

Amendments to WHOIS output for Nameservers

Contents

1. Introduction	1
2. Background	1
3. Proposal	1
4. Recommendation	1

1. Introduction

This paper proposes a small change to the whois output that will reduce the workload of the whois server and increase it's processing speed.

2. Background

The whois server attempts to display the IP address of each of the nameservers listed for a domain whether or not this information is stored in the register. If the IP address of a nameserver is not known then the whois server will attempt to lookup that address in order to display it. This lookup causes several problems:

1. It can take several seconds if the customer nameservers have not been set up correctly (an example is 121talk.co.uk) delaying the response to the whois query by this long.
2. When the whois cannot validate the IP address it says so with the text "(unable to validate IP)". This regularly leads to calls from confused registrants and tagholders as it gives the impression that we will not enter these details into the zone file (when we will).
3. A clever attacker could use this to attempt a denial of service attack on the whois by deliberately triggering this functionality.

It should also be noted that this lookup is not IPv6 compliant and so would need amending if this were required.

3. Proposal

It is the view of the executive that this lookup is unnecessary and goes beyond the remit of how a well run whois should operate. If anything it is any unwanted risk.

The proposal is therefore to only display the IP address of a nameserver where that is held on the register as the glue data. Where this information is not known this part of the whois output will be left blank.

4. Recommendation

The PAB is asked to consider the following resolution

"The PAB resolves to recommend that the whois output be changed to no longer display the IP addresses of nameservers where that information is not held on the register."