RFC 4948 : Report from the IAB workshop on Unwanted Traffic March 9-10, 2006

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 septembre 2007

Date de publication du RFC : Août 2007

http://www.bortzmeyer.org/4948.html

La sécurité sur Internet est un problème très fréquemment mentionné. Rien d'étonnant donc à ce que l'IAB, organisme chargé entre autres de superviser les développements de l'architecture de l'Internet, aie décidé de réunir un certain nombre d'experts pour un séminaire sur « le trafic Internet non désiré ». Ce RFC est le compte-rendu de ce séminaire.

Le séminaire s'est tenu à Marina del Rey en mars 2006 et on peut déplorer l'extrême lenteur que met toujours l'IAB à publier les compte-rendus de ses intéressants séminaires.

De quoi a t-on parlé pendant ce séminaire ? D'abord, la définition de « trafic non désiré » s'est concentrée sur deux phénomènes spécifiques, le spam et les DoS. Ensuite l'IAB note qu'un des messages les plus importants à faire passer est que le trafic non désiré n'est pas seulement produit par quelques adolescents perturbés mais est majoritairement l'œuvre d'entreprises criminelles bien organisées au sein de ce que l'IAB appelle (section 2 et notamment 2.1 du RFC) l'économie souterraine. (Je prends mes distances face à ce terme car je ne suis pas sûr qu'elle soit si souterraine que cela, ni si distincte de l'économie légale. L'utilisation de paradis fiscaux ou de la fraude fiscale n'est pas spécifique à la Mafia. Mais revenons à la sécurité de l'Internet.)

Bref, au revoir l'image du boutonneux qui s'attaque aux serveurs du Pentagone pour impressionner ses copains. Place aux professionnels, qui agissent pour l'argent.

Cette économie souterraine fait que des ressources humaines, financières et techniques importantes sont dédiées aux utilisations illégales de l'Internet. Dans un réseau ouvert, ces utilisations peuvent faire beaucoup de dégâts, d'autant plus que beaucoup d'utilisateurs ne sont pas conscients de l'ampleur des dangers que courent leurs machines. Outre son caractère ouverte et l'absence de traçabilité construite dans le réseau lui-même, l'Internet doit une partie de sa vulnérabilité à son caractère international.

On ne peut pas compter sur la police russe pour traquer ceux qui ont attaqué les réseaux informatiques <http://www.wired.com/politics/security/magazine/15-09/ff_estonia> en Estonie puisque ces attaquants agissaient sous la bienveillance de leur propre gouvernement.

Quelles sont les machines participant aux attaques ? Aujourd'hui, ce ne sont que rarement celles appartenant à l'attaquant (section 2.3). Celui-ci se sert plutôt de zombies, des machines piratées et asservies. Le RFC note que la grande majorité des machines connectées à Internet est vulnérable. En partie à cause des faiblesses de Microsoft Windows (que l'IAB minimise par souci du « politiquement correct ») mais aussi parce que ces machines ne sont pas gérées par des professionnels responsables. Même prévenu, il est rare que l'utilisateur d'une machine zombie la nettoie. Les problèmes sont pour les autres, pas pour lui et l'absence de responsabilité crée un terrain favorable pour les recruteurs de zombies.

Notons que le séminaire n'avait pas pour but de trouver une solution magique mais d'étudier le problème. Le compte-rendu est donc souvent balancé, car il n'y a pas de solution parfaite, uniquement des compromis. C'est ainsi que la section 2.4 rappelle que, si on change le réseau pour augmenter la traçabilité, ces nouvelles possibilités de surveillance vont certainement attirer des gens peu recommandables, qui seraient ravis d'utiliser ces nouvelles possibilités pour surveiller les citoyens.

La section 3 est ensuite consacrée à une étude de l'ampleur du problème, pour les différents acteurs, et aux stratégies qu'ils utilisent pour se défendre. C'est là par exemple que l'IAB rappelle que le RFC 2827 [1] (alias BCP 38 <http://www.bortzmeyer.org/bcp38.html>), qui permettrait de sérieusement limiter l'usurpation d'adresse IP, n'est pratiquement pas déployé aujourd'hui, par suite du manque d'intérêt financier à le faire (la section 4.2.1 détaille également ce problème, où le marché est incapable de déployer une solution qui bénéficierait à tous mais coûterait un peu à chacun).

La section 3.4 concerne les fournisseurs de services DNS. Sa principale recommandation est le déploiement rapide de l'anycast sur les serveurs importants. Notre RFC étant consacré aux trafic non désiré et notamment aux DoS, il n'est pas étonnant que les conseils qu'il donne n'aille pas dans le même sens que ceux des RFC qui se penchent surtout sur l'intégrité des données. Ainsi, DNSSEC est présenté comme un risque plutôt que comme une solution (la section 4.3.2 exprime également une certaine méfiance par rapport à la cryptographie).

La section 4 commence à s'attaquer aux solutions. On notera que plusieurs participants au séminaire ont estimé qu'on avait déjà toutes les solutions techniques nécessaires, le défi était de les déployer. Si le déploiement doit se faire sur les réseaux des grands opérateurs commerciaux, il est freiné par l'absence de retour sur investissement. Si le déploiement doit se faire sur les machines des utilisateurs, il est freiné par la difficulté d'éducation.

Compte-tenu de l'ampleur du problème, ne faut-il pas adopter des mesures drastiques, qui changeraient radicalement le modèle de l'Internet ? C'est par exemple ce que propose le projet « table rase » de l'université de Stanford, qui se propose de refaire complètement l'Internet, autour d'un modèle bien plus fermé où tout devrait être autorisé préalablement. Les sections 4.3.4 et surtout 5.1 sont consacrées à l'examen de telles solutions, qui évoquent le médecin assassinant le malade pour le guérir...

Les présentations faites lors du séminaire sont en partie en ligne <http://utgard.ietf.org/iab/about/workshops/unwantedtraffic/index.html>, à l'exception de celles qui sont trop sensibles. Un compte-rendu du séminaire, plus court et plus vivant que le RFC, a été fait dans le numéro 70 de l'IETF Journal <http://www.isoc.org/tools/blogs/ietfjournal/?cat=14>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2827.txt