The consequence of non-cooperation in the fight against phishing

Tyler Moore and Richard Clayton

CRCS, Harvard University
Computer Laboratory, University of Cambridge

3rd APWG eCrime Researchers Summit
October 16, 2008

HARVARD
School of Engineering and Applied Sciences

Outline

HARVARD
School of Engineering and Applied Sciences

Phishing website take-down

- We empirically examine phishing website 'take-down'
  - Widely-used countermeasure in fight against phishing
  - Banks, or 3rd party take-down companies, collect 'feeds' of phishing URLs
  - Feeds obtained from banks, third parties and using proprietary spam traps
  - Verify URLs in feed, then issue take-down notices to relevant ISPs and/or registrars
- Average phishing website lifetimes
  - According to industry: from '5 hours' to 'less than 24 hours'
  - Our measurements (eCrime '07): 62 to 95 hours
  - Why the disparity?

HARVARD
School of Engineering and Applied Sciences

Data collection methodology

- Amalgamate several phishing 'feeds'
  - One large brand owner
  - PhishTank
  - APWG
  - Two take-down companies (each a combination of outside feeds and proprietary collection)
- Automated testing system
  - Data collection period: October 2007–March 2008
  - Continuously query sites until they stop responding or change
  - Distinguish between 'ordinary', 'rock-phish', and 'fast-flux'
  - Verification (ordinary phishing): fetch HTML and check whether bank name is present

HARVARD
School of Engineering and Applied Sciences

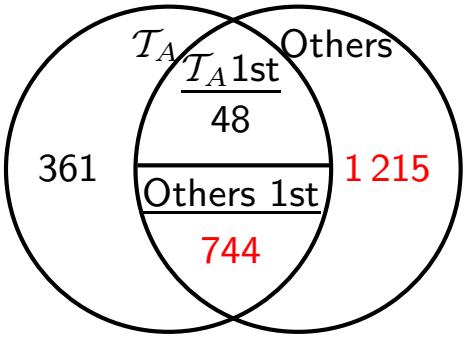
How we measure cooperation

- Focus on URL feeds from take-down companies $\mathcal{T}_A$ and $\mathcal{T}_B$
  - Feeds represent their global view
  - $\mathcal{T}_A$: 54 client banks attacked 10/07–3/08
  - $\mathcal{T}_B$: 66 client banks attacked 10/07–3/08
  - We only examine phishing attacks on these 120 brands
  - Take-down companies only care about phishing sites targeting their clients, but they also detect other phishing sites

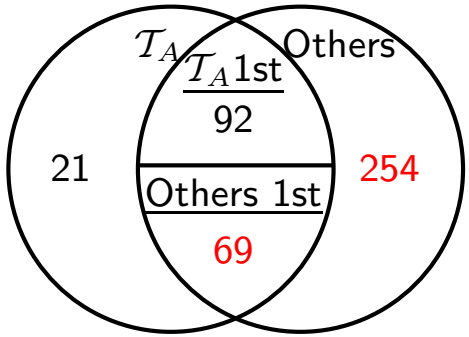
HARVARD
School of Engineering and Applied Sciences

How one bank suffers when take-down companies don't share phishing URLs

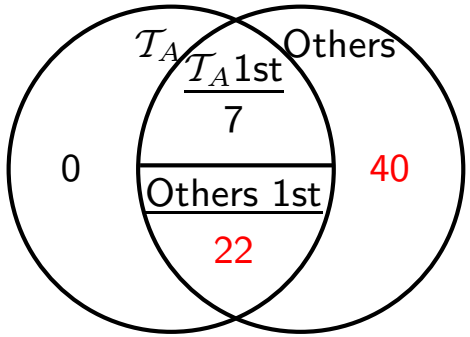
Ordinary phishing sites



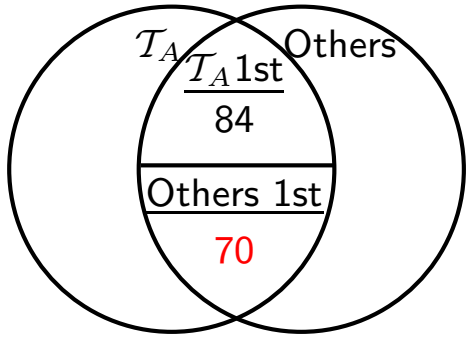
Mean lifetime (hours)



Median lifetime (hours)



Mean difference (hours)

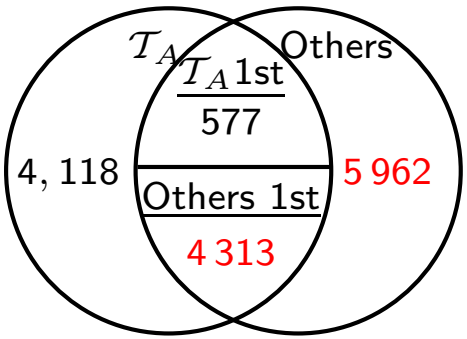


HARVARD
School of Engineering and Applied Sciences

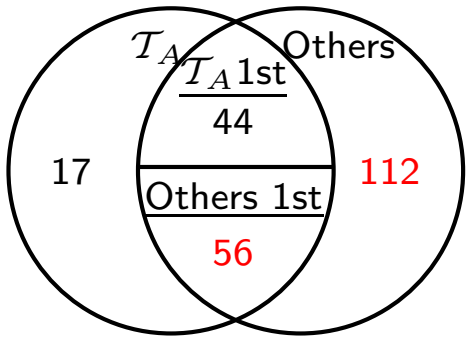
Most banks suffer when phishing URLs are not shared

$\mathcal{T}_A$'s 54 client banks attacked 10/07–3/08

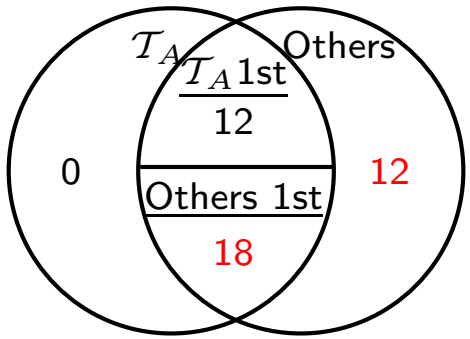
Ordinary phishing sites



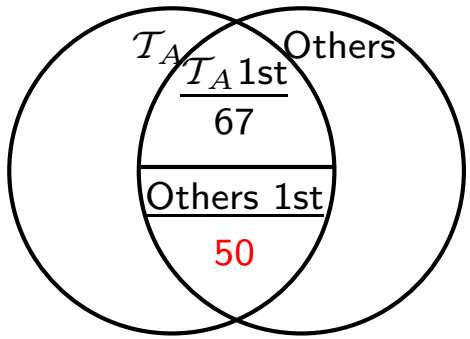
Mean lifetime (hours)



Median lifetime (hours)

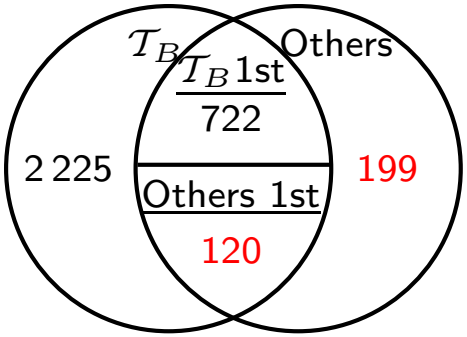


Mean difference (hours)

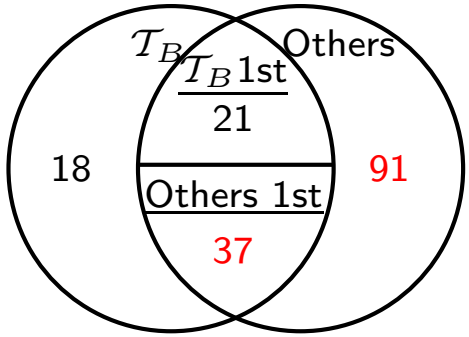


$\mathcal{T}_B$'s 66 client banks attacked 10/07–3/08

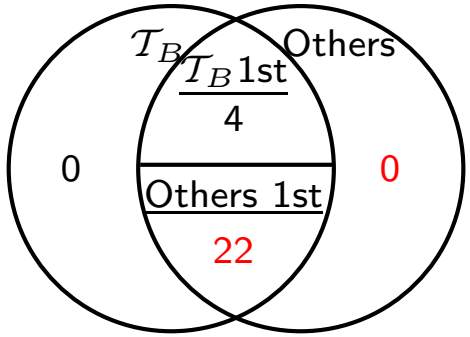
Ordinary phishing sites



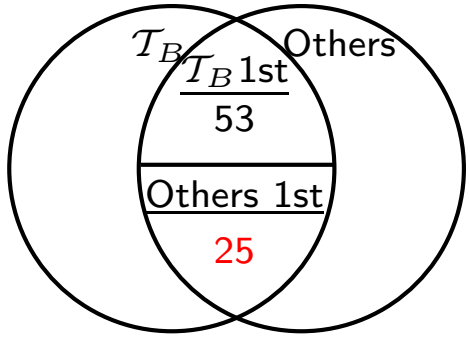
Mean lifetime (hours)



Median lifetime (hours)

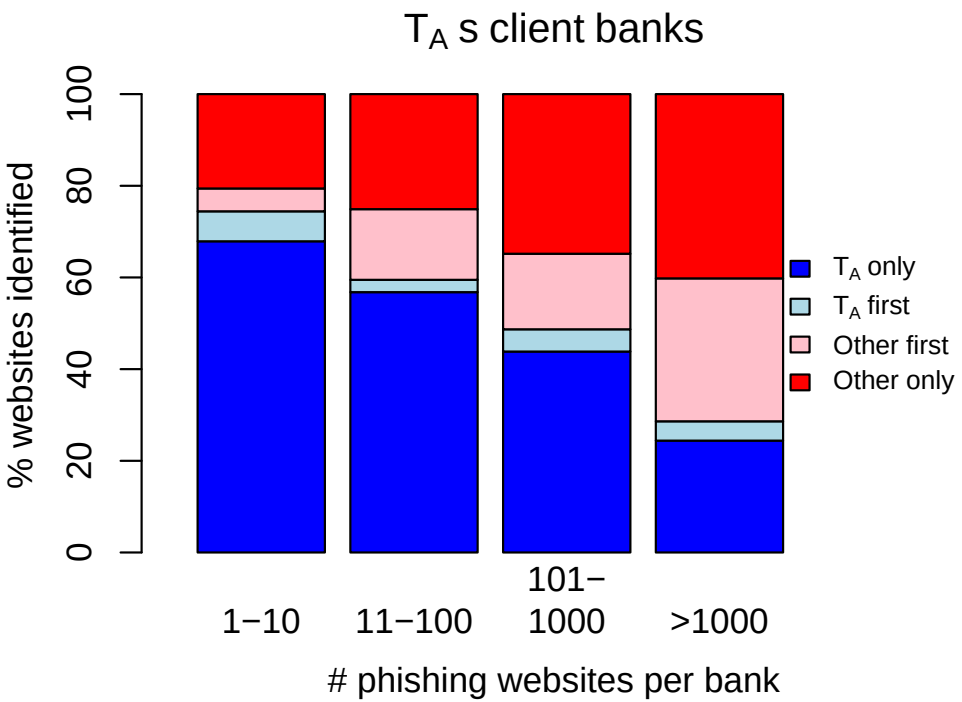


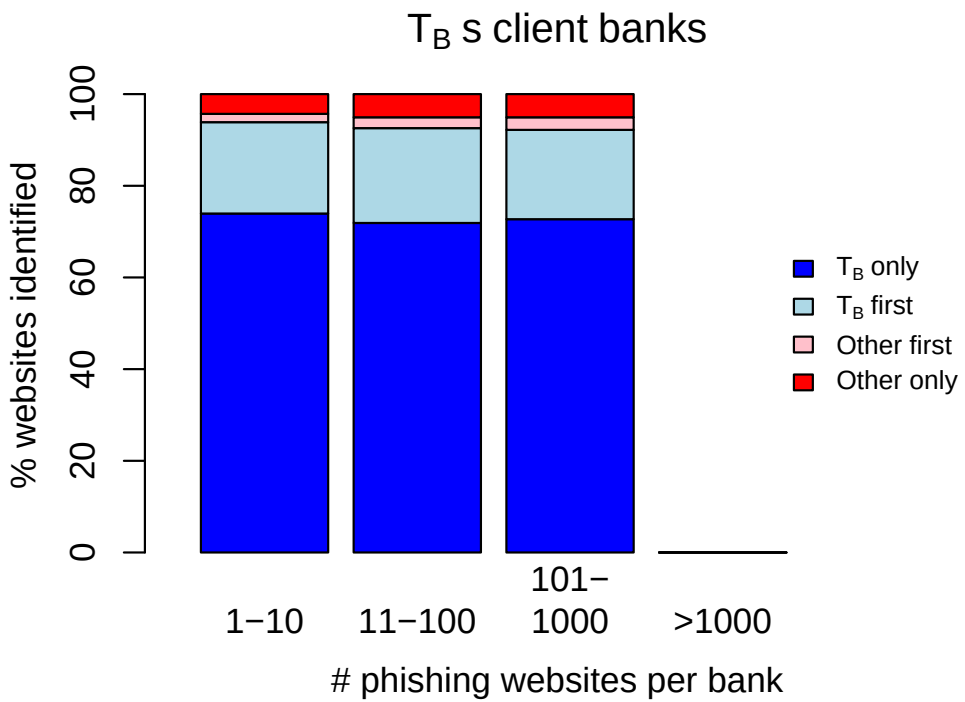
Mean difference (hours)



HARVARD
School of Engineering and Applied Sciences

Popularity of phishing target affects gain from sharing

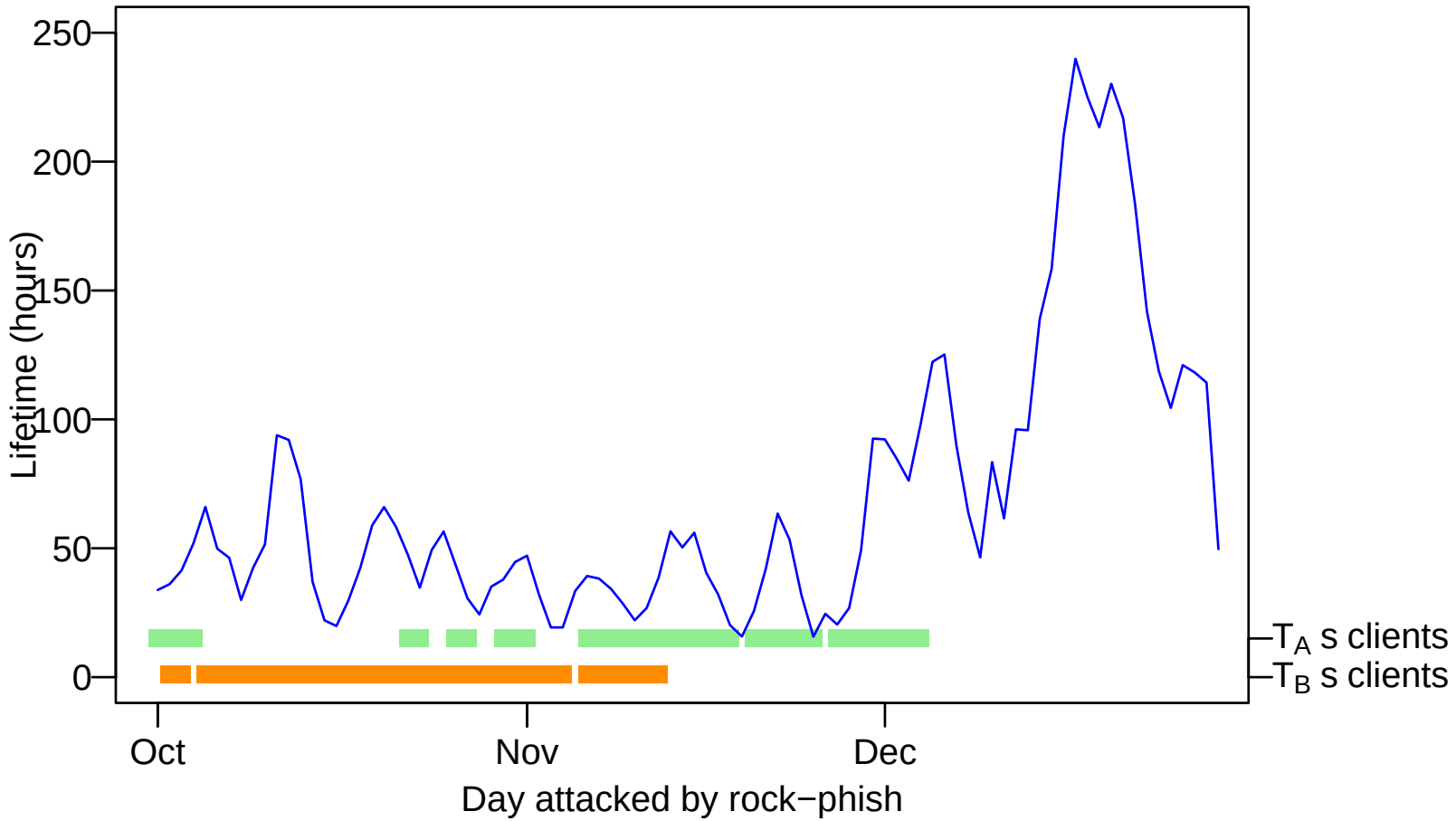




Long-lived phishing websites caused by not sharing URLs

HARVARD
School of Engineering and Applied Sciences

Rock-phish website lifetimes depend on $\mathcal{T}_A$ and $\mathcal{T}_B$'s effort



HARVARD
School of Engineering and Applied Sciences

How can we estimate the cost of non-cooperation

- Estimating user response to phishing
  - We automatically collect world-readable 'Webalizer' web page usage statistics from phishing sites
  - We measure user response to phishing over time (eCrime '07)
  - Florêncio and Herley create similar estimate using different method
- Gartner estimate cost of identity theft to be $572 per victim
- Consequently, we derived an estimate of financial risk as a consequence of phishing website uptime

HARVARD
School of Engineering and Applied Sciences

What is the cost of non-cooperation?

- We can estimate losses caused by not sharing feeds
  - Compare the lifetimes of phishing websites known to $\mathcal{T}_A$ and $\mathcal{T}_B$ to the lifetimes of websites unknown to them
  - Time difference is a direct consequence of not sharing feeds
- Financial exposure for $\mathcal{T}_A$'s clients
  - Total exposure of $\mathcal{T}_A$'s 54 targeted banks 10/07–3/08: \$276m
  - 5 962 sites impersonating $\mathcal{T}_A$'s clients missed by $\mathcal{T}_A$: \$119m
  - 4 313 websites found by $\mathcal{T}_A$ 50 hours after other sources: \$44m

HARVARD
School of Engineering and Applied Sciences

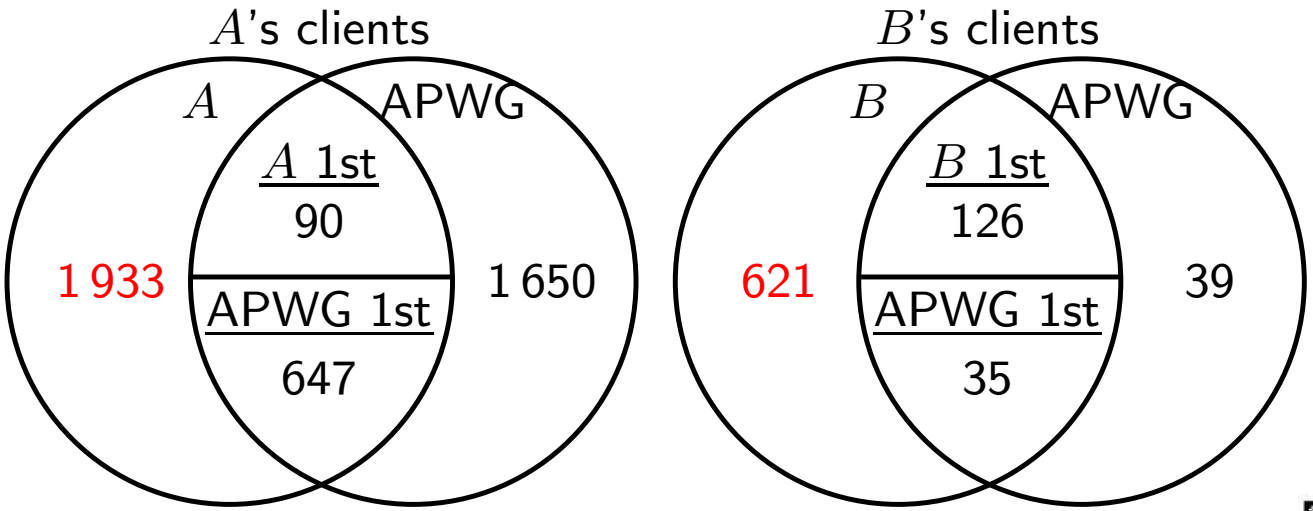
Cost of non-cooperation (prolonged lifetimes and $)

Exposure figures (6-month totals)	$\mathcal{T}_A$**'s client banks**	$\mathcal{T}_B$**'s client banks**
Actual values	1 005k hrs ($276m)	78k hrs ($32.0m)
Effect of not sharing	587k hrs ($163m)	17k hrs ($3.5m)
Expected if sharing	418k hrs ($113m)	61k hrs ($28.5m)

HARVARD
School of Engineering and Applied Sciences

How can we improve cooperation?

- Leverage existing industry cooperation
  - The APWG distributes a feed based on contributions from its members and the public
  - The take-down companies already take the APWG's feed, they should be encouraged to give back



HARVARD
School of Engineering and Applied Sciences

How can we improve cooperation?

- Cooperation is not without precedent
  - Anti-virus companies exchange virus/malware samples
  - Each company verifies the sample's legitimacy and develops custom signatures
  - Similarly, take-down companies could share raw feeds, and add value by individually sorting out the incorrect submissions and certifying their assessments
- No one ever said cooperation is easy
  - Competitive concerns (lower barrier to entry, perceived leaders don't stand to gain much)
  - Free-riding potential
- The stakes are too high for the banks to not demand better cooperation

HARVARD
School of Engineering and Applied Sciences

Conclusions

- We have shown that phishing URL feeds are not shared between competing take-down companies
- Lack of cooperation substantially increases the lifetimes of phishing websites, and, consequently, banks' financial exposure
- Banks should demand take-down companies share raw URL feeds (perhaps via the APWG's existing feed)
- For more, see
  `http://www.lightbluetouchpaper.org/`
  `http://people.seas.harvard.edu/~tmoore/`
- Email: `tmoore@seas.harvard.edu`

HARVARD
School of Engineering and Applied Sciences