FAUT-IL VRAIMENT POUVOIR REBOUTER L'INTERNET ?

LE 2 AOÛT 2010 ***STÉPHANE BORTZMEYER***

Panique et confusion dans les médias généralistes: sept personnes seraient en mesure de rebooter Internet. Stéphane Botzmeyer revient sur les aspects techniques de cette "légende".

Sept personnes seraient en mesure de rebooter Internet: panique et confusion dans les médias généralistes. **Nous nous étions interrogés** sur la pertinence technique d'une telle information. Stéphane Botzmeyer, ingénieur informaticien à l'AFNIC, analyse les écueils de cette "légende".

On le sait, la grande majorité des articles concernant l'**Internet** sont faux et, en prime, souvent ridiculement faux. Cela concerne évidemment les médias traditionnels (**presse**, **télévision**, etc) mais aussi les forums en ligne où les deux cents commentaires à un article sont écrits par des gens dont la seule compétence technique est l'installation de **WordPress** (et, parfois, ne soyons pas trop méchants, l'écriture de dix lignes de **PHP**). Mais des records ont été récemment battus à propos de la légende comme quoi « Sept personnes ont les clés pour **rebouter** l'Internet ».

Le point de départ de la légende semble avoir été un communiqué publicitaire

de l'Université de **Bath**, « ***Bath entrepreneur holds key to internet security*** ». Ce communiqué outrageusement cireur de pompes contenait beaucoup d'erreurs et a été repris, aussi bien dans la presse bas de gamme comme **Metro** (« ***Brit given a key to 'unlock' the internet*** ») que dans des médias prétendument sérieux comme la **BBC** (« ***Bath entrepreneur 'holds the key' to internet security*** », notez la reprise quasi-littérale du titre du communiqué de presse) ou comme le **Guardian** (« ***Is there really a key to reboot the internet?*** », l'article le moins mauvais du lot).

La légende a ensuite franchi la **Manche** et, dans la traduction, le côté chauvin et la publicité pour une personne particulière ont disparu. Cela a donné « **Sept personnes ont les clés d'Internet !** », « **Les sept clés de l'Internet sécurisé** » ou « **Rebooter internet – Comment ça marche ?** » (de moins mauvaise qualité).

Bon, qu'il y a t-il de vrai dans cette légende ? Sur quoi cela s'appuie t-il ? Depuis le 15 juillet dernier, le processus de signature de la racine du **DNS** par le système **DNSSEC** est complet : les **serveurs de noms de la racine** diffusent désormais des informations signées, ce qui permet de détecter des tentatives de modification des données, comme celles utilisant la **faille Kaminsky**. Tout ce processus est largement documenté sur le site officiel **`http://www.root-dnssec.org/`** et il est symptomatique qu'aucune des personnes qui ait écrit à ce sujet ne l'ait consulté. À l'ère d'Internet, toute l'information est gratuitement et librement disponible, encore faut-il la lire !

Notons d'abord que ce processus ne concerne que le **DNS**. Certes, ce protocole d'infrastructure est indispensable au bon fonctionnement de la quasi-totalité de l'Internet.

Sans lui, on serait limité à des **ping** (en indiquant l'**adresse IP**) et à des **traceroute** (avec l'option `-n`). Certains services, comme le **Web**, dépendent encore plus du DNS. Néanmoins, on voit que parler d'un « redémarrage de l'Internet » est ridicule, que DNSSEC fonctionne ou pas n'empêchera pas le réseau de faire passer des **paquets**.

Ensuite, dans ce processus, quel est le rôle des fameux sept gusses ? Leur nom est disponible **sur le site officiel** (alors que certains articles disaient « on ne connait que certains d'entre eux » et autres phrases censées faire croire qu'on révélait au lecteur des secrets stratégiques). Leur rôle est décrit dans le document « ***Trusted Community Representatives Proposed Approach to Root Key Management*** », document qui a été publié il y a des mois. Le processus complet figure dans « ***DNSSEC Practice Statement for the Root Zone KSK Operator*** ». DNSSEC fonctionne en **signant cryptographiquement** les enregistrements distribués. Il dépend donc d'une **clé privée** qui doit à la fois être disponible (pour signer) et être protégée pour éviter que les méchants ne mettent la main dessus. (À propos de méchant, tout article qui parle d'« attaque terroriste » est grotesque. Comme si **Al-Qaida**, spécialiste des bombes et des égorgements, avait tout à coup envie d'empêcher les riches pays du Nord de regarder **YouTube**.) Un des risques possibles est la perte complète de la clé privée (suite à un incendie ou à un tremblement de terre, risques autrement plus importants que la mythique attaque terroriste). Il y a donc des **sauvegardes** mais celles-ci sont protégées par **chiffrement**. Et c'est là qu'interviennent les TCR.

Il y a deux sortes de TCR (« *Trusted Community Representatives* »), choisis pour assurer des rôles de gestions des clés cryptographiques de DNSSEC. Il y a les « *Crypto Officers* » qui vont s'occuper de la génération des clés (au cours de **solennelles cérémonies**) et les « *Recovery Key Share Holders* » (les fameux sept). Ces derniers sont simplement chargés de garder une partie de la clé qui permettra le déchiffrement des sauvegardes. C'est tout. Ils ne peuvent pas « redémarrer l'Internet », ce qui ne veut rien dire. Mais, si les articles sensationnalistes avaient commencé par « Sept personnes peuvent restaurer les sauvegardes des clés DNSSEC », gageons qu'ils auraient eu moins de succès…

Enfin, il faut relativiser : à l'heure actuelle, si un certain nombre de **domaines** sont signés par DNSSEC (par exemple, hier, **`.dk`** et **`.edu`** ont rejoint la liste des **TLD** dont la racine authentifie la signature), pratiquement aucun **résolveur** DNS (les serveurs directement interrogés par les utilisateurs) ne valide avec DNSSEC. Que la clé privée soit compromise ou pas ne changera rien, puisque les signatures sont ignorées. Il faudra sans doute des années avant que les résolveurs de M. Tout-le-Monde dépendent d'une signature DNSSEC. La remarque de **Bruno**, « les 7 gugusses et leurs cartes à puce ont autant de pouvoir sur le bon fonctionnement d'Internet que mon chat sur le problème des embouteillages sur le periph parisien » est donc à 100 % justifiée.

Article initialement publié sur le blog de Stéphane Bortzmeyer

Illustrations CC FlickR par **edfrz** et **kalleboo**

GLOPGLOP
le 2 août 2010 - 15:49 • SIGNALER UN ABUS - PERMALINK

L'article est précis et bien documenté, bravo. Je crois me souvenir que dans un passé pas si lointain on a déja frôlé la catastrophe 9 des dns root était tombés en rideau sur les 12 suite à une panne…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LOHIEL
le 2 août 2010 - 22:49 • SIGNALER UN ABUS - PERMALINK

Dans un épisode de 1995 de X-Files, le doublage français contenait cette phrase qui m'avait fait hurler de rire "je vais appeler Internet et demander qu'on me faxe… etc." (pour "Online service" en anglais)

on peut voir le passage ici
http://www.youtube.com/watch?v=FF2znL-V6yY

Bon, à l'époque, c'était encore assez loin de démarrer vraiment en France (sacré minitel !) – et c'était ridicule, mais pas incompréhensible : l'équipe de doublage n'avait pas la moindre idée de ce dont il s'agissait. Maintenant, aujourd'hui, il serait quand même nécessaire que les gens comprennent de quoi Internet est fait (à part les chats :-))

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI REPONDRE

LAURENT
le 3 août 2010 - 13:17 • SIGNALER UN ABUS - PERMALINK

Merci pour ces précisions, je me disais bien que tous ces titres étaient un peu pompeux. Honte à moi je n'avais pas cherché plus loin.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GASTON
le 9 août 2010 - 18:54 • SIGNALER UN ABUS - PERMALINK

C'est dommage.
L'auteur fait le malin en début d'article pour sortir une bêtise quelques lignes plus loin.

"Notons d'abord … réseau de faire passer des paquets."

Le DNS n'est en rien indispensable, il n'a aucune utilité au niveau infrastructure. C'est simplement un service d'annuaire, faire correspondre un nom (ex:www.google.com) avec une adresse IP (xxx.xxx.xxx.xxx).
Alors les DNS peuvent bien disparaitre les sites Internet seront toujours accessibles (du moins par leur adresse IP).

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

STEPHANEBORTZMEYER
le 23 août 2010 - 17:55 • SIGNALER UN ABUS - PERMALINK

@Gaston Ah non, vous vous trompez. Je vous suggère une expérience simple : supprimer votre(vos) résolveur(s) DNS de votre configuration Internet (sur Unix, éditez /etc/resolv.conf et virez les lignes incluant "nameserver") et regardez si vous arrivez à naviguer loin sans le DNS… (Vous auriez fait cette expérience avant, votre réputation eût été sauvegardée).

Deux points techniques à garder en tête, concernant le Web :

1) La plupart des sites Web partagent l'adresse IP d'autres sites et seul le nom (envoyé par le champ Host: du protocole HTTP) permet au serveur de s'y retrouver. Remplacer le nom de domaine par une adresse IP dans l'URL ne marche pas…

2) Même si on arrive à avoir la première page, le premier lien qu'on cliquera générera une erreur puisque les liens dans un source HTML comprennent rarement une adresse IP…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

STEPHANEBORTZMEYER
le 23 août 2010 - 17:57 • SIGNALER UN ABUS - PERMALINK

@glopglop La dernière fois où la majorité des serveurs DNS de la racine sont tombés, c'était en 2002, soit bien avant le déploiement de l'anycast. Aujourd'hui, cela serait bien plus difficile comme l'a montré l'attaque ratée de 2007.

http://www.bortzmeyer.org/attaque-serveurs-racine.html

http://www.bortzmeyer.org/combien-serveurs-racines.html

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GASTON
le 25 août 2010 - 14:55 • SIGNALER UN ABUS - PERMALINK

@STEPHANEBORTZMEYER: Ce que vous dites est juste, mais quand on essaye d'expliquer quelque chose de technique il faut avant tout être rigoureux ("Sans

lui, on serait limité à des ping et à des traceroute" ceci n'est pas vrai).
Bien sur plusieurs sites peuvent être hébergés "sur" une même IP et un site peut être accessible à partir de plusieurs IP également. C'est site la seront bien entendu innaccessibles.

C'est un peu comme si on enlevait les panneaux de direction des routes, ça risque d'être légèrement compliqué mais la route n'en est pas moins praticable.

J'espère que ma réputation est sauve ^^.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

VPN HADOPI
le 11 novembre 2010 - 13:33 • SIGNALER UN ABUS - PERMALINK

5€ par mois pour télécharger tranquille avec un VPN anti hadopi

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

3 pings

Les tweets qui mentionnent Faut-il vraiment pouvoir rebouter l'Internet ? » Article » OWNI, Digital Journalism -- Topsy.com le 2 août 2010 - 15:52

[...] Ce billet était mentionné sur Twitter par Nicolas Voisin, Alberte Denis et Jourdan Buatois, Owni. Owni a dit: [#owni] Faut-il vraiment pouvoir rebouter l'Internet ? http://goo.gl/fb/weMEn [...]

« Rebooter internet » Non, désolé, ce ne sera pas possible ! | Le blog de Buz le 2 août 2010 - 16:36

[...] n'ai pas trop envie de m'attarder sur les absurdités de cet article, OWNI l'a déjà très bien [...]

Quick & Dirty (20) « Journal du Hack le 2 août 2010 - 16:54

[...] Owni.fr -A force de se préoccuper de vendre de la musique, on en oublie l'Art -Faut-il vraiment pouvoir rebooter internet? [...]