The ICANN GNSO "Business Constituency"

Comments on
Study of Whois Misuse

Status: FINAL

Version: 2

17-Jan-2014

Business Constituency Submission

GNSO//CSG//BC

Background

This document is the response of the ICANN Business Constituency (BC). The BC's comments arise from the perspective of Business users and registrants, as defined in our Charter[1]:

> The mission of the Business Constituency is to ensure that ICANN policy positions are consistent with the development of an Internet that:
>
> 1. promotes end-user confidence because it is a safe place to conduct business
> 2. is competitive in the supply of registry and registrar and related services
> 3. is technically stable, secure and reliable.

ICANN opened a public comment period on an external study of 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).

BC Comment

The WhoIs Misuse study is by its own admission limited in scope and by the level of responses, particularly from Registrants, more speculative than other studies done to understand and test the limits of the WhoIs database.

This makes the findings illustrative, if not definitive, but even then, they are helpful in understanding two key points:

1. The WhoIs database is a source of information for a host of bad actors and bad actions.

   The fact that the study was able to quantify a set of specific misuses of WhoIs data is significant. While email spam would seem obvious, there were statistically significant findings of phishing, postal span, voice mail abuse, injecting viruses, ID theft, even what was labeled "blackmail" and resulted in "demands and intimidation."

2. There are mitigating actions that can be taken to limit such misuse.

It is clear that the perfect need not be the enemy of the good when it comes to WhoIs misuse. Whether it is deploying either a temporary or permanent blacklist, rate limiting queries to Port 43, adding CAPTCHA challenges, even proper use of proxy registrations it is clear there are proven methods.

In light of these insights, the Business Constituency (BC) urges that all domain name registries and registrars adopt a fully-integrated set of mitigating actions. The study found that the misuse varied by registry. A consistent set of mitigating actions, equally applied, can make the problem only as large as the smallest variation.

It is also the view of the BC that what seem to be high percentages of certain kinds of misuse (e.g., 44 percent email abuse) not lead to false conclusions. For example, there is a wider analysis being done with regard to creating a more accurate WhoIs or Directory Services regime. It would be wrong to use the current misuse findings to slow that effort.

In fact, the low response from registrants to the study questions despite their importance suggests that such research should be on-going. In this way, it can both educate registrants and reinforce the market for implementing the mitigating actions. The goal ought to be to create a shared commitment among registrars, registries and registrants to collaborate on raising the barriers to misuse.

Finally, any restrictions on Whois access that might be contemplated as a result of this study should nonetheless preserve access by any party needing to know the identity of those registering a domain where there is evidence of actionable harm.

Jimson Olufuye, Susan Kawaguchi, and John Berard led drafting of these comments, which were approved in accordance with the BC Charter.

[1] Business Constituency Charter, at http://www.bizconst.org/charter.htm.