What we now know about phishing websites

(summer 2009 version)

Richard Clayton

(joint work with Tyler Moore & Henry Stern)
What is phishing?

- Capture of user credentials through impersonation
  - in 1996 this was pretending to be an AOL sysop
  - since 2003 has been the creation of fake bank websites
- “Bank” is merely generic – attackers impersonate auction sites, payment processors, online games, Habbo, IRS etc, etc
  - common theme is that credentials are worth money
- Losses often quoted as over $2 billion/year
  - loss figures are (dubiously) scaled up from phone interviews
  - Some of Gartners figures included lottery fraud scams
  - UK banks lost £53 million in 2008 (£20m-30m in previous years)
- Phishing rare in (eg) Germany – attacks are mainly keyloggers
- Some markets use 2-factor (TANs, CAP, SecureID etc)
  - just means that attacks must be done in real-time
Academics & phishing

• Everyone can play! Display instant expertise!!
  ▪ examine psychology, attempt to block spam, detection of websites, browser enhancements, password mangling, reputation systems etc

• Our approach: Security Economics
  ▪ phishing will continue, so we measure impact, assess the effectiveness of countermeasures, aim to work out how to change incentives so that problem tends to fix itself...

• Hard to report on an on-going understanding
  ▪ papers have to be “novel research”, PhDs have to be “a contribution” – so we pick the “low hanging fruit” and move on

• Errors in early papers often go uncorrected
  ▪ “peer review” process needs knowledgeable peers
  ▪ natural tendency not to want to report failures
  ▪ natural tendency not to admit mistakes
Types of phishing website (Jan 2008)

- **Misleading domain name** (unusual at present)
  - http://www.banckname.com/
  - http://www.bankname.xtrasecuresite.com/

- **Insecure end user or machine** (76% of sites)
  - http://www.example.com/~user/www.bankname.com/
  - http://www.example.com/bankname/login/

- **Free web hosting** (17% of sites)

- **Specialist attackers**
  - distinctive patterns, often rely on wildcard DNS
  - figures only meaningful after canonicalisation
  - rock-phish 4%, fast-flux 1.4%, “ark” 1.4%
Rock-phish & fast-flux mechanisms!

- Rock-phish (originally used /rock then /r1)
  - compromised machines run a proxy
  - domains do not infringe trademarks
  - name servers usually done in similar style
  - distinctive URL style
    
    http://session9999.bankname.com.lof80.info/signon/

- “fast-flux” appeared in Feb’07, exclusive since July 08
  - also uses proxy machines that relay “mothership” traffic
  - hostname resolves to 5 (or 10...) IP addresses at once
  - BUT in 20 minutes time, resolves to a different set of machines
  - name server operates in the same way

- Tackling these sites means suspending the domain name, because cannot tackle the proxies fast enough
## Take-down time measurements (Jan 2008)

<table>
<thead>
<tr>
<th>Category</th>
<th>Total</th>
<th>Mean (hours)</th>
<th>Median (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free webhosting</td>
<td>395</td>
<td>48</td>
<td>0</td>
</tr>
<tr>
<td>when brand owner aware</td>
<td>240</td>
<td>4.3</td>
<td>0</td>
</tr>
<tr>
<td>when brand owner unaware</td>
<td>155</td>
<td>115</td>
<td>29</td>
</tr>
<tr>
<td>Compromised machines</td>
<td>193</td>
<td>49</td>
<td>0</td>
</tr>
<tr>
<td>when brand owner aware</td>
<td>105</td>
<td>3.5</td>
<td>0</td>
</tr>
<tr>
<td>when brand owner unaware</td>
<td>155</td>
<td>104</td>
<td>10</td>
</tr>
<tr>
<td>Rock-phish domains</td>
<td>821</td>
<td>70</td>
<td>33</td>
</tr>
<tr>
<td>Fast-flux domains</td>
<td>314</td>
<td>96</td>
<td>25</td>
</tr>
</tbody>
</table>
Why are brand owners “unaware”

• Most brand-owners outsource take-down to specialist “brand protection” companies

• These companies compete not only on removal times, but also on how many websites they know of (“the quality of their feed”)

• They get data from “industry” lists (APWG etc) and also from their own spam-traps (old domains, honeypots etc)

• So if Bank X hires company A, but only company B knows about the phishing site then it isn’t removed

• However, as neutral academics we get data from both A and B, we know of the site and measure its (rather slow) removal

• We recommend industry-wide data sharing; the companies buying services from the competition as well!
Free web-hosting take-down data (Spring 2007)

<table>
<thead>
<tr>
<th>Site lifetime (in hours)</th>
<th># sites</th>
<th>mean</th>
<th>median</th>
</tr>
</thead>
<tbody>
<tr>
<td>yahoo.com</td>
<td>174</td>
<td>23.8</td>
<td>6.9</td>
</tr>
<tr>
<td>doramail</td>
<td>155</td>
<td>32.8</td>
<td>18.1</td>
</tr>
<tr>
<td>pochta.ru</td>
<td>1253</td>
<td>33.8</td>
<td>16.8</td>
</tr>
<tr>
<td>alice.it</td>
<td>159</td>
<td>52.4</td>
<td>18.8</td>
</tr>
<tr>
<td>by.ru</td>
<td>254</td>
<td>53.1</td>
<td>38.2</td>
</tr>
</tbody>
</table>

BUT interpret this data carefully: almost all sites (except on Yahoo!) were eBay (65 hour average; this is 1/3 of their total)

ALSO these figures do not account for “awareness”
The gaining of “clue”
Registrars can also have a “clue” issue.
How many visitors?

• Some (non rock-phish) sites had world-readable “webalizer” statistics pages which we checked for phishing page visits
  ▪ could determine number who filled in the forms each day
  ▪ 22 on day first reported, 24 next day (then less, but NOT zero)

• Some sites had world readable files of compromised credentials
  ▪ about 50% were “die spammer die” responses

• Hence able to do a sum (Spring 2007 figures)
  ▪ 56 days, 1448 banking websites (exclude eBay)
  ▪ Average lifetime was 57 hours, hence 33 real victims per site
  ▪ Gartner loss estimate of $572/victim (from a $2 billion total)
  ▪ Hence $178 million per year
  ▪ These sites are 1/3 the spam... so $500 million
  ▪ NB: complete hand-waving !!!
  ▪ BUT: is 0.34% of US users; cf Florêncio/Herley 0.40%
Non-$hared info al$o repre$ent$ ri$k

- Longer lifetimes => more visitors (Webalizer logs)
- Hence we can assess impact of longer lifetimes:

<table>
<thead>
<tr>
<th>Exposure figures (6 month totals)</th>
<th>A’s banks</th>
<th>B’s banks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>K hour</td>
<td>$ million</td>
</tr>
<tr>
<td>Actual values</td>
<td>1005</td>
<td>$276</td>
</tr>
<tr>
<td>Expected if sharing</td>
<td>418</td>
<td>$113</td>
</tr>
<tr>
<td>Effect of no sharing</td>
<td>587</td>
<td>$163</td>
</tr>
</tbody>
</table>

- Don’t use this table to select a take-down company!
  - A’s clients are mainly large banks where lots of phishing sites exist; however, B’s clients are smaller and have very few attacks.
How are insecure machines found?

- Traditionally machines found by “scanning” hence interest in Intrusion Detection Systems, “slow scan” software etc etc
- But the Webalizer also parses referrer strings to determine the search terms used to locate the sites...
- Hand categorisation of terms, but most were obvious
  - many searches for MP3s in the logs ! these were ignored
- Types of searches:
  - Vulnerability
    - phpizabi v0.848b c1 hfp1 (CVE-2008-0805)
  - Compromise
    - allintitle:welcome paypal
  - Shell
    - c99shell drwxrwx
Webalizer logs (June 07 – March 08)

- 2486 domains with world-readable logs
  - 1320 (53%) had one or more “evil” search terms (they are sometimes called “googledorks”)
- 25 cases where we had sufficient data to prove that searches were linked to the compromise

<table>
<thead>
<tr>
<th>Search Type</th>
<th>Domains</th>
<th>Phrases</th>
<th>Visits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any evil search</td>
<td>204</td>
<td>456</td>
<td>1207</td>
</tr>
<tr>
<td>Vulnerability search</td>
<td>126</td>
<td>206</td>
<td>582</td>
</tr>
<tr>
<td>Compromise search</td>
<td>56</td>
<td>99</td>
<td>265</td>
</tr>
<tr>
<td>Shell search</td>
<td>47</td>
<td>151</td>
<td>360</td>
</tr>
</tbody>
</table>
Recompromise

- Consider phishing pages on same site more than a week apart (likely a different attacker)
- 9% of all sites recompromised within 4 weeks, rising to 19% within 24 weeks
- For Webalizer sites this is 15% rising to 33%
- If evil search terms present then this becomes 19% rising to 48% (14% to 29% if no terms)
- This doubling is statistically significant!
- The “take-home” from this is:
  - independent attackers are using “search” and finding the same sites
  - websites are being cleaned, but the underlying problem isn’t fixed
Must consider email spam data (Sep 08)

- Email drives visitors to phishing websites
  - assuming equally convincing, this means that losses to customers will correlate closely with spam volumes

- Considered all new sites 24–30 Sep 2008
  - 4084 websites (compromised & free hosting), 120 fast-flux domains

- Matched (generic) URL to an email dataset from IronPort

- Limited spam coverage (surprisingly!?!)
  - 430 sites (11%), 103 fast-flux domains (86%)

- “Fast flux” websites had spam campaigns that corresponded very closely in length to website lifetime

- Other websites sometimes advertised weeks beforehand, and for several days after removal (!)
What’s doing the most harm?

- Rapid removal of website will of course mitigate impact
- Total lifetimes split 2:1 between “other” and “fast flux”
- Total spam split 1:2 between “other” and “fast flux”
- Number of websites (and amount of spam) affects public perceptions, possibly eroding trust in eCommerce generally
- But sheer volume of spam may better correlate to total losses

<table>
<thead>
<tr>
<th></th>
<th>Websites</th>
<th>Lifetime (hrs)</th>
<th>Spam volume</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>%</td>
<td>Total</td>
</tr>
<tr>
<td>Ordinary</td>
<td>4084</td>
<td>97%</td>
<td>20603</td>
</tr>
<tr>
<td>Fast-flux</td>
<td>120</td>
<td>3%</td>
<td>9674</td>
</tr>
</tbody>
</table>
PhishTank – a community approach

- “PhishTank” is a community site verifying phish reports
  - summer 2007: average verification = 46 hrs (15 hrs median)
  - cf brand protection company “8 seconds”

- Errors:
  - submissions: 44% single submitters, but 1.2% from most active
  - voting: 39 false +ve, 3 false −ve

- Inaccuracy of voting (count disagreements):
  - fewer than 100 votes: 14% of time
  - most active voters: 3.7% of time
  - “high-conflict” users make the same mistakes

- Hard to defend against wicked participation
  - power-law distribution of submissions, and voting participation
  - easy to get an accurate reputation (97% phish)
“Wisdom of crowds” & security

- Distribution of user participation matters
  - power laws put power into the hands of the few
  - however, you do want keen people...

- Decisions must be difficult to guess
  - you want people participating not robots

- Do not make users work harder than needed
  - canonicalise the data
Comparing take-down times

- Defamation – believed to be quick (days)
- Copyright violation – also prompt(ish)
  - experimentally “days”
  - albeit with prompting, suggesting perseverance matters
- Fake escrow agents
  - average 9 days, median 1 day
  - note that AA419 aware of around 25% of sites
- Mule recruitment sites (Sydney Car Center etc)
  - average 13 days, median 8 days
  - doesn’t attack any particular bank, so they ignore the issue
  - slower than escrow sites (vigilantes more motivated?)
- Fake pharmacies
  - no vigilante groups – so lifetime is ~2 months
Child sexual abuse images (CAI)

- Provided with anonymised data by IWF
  - Jan–Dec 2007 there were 2585 different domains
  - ignoring 8 (free-web?) domains with >100 reports
- Computed initial take-down time (ignored recompromise)
  - mean 21 days, median 11 days
- If include sites with no removal at all
  - mean 30 days (and growing), median 12 days
- Fast in UK: IWF checks with police and then contacts the ISP
  - but “not authorised” to act internationally
  - passes data via UK police to foreign forces
  - also pass to another INHOPE member
- Confusion of aims (removal/catch criminals)
At present...

- The phishing site take-down industry is putting significant funds at risk by not co-operating with each other.
- The police are chasing the right gang!
- Search engines are widely used to find websites to compromise (and re-compromise).
- Takedown times quite clearly affected by “incentives”
- Slowness of removal of CAI is a scandal.
- We still don’t know “how many phishers are there?”
- We still don’t know “is this their day job?”
- We still don’t know “what’s the best way to disrupt phishing?”
- We still need better data to improve our understanding!
What we now (Summer 2009) know about phishing websites

BLOG: http://www.lightbluetouchpaper.org/

http://www.cl.cam.ac.uk/~rnc1/
http://people.seas.harvard.edu/~tmoore/

PAPERS: http://www.cl.cam.ac.uk/~rnc1/publications.html