At-Large Study on Whois Misuse Workspace

Comment Close Date	Statement Name	Status	Assignee (s) and RALO(s)	Call for Comments	Call for Comments Close	Vote Announcement	Vote Open	Vote Reminder	Vote Close	Date of Submission	Staff Contact and Email
27.12.2013	Study on Whois Misuse	**ADOPTED** 12Y, 0N, 0A	• Carlton Samuels (LACRALO) • Holly Raiche (APRALO)	23.12.2013	03.01.2014	06.01.2014	06.01.2014	09.01.2014	10.01.2014	11.01.2014	Mary Wong policy-staff@icann.org

For information about this PC, please click here >>

Comment / Reply Periods (*)

Comment Open Date:
27 November 2013
Comment Close Date:
27 December 2013 - 23:59 UTC
Reply Open Date:
28 December 2013
Reply Close Date:
18 January 2014 - 23:59 UTC

Important Information Links
Public Comment Announcement
To Submit Your Comments (Forum)
View Comments Submitted

Brief Overview
Originating Organization:
GNSO
Categories/Tags:

- Policy Processes

Purpose (Brief):
This study, conducted by Carnegie Mellon University's Cylab (CMU), examines the extent to which public Whois contact information for gTLD domain names is misused (i.e. harmful actions such as spam, phishing, identity theft or data theft are taken using gTLD registration data).

The findings from the study provide empirical data needed by the ICANN community to assess community concerns about misused Whois contact information, identify the most common forms of misuse, and highlight the effectiveness of anti-harvesting measures in reducing misuse. The findings will also inform future policy development by ICANN and the GNSO in relation to improvements to the Whois system.
Current Status:
This Public Comment solicitation represents an opportunity for the community to consider the study results detailed in this report, provide feedback and request further clarifications. In parallel, ICANN and CMU will conduct Webinars to facilitate feedback by summarizing this study's purpose, methodology, key findings, and conclusions.
Next Steps:
CMU will consider all comments submitted to this Public Comment forum during the comment period, incorporate any needed clarifications, and then publish a final version of this Whois Misuse study report. It is expected that this report will inform future GNSO policy development in relation to the Whois system.
Staff Contact:
Mary Wong
Email Staff Contact

Detailed Information

Section I: Description, Explanation, and Purpose:

Having concluded that a comprehensive, objective and quantifiable understanding of key factual issues regarding the gTLD Whois system would benefit future GNSO policy development efforts, the GNSO Council in March 2009 requested ICANN staff to research the feasibility and cost of studying several high priority aspects of Whois. In September 2010, the GNSO Council approved this Whois Misuse study. The purpose of this study was to attempt to prove or disprove the following hypothesis: ***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.***

The overall study consisted of two related studies. First, the research team surveyed (1) registrants of a representative sample of domain names registered in the top five gTLDs – .biz, .com, .info, .net and .org; (2) registries and registrars associated with registration of the surveyed domain names to identify Whois anti-harvesting mechanisms they employ; and (3) cybercrime researchers and law enforcement organizations to gather examples and statistics related to harmful acts attributed to Whois misuse. Secondly, the research team designed and conducted an experiment to measure Whois misuse by registering 400 domains across 16 registrars, associating unique, synthetic Whois contact information with test domains and monitoring incidents of misuse for six months.

This draft report summarizes the various project activities, methodology, sampled data and findings of the research team.

The GNSO Council is now seeking community review and feedback on the draft report. The purpose of this Public Comment period is to ensure that study results have been communicated clearly and to solicit feedback on desired clarifications (if any).

Section II: Background:

As part of its effort to develop a comprehensive understanding of the gTLD Whois system, the GNSO Council had chartered a number of Working Groups and Drafting Teams to develop various possible hypotheses for studies to be performed in relation to several key aspects of Whois. These efforts include the Whois Working Group chartered in 2007 and work done in 2008 by the Whois Studies Working Group, the Whois Hypothesis Working Group and the Whois Study Drafting Team. At the GNSO Council's request, ICANN issued a Request for Proposal (RFP) in September 2009 and related Terms of Reference describing a study to analyze different types of Whois misuse reported by registrants (e.g. spam, phishing, identity theft and data theft), to determine which occurs most often and is most impactful on registrants, and to correlate these findings with anti-harvesting measures that registries and registrars apply to Whois queries (e.g. rate limiting or the use of CAPTCHA phrases). Because of limitations of particular study methods, the study was to consist of two complementary approaches: a descriptive (survey) and an experimental study. The descriptive study would document and analyze Whois misuse incidents (i.e. harmful acts) that have already occurred, while the experimental study would simulate and record misuse to measure more reliably the impact of making Whois data public and of measures applied to deter data harvesting.

After considering RFP responses received from researchers willing to undertake this Whois Misuse study, in March 2010 ICANN staff reported [PDF, 488 KB] to the GNSO Council that it was not clear whether it would be possible to either quantitatively or qualitatively assess the extent to which Whois misuse is "significant", although it was possible to measure and categorize many different types of harmful acts often attributed to the use of Whois data. In September 2010, the GNSO Council decided to proceed with the Whois Misuse study in the manner described in ICANN staff's March report. In April 2011, ICANN announced that CMU had been selected to conduct the study.

The findings from this study are intended to provide empirical data needed to assess the ICANN community's concerns over the use of public Whois data to conduct harmful acts. This empirical data is intended to informICANN's policy work on the Whois system, including future policy development work by the GNSO.

Section III: Document and Resource Links:

Whois Misuse Study Draft Report [PDF, 1.15 MB]

Section IV: Additional Information:

Whois Misuse Study Terms of Reference [PDF, 167 KB]

ICANN Staff Update on Whois Studies [PDF, 488 KB]

GNSO Council motion to pursue Whois Misuse Study

CMU Cylab selected to perform Whois Misuse study

Additional Whois studies have also been conducted at the request of the GNSO Council, as summarized at:http://gnso.icann.org/issues/whois/

(*) Comments submitted after the posted Close Date/Time are not guaranteed to be considered in any final summary, analysis, reporting, or decision-making that takes place once this period lapses.

FINAL VERSION TO BE SUBMITTED IF RATIFIED

Please click here to download the PDF below.
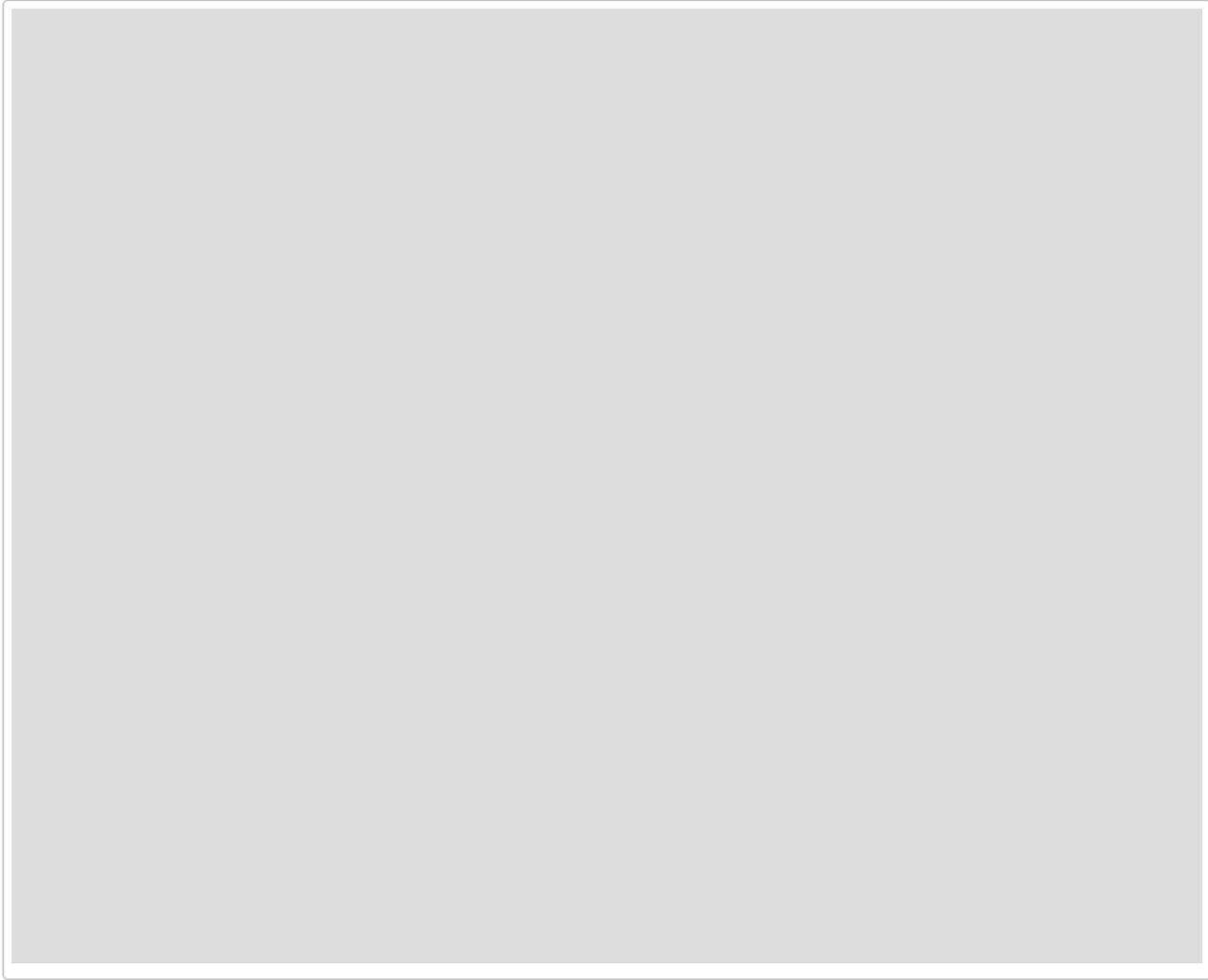
FINAL DRAFT VERSION TO BE VOTED UPON BY THE ALAC

The ALAC has studied the WHOIS Misuse Study commissioned by ICANN and executed by researchers from Carnegie Mellon University over the period. We note the study has returned findings that align with individual experience of At-Large constituents plus the evidence of widespread occurrence has validated similar research undertaken by At-Large connected researchers. The question for the ALAC has never been whether misuse was factual. Rather, it was whether the level of misuse warranted measures to reduce or eliminate and, what would be appropriate responses from policy or operational perspectives, in context.

The ALAC is aware that sectors in the ICANN community have weighed in on the results of this study, with one or other concerned questions on the methodology, size of dataset, geographic scope of study and/or the analysis of the data, all intended to undermine the findings. Nothing we have seen to date would have shaken our confidence in this baseline fact; WHOIS misuse is factual and widespread, as the evidence from 44% of sampled registrants across the several domains attest. Given the continued threat this poses to the security and confidence in the use of the Internet, the public interest demands measures to address and abate its impact.

The ALAC will support any useful measure to abate misuse, including but not limited to WHOIS data anti-harvesting techniques. And even as the study identifies some gTLDs as more susceptible than others, we believe that adopting the best practices from every domain that have proven and useful anti-harvesting implementations of WHOIS data would be a useful beginning for a coordinated response from registries and registrars.

FIRST DRAFT SUBMITTED

The ALAC has studied the WHOIS Misuse Study commissioned by ICANN and executed by researchers from Carnegie Mellon University over the period. We note the study has returned findings that align with individual experience of At-Large constituents plus the evidence of widespread occurrence has validated similar research executed by At-Large connected researchers. The question for the ALAC has never been whether misuse was factual. Rather, it was whether the level of misuse warranted measures to reduce or eliminate and, what would be appropriate responses from policy or operational perspectives, in context.

The ALAC is aware that sectors in the ICANN community have weighed in on the results of this study, with one or other concerned questions on the methodology, size of dataset, geographic scope of study and/or the analysis of the data, all intended to undermine the findings. Nothing we have seen to date would have shaken our confidence in this baseline fact; WHOIS misuse is factual and widespread, as the evidence from 44% of sampled registrants across the several domains attest. Given the continued threat this poses to the security and confidence in the use of the Internet, the public interest demands measures to address and abate its impact.

The ALAC will support any useful measure to abate misuse, including but not limited to WHOIS data anti-harvesting techniques. And even as the study identifies some gTLDs as more susceptible than others, we believe that adopting the best practices from every domain that have proven and useful anti-harvesting implementations of WHOIS data would be a useful beginning for a coordinated response from registries and registrars.