Putting out a HIT
Crowdsourcing Malware Installs

Chris Kanich  Stephen Checkoway  Keaton Mowery

UC San Diego
Mechanical Turk

Mechanical Turk is a marketplace for work. We give businesses and developers access to an on-demand, scalable workforce. Workers select from thousands of tasks and work whenever it’s convenient.

72,108 HITs available. View them now.

Make Money by working on HITs

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

Abstracts compromise from monetization

Broker buys and sells “installs” in bulk

Sellers compromise hosts and install “droppers”

Sellers need exploits and traffic

Buyers monetize hosts (or install other droppers)

We act as hypothetical install sellers

Can we turn a profit selling installs from mturk?
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

Please type the name of your antivirus program in the text box below. If you are not running any antivirus, type “no antivirus.”

Submit Data

• 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

Begin clicking the button below as quickly as possible. Your number of clicks will be shown to you. At the end of five seconds, your score will be submitted to Amazon and you will have successfully completed this HIT.

Click to Start

- Ran this at 1¢ only
Worker Uptake

>400 hosts by \( t = 48 \) hours
Worker Demographics

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

400-500 hosts per region by t = 5 days
# Vulnerability Oracle

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

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Windows</th>
<th>Mac OS X</th>
<th>Linux</th>
<th>CVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Flash Player</td>
<td>10.2.154.13</td>
<td>10.2.154.13</td>
<td>10.2.154.13</td>
<td>CVE-2011-0609</td>
</tr>
<tr>
<td>Adobe Reader*</td>
<td>10.0.2</td>
<td>10.0.2</td>
<td>9.4.1</td>
<td>CVE-2011-0610, CVE-2011-0611</td>
</tr>
<tr>
<td>Adobe Shockwave Player</td>
<td>11.5.9.615</td>
<td>11.5.9.615</td>
<td></td>
<td>CVE-2011-0557</td>
</tr>
<tr>
<td>Apple QuickTime</td>
<td>7.6.8</td>
<td>7.6.8</td>
<td></td>
<td>CVE-2010-3787</td>
</tr>
<tr>
<td>Microsoft Silverlight</td>
<td>3.0.50106.0</td>
<td>3.0.40818.0</td>
<td></td>
<td>CVE-2010-1898</td>
</tr>
<tr>
<td>Java†</td>
<td>1.6.0–1.6.0.21</td>
<td>1.6.0–1.6.0.21</td>
<td>1.6.0–1.6.0.21</td>
<td>CVE-2010-3571</td>
</tr>
<tr>
<td>RealPlayer‡</td>
<td>11.0–11.1</td>
<td>11.0–11.1</td>
<td>11.0.2.1744</td>
<td>CVE-2010-4397</td>
</tr>
<tr>
<td>VLC media player</td>
<td>1.1.7</td>
<td></td>
<td></td>
<td>CVE-2010-3276</td>
</tr>
</tbody>
</table>
Vulnerability of Workers

![Bar chart showing percentage of workers vulnerable to plugins by country.

- U.S.
- India
- Other

Vulnerable plugins range from 1 to 9.]
Economic feasibility

• For 5¢ hosts:

<table>
<thead>
<tr>
<th></th>
<th>% vulnerable</th>
<th>% previewed</th>
<th>% accepted</th>
<th>% completed</th>
<th>cost ($/1000 hosts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td>84.9</td>
<td>99.5</td>
<td>87.9</td>
<td>81.0</td>
<td>52.52</td>
</tr>
<tr>
<td>India</td>
<td>96.3</td>
<td>99.5</td>
<td>87.6</td>
<td>80.2</td>
<td>45.83</td>
</tr>
<tr>
<td>Other</td>
<td>87.2</td>
<td>98.3</td>
<td>91.3</td>
<td>85.7</td>
<td>54.04</td>
</tr>
</tbody>
</table>

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's iframe interface is powerful
- AV penetration high; up-to-date not so much
- Criminals might not pay victims

<table>
<thead>
<tr>
<th></th>
<th>AV installed (%)</th>
<th>up to date (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td>98.7</td>
<td>22.8</td>
</tr>
<tr>
<td>India</td>
<td>92.7</td>
<td>68.7</td>
</tr>
<tr>
<td>Other</td>
<td>95.2</td>
<td>37.3</td>
</tr>
</tbody>
</table>

UCSD CSE
Computer Science and Engineering
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!

UCSD CSE
Computer Science and Engineering