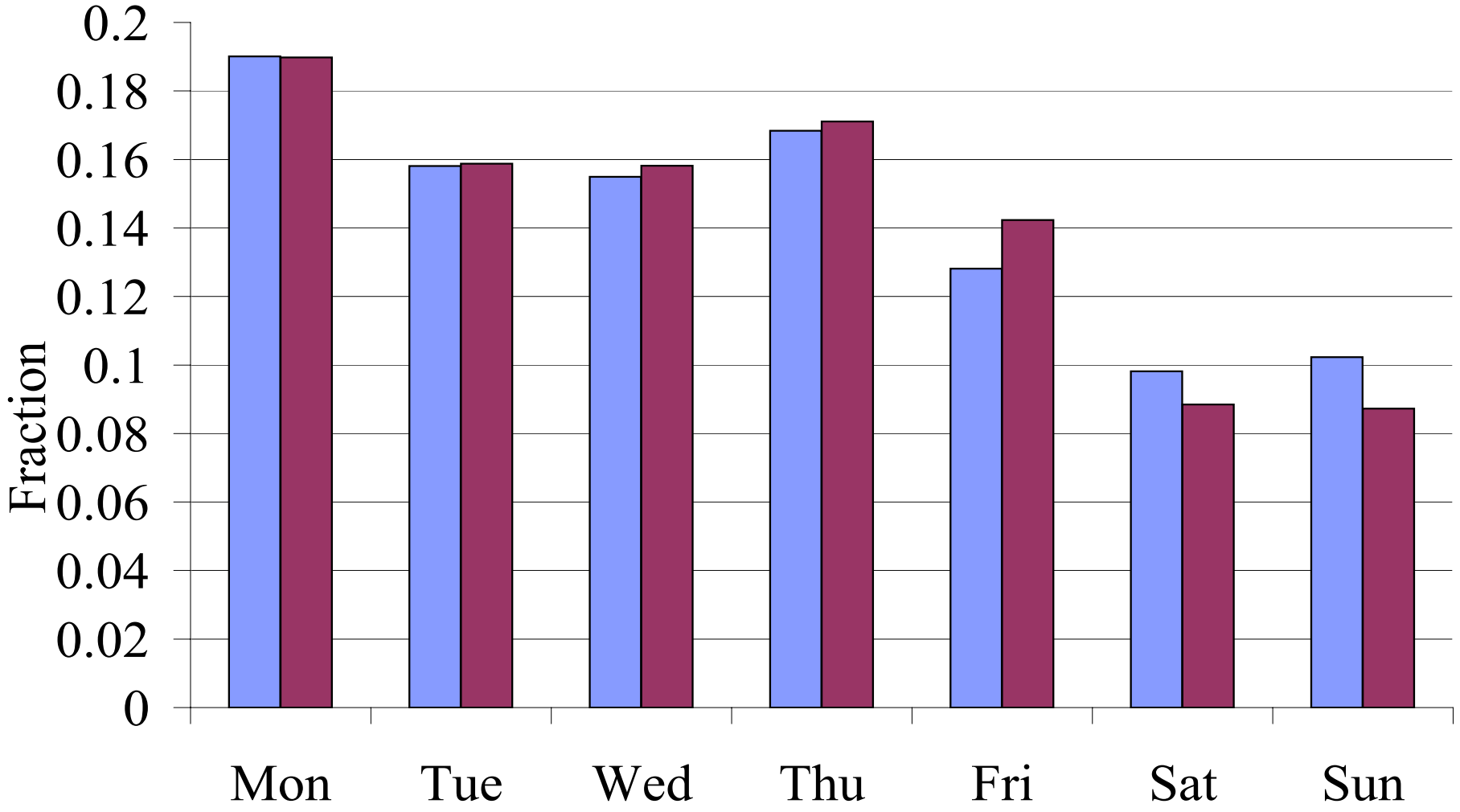
- Some (non rock-phish) sites had world readable “webalizer” statistics pages
  - could determine number of visitors on each day
  - 22 on day first reported, 24 next day and then tails off a bit (but NOT to zero)
- Some sites had world readable files of compromised credentials
  - about 50% were “die spammer die” responses

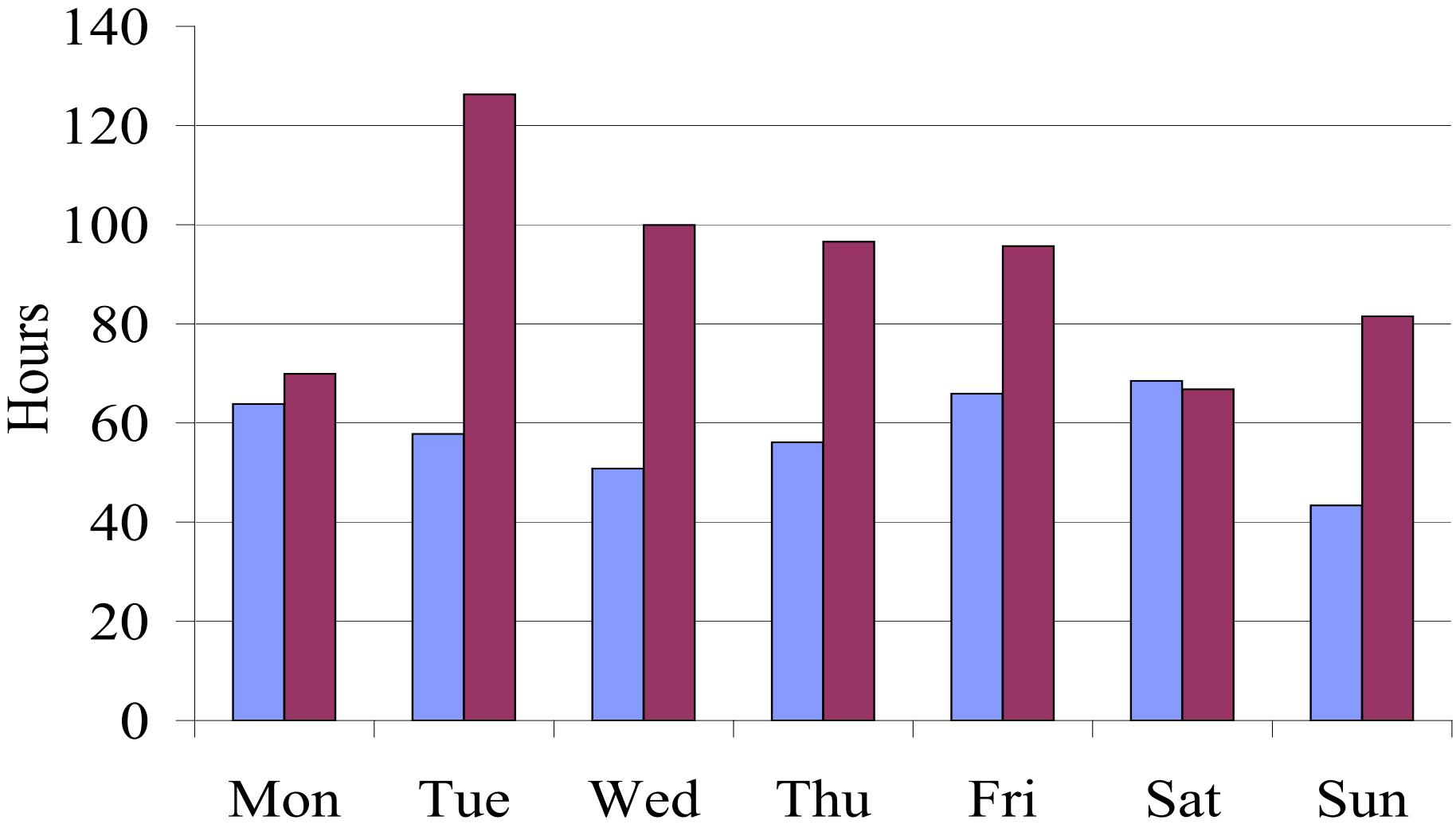
What's the co$t of phishing?

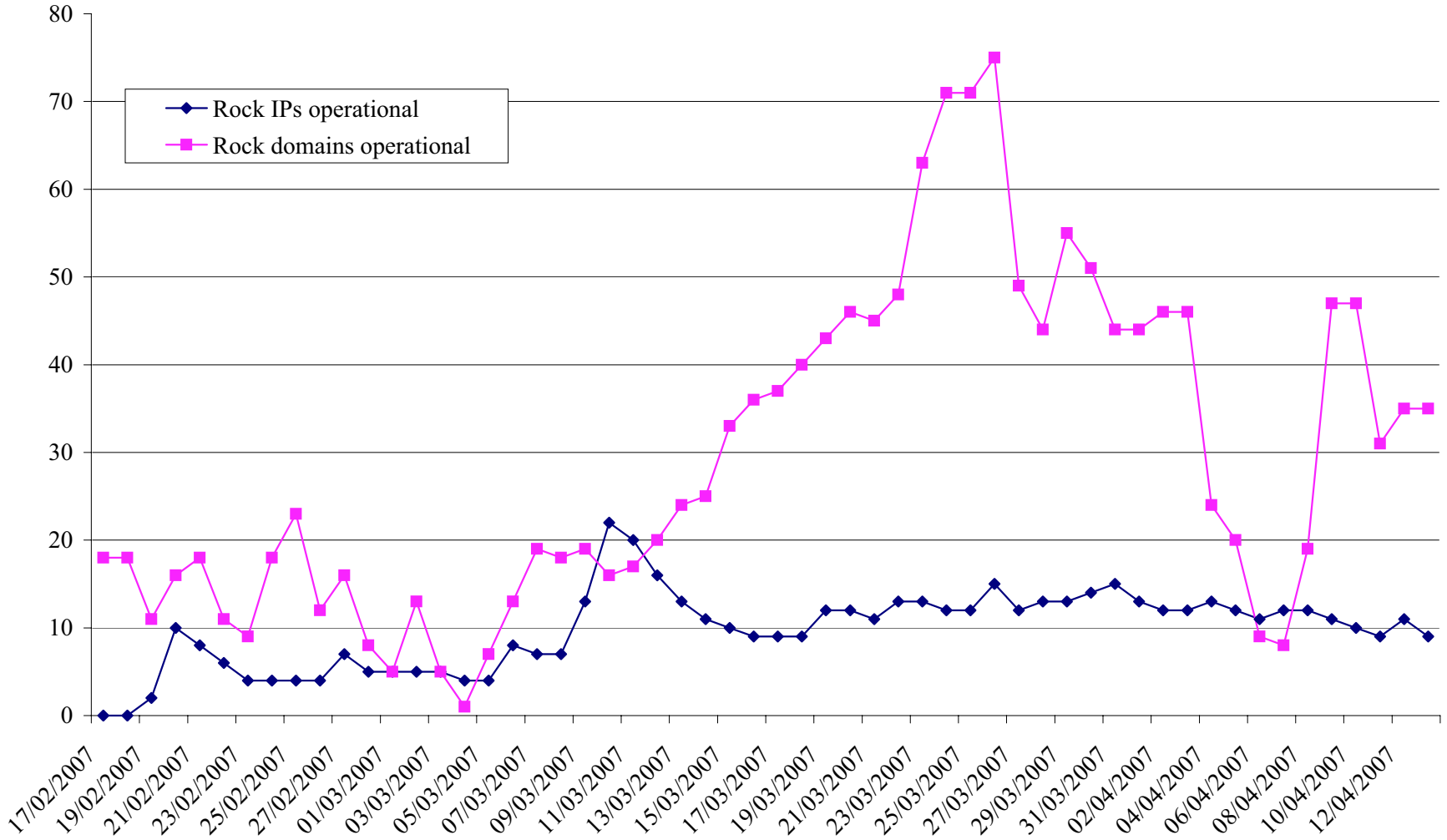
- 56 days, 1448 banking websites (exclude eBay)
- Average lifetime was 57 hours
- Hence 33 real victims per site
- Gartner loss estimate of $572/victim
- Hence $178 million per year
- Rock-phish is half the spam… so $350 million
  - NB: complete hand-waving !!!
  - and cf. Gartner total estimate of $2 billion

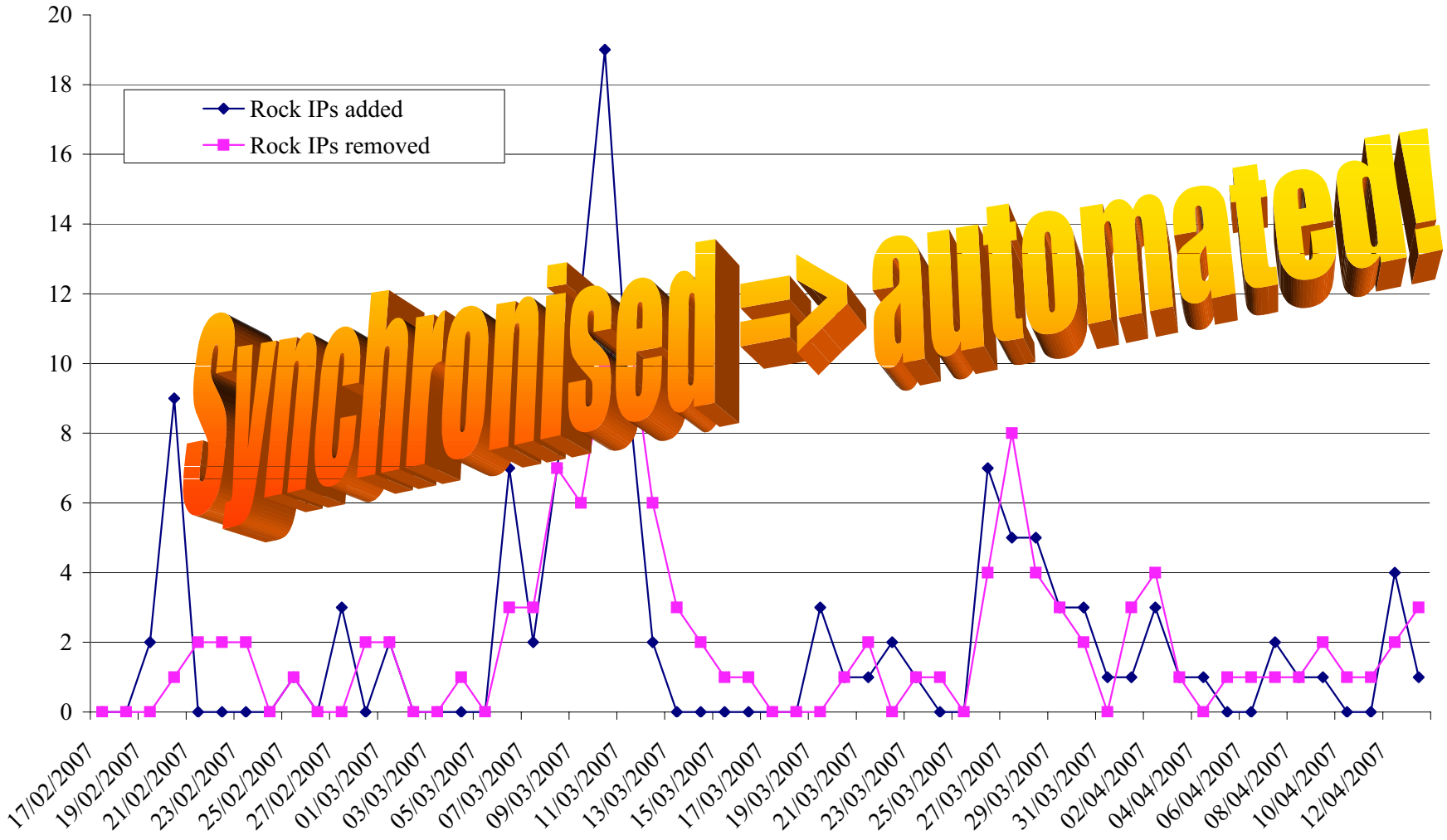
When are phishing sites first reported?

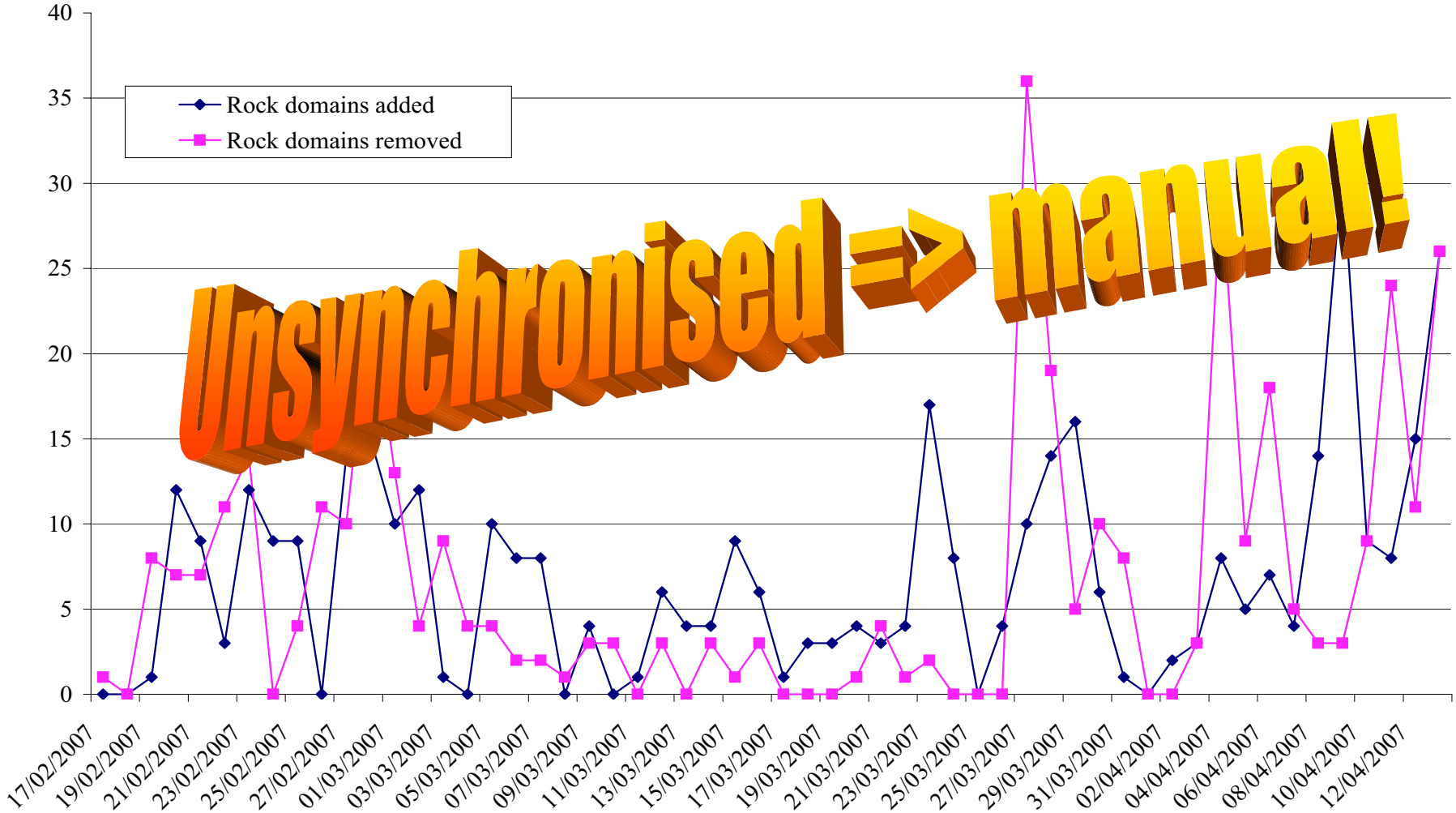
(blue = rock, red = non-rock)

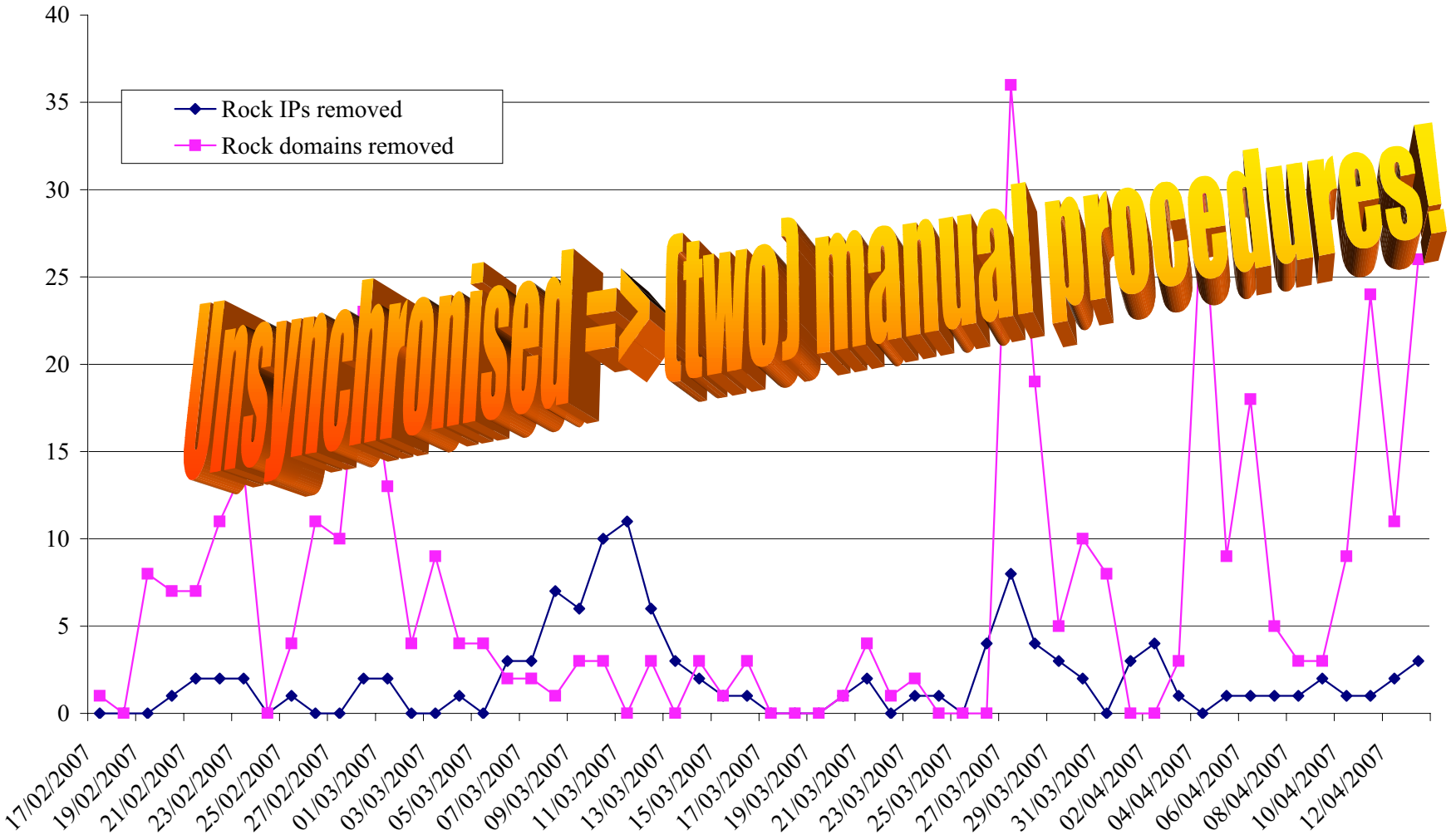


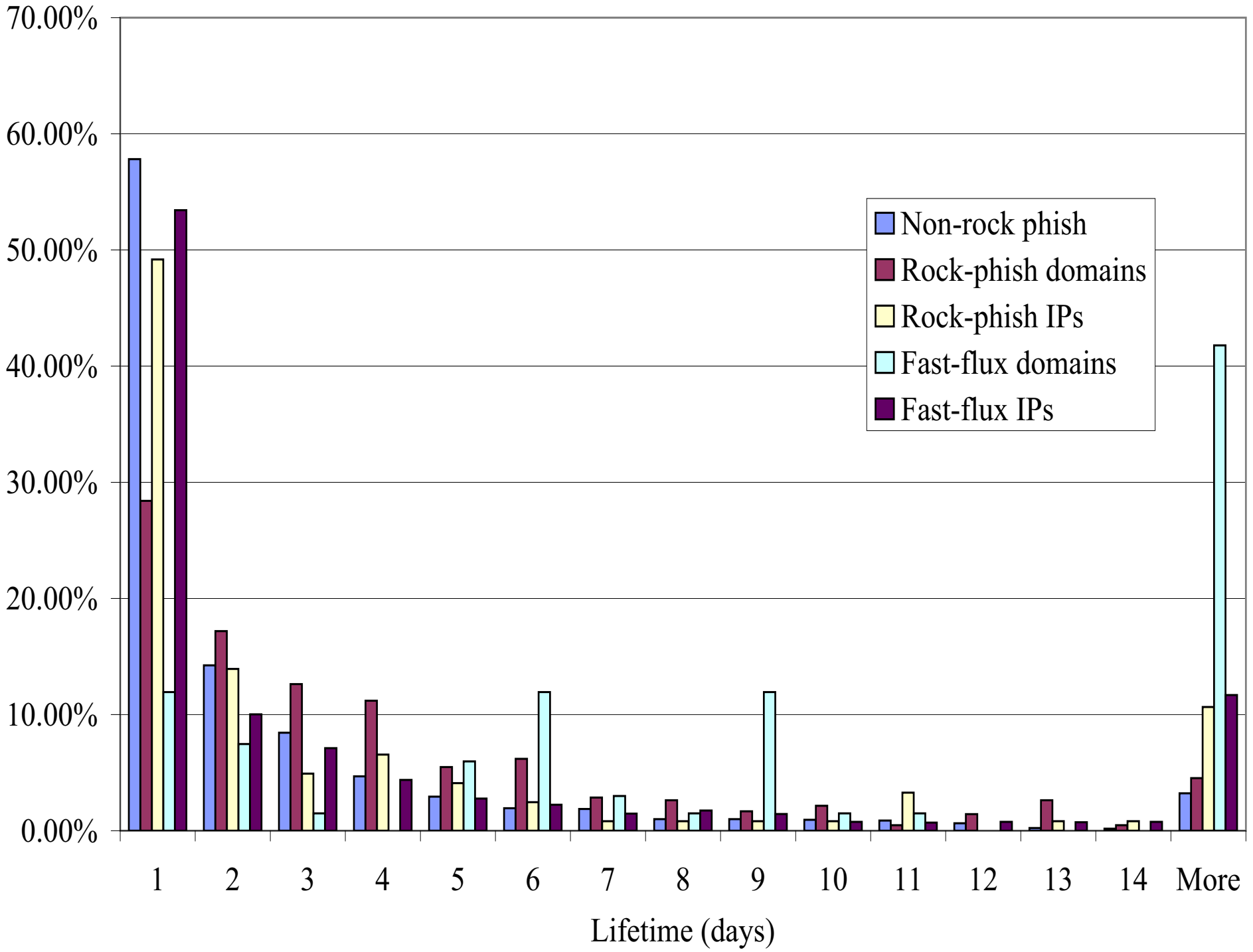

140
120
100
80
60
40
20
0
Hours
Mon
Tue
Wed
Thu
Fri
Sat
Sun

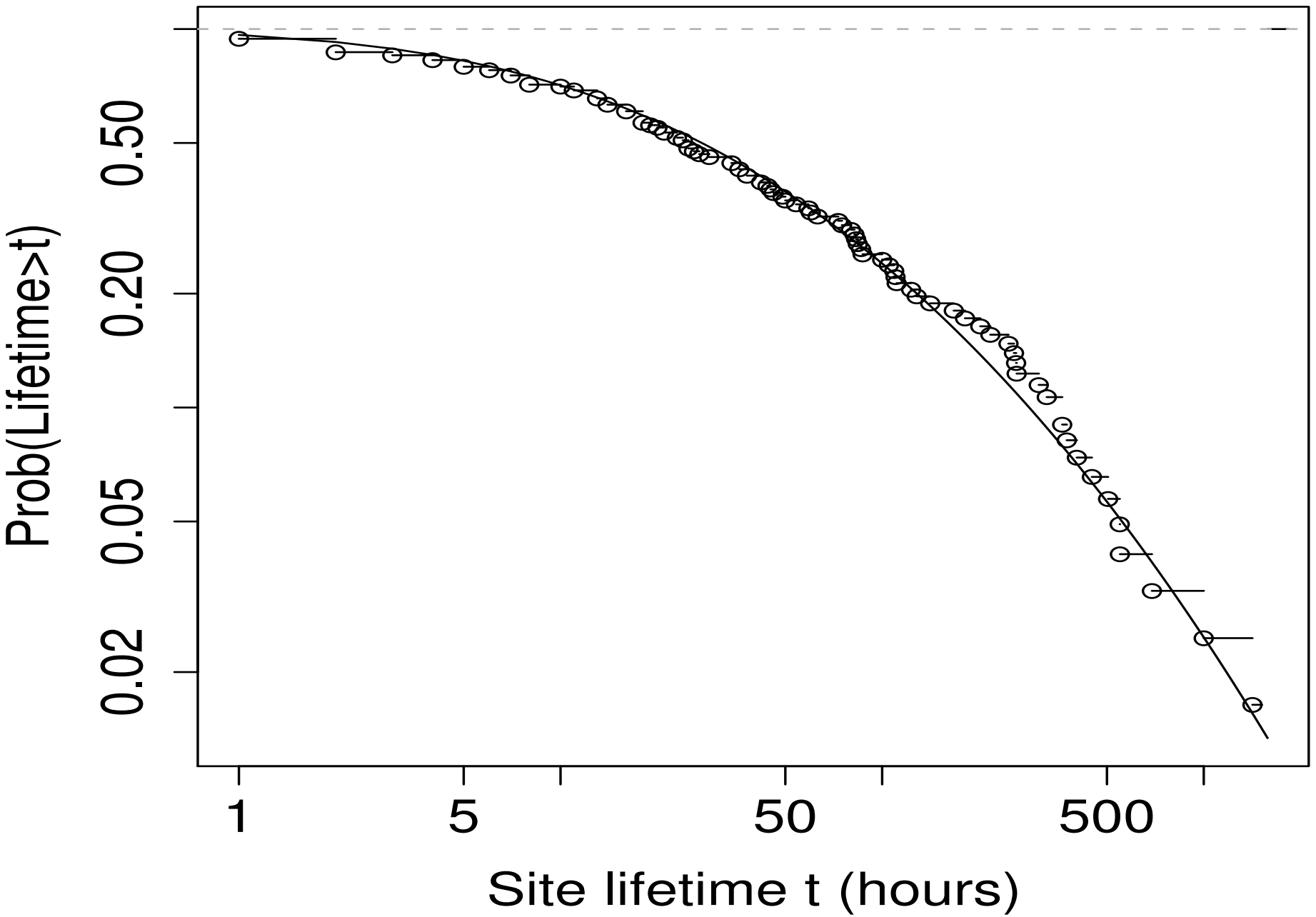

Rock IPs operational
Rock domains operational
80
70
60
50
40
30
20
10
0
17/02/2007
19/02/2007
21/02/2007
23/02/2007
25/02/2007
27/02/2007
01/03/2007
03/03/2007
05/03/2007
07/03/2007
09/03/2007
11/03/2007
13/03/2007
15/03/2007
17/03/2007
19/03/2007
21/03/2007
23/03/2007
25/03/2007
27/03/2007
29/03/2007
31/03/2007
02/04/2007
04/04/2007
06/04/2007
08/04/2007
10/04/2007
12/04/2007


Rock IPs added
Rock IPs removed
Synchronised => automated!
20
18
16
14
12
10
8
6
4
2
0
17/02/2007
19/02/2007
21/02/2007
23/02/2007
25/02/2007
27/02/2007
01/03/2007
03/03/2007
05/03/2007
07/03/2007
09/03/2007
11/03/2007
13/03/2007
15/03/2007
17/03/2007
19/03/2007
21/03/2007
23/03/2007
25/03/2007
27/03/2007
29/03/2007
31/03/2007
02/04/2007
04/04/2007
06/04/2007
08/04/2007
10/04/2007
12/04/2007


Rock domains added
Rock domains removed
Unsynchronised => manual!
40
35
30
25
20
15
10
5
0
17/02/2007
19/02/2007
21/02/2007
23/02/2007
25/02/2007
27/02/2007
01/03/2007
03/03/2007
05/03/2007
07/03/2007
09/03/2007
11/03/2007
13/03/2007
15/03/2007
17/03/2007
19/03/2007
21/03/2007
23/03/2007
25/03/2007
27/03/2007
29/03/2007
31/03/2007
02/04/2007
04/04/2007
06/04/2007
08/04/2007
10/04/2007
12/04/2007


Rock IPs removed
Rock domains removed
Unsynchronised => (two) manual procedures!
40
35
30
25
20
15
10
5
0
17/02/2007
19/02/2007
21/02/2007
23/02/2007
25/02/2007
27/02/2007
01/03/2007
03/03/2007
05/03/2007
07/03/2007
09/03/2007
11/03/2007
13/03/2007
15/03/2007
17/03/2007
19/03/2007
21/03/2007
23/03/2007
25/03/2007
27/03/2007
29/03/2007
31/03/2007
02/04/2007
04/04/2007
06/04/2007
08/04/2007
10/04/2007
12/04/2007


70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
Non-rock phish
Rock-phish domains
Rock-phish IPs
Fast-flux domains
Fast-flux IPs
1
2
3
4
5
6
7
8
9
10
11
12
13
14
More
Lifetime (days)


Prob(Lifetime>t)
0.02
0.05
0.20
0.50
1
5
50
500
Site lifetime t (hours)

Fake escrow sites

- Large number (a dozen or so) of sets of fake escrow sites used for auction scams
- Tracked by “AA419” and taken down by amateur “vigilantes”
- Speed of removal will indicate contribution being made by financial institutions

Other types of scam

- Mule recruitment
  - Mixture of real companies and fake ones
  - Take-down appears to be mainly vigilantes
- Canadian Pharmacy &c (pills and penises)
  - Hosted on same fast-flux pools as some of the phishing sites
- Post-modern Ponzi-schemes
  - No take-down, but leveraging reputation

Our research goals

- How many phishers are there ?
- How much phishing is phishing ?
- How do we fix the incentives to prevent phishing from being effective ?
- Phishing is now mechanised and uses standard kits – we believe we know how to disrupt these kits, giving a short-term edge!
- Find communities trading in fake reputation

Summary

- Take-down has an impact
  - but it is not fast enough to make losses zero
- Rock-phish gang have a good recipe
  - planned ? or just stumbled upon ?
- Wide variations in bank performance
  - incompetence? or facing better attackers?
- Some “phishing losses” are indeed phishing
  - but sums too rough to discount key-loggers &c

The impact of website take-down on phishing

BLOG: http://www.lightbluetouchpaper.org/

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

http://www.cl.cam.ac.uk/~twm29/

http://www.cl.cam.ac.uk/~rnc1/weis07phishing.pdf

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

San Francisco
31st July 2007