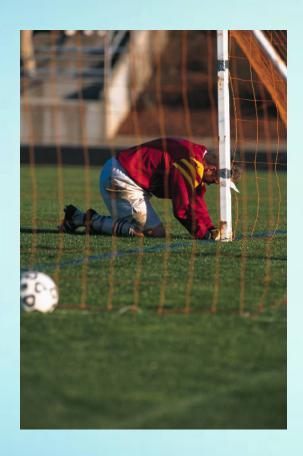
Update report on GNSOrequested WHOIS studies



Liz Gasster Senior Policy Counselor October 2010

Goals of WHOIS studies



- WHOIS policy has been debated for many years
- Many competing interests with valid viewpoints
- GNSO Council hopes that study data will provide objective, factual basis for future policy making
- Council identified several WHOIS study areas to test hypotheses that reflect key policy concerns
- Council asked staff to determine costs and feasibility of conducting those studies
- Staff used an RFP approach to do so



1. WHOIS Misuse

- Assess whether public WHOIS significantly increases harmful acts and impact of anti-harvesting measures
 - 1. Survey registrants, registrars, research and law enforcement orgs about past acts.
 - 2. Measure variety of acts aimed at WHOIS published vs. unpublished test addresses.

Status

- 3 RFP responses received and analyzed in March 2010
- Council decided to proceed with study in September 2010
- Contract establishment now underway



http://gnso.icann.org/issues/whois/ tor-whois-misuse-studies-25sep09-en.pdf

2. WHOIS Registrant Identification

- Determine how registrants identify themselves in WHOIS, and to what extent are domains registered by businesses or used for commercial purposes
 - 1. Are not clearly identified as such in WHOIS; and
 - 2. Related to use of Privacy & Proxy registration services
- Status
 - 5 RFP responses received and analyzed in March 2010
 - Pending GNSO council motion (if any) to proceed





3. WHOIS Privacy/Proxy Abuse

- Compare broad sample of Privacy & Proxy-registered domains associated with alleged harmful acts to assess
 - 1. How often "bad actors" try to obscure identity in WHOIS
 - 2. How this rate of abuse compares to overall P/P use
 - 3. How this rate compares to alternatives like falsified WHOIS data, compromised machines, and free web hosting

Status

- 3 RFP responses received and analyzed in September 2010
- Pending GNSO council motion (if any) to proceed



http://gnso.icann.org/issues/whois/
gnso-whois-pp-abuse-studies-report-05oct10-en.pdf

Staff analysis

- Estimated cost/duration -- \$150,000, < 1 year to complete
- Live-feed sampling tractable for many activities, including
 - Spam, phishing, malware, software piracy, counterfeit merchandise, money laundering, child pornography, and cyber/typo squatting
- Researchers found some activities irrelevant or too difficult
 - On-line stalking, DoS, DNS poisoning, media piracy, fee fraud
- Unlikely to reliably filter out "false positives"
- Despite limitations, results might be useful to:
 - Supply empirical data on how often alleged bad actors obscure their identity using methods including (but not limited to) P/P abuse
 - If P/P rate is high among bad actors, as compared to a control sample or alternative methods, policy changes may be warranted



4. WHOIS P/P Relay & Reveal

- Analyze communication relay and identity reveal requests sent for Privacy & Proxy-registered domains:
 - 1. To explore and document how they are processed, and
 - 2. To identify factors that may promote or impede timely communication and resolution.
- Status
 - RFP posted 29 September 2010
 - Responses due 30 November from interested bidders



http://www.icann.org/en/announcements/ announcement-29sep10-en.htm

Study Area/Topic	Proposal X-ref	Specific studies defined	Current status	Other Information
1. WHOIS Misuse Studies Extent to which publicly displayed WHOIS data is misused	Study # 1, #14, #21 GAC data set 2	1. Experimental: register test domains and measure harmful messages resulting from misuse 2. Descriptive: study misuse incidents reported by registrants, researchers/law enforcement	Council decided 8 Sept 2010 to proceed with this study. Cost: 150,000 Time estimate: 1 year	 Can count and categorize harmful acts attributed to misuse and show data was probably not obtained from other sources Some acts might be difficult to count Cannot tie WHOIS queries to harmful acts, which makes it difficult to prove that reductions in misuse were caused by specific anti-harvesting measures Difficult to assess whether misuse is "significant"
2. WHOIS Registrant Identification Study	GAC 5, GAC 6 #13a, #18 GAC 9, GAC 10	1. Gather info about how business/commercial domain registrants are identified 2. Correlate such identification with use of proxy/privacy services	5 RFP responses received. Staff analysis to Council on 23 March 2010. Cost: 150,000 Time estimate: 1 year	 Can classify ownership and purpose of what appear to be commercial domains without clear registrant information, and measure how many were registered using a P/P service Might provide insight on why some registrants are not clearly identified Use of P/P services by businesses
3. WHOIS Privacy and Proxy "Abuse" Study	#17, #19 GAC 1, GAC 11	Compare broad sample of P/P- registered domains associated with alleged harmful acts with overall frequency of P/P registrations gnso.icann.org/issues/whois/ gnso-whois-pp-abuse-studies- report-05oct10-en.pdf	3 RFP responses received. Staff analysis to Council on 5 October 2010. Cost: 150,000 Time estimate: < 1 year	 Can sample many harmful acts to assess how often alleged "bad actors" try to obscure identity in WHOIS Compare bad actor P/P abuse rate to control sample and to alternatives like falsified WHOIS data, compromised machines, and free web hosting Some kinds of acts not sampled due to irrelevance and/or difficulty Cannot reliably filter out "false positive" incident reports
4. WHOIS Privacy and Proxy "Relay & Reveal" Study	#3, #13b, #13c, #20	Analyze relay and reveal requests sent for P/P-registered domains to explore and document how they are processed	RFP posted on 29 September, responses due 30 November 2010.	RFP and Terms of Reference: www.icann.org/en/announcements/ announcement-29sep10-en.htm