Update on Whois Studies
Current Status

• Final GNSO-commissioned Whois studies now completed, awaiting public comment

• Whois Privacy & Proxy Abuse Study
  – Performed by National Physical Laboratory, UK
  – Public comment period closed 13 November 2013

• Whois Misuse Study
  – Performed by Carnegie Mellon University, USA
  – Public Comment after Buenos Aires
NPL’s Whois Privacy & Proxy Abuse Study: Summary of Findings & Public Comments

• Study tested two hypotheses

#1: “A significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via Privacy or Proxy services to obscure the perpetrator's identity.”

➤ Finding: TRUE

#2: “The percentage of domain names used to conduct illegal or harmful Internet activities that are registered via Privacy or Proxy services to obscure identity is significantly greater than the equivalent percentage of domain names used for entirely lawful Internet activities.”

➤ Finding: ONLY PARTLY TRUE
NPL’s Whois Privacy & Proxy Abuse Study: Additional assessments to enable comparison

- Accuracy of Whois phone numbers for domain names used to conduct illegal or harmful Internet activities. Finding: “Domains registered for illegal/harmful activity rely on multiple ways to hide contact details, but an above-average number of legitimate domains also do not provide accurate contact information (phone number)”

- Whois for domains used to conduct certain lawful/harmful activities, chosen to mirror bad actors

Note: This study was NOT designed to assess privacy/proxy use across ALL domains
NPL’s Whois Privacy & Proxy Abuse Study: Scope of Activities Studied

**Studied**
- Phishing
- Advanced Fee Fraud and other complex scams
- Unlicensed Pharmacies
- Typosquatting
- Child Sexual Abuse Image websites
- Domains appearing in Spam (SURBL)
- Domains associated with Malware (StopBadware)
- Domains subject to UDRP Process
- Lawful/Harmless websites chosen to mirror above

**Did Not Study**
- Spam beyond Phishing/Fake Pharma
- DoS or DNS Cache Poisoning
- Intellectual Property Theft beyond Typosquatting, Fake Pharma, Spam
- Media Piracy
- Identity Theft
- Harrassment or Stalking
- Different use rates by country
- Differences between privacy vs. proxy service (and vice versa)
### NPL’s Whois Privacy & Proxy Abuse Study: Summary of Findings

<table>
<thead>
<tr>
<th>Work package</th>
<th>Maliciously registered?</th>
<th>Usage of privacy or proxy services</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP6.4 Legal pharmacies</td>
<td>no</td>
<td>low</td>
</tr>
<tr>
<td>WP6.3 Law firms</td>
<td>no</td>
<td>low</td>
</tr>
<tr>
<td>WP1t Phishing: third parties</td>
<td>no</td>
<td>low</td>
</tr>
<tr>
<td>WP6.6 Typosquatted domains</td>
<td>no</td>
<td>average</td>
</tr>
<tr>
<td>WP8 StopBadware domains</td>
<td>some</td>
<td>average</td>
</tr>
<tr>
<td>WP6.2 Executive search consultants</td>
<td>no</td>
<td>average</td>
</tr>
<tr>
<td>WP1c Phishing: compromised sites</td>
<td>no</td>
<td>average</td>
</tr>
<tr>
<td>WP6.1 Banks</td>
<td>no</td>
<td>high</td>
</tr>
<tr>
<td>WP5 Child sexual abuse image websites</td>
<td>yes</td>
<td>high</td>
</tr>
<tr>
<td>WP1m Phishing: malicious registration</td>
<td>yes</td>
<td>very high</td>
</tr>
<tr>
<td>WP9 Domains subject to UDRP</td>
<td>some</td>
<td>very high</td>
</tr>
<tr>
<td>WP7 SURBL domains</td>
<td>mostly</td>
<td>very high</td>
</tr>
<tr>
<td>WP6.5 Adult websites</td>
<td>no</td>
<td>very high</td>
</tr>
<tr>
<td>WP2 Advanced Fee Fraud</td>
<td>yes</td>
<td>extremely high</td>
</tr>
<tr>
<td>WP4 Typosquatting</td>
<td>yes</td>
<td>extremely high</td>
</tr>
<tr>
<td>WP3 Unlicensed pharmacies</td>
<td>yes</td>
<td>extremely high</td>
</tr>
</tbody>
</table>
CMU’s Whois Misuse Study: An Update

- Analyzes the extent, nature, and impact of harmful actions taken by those who misuse Whois contact information by
  (1) surveying registrants, registries, registrars, experts and law enforcement;
  (2) conducting experiments to measure Whois contact misuse
- Hypothesis tested by CMU:
  Public access to Whois data leads to a measurable degree of misuse – that is, to actions that cause actual harm, are illegal or illegitimate, or otherwise contrary to the stated legitimate purpose.
CMU’s Whois Misuse Study: Preview of Findings

- Although survey responses rates were low
  - 29.8% of surveyed Registrants reported Whois email address misuse
  - 12.3% of surveyed Registrants reported Whois phone number misuse
  - 29.8% of surveyed Registrants reported Whois postal address misuse

- No other type of misuse was reported or measured at a statistically-significant level

- CMU’s draft report will contain further details regarding significance of gTLD, domain price, registrant type, anti-harvesting on Whois Misuse
Next Steps

- ICANN staff to summarize and analyze public comments to NPL’s study (end Nov.)
- CMU’s Misuse study to be published for public comment after Buenos Aires
- CMU team will present findings at webinar (early Dec.)
- GNSO to consider next steps concerning study findings and important issues not addressed by the studies
Further Information

- Whois Studies Overview & Status
  [http://gnso.icann.org/en/group-activities/other/whois/studies](http://gnso.icann.org/en/group-activities/other/whois/studies)

- Public Comment Forum for NPL Whois Privacy & Proxy Abuse Study

- Terms of Reference for CMU Misuse Study: