Anti-Phishing Working Group

www.antiphishing.org

Internet Policy Committee Initiative Update

Dave Piscitello, Sr. Security Technologist, ICANN
Policy Legate for the APWG
APWG Internet Policy Committee (IPC)

- 50+ members
- Participants include
  - registries, registrars, ISPs
  - CERTs, Law Enforcement
  - solution providers, researchers, financial institutions, etc.
- Ensure that anti-phishing concerns are represented during the creation or modification of Internet policies
Initiatives

- Accelerated Domain Suspension by Registries
- Registrar Best Practices
- Phishing Site “Landing” page to educate victims
- Large-scale data study for 2007 phishing
Accelerated Suspension Plan

• Reduce site uptime of domains provably linked to phishing
• Define standard processes to suspend a phish domains
  – Assure small incidence of “false positives”
  – Hacked domains and shared hosting environments are not eligible for suspension
  – Appeal process and penalties for mistakes
• Establish APWG accredited entities
  – Trusted parties accredited by an agency chosen by a registry
  – Entities contact registry operators directly when registrar or registrant does not take action
• .ASIA and APWG formulating deployment plan
Accelerated Suspension Plan

APWG accredited takedown entity identifies a .asia phish domain

Takedown entity contacts registrant, registrar, registry and ISP to notify them of phish site

2 hours elapses and no response from registrant or registrar

Registry suspends phish domain and notifies registrant of appeal procedures

Takedown entity contacts registry about suspending phish site

Committed to wiping out Internet scams and fraud
Phishing Site Landing Page

- Use deleted phish URLs as an educational opportunity
  - Redirect people who fall for phishing lures to a page that teaches them how to avoid being phished
- Logistics
  - Hosted by APWG partner with hardened infrastructure
  - Available for use and “branding” by targeted FI’s
  - Text and graphical versions
  - Translated to multiple languages

http://education.apwg.org/
Registrar Best Practices

• Provide **recommendations** to registrars so they can play a stronger role in combating phishing
  – How to process and preserve evidence
  – How to offer effective registrant education
  – Phishing domain takedown assistance
  – Promote resources to help identify malicious activities
• Best practices have evolved into a broad initiative
  – Draft in review by registrars
  – gTLD and ccTLD operators forming group with registry focus
• Early success stories (HKDNR)
  – Implemented far better fraud-checking up-front
  – Improved policy surrounding domain suspension
  – Empowered support staff to handle domain suspension
Global Phishing Survey 2007

• Studies domain names and URLs to:
  – Measure scope of phishing problem world-wide
  – Understand what phishers are doing and why
  – Suggest anti-abuse measures

• Sources of data used in study
  – APWG, phishing feeds, private sources, honeypots
  – Millions of phishing URLs
  – 51,989 unique domain names plus 11,553 unique IP addresses
Compromised Domain or Malicious Registration?

• Compromised domain
  – Innocent (legitimate) site hacked by a phisher
  – Popular with phishers because they are hard to take down ("free" hosting, typically not blacklisted, …)

• Malicious registration
  – Domain name was registered by a phisher
  – At least 20% of domains were maliciously registered
  – May be much higher
Trends in URL Construction

• Of the 10,773 maliciously registered domains:
  – 10,515 had the phish placed in subdomains or subdirectories
  – Only 258 had phish on “base” domain or home page
  – % of phishing URLs containing brand names increased in 2007
  – Phishers avoiding brand names in domain names
    • Brands in subdomains allows multiple phish per domain name

• Conclusions
  – Phishers don’t care much what domain name they use. Any domain name (and any TLD) will do
  – To detect phish, study spam to identify phishing URLs and untrustworthy name servers.
Subdomain Services

- Phishers using subdomains of social networks or subdomain registries
  - `<customer_term>..<service_provider_sld>.TLD`
  - 11,443 subdomain sites/accounts on 448 unique second-level domains
  - Would represent 18% of all phishing domains if included in survey

- VERY difficult to take down
  - Most are free services
  - Mostly offered by small companies
  - No WHOIS
  - Spotty abuse resolution processing
Phishing by Top-Level Domain (TLD)

- 51,989 phishing domains
- 182 top-level domains (of 273) were phished
- Only 12 internationalized domain names (IDNs) used for phishing
- 150,689,751 total domain names in the 105 TLDs
Phishing by TLD: Scoring System

• New metric defined for this study
  – Phishing domains per 10,000
• Median score was 4.7
• .COM score 3.4
• Scores skew higher for smaller TLDs
# Phishing by TLD: Top 10
(minimum 30,000 domains and 30 phishing incidents)

<table>
<thead>
<tr>
<th>TLD</th>
<th>TLD Location</th>
<th>Domains in registry in November 2007</th>
<th>Domain names used for phishing in 2007</th>
<th>Score: Phishing domains per 10,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>hk</strong> Hong Kong</td>
<td>150,799</td>
<td>1,707</td>
<td>113.2</td>
</tr>
<tr>
<td>2</td>
<td><strong>th</strong> Thailand</td>
<td>33,000</td>
<td>171</td>
<td>51.8</td>
</tr>
<tr>
<td>3</td>
<td><strong>li</strong> Liechtenstein</td>
<td>50,100</td>
<td>221</td>
<td>44.1</td>
</tr>
<tr>
<td>4</td>
<td><strong>ro</strong> Romania</td>
<td>242,484</td>
<td>316</td>
<td>13.0</td>
</tr>
<tr>
<td>5</td>
<td><strong>cl</strong> Chile</td>
<td>195,513</td>
<td>222</td>
<td>11.4</td>
</tr>
<tr>
<td>6</td>
<td><strong>bz</strong> Belize</td>
<td>42,360</td>
<td>48</td>
<td>11.3</td>
</tr>
<tr>
<td>7</td>
<td><strong>tw</strong> Taiwan</td>
<td>341,462</td>
<td>361</td>
<td>10.6</td>
</tr>
<tr>
<td>8</td>
<td><strong>lt</strong> Lithuania</td>
<td>64,554</td>
<td>65</td>
<td>10.1</td>
</tr>
<tr>
<td>9</td>
<td><strong>ee</strong> Estonia</td>
<td>50,000</td>
<td>47</td>
<td>9.4</td>
</tr>
<tr>
<td>10</td>
<td><strong>cz</strong> Czech Repub.</td>
<td>347,989</td>
<td>286</td>
<td>8.2</td>
</tr>
</tbody>
</table>
# Phishing by TLD: gTLDs

(Median Score for all TLDs = 4.7)

<table>
<thead>
<tr>
<th>TLD</th>
<th>Domains in registry November 2007</th>
<th>Domain names used for phishing</th>
<th>Score: Phishing domains per 10,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>.ORG</td>
<td>6,412,064</td>
<td>2,627</td>
<td>4.1</td>
</tr>
<tr>
<td>.BIZ</td>
<td>1,944,453</td>
<td>764</td>
<td>3.9</td>
</tr>
<tr>
<td>.NET</td>
<td>10,581,849</td>
<td>3,973</td>
<td>3.8</td>
</tr>
<tr>
<td>.COM</td>
<td>70,698,420</td>
<td>23,860</td>
<td>3.4</td>
</tr>
<tr>
<td>.INFO</td>
<td>4,954,266</td>
<td>1,295</td>
<td>2.6</td>
</tr>
</tbody>
</table>
## Low-Scoring Large TLDs

<table>
<thead>
<tr>
<th>TLD</th>
<th>TLD Location</th>
<th>Domains in registry in November 2007</th>
<th>Domain names used for phishing in 2007</th>
<th>Score: Phishing domains per 10,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>China</td>
<td>8,459,174</td>
<td>1,853</td>
<td>2.2</td>
</tr>
<tr>
<td>ws</td>
<td>Samoa</td>
<td>522,221</td>
<td>114</td>
<td>2.2</td>
</tr>
<tr>
<td>name</td>
<td>sponsored TLD</td>
<td>265,638</td>
<td>55</td>
<td>2.1</td>
</tr>
<tr>
<td>se</td>
<td>Sweden</td>
<td>685,000</td>
<td>127</td>
<td>1.9</td>
</tr>
<tr>
<td>ar</td>
<td>Argentina</td>
<td>1,451,727</td>
<td>230</td>
<td>1.6</td>
</tr>
<tr>
<td>de</td>
<td>Germany</td>
<td>11,524,091</td>
<td>1,798</td>
<td>1.6</td>
</tr>
<tr>
<td>uk</td>
<td>United Kingdom</td>
<td>6,445,465</td>
<td>992</td>
<td>1.5</td>
</tr>
<tr>
<td>eu</td>
<td>European Union</td>
<td>2,671,846</td>
<td>197</td>
<td>0.7</td>
</tr>
<tr>
<td>mobi</td>
<td>sponsored TLD</td>
<td>761,549</td>
<td>48</td>
<td>0.6</td>
</tr>
</tbody>
</table>
What Affects a TLD’s Score?

- These factors make a difference
  - Registration requirements (citizenship, documentation)
  - Domain usage rates
  - Malicious registrations
  - Anti-abuse policies and procedures

- These factors do not
  - Registrant
  - Price
  - Registrar network
## Malicious Registrations

**Make a Difference**

<table>
<thead>
<tr>
<th>TLD</th>
<th>TLD Location</th>
<th>Domains in registry in November 2007</th>
<th>Domain names used for phishing in 2007</th>
<th>Score: Phishing domains per 10,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>ly</td>
<td>Libya</td>
<td>3,100</td>
<td>84</td>
<td>271.0</td>
</tr>
<tr>
<td>mn</td>
<td>Mongolia</td>
<td>5,087</td>
<td>93</td>
<td>182.8</td>
</tr>
<tr>
<td>hk</td>
<td>Hong Kong</td>
<td>150,799</td>
<td>1,707</td>
<td>113.2</td>
</tr>
<tr>
<td>edu</td>
<td>U.S. education</td>
<td>6,997</td>
<td>67</td>
<td>95.8</td>
</tr>
<tr>
<td>th</td>
<td>Thailand</td>
<td>33,000</td>
<td>171</td>
<td>51.8</td>
</tr>
<tr>
<td>li</td>
<td>Liechtenstein</td>
<td>50,100</td>
<td>221</td>
<td>44.1</td>
</tr>
</tbody>
</table>
Conclusions

- Phishers are always experimenting
  - Are avoiding brand filters
  - Are systematically exploiting vulnerable registrars and registries over time
  - Are using subdomain services more often
- Phishers are TLD-agnostic
- Registries and registrars should concentrate on curbing malicious domain name registrations