Ne jamais avoir de listes noires statiques

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 décembre 2008

https://www.bortzmeyer.org/pas-de-listes-noires-statiques.html

---

Quand on arrive dans un nouvel emploi d'ingénieur système & réseaux, ou bien lorsqu'on fait un petit audit d'un site existant, on tombe souvent sur des listes noires, en général d'adresses IP refusées. Ces listes ont typiquement été créées suite à un incident de sécurité et, malheureusement, sont souvent **statiques**, c'est-à-dire jamais mises à jour. En général, la date où a été créée une entrée donnée n'est jamais indiquée <https://www.bortzmeyer.org/mettre-date-fichiers-config.html>. Au bout d'un certain temps, ces listes deviennent donc plus dangereuses qu'utiles.

Il ne faut jamais utiliser une telle liste sans avoir une procédure (de préférence automatique, et surveillée, pas un cron que tout le monde a oublié) de mise à jour. Autrement, c'est votre successeur, dans deux ans, qui tombera sur le problème.

Ainsi, l'excellent site Cymru <http://www.team-cymru.org/> fournit tout ce qu'il faut pour cela. Leurs listes noires de "*bogons*" <http://www.team-cymru.org/Services/Bogons/>, par exemple, peuvent être automatiquement mises à jour via BGP, le DNS, etc.

Comme, malgré de tels services, la plupart des listes de "*bogons*" sont laissées à elles-mêmes, jamais mises à jour, le malheureux qui récupère des adresses dans un préfixe qui vient d'être alloué va souffrir. Certains ont même menacé l'ARIN ou d'autres RIR de procès, pour leur avoir « vendu » des adresses IP inutilisables.

Idem pour les listes noires liées au spam ou d'autres problèmes de sécurité. Si une adresse IP a une fois servi à spammer, elle est gâtée pour toujours. Cela a même mené à une proposition d'évaluation de la valeur des adresses IP <https://www.bortzmeyer.org/evaluation-adresses-ip.html> selon leur historique.

Certaines de ces listes statiques sont parfois redistribuées et des ignorants les utilisent sans connaitre leurs limites.

Faites le test dans votre organisation : pour chaque liste de "*bogons*", pour chaque liste noire, ou équivalent, existe t-il une procédure documentée de mise à jour ? Si non, supprimez cette liste d'urgence.

Le message attaché est un exemple ultra-classique des problèmes des listes de "*bogons*" pas à jour, tels qu'ils sont vus par les opérateurs. De tels messages sont très fréquents (ici, sur la liste SANOG, le groupe des opérateurs réseau d'Asie du Sud) et dureront tant que les gens continueront à utiliser ces listes noires statiques.

Date: Sat, 15 Sep 2007 05:13:48 -0400 (EDT)
From: Sri <jaadhoo@yahoo.com>
Subject: [SANOG] 99/8 IP Block (was Bogons)
To: sanog@sanog.org

Hello all,
I am Sri from Rogers Cable Inc. ISP in Canada. We have IP block
99.x.x.x assigned to our customers. Which happened to be bogons block
in the past and was given to ARIN in Oct 2006. As we have recently
started using this block, we are getting complaints from our customers
who are unable to surf some web sites. After investigation we found
that there are still some prefix lists/acls blocks this IP block.

We got the following blocks:

99.224.0.0/12
99.240.0.0/13
99.248.0.0/14
99.252.0.0/16
99.253.128.0/19

  Here are the few pingable ips 99.246.224.1 & 99.244.192.1

Please update your bogons list.

If anyone has any questions, or I can provide any additional
information which anyone may require, please feel free to email me
directly or call our TAC @ 416.935.5700.

Thanks in advance for your support,

Sri

--
This is the SANOG (http://www.sanog.org/) mailing list.