# abuse@BIGISP.net ne répond pas

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 juin 2009

https://www.bortzmeyer.org/abuse-ne-repond-pas.html

---

Comment signale-t-on un problème sur l'Internet ? Si un ver fait des requêtes HTTP <https://www.bortzmeyer.org/ver-du-jour.html> répétées à la recherche d'une vulnérabilité ? Si un autre ver se connecte en SSH en permanence à votre Kimsufi en tentant le compte `guest` ? Si un script utilise automatiquement votre service <https://www.bortzmeyer.org/mason-403.html> en dépit des conditions d'utilisation ? Si vous recevez du spam depuis telle ou telle machine ? En théorie, il existe une adresse de courrier standard pour cela. Spécifiée dans le RFC 2142 [1], c'est `abuse@DOMAIN.EXAMPLE` où `DOMAIN.EXAMPLE` est le domaine en cause. Mais le courrier envoyé à `abuse` n'obtient jamais de réponse et, souvent, n'est même pas lu. Pourquoi ?

Au cours de ma carrière, j'ai été des deux côtés de la barrière, du côté de ceux qui reçoivent les messages envoyés à `abuse` et du côté de ceux qui les envoient. Du côté du simple utilisateur, qui voudrait signaler un problème, le bilan n'est pas très glorieux. Les réponses reçues sont rarissimes. La plupart du temps, c'est le silence complet. Parfois, on reçoit un avis de non-remise « il n'y a pas de compte `abuse` à l'adresse indiquée ». Parfois une réponse standard inutile.

Est-ce qu'au moins les messages sont lus, même si `abuse` ne peut pas répondre à tous ceux qui lui écrivent ? Même pas. La plupart du temps, les messages atterissent directement dans `/dev/null`, ou bien, à la rigueur, dans la boîte d'un stagiaire embauché pour faire le support utilisateur, qui n'y connait rien et n'est pas assez payé pour qu'on puisse lui demander de travailler <https://www.bortzmeyer.org/personne-ne-s-est-plaint.html> sérieusement.

Même si certains gros FAI s'obstinent à nier et affirment, contre toute évidence, que les messages sont lus soigneusement, la triste réalité est qu'écrire à `abuse` ou bien jouer à "*World of Warcraft*" donneront le même résultat (et, dans le second cas, au moins, on voit les monstres qu'on combat).

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2142.txt`

Est-ce de la paresse ou de la méchanceté de la part des FAI ? En partie oui, bien sûr, c'est vrai qu'ils se moquent totalement de ce que leurs propres utilisateurs peuvent raconter. Alors, quand il s'agit d'inconnus... Mais il faut aussi remarquer que le problème n'est pas simple. D'abord, sur l'Internet, il y a tout le temps des problèmes. Si on héberge un parc de dix mille machines Unix dédiées et louées à des clients, il y en a forcément toujours un bon nombre qui se lancent dans des attaques, soit parce que le locataire est un méchant, soit parce qu'il a laissé un script PHP vulnérable sur sa machine. Si on connecte des dizaines de milliers de foyers où se trouvent des machines MS-Windows, c'est encore pire, un bon nombre a été transformé en zombies et les attaques qu'elles lancent vaudront certainement à `abuse` pas mal de courrier.

Mais il y a un autre problème : la très grande majorité des rapports envoyés à `abuse` sont inutilisables. Aucun détail, aucune précision, l'heure de l'attaque n'est pas indiquée (ou alors en heure locale, sans indication du fuseau horaire), les messages sont résumés et mal traduits au lieu d'être cités littéralement, etc. Le message typique reçu par `abuse` (rappelez-vous qu'un gros hébergeur peut avoir des dizaines de milliers de machines, voire davantage pour les très gros) est simplement « Mon firewall [sic] me dit que votre machine m'attaque, arrêtez tout de suite » (et encore, je n'ai pas respecté l'orthographe). Il est même fréquent que le message soit 100 % erroné et qu'il n'y ait pas d'attaque du tout (comme le voit fréquemment l'IANA <`https://www.iana.org/abuse/`>).

Plus drôle, les messages à abuse sont parfois des tentatives d'attaque <`http://www.zdnet.fr/blogs/securite-cybercriminalite/services-abuse-la-nouvelle-cible-des-cybercriminels-3`
`htm`>.

Analyser de tels messages sérieusement nécessiterait du temps et une main d'œuvre qualifiée, alors qu'en général on met au « support de premier niveau » les gens les moins payés de l'entreprise. Il faudrait demander des précisions, faire preuve de patience, suivre le dossier, tout ce que fait un avocat d'affaires payé très cher de l'heure, mais pas ce que peut faire le Marocain ou l'Indien qui travaille dans un "*call center*". Pour des simples raisons économiques, les messages à `abuse` sont donc traités vite et mal.

`abuse` est d'autant moins enclin à lire ses messages qu'un certain nombre d'utilisateurs spamment à tout vent et écrivent, lors de n'importe quel problème, à toutes les adresses de courrier qu'ils peuvent trouver en interrogeant whois.

Et les messages de qualité ? En général, vu l'afflux de messages inutilisables, les rares messages corrects, précis et complets sont traités comme les autres, perdus au milieu du flot.

Une bonne introduction au rôle (théorique) d'un service « "*abuse*" » est « Le service abuse des hébergeurs : comment ça fonctionne ? <`http://www.hackersrepublic.org/culture-du-hacking/le-service-abuse-des-hebergeurs`> ».

---

`https://www.bortzmeyer.org/abuse-ne-repond-pas.html`