La curieuse annonce des adresses IPv4 de l'armée états-unienne

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 avril 2021

https://www.bortzmeyer.org/as8003.html

Le 20 janvier 2021, l'armée des États-Unis a soudainement annoncé sur l'Internet des millions d'adresses IP qui n'avaient jamais été actives sur l'Internet. Les causes exactes ne sont pas connues (il y a des explications officielles mais qui ne répondent pas à toutes les questions). Comment a-t-on vu cela et quelles conclusions (forcément assez spéculatives) peut-on en tirer ?

Au début, cela ressemblait à un détournement BGP classique, provoqué soit par une erreur humaine (cas de l'accident malaisien <https://www.bortzmeyer.org/bgp-malaisie.html>), soit par une volonté délibérée de détourner du trafic (cas de l'attaque contre MyEtherWallet <https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/>). Le protocole BGP permet à un routeur Internet d'annoncer les préfixes d'adresses IP qu'il sait joindre. S'il se trompe ou qu'il ment, ses pairs vont parfois accepter l'annonce et l'utiliser, envoyant alors le trafic vers les détourneurs. Le 20 janvier 2021, ce fut la première réaction, « quelqu'un annonce les adresses IP de l'armée ». Comment le voit-on ? Rappelez-vous que l'Internet est très transparent. Tout routeur de la DFZ va voir les annonces et, même si vous n'avez pas accès à un tel routeur, plusieurs services vous fournissent les données. Servons-nous du classique RouteViews <http://www.routeviews.org/>. Vous pouvez récupérer toutes les annonces du 20 janvier 2021 et les analyser (ici, on convertit les données qui étaient au format MRT du RFC 6396 [1], avec l'outil bgpdump <https://github.com/RIPE-NCC/bgpdump>) :

```
% wget http://archive.routeviews.org/bgpdata/2021.01/UPDATES/updates.20210120.1645.bz2
% bunzip2 updates.20210120.1645.bz2
% bgpdump updates.20210120.1645 > updates.20210120.1645.txt
```

On a alors un fichier texte avec les annonces BGP, qu'on peut regarder avec l'éditeur ou l'afficheur de son choix. Voici la première annonce bizarre (l'heure est évidemment UTC) :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6396.txt

```
TIME: 01/20/21 16:57:35.081428
TYPE: BGP4MP_ET/MESSAGE/Update
FROM: 64.71.137.241 AS6939
TO: 128.223.51.102 AS6447
ORIGIN: IGP
ASPATH: 6939 8003
NEXT_HOP: 64.71.137.241
ANNOUNCE
   11.0.0.0/8
```

(La dernière annonce pour ce même préfixe, relayée par plusieurs routeurs avant d'atteindre Route-Views, a été vue à 17 :04 :19.316776, ce qui donne une idée de la rapidité de la propagation des routes dans l'Internet.)

En quoi est-ce que cette annonce était bizarre ? D'abord, le préfixe `11.0.0.0/8`, un préfixe comportant beaucoup d'adresses (surtout depuis l'épuisement des adresses IPv4 <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>) n'avait jamais été annoncé publiquement sur l'Internet avant (comme on peut le voir sur RIPEstat <https://stat.ripe.net/widget/routing-history#w.resource=11.0.0.0%2F8>) ou, plus exactement, jamais été annoncé en dehors de quelques détournements ponctuels. Mais qui, en 2021, a encore un préfixe /8 non annoncé ? whois nous montre que c'est le DoD :

```
% whois 11.0.0.0
...
NetRange:       11.0.0.0 - 11.255.255.255
CIDR:           11.0.0.0/8
NetName:        DODIIS
NetType:        Direct Allocation
OriginAS:
Organization:   DoD Network Information Center (DNIC)
RegDate:        1984-01-19
Updated:        2007-08-22
...
OrgName:        DoD Network Information Center
```

(Pour la petite histoire, ce préfixe a été alloué au DoD en 1985, dans le RFC 943 ; oui, à l'époque, les RFC servaient de registres d'adresses IP.)

Tout de suite, on pense à un détournement des adresses IP de l'armée états-unienne par des Chinois/Russes/Cubains/Iraniens. D'autant plus que la date est curieuse : 16 :57 :35.081428 UTC, c'est moins de trois minutes avant la fin officielle du mandat de Trump, fin de mandat qui avait été marquée par plusieurs troubles graves. Et puis l'AS qui a fait les annonces, l'AS 8003, n'était pas tellement connu avant, appartenant à une entreprise très discrète <https://opencorporates.com/companies/us_fl/M20000009226> et sur laquelle les investigations n'ont pas révélé grand-chose, à part son association passée à des activités bizarres. (`whois AS8003` pour avoir les informations sur cet AS.)

Dans les jours et les semaines suivants, d'autres préfixes autrefois inutilisés ont été annoncés, par exemple le `7.0.0.0/8`.

Finalement, le Pentagone (via son service DDS <https://www.defense.gov/Explore/News/Article/Article/1858615/defense-digital-service-delivers-mission-aligned-tech-for-dod/>) a révélé que l'annonce était normale : il ne s'agit pas d'un détournement mais d'une opération légitime. Mais quels sont ses buts ? Pourquoi l'armée qui n'annonçait pas ses adresses IP depuis si longtemps (ce qui ne veut pas dire qu'elles n'étaient pas utilisées en interne) a-t-elle tout à coup changé sa politique ? Inutile de préciser qu'on ne saura de toute façon pas tout. Mais on peut toujours spéculer :

— Un tel volume d'adresses IP représente beaucoup d'argent en période de pénurie (le marché est entre 20 et 30 dollars par adresse),
— ou bien l'armée est en train de monter un pot de miel géant, pour attraper plein de trafic malveillant,
— certains administrateurs réseau ont été assez incompétents et imprudents pour utiliser ces préfixes d'adresses IP apparemment inutilisés pour numéroter leurs réseaux internes ; l'annoncer sur l'Internet permettrait de capter ce trafic interne (on dit que l'armée chinoise était dans ce cas),
— ou encore le but est vraiment de s'en servir, par exemple pour y héberger des services.

La possibilité d'une vente de ces adresses, et donc peut-être d'un test pour s'assurer qu'elles ne posaient pas de problèmes techniques, a été souvent mentionnée, vu le « trésor » d'adresses IP de l'armée. Mais relativisons : au cours actuel (mais qui baisserait si le DoD vendait d'un coup toutes ces adresses), cela ferait certes plusieurs centaines de millions de dollars mais c'est une goutte d'eau par rapport aux budgets militaires de ce pays. Et puis le GAO (la « Cour des Comptes ») avait noté dans un rapport de 2020 <https://www.gao.gov/assets/gao-20-402.pdf> les difficultés, notamment légales, à vendre ces adresses IP. Un rapport parlementaire <https://www.govinfo.gov/content/pkg/CRPT-116hrpt120/html/CRPT-116hrpt120-pt2.htm> estimait que la vente d'adresses IP par le DoD soulevait de nombreux problèmes et n'était pas forcément une solution viable.

Autre hypothèse, celle du pot de miel. C'est nettement plus vraisemblable : tout préfixe important annoncé sur l'Internet reçoit un « rayonnement de fond », l'"*Internet Background Radiation (IBR)*", et les nouveaux préfixes annoncés vont certainement attirer beaucoup de trafic, permettant des études qui intéressent certainement les services de cyberguerre.

Et, en parlant de cyberguerre, qu'en est-il de l'hypothèse d'un détournement délibéré du trafic des réseaux qui ont été assez stupides pour utiliser ces préfixes d'adresses IP ? Là, je ne vous étonnerai pas en vous disant que mes contacts au Pentagone sont muets et ne m'ont pas tenu informé :-)

Enfin, s'agissant de l'hébergement de services, ça reste possible mais l'annonce faite par une petite société inconnue et discrète ne plaide pas en ce sens. Notez que le très utile Shodan trouve déjà des machines connectées dans le préfixe `11.0.0.0/8`. (Attention si vous essayez de les pirater : le propriétaire n'a pas le sens de l'humour.) Ma préférée (mais rappelez-vous qu'il peut s'agir d'un pot de miel) est un routeur Ubiquiti annonçant comme nom `HACKED-ROUTER-HELP-SOS-HAD-DUPE-PASSWORD`.

Quelques lectures en plus :
— La meilleure source technique, qui a fait connaitre ce cas, l'article de Doug Madory <https://www.kentik.com/blog/the-mystery-of-as8003/>,
— une autre analyse technique est celle de Geoff Huston <https://www.potaroo.net/ispcol/2021-04/dodv4.html>,
— la dépêche Associated Press <https://apnews.com/article/technology-business-government-and-p avec notamment leurs recherches infructueuses concernant la société qui gère l'AS 8003, et ses possibles liens avec d'autres activités douteuses,
— l'article du Washington Post <https://www.washingtonpost.com/technology/2021/04/24/pentagon-internet-address-mystery/> contient également des informations sur la société Global Resources System (notez qu'il y en a deux, ayant la même adresse, une créée en 2006 <https://opencorporates.com/companies/us_fl/M06000001699> et une créée en 2020 <https://opencorporates.com/companies/us_fl/M20000009226>).