APWG Global Phishing Survey
2H2010

Rod Rasmussen

Greg Aaron

June 21, 2011
Goals

Study domain names and URLs to:
• Provide a consistent benchmark for scope of phishing problems worldwide
• Understand what phishers are doing
• Identify new trends
• Find hot-spots and success stories
• Suggest anti-abuse measures
Data Set

- Comprehensive sources: APWG, phishing feeds, private sources, honeypots
- Millions of phishing URLs → small number of domain names and attacks.
- Total of 205,715,855 domain names in the TLDs we have stats for ~ 99.5% of domain names in the world.
## Basic Statistics

<table>
<thead>
<tr>
<th></th>
<th>2H2010</th>
<th>1H2010</th>
<th>2H2009</th>
<th>1H2009</th>
<th>2H2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing domain names</td>
<td>42,624</td>
<td>28,646</td>
<td>28,775</td>
<td>30,131</td>
<td>30,454</td>
</tr>
<tr>
<td>Attacks</td>
<td>67,677</td>
<td>48,244</td>
<td>126,697</td>
<td>55,698</td>
<td>56,959</td>
</tr>
<tr>
<td>TLDs used</td>
<td>183</td>
<td>177</td>
<td>173</td>
<td>171</td>
<td>170</td>
</tr>
<tr>
<td>IP-based phish (unique IPs)</td>
<td>2,318</td>
<td>2,018</td>
<td>2,031</td>
<td>3,563</td>
<td>2,809</td>
</tr>
<tr>
<td>Maliciously registered domains</td>
<td>11,769</td>
<td>4,755</td>
<td>6,372</td>
<td>4,382</td>
<td>5,591</td>
</tr>
<tr>
<td>IDN domains</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>13</td>
<td>10</td>
</tr>
</tbody>
</table>
Phishing in China

• Data contribution from CNNIC and APAC (Anti-Phishing Alliance of China)

• Observers outside of China were detecting only about 20% of the phishing that targeted Chinese institutions.

• Attacks on Chinese banks, e-commerce sites.
  – Lures: Chinese-language e-mails, Chinese instant message services
  – WHOIS: registrants often listed in China, and list Chinese freemail services such as QQ.com
Phishing in China

• 2H2010: 12,282 attacks on Chinese institutions, using 6,382 unique domain names. (That’s 18% of all attacks worldwide)
• 74% of those attacks targeted Taobao.com
• Few .CN names used. CN registration policy became very restrictive in December 2009. Only 278 .CN names used in 2H2010, some hacked.
• Phishers simply switched to using other resources to phish Chinese targets:
  – Used 4,737 free CO.CC subdomains
  – Used large numbers of .COM, .TK, .INFO, .US, .IN domains
• Chinese phishers prefer to register domain names – only 8% looked hacked.
Phishing Site Uptime 2H2010: 73 hours average, 15:19 hours median
Why So High?

- Absence of Avalanche domains
- There were 4,963 phishing attacks using free CO.CC subdomains. Their median uptime was almost 60 hours – compared with 15:19 hours for all phish.
- Don’t know the uptimes for the phish uniquely recorded by CNNIC/APAC
ccTLD Uptimes
(HH:MM:SS)

ccTLDs Average Phishing Uptimes 2H2010 (HH:MM:SS)

Jul Aug Sep Oct Nov Dec

ALL TLDs

.CC
.TK
.BR
.UK
.RU
.FR

Singapure 41
19-24 June 2011
gTLD Uptimes
(HH:MM:SS)

gTLDs Average Phishing Uptimes 2H2010 (HH:MM:SS)

- .COM
- .NET
- .ORG
- .INFO
- .BIZ
- ALL TLDs

<table>
<thead>
<tr>
<th></th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
</tr>
</thead>
<tbody>
<tr>
<td>0:00:00</td>
<td>24:00:00</td>
<td>48:00:00</td>
<td>72:00:00</td>
<td>96:00:00</td>
<td>120:00:00</td>
<td>144:00:00</td>
</tr>
</tbody>
</table>
Phishing Rates by TLD: roughly proportional by TLD size

All Phishing Attacks, by TLD 2H2010

- .com: 41.4%
- Other (174): 20.9%
- .cc: 7.3%
- .net: 7.2%
- .ru: 1.6%
- .fr: 1.4%
- .org: 4.0%
- IP Based: 4.5%
- .tk: 3.7%
- .br: 2.9%
- .info: 2.8%
- .uk: 2.5%
- .info: 2.8%
Phishing by TLD: Score

• Metric: “Phishing Domains per 10,000”
  – Measures prevalence of phishing in a TLD
  – Median score: 3.2
  – .COM score: 2.1
  – Scores between 2.1 and 3.2 are “normal”
  – Scores skew higher for smaller TLDs.

• Metric: “Attacks per 10,000 Domains”
# Top TLDs by Domain Score (minimum 30,000 domains and 25 phish)

<table>
<thead>
<tr>
<th>RANK</th>
<th>TLD</th>
<th>TLD Location</th>
<th># Unique Phishing attacks 2H2010</th>
<th>Unique Domain Names used for phishing 2H2010</th>
<th>Domains in registry Oct 2010</th>
<th>Score: Phish per 10,000 domains 2H2010</th>
<th>Score: Attacks per 10,000 domains 2H2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.TH</td>
<td>Thailand</td>
<td>125</td>
<td>65</td>
<td>51,438</td>
<td>12.6</td>
<td>24.3</td>
</tr>
<tr>
<td>2</td>
<td>.IR</td>
<td>Iran</td>
<td>295</td>
<td>169</td>
<td>175,600</td>
<td>9.6</td>
<td>17.0</td>
</tr>
<tr>
<td>3</td>
<td>.MA</td>
<td>Morocco</td>
<td>73</td>
<td>34</td>
<td>36,669</td>
<td>9.3</td>
<td>20.2</td>
</tr>
<tr>
<td>4</td>
<td>.IE</td>
<td>Ireland</td>
<td>112</td>
<td>96</td>
<td>151,023</td>
<td>6.4</td>
<td>7.7</td>
</tr>
<tr>
<td>5</td>
<td>.TK</td>
<td>Tokelau</td>
<td>2,533</td>
<td>2,429</td>
<td>4,030,709</td>
<td>6.0</td>
<td>6.3</td>
</tr>
<tr>
<td>6 (tie)</td>
<td>.KZ</td>
<td>Kazakhstan</td>
<td>49</td>
<td>28</td>
<td>50,534</td>
<td>5.5</td>
<td>9.7</td>
</tr>
<tr>
<td>6 (tie)</td>
<td>.CC</td>
<td>Cocos (Keeling) Islands</td>
<td>4,963</td>
<td>55</td>
<td>100,000 (estimated)</td>
<td>5.5</td>
<td>496.3</td>
</tr>
<tr>
<td>8</td>
<td>.IN</td>
<td>India</td>
<td>523</td>
<td>421</td>
<td>791,165</td>
<td>5.3</td>
<td>6.6</td>
</tr>
<tr>
<td>9</td>
<td>.MY</td>
<td>Malaysia</td>
<td>68</td>
<td>55</td>
<td>108,211</td>
<td>5.1</td>
<td>6.5</td>
</tr>
<tr>
<td>10</td>
<td>.HU</td>
<td>Hungary</td>
<td>365</td>
<td>255</td>
<td>542,000</td>
<td>4.7</td>
<td>6.7</td>
</tr>
</tbody>
</table>
Malicious Domain Registrations

Of the 42,624 phishing domains:

• ~72% were compromised/hacked
• ~28% were registered by phishers (11,769). Most of those domains (6,382) were registered to attack Chinese targets.
• 9% of domains (1,503) contained a relevant brand name or brand misspelling. (Especially Taobao.com)
2,066 maliciously registered domains targeted WarCraft and Battle.net
Use of Subdomain Services

• `<customer_name>..<provider>..TLD`

• Use of these services by phishers almost doubled in 2H2010, to 11,768 subdomains.

• *If we counted these unique subdomains as “regular” domain names, they would represent 22% of all domains used for phishing.*

• 40% of phishing subdomains were on CO.CC
Subdomain Service Phish

Select Subdomain Reseller Phish, 2H2010

- co.cc
- t35.com
- 110mb.com
- altervista.org
- yourfreehosting.net
- hdfree.com.br
- tripod.com
Virtual Hosts

Virtual Host Phish
1H2009 - 2H2010
Internationalized Domain Names (IDNs)

- In last three years, we have only found two homographic attacks.
- July 12, 2010:
- 36 new IDN TLDs have been approved
  - Russian Federation: .РФ (.RF in Cyrillic, .xn--p1ai)
Conclusions

• Clamp down in one place and the problems simply move elsewhere.
• Free services like CO.CC and .TK are being abused heavily by phishers.
• Subdomain services are as big a problem as the registration of regular domain names.
• Uptimes got higher – watch out!
APWG Global Phishing Survey 2H2010
Thank You!

For more information or data for your TLD:

Rod Rasmussen rod.rasmussen <at> internetidentity.co

Greg Aaron gaaron <at> afilias.info