Souriez, vous (enfin, votre résolveur DNS) sert à la science

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 septembre 2012

https://www.bortzmeyer.org/experience-dnssec-verisign.html

Depuis ce matin, une bonne partie des visiteurs de ce blog participe (involontairement) à une expérience de mesure du déploiement de la validation DNSSEC.

Regardez le code source de chaque page, vers le bas. Vous trouverez un lien <a> vide vers prefetch.validatorsearc
Ce nom est servi par des serveurs DNS un peu spéciaux, qui répondent de manière inhabituelle, de manière à étudier le comportement du résolveur qui les interroge, afin de savoir s'il fait du DNSSEC ou pas (en France, aucun FAI n'a encore activé la validation DNSSEC, à ma connaissance). Si votre navigateur Web met en œuvre le "*prefetching*" DNS (la récupération anticipée d'informations DNS, avant tout clic de l'utilisateur), votre résolveur contactera automatiquement les serveurs de validatorsearch.verisignlabs.co
J'encourage tous les gérants de sites Web à inclure également ce petit bout de code HTML : <a href="http://prefetch
(L'ISOC le demande aussi <http://www.internetsociety.org/deploy360/blog/2012/09/can-you-add-1-li
>.)

L'expérience est menée par VeriSign et il existe une page officielle <http://validatorsearch.verisignlabs.com/> avec, notamment, les résultats préliminaires (un peu plus de 3 % de résolveurs validant avec DNSSEC). Attention, comme les serveurs de validatorsearch.verisignlabs.com sont très spéciaux, il peut y avoir des problèmes à accéder à cette page avec certains résolveurs (par exemple Unbound).

Quelques notes sur la protection de la vie privée :

— Inclure ce code HTML dans sa page n'envoie pas seulement les données du webmestre à VeriSign mais aussi celles des innocents visiteurs. Il faut donc bien réfléchir.
— La connexion avec VeriSign est uniquement en DNS : le lien est invisible et, même si quelqu'un arrivait à cliquer dessus, l'adresse associée est celle de localhost. Il n'y aura donc jamais d'échange en HTTP avec VeriSign (donc pas de "*cookies*" ou de trucs comme ça).
— Ce n'est pas votre adresse IP que verra VeriSign mais celle de votre résolveur DNS : dans la plupart des cas, un serveur de votre FAI.
— La requête DNS ne contient rien sur le site Web que vous visitiez.