Les (amusantes) versions annoncées par les serveurs DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 août 2011

https://www.bortzmeyer.org/versions-serveurs-dns.html

Les serveurs DNS ont souvent une option (complètement non officielle) pour obtenir le numéro de version du logiciel utilisé. Par souci de dissimulation, ou tout simplement pour s'amuser, certains administrateurs système décident d'afficher à la place un petit texte, souvent humoristique.

Cette option est une simple convention : aucun RFC ne l'a jamais normalisé. Mais, si vous interrogez un serveur DNS pour le nom `version.bind`, type `TXT`, classe `CH`, vous obtenez cette information :

```
% dig @ns1.dns.example CH TXT version.bind
...
;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.6.2-P3"
...
```

Comme son nom l'indique, cette option vient à l'origine de BIND mais on la trouve dans bien d'autres serveurs, comme NSD. BIND permet de la débrayer, ou bien de remplacer le texte (option `version` dans le bloc `options`, par exemple `version "No information";`). On voit ainsi des choses comme :

```
% dig @dns.sncf.fr. CH TXT version.bind
...
;; ANSWER SECTION:
version.bind.           0       CH      TXT     "S.N.C.F. French Railways"
```

Si on lance DNSdelve <http://www.dnsdelve.net> à l'assaut de tout `.fr` pour regarder les textes ainsi diffusés, on trouve de nombreuses perles. Par exemple :

— Des classiques purement informatifs comme « *"No version info available"* », « *"[Private Information]"* », « *"You are not cleared for that information"* » ou « *"Not Allowed"* »,

— Des textes plus menaçants comme « *"None of your business"* », « *"request logged and reported to abuse!"* », « *"mind your own business!"* » ou « *"This information is restricted, Your query has been logged."* », « *"Your attempt to obtain details of this service has been duly noted!"* » ou « *"Guess, bitch"* »,
— Des références *"geeks"* comme « *"All your base are belong to us"* », « *"Nobody here but us chickens!"* », « *"WE ARE THE BORG. RESISTANCE IS FUTILE"* » ou « *"This is not the port you're looking for."* »,
— Des textes écrits par le service juridique comme « *"If you have a legitimate reason for requesting this info, please contact hostmaster@Level3.net"* »,
— Diverses formes d'humour comme « *"Do you realy want version of this server? Is your mother know what you do? ? ? Probably no!"* », « *"Toaster connected to coffee cup"* », « *"This space is intentionally left blank"* », « *"My version is so secret that even I don't know what I'm running on"* », « *"Uppps, I lost my version number"* » ou « *"Insert your credit card"* » ou simplement « 0.0 ».

Merci à Nicolas Delvaux pour le programme. Et une dernière pour la route :

```
% dig +short @rigel.illyse.org CH TXT version.bind
"OpenOffice DNS server 1.0"
```

Pour ceux qui se souviennent du pare-feu d'OpenOffice <http://www.numerama.com/magazine/12508-albanel-le-ministere-de-la-culture-a-comme-pare-feu-open-office-maj.html>... Autre exemple rigolo en dehors de `.fr` :

```
% dig +short @ns1.conostix.com CH TXT version.bind
"'\; DROP DATABASE mysql\; --"
```

L'auteur a tenté une injection SQL <https://www.bortzmeyer.org/sql-injection.html> avec le DNS...