Putting out a HIT

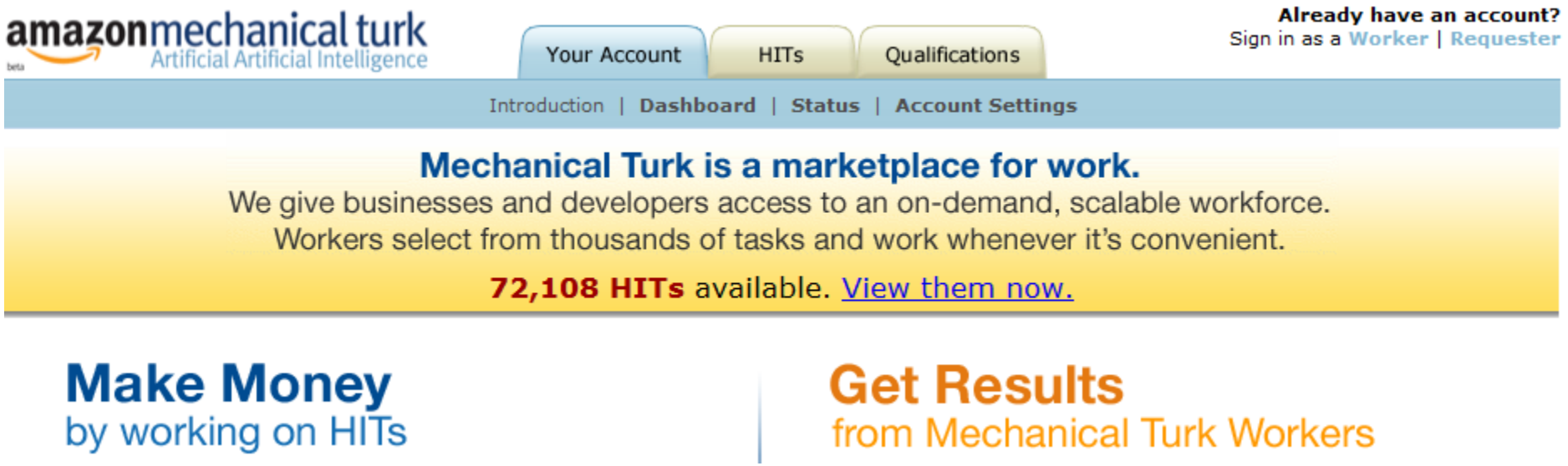
Crowdsourcing Malware Installs

Chris Kanich Stephen Checkoway Keaton Mowery

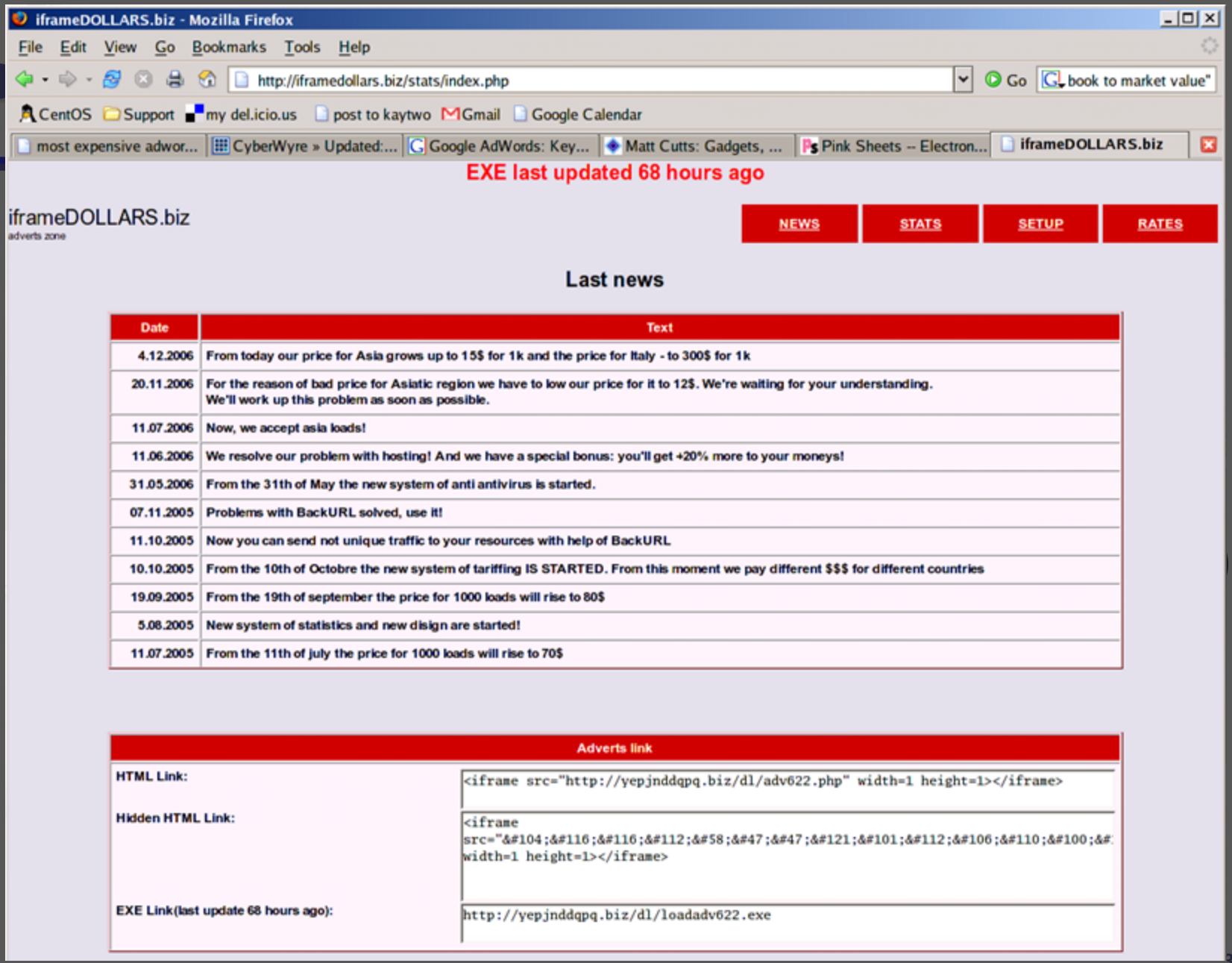
UC San Diego

UCSDCSE
Computer Science and Engineering

Mechanical Turk



- Crowdsourcing platform
- Requesters post tasks paying 1¢ – $10
- Workers perform HITs – Human Intelligence Tasks
- Amazon takes a 10% cut of each reward


iframeDOLLARS.biz - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://iframedollars.biz/stats/index.php
Go
book to market value"
CentOS Support my del.icio.us post to kaytwo Gmail Google Calendar
most expensive adwor... CyberWyre » Updated:... Google AdWords: Key... Matt Cutts: Gadgets, ... Pink Sheets -- Electron... iframeDOLLARS.biz
EXE last updated 68 hours ago
iframeDOLLARS.biz
adverts zone
NEWS STATS SETUP RATES
Last news
Date
Text
4.12.2006
From today our price for Asia grows up to 15$ for 1k and the price for Italy - to 300$ for 1k
20.11.2006
For the reason of bad price for Asiatic region we have to low our price for it to 12$. We're waiting for your understanding.
We'll work up this problem as soon as possible.
11.07.2006
Now, we accept asia loads!
11.06.2006
We resolve our problem with hosting! And we have a special bonus: you'll get +20% more to your moneys!
31.05.2006
From the 31th of May the new system of anti antivirus is started.
07.11.2005
Problems with BackURL solved, use it!
11.10.2005
Now you can send not unique traffic to your resources with help of BackURL
10.10.2005
From the 10th of Octobre the new system of tariffing IS STARTED. From this moment we pay different $$$ for different countries
19.09.2005
From the 19th of september the price for 1000 loads will rise to 80$
5.08.2005
New system of statistics and new disign are started!
11.07.2005
From the 11th of july the price for 1000 loads will rise to 70$
Adverts link
HTML Link:
<iframe src="http://yepjnddqpq.biz/dl/adv622.php" width=1 height=1></iframe>
Hidden HTML Link:
<iframe
src="http://yepjnd&#
width=1 height=1></iframe>
EXE Link(last update 68 hours ago):
http://yepjnddqpq.biz/dl/loadadv622.exe

Summary

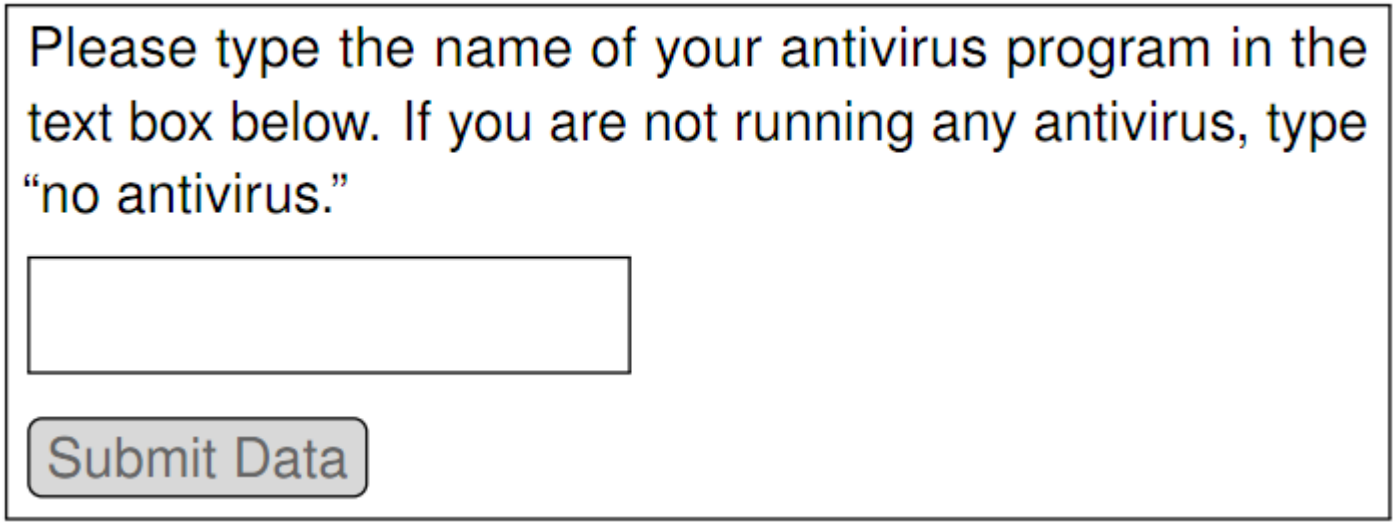
- Drive-bys on Turkers **are** economically feasible
  - Volume leaves something to be desired…
- Very high “exploitability” figures are common
  - AV up-to-date-ness in a similar state
- Low-wage Turkers majority Indian

Methodology

- Goal: accurately simulate machine takeover and determine its economic profitability
- Find a vulnerable population (Mturk workers)
- Determine their vulnerability
- Is host value > Mturk cost?

Cost = 110% x (mturk wage) x (vulnerable ratio)

Mechanical Turk HITs



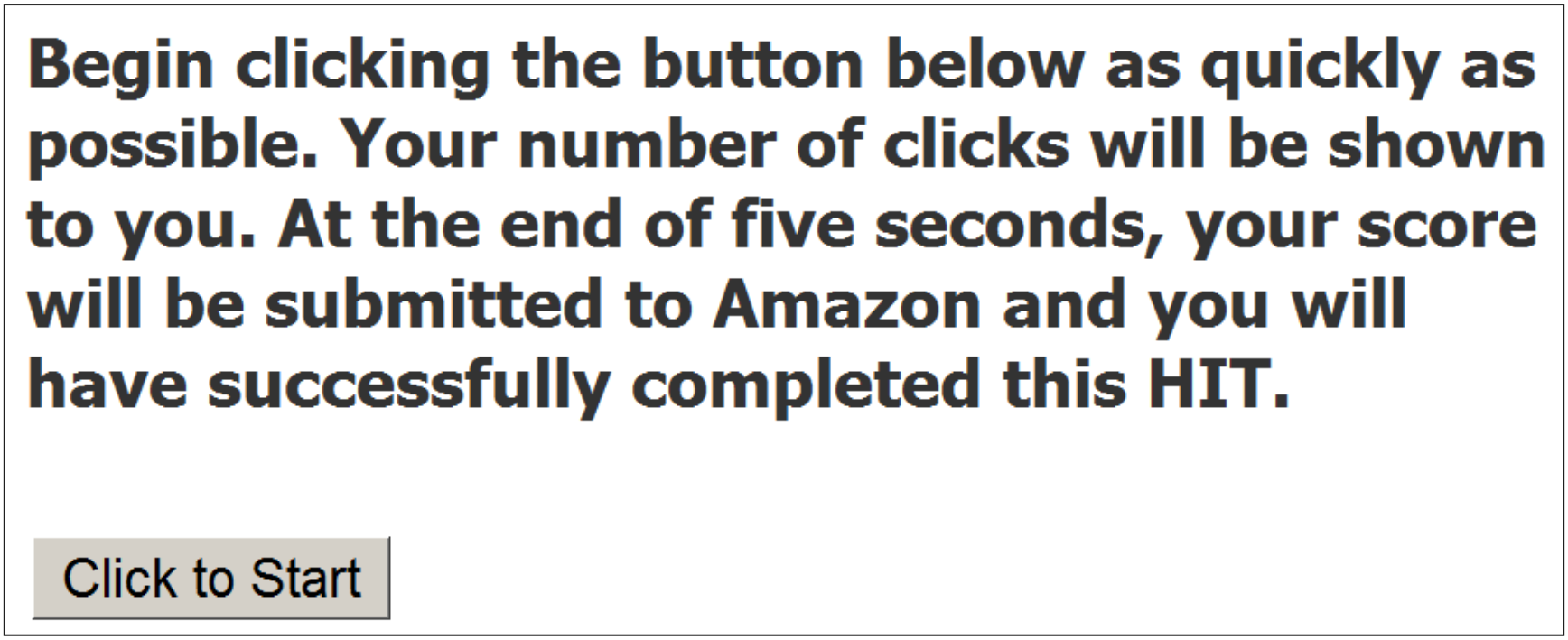
- Ran this at both 1¢ and 5¢

Mechanical Turk HITs

> **For a bonus of 11 cents**, we can also collect additional information about your antivirus if you download and run this script. This script does not harm or change your computer in any way. You may inspect the script to verify this. After the script has run, a Notepad window will pop up including information about your running antivirus. COPY and PASTE everything in the Notepad window into the text box below.

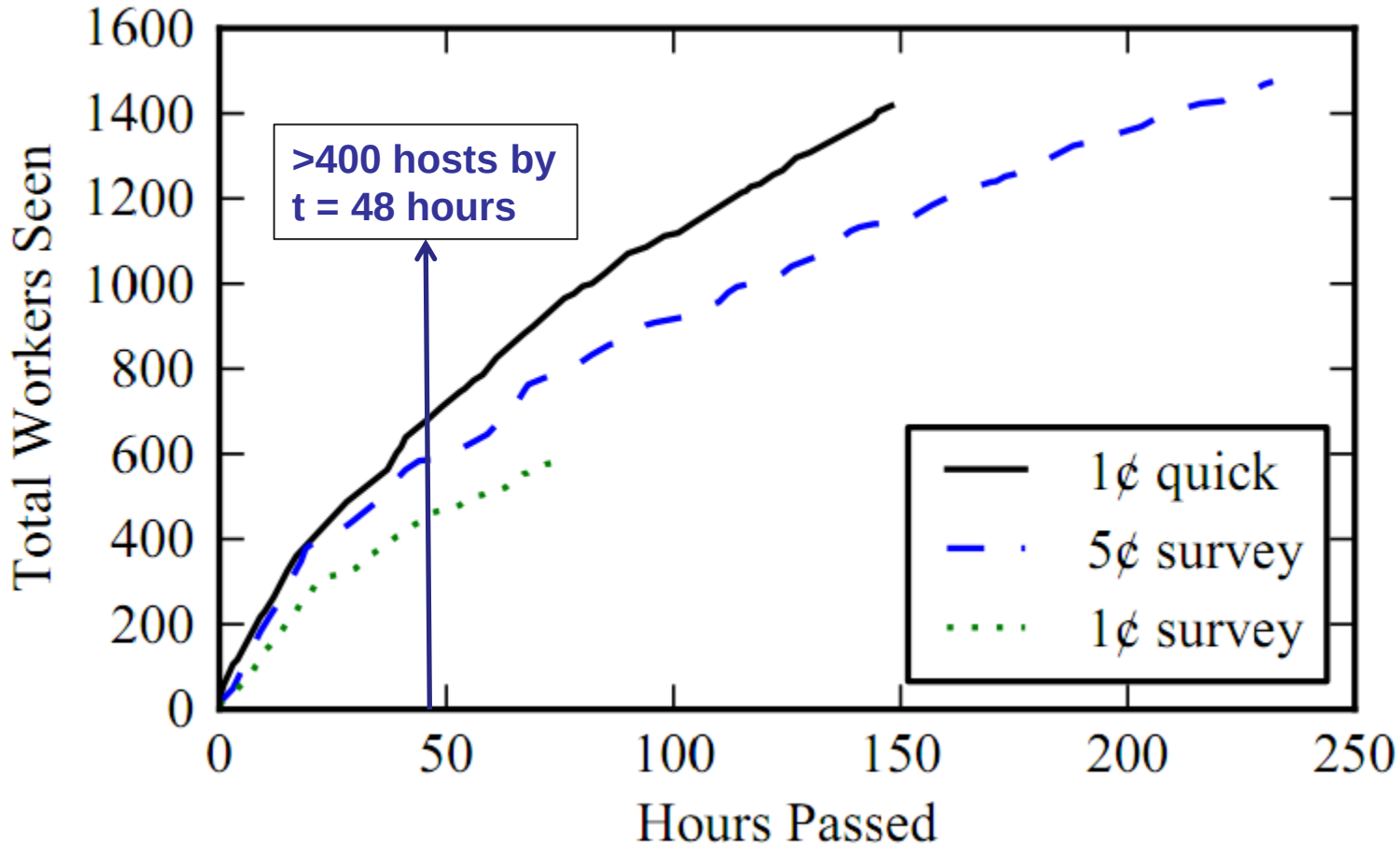
- 38% conversion rate

Mechanical Turk HITs



- Ran this at 1¢ only

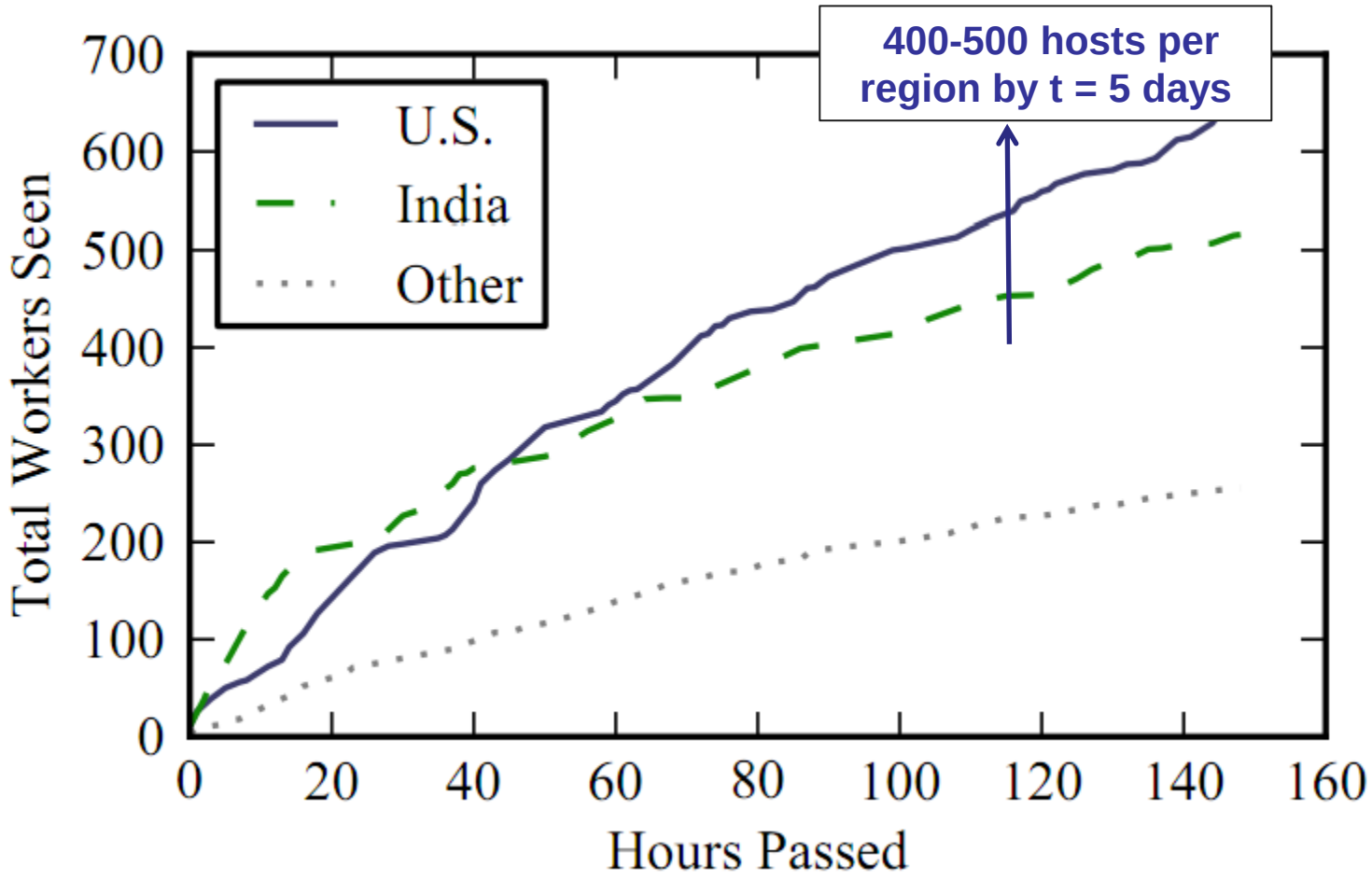
Worker Uptake



Worker Demographics

- 61.3% in India
- 23.2% in the U.S.
- Remaining 15.5% in 75 other countries
- English language HIT

Worker Uptake

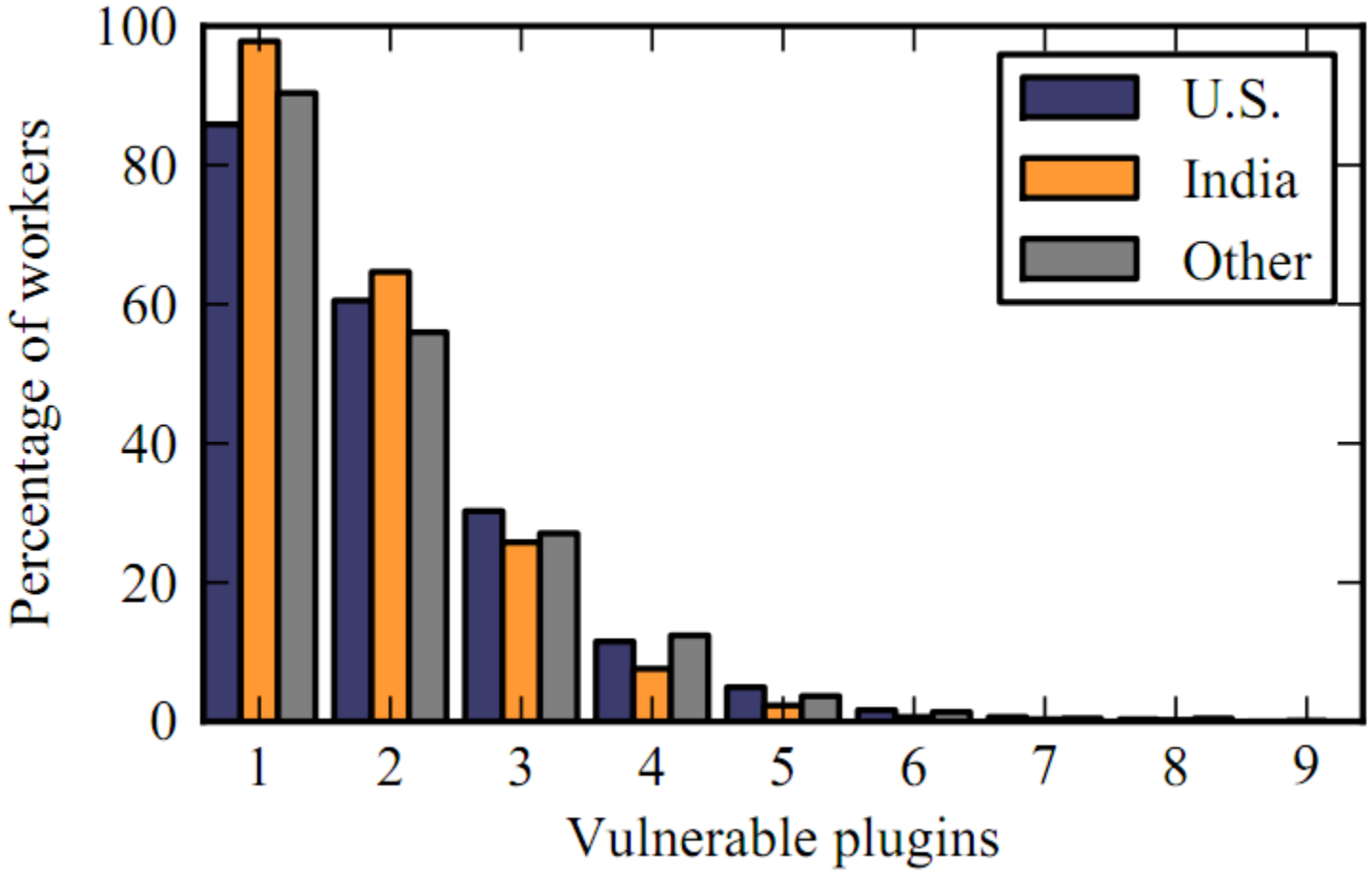


Vulnerability Oracle

- Surveyed CVEs for popular browser plugins
- Determined vulnerable version range
- Limited to remotely exploitable CVEs

Plugin	Windows	Mac OS X	Linux	CVE
Adobe Flash Player	10.2.154.13	10.2.154.13	10.2.154.13	CVE-2011-0609
Adobe Reader*	10.0.2	10.0.2	9.4.1	CVE-2011-0610 CVE-2011-0611
Adobe Shockwave Player	11.5.9.615	11.5.9.615		CVE-2011-0557
Apple QuickTime	7.6.8	7.6.8		CVE-2010-3787
Microsoft Silverlight	3.0.50106.0	3.0.40818.0		CVE-2010-1898
Java†	1.6.0–1.6.0.21	1.6.0–1.6.0.21	1.6.0–1.6.0.21	CVE-2010-3571
RealPlayer‡	11.0–11.1	11.0–11.1	11.0.2.1744	CVE-2010-4397
VLC media player	1.1.7			CVE-2010-3276

Vulnerability of Workers



Economic feasibility

- For 5¢ hosts:

	% vulnerable	% previewed	% accepted	% completed	cost ($/1000 hosts)
U.S.	84.9	99.5	87.9	81.0	52.52
India	96.3	99.5	87.6	80.2	45.83
Other	87.2	98.3	91.3	85.7	54.04

PPI purchase price:

- $100 – $180 for U.S. hosts
- $7 – $8 for Asian hosts

Drawbacks

- Synthetic exploitation oracle
  - Exploit “startup cost” not factored in
  - Detection might hamper success
- Uptake rate
  - PPI affiliates expect 1000s of hosts/week
  - Only feasible as a supplement to other infections
- Only useful if crowdsourcing takes off

Additional observations

- Mturk allows targeting by country
- Mturk
- AV pe much
- Crimi

	AV installed (%)	up to date (%)
U.S.	98.7	22.8
India	92.7	68.7
Other	95.2	37.3

Conclusions

- Antivirus use very high; correct use very low
- Turker browsers very vulnerable
- Mturk is very expensive as traffic acquisition
- Mturk based drive-bys economically profitable, but perhaps not economically practical.

Thank You!

UCSDCSE
Computer Science and Engineering