Co-operating to tackle "phishing" ?

Dr Richard Clayton

(joint work with Dr Tyler Moore)

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

TWENTY-SIXTH INTERNATIONAL SYMPOSIUM ON ECONOMIC CRIME
3rd September 2008

What is “phishing”

- Person receives email from their bank indicating their information must be updated
- URL looks convincing

  `http://session-10999042.www.mybank.com.info80.cn`
- Website looks convincing: so they login…
  – usually copied from the real thing !
- Multi-billion dollar losses occurring
  – risk that confidence in online banking will falter

Our research

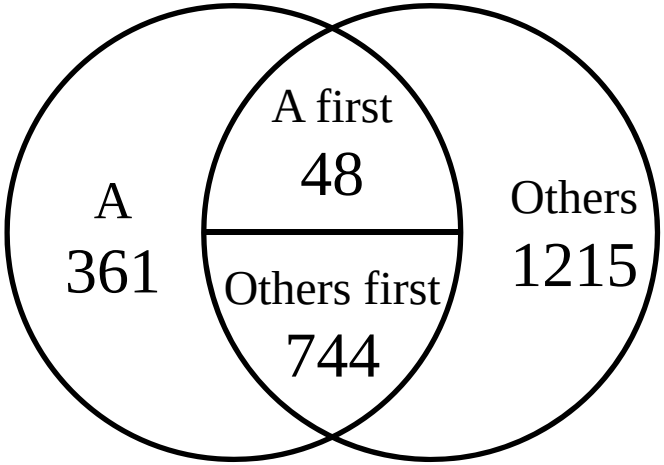
- Studying phishing since early 2007
- Measuring fake website take-down times
  - removal of sites reduces visitors
- Identified “rock-phish” gang and showed how their methods led to longer lifetimes
  - also tracked rise of hard-to-remove “fast-flux”
- Showed how “mule recruitment” sites ignored by the banking industry [ISEC XXV 2007]

Data sources

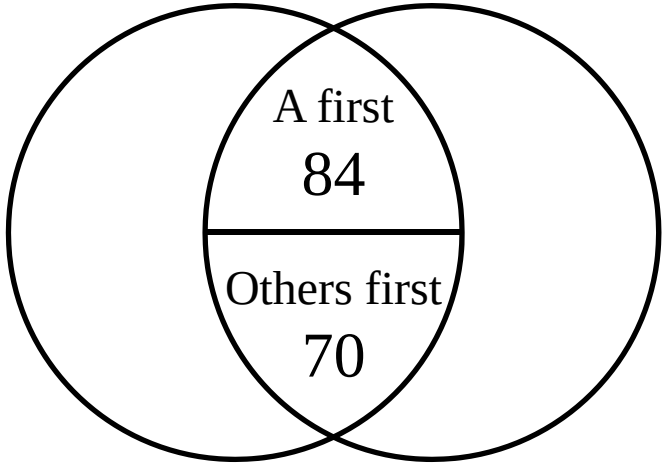
- Originally mining PhishTank dataset
  - free and apparently accurate and substantial
- Now getting data from a brand owner and two brand protection companies (plus PhishTank and “Artists Against 419”)
- These phishing “feeds” have common components but turn out to be different…

Feeds are not shared

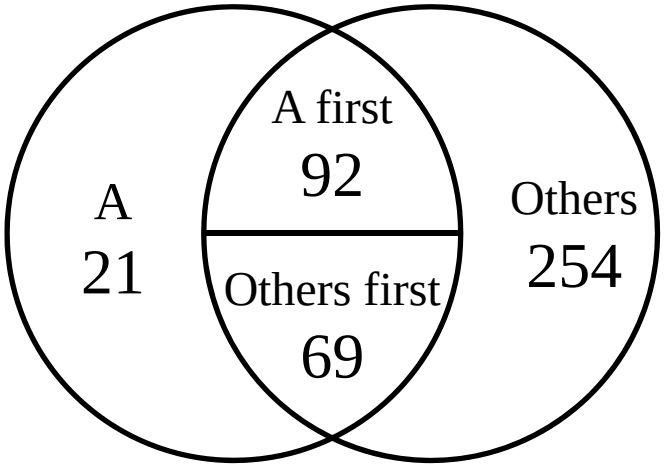
- Brand-protection companies obtain feeds from many places
- They also run their own detectors
- They sell feeds, but don’t share them
- Hence Company A, who sells services to Bank A1, can be unaware of sites detected by Company B – and doesn’t take them down



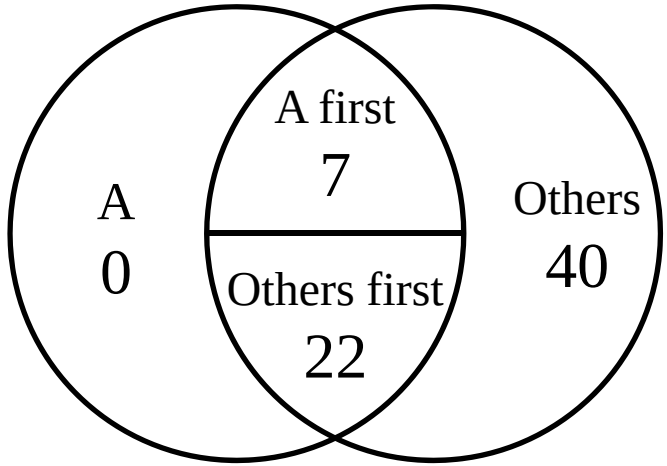
Ordinary phishing sites



Delay in detecting (hours)



Mean lifetime (hours)



Median lifetime (hours)

Bank A1’s experience as a client of BrandProtection company A

Company A v Company B

- Same pattern continues for top 6 banks for Company A and B, and for all *n* clients
- However, less pronounced for B: which seems to have a better feed [or maybe just one that is much more aligned with ours!]
- But A's clients bigger and proportion missed goes up with size; so B's prowess may be more a structural issue than just extra effectiveness

Phishing Lifetimes (hrs)	sites	mean	median
Free-web hosting			
all	395	47.6	0
brand-owner aware	240	4.3	0
brand-owner unaware	155	114.7	29
Compromised machines			
all	193	49.2	0
brand-owner aware	105	3.5	0
brand-owner unaware	155	103.8	10
Rock-phish domains	821	70.3	33
Fast-flux domains	315	96.1	25.5

Thi$ repreent ri$k

- Longer lifetimes => more visitors
- Hence we can assess impact of longer lifetimes:

Exposure figures (6 month totals)	A's banks		B's banks	
	Khour	$m	Khour	$m
Actual values	1005	276	78	32
Expected if sharing	418	113	61	28.5
Effect of no sharing	**587**	**163**	**17**	**3.5**

Hence…

- Banks should force brand-protection companies to share feeds
  - cf the anti-virus community for last 15 years
- Brand-protection companies could form a "club" to prevent new entrants from free-riding
  - don't have to make feeds "free", just share them
- Expect some excitement as our message begins to sink in during this Autumn…

Co-operating to tackle “phishing” ?

http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory