Misuse of Domain Privacy Protection Services by Spammers: Act II

ICANN: Dave Piscitello, Steve Sheng
CMU: Ryan Su, Nicolas Christin
Presented at APWG eCrime Researchers Summit 2010

Domain Name Privacy Conundrum

- **Privacy** is the ability to control what one reveals about oneself over the Internet and who can access that personal information
- **Privacy controls** for domain name registrations vary across registries and registrars
- Criminals exploit privacy controls to evade detection
Relevant prior studies

• Prevalence of private registrations among malicious domains hosted at 3FN (Oct 2009)
  – 38% of malicious domains hosted at 3FN used privacy protection services

• Misuse of Domain Name Privacy Protection Services (Act I, Apr 2010)
  – 31% of domains randomly selected from SpamHaus DBL used privacy protection services

• NORC WHOIS data accuracy study (Sep 2010)
  – 18% of domains randomly selected from general population used privacy protection services

Current activities

• Iterate prior study of spam domains
  – Look for patterns of behavior over time, e.g., flocking or migratory behaviors
  – See where the data lead us

• Improve automation, study larger samples
  – ICANN: collect random sample of alleged spam domains in gTLDs from SpamHaus DBL, retrieve Whois records as we sample
  – CMU: Develop parsers to overcome variation among WHOIS data stores
Study Results, Comparisons

- In both samples, spam domains have higher percentage of privacy protection services than general population domains.
- Percentage did not change significantly from one study of alleged spam samples to next.

<table>
<thead>
<tr>
<th>Description</th>
<th>May 2010</th>
<th>Sep 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total general population of domains used in NORC study</td>
<td>1419</td>
<td></td>
</tr>
<tr>
<td>Percent of domains NORC identified as using privacy protection service</td>
<td>25%</td>
<td></td>
</tr>
<tr>
<td>Total number of alleged SPAM domains in our MAY 2010 sample</td>
<td>1286</td>
<td></td>
</tr>
<tr>
<td>Percent of spam domains that used privacy protection services</td>
<td>31%</td>
<td></td>
</tr>
<tr>
<td>Total number of alleged SPAM domains in our SEP 2010 sample</td>
<td>57998</td>
<td></td>
</tr>
<tr>
<td>Percent of spam domains that used privacy protection services</td>
<td>31%</td>
<td></td>
</tr>
</tbody>
</table>

- Domains in May 2010 DBL sample that used privacy protection services

<table>
<thead>
<tr>
<th>Service</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>WhoisGuard Protected</td>
<td>38%</td>
</tr>
<tr>
<td>Domains by Proxy, Inc.</td>
<td>24%</td>
</tr>
<tr>
<td>Protected Domain Services</td>
<td>13%</td>
</tr>
<tr>
<td>Moniker Privacy Services</td>
<td>9%</td>
</tr>
<tr>
<td>Dynamic Dolphin Privacy Protect</td>
<td>7%</td>
</tr>
<tr>
<td>Whois Privacy Protection Service, Inc.</td>
<td>3%</td>
</tr>
<tr>
<td>Domain Manager</td>
<td>3%</td>
</tr>
<tr>
<td>Contactprivacy.com</td>
<td>2%</td>
</tr>
<tr>
<td>PrivacyProtect.org</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>
Domains in Sep 2010 DBL sample that used privacy protection services

- WhoisGuard Protected: 52%
- Domains by Proxy: 33%
- PrivacyGG Limited: 2%
- Netowl: 5%
- Others: 1%

Compare to market share:

<table>
<thead>
<tr>
<th>Privacy service</th>
<th>Market Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains by Proxy</td>
<td>34%</td>
</tr>
<tr>
<td>WHOIS Privacy Protection</td>
<td>9%</td>
</tr>
<tr>
<td>WhoisGuard</td>
<td>9%</td>
</tr>
<tr>
<td>Moniker Privacy Protection</td>
<td>7%</td>
</tr>
<tr>
<td>Global Internet Private Registration</td>
<td>5%</td>
</tr>
<tr>
<td>1&amp;1 Private Registration</td>
<td>5%</td>
</tr>
<tr>
<td>Domain Privacy</td>
<td>5%</td>
</tr>
</tbody>
</table>

Source: anonwhois.org

Do targets shift over time?

Some targets are statistically significant, need more samples.
Automation offers new insights

- Our samplings are larger and span longer time periods
- We observe more from these than single {day, week, event} snapshots, i.e.,
  - When spikes in registrations occur
  - Who is targeted and when
  - Intervals between alleged SPAM campaigns
  - Frequency of alleged SPAM campaigns
Spikes

Samples SpamHaus DBL domains, by registrar

What causes spikes?

• Dates correspond to SpamHaus reporting all domains of a given spammer, or a SPAM campaign
• What made these dates attractive?
  – Will work with registrars and registries to see if there is any correlation to registrar promotions, discounts, bundling
• Worth pursuing?
  – If a correlation is found, can it be used to anticipate or detect early onset of spam attack?
Conclusions, future work

- Studies indicate that a higher percentage of spam domains use privacy protection registration services than the general population
- Continued sampling of DBL may provide additional insights, trends
  - Will increased frequency of samples tell us more?
  - Can we learn more from spikes if we correlate registrar promotions, discounts, or bundling? Do spammers see these as opportunities?
  - Can we apply what we learn to deter spam registrations?

Thank you

- Contact information
  - Dave Piscitello
dave.piscitello@icann.org
  - Steve Sheng
steve.sheng@icann.org
  - Nicolas Christin
nicolasc@andrew.cmu.edu
  - Ryan Su
  - yulos@andrew.cmu.edu
Related studies

- Private Domain Registrations at 3FN (APWG ceCOS, Oct 2009)
- Domain Name Privacy Misuse Studies (APWG ceCos, Apr 2010)
- Privacy Proxy Registration Services Study Report (NORC, Sep 2010)