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
Phishing website take-down
  • Introduction
  • Data collection and measurement methodology

Non-cooperation when countering phishing
  • Comparing lifetimes for different take-down company feeds
  • Rock-phish and non-cooperation
  • Estimating the cost of phishing

How can we improve cooperation?
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?
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
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
How one bank suffers when take-down companies don’t share phishing URLs

<table>
<thead>
<tr>
<th>Ordinary phishing sites</th>
<th>Mean lifetime (hours)</th>
<th>Median lifetime (hours)</th>
<th>Mean difference (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA 1st: 361</td>
<td>TA 1st: 21</td>
<td>TA 1st: 0</td>
<td>TA 1st: 84</td>
</tr>
<tr>
<td>Others: 744</td>
<td>Others: 254</td>
<td>Others: 40</td>
<td>Others: 70</td>
</tr>
<tr>
<td>TA 1st: 1215</td>
<td>Others: 92</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TA 1st: 48</td>
<td>Others: 69</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others: 7</td>
<td>Others: 22</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tyler Moore

Consequence of non-cooperation in the fight against phishing
Most banks suffer when phishing URLs are not shared

<table>
<thead>
<tr>
<th>Ordinary phishing sites</th>
<th>Mean lifetime (hours)</th>
<th>Median lifetime (hours)</th>
<th>Mean difference (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( T_A )</td>
<td>Others</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4,118</td>
<td>5,962</td>
<td>4,313</td>
</tr>
<tr>
<td></td>
<td>( T_A ) 1st</td>
<td>577</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Others 1st</td>
<td>17</td>
<td>112</td>
</tr>
<tr>
<td></td>
<td>Others</td>
<td>199</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>( T_B )</td>
<td>2,225</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>( T_B ) 1st</td>
<td>722</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Others 1st</td>
<td>18</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Others</td>
<td>120</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>( T_B )</td>
<td>2,225</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>( T_B ) 1st</td>
<td>722</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Others 1st</td>
<td>18</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Others</td>
<td>120</td>
<td>22</td>
</tr>
</tbody>
</table>

\( T_A \)'s 54 client banks attacked 10/07–3/08

\( T_B \)'s 66 client banks attacked 10/07–3/08

Tyler Moore

Consequence of non-cooperation in the fight against phishing
Popularity of phishing target affects gain from sharing

**TA's client banks**

- 1-10 websites: T_A only (70%), T_A first (15%), Other first (10%), Other only (5%)
- 11-100 websites: T_A only (60%), T_A first (20%), Other first (15%), Other only (5%)
- 101-1000 websites: T_A only (50%), T_A first (30%), Other first (15%), Other only (5%)
- >1000 websites: T_A only (40%), T_A first (30%), Other first (20%), Other only (10%)

**TB's client banks**

- 1-10 websites: T_B only (80%), T_B first (10%), Other first (10%), Other only (0%)
- 11-100 websites: T_B only (70%), T_B first (15%), Other first (15%), Other only (0%)
- 101-1000 websites: T_B only (60%), T_B first (20%), Other first (20%), Other only (0%)
- >1000 websites: T_B only (50%), T_B first (25%), Other first (25%), Other only (0%)

*Tyler Moore*

Consequence of non-cooperation in the fight against phishing
Long-lived phishing websites caused by not sharing URLs

- % websites lasting > 1 week
- TA
- TA-unaware sites
- All sites
- TB
- TB-unaware sites
- All sites

- Consequence of non-cooperation in the fight against phishing

- Tyler Moore
Rock-phish website lifetimes depend on $T_A$ and $T_B$'s effort.

- $T_A$'s clients
- $T_B$'s clients

Day attacked by rock-phish

Lifetime (hours)

Oct  Nov  Dec
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
What is the cost of non-cooperation?

- We can estimate losses caused by not sharing feeds
  - Compare the lifetimes of phishing websites known to $T_A$ and $T_B$ to the lifetimes of websites unknown to them
  - Time difference is a direct consequence of not sharing feeds
- Financial exposure for $T_A$’s clients
  - Total exposure of $T_A$’s 54 targeted banks 10/07–3/08: $276m
  - 5,962 sites impersonating $T_A$’s clients missed by $T_A$: $119m
  - 4,313 websites found by $T_A$ 50 hours after other sources: $44m
# Cost of non-cooperation (prolonged lifetimes and $)

<table>
<thead>
<tr>
<th>Exposure figures (6-month totals)</th>
<th>$T_A$’s client banks</th>
<th>$T_B$’s client banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual values</td>
<td>1,005k hrs ($276m)</td>
<td>78k hrs ($32.0m)</td>
</tr>
<tr>
<td>Effect of not sharing</td>
<td>587k hrs ($163m)</td>
<td>17k hrs ($3.5m)</td>
</tr>
<tr>
<td>Expected if sharing</td>
<td>418k hrs ($113m)</td>
<td>61k hrs ($28.5m)</td>
</tr>
</tbody>
</table>
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
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
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