Du nouveau dans la (l'in)sécurité de l'Internet ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 janvier 2024

https://www.bortzmeyer.org/orange-espagne-bgp.html

Le 3 janvier 2024, une partie du trafic IP à destination de la filiale espagnole d'Orange n'a pas été transmis, en raison d'un problème BGP, le système dont dépend tout l'Internet. Une nouveauté, par rapport aux nombreux autres cas BGP du passé, est qu'il semble que le problème vienne du piratage d'un compte utilisé par Orange. Quelles leçons tirer de cette apparente nouveauté ?

D'abord, les faits. Le 3 janvier 2024, vers 14 :30 UTC, le trafic avec l'AS 12479 <https://apps.db.ripe.net/db-web-ui/lookup?source=ripe&key=AS12479&type=aut-num>, celui d'Orange Espagne chute brutalement. Cela se voit par exemple sur Radar, le tableau de bord <https://radar.cloudflare.com/traffic/as12479> de Cloudflare, recopié ici :

Pourquoi ? Le problème est lié à BGP, ce qui est logique puisque ce protocole de routage est la vraie infrastructure de l'Internet. C'est BGP qui permet à tous les routeurs de savoir par où envoyer les paquets IP. On voit l'augmentation importante du trafic BGP de cet AS sur RIPE stat <https://stat.ripe.net/ui2013/widget/bgp-update-activity#w.starttime=2023-12-22T07%3A00%3A00&w.endtime=2024-01-05T07%3A00%3A00&w.resource=AS12479> :

Mais il ne s'agit pas d'un détournement par le biais d'une annonce BGP mensongère comme on l'a vu de nombreuses fois <https://www.bortzmeyer.org/pakistan-pirate-youtube.html>. Ici, le problème était plus subtil. Si on regarde l'archive des annonces BGP à RouteViews <http://routeviews.org/>, on ne trouve pas une telle annonce « pirate ». Prenons le fichier d'annonces BGP https://archive.routeviews.org/route-views3/bgpdata/2024.01/UPDATES/updates.20240103.1400. (attention, il est gros) et convertissons les données (qui étaient au format MRT du RFC 6396 [1]), avec l'outil bgpdump <https://github.com/RIPE-NCC/bgpdump> : on trouve des retraits massifs d'annonces des préfixes d'Orange Espagne comme :

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: 01/03/24 14:13:17.792524
TYPE: BGP4MP_ET/MESSAGE/Update
FROM: 208.94.118.10 AS40630
TO: 128.223.51.108 AS6447
WITHDRAW
  85.50.0.0/22
  85.51.12.0/22
  85.53.56.0/22
  85.53.100.0/22
  85.54.36.0/22
...
```

Mais pas d'annonce usurpatrice. Le problème est très différent et semble venir d'un détournement d'un mécanisme de sécurité de BGP.

En effet, BGP est, par défaut, très vulnérable. N'importe quel routeur de la DFZ peut annoncer une route vers n'importe quel préfixe et ainsi capter du trafic (un grand classique <https://www.bortzmeyer.org/bgp-malaisie.html>, on l'a dit). Rassurez-vous, il existe plusieurs mécanismes de sécurité pour limiter ce risque. Mais comme rien n'est parfait en ce bas monde, ces mécanismes peuvent à leur tour créer des problèmes. En l'occurrence, le problème semble avoir été avec la RPKI. Ce système, normalisé dans le RFC 6480, permet de signer les ressources Internet, notamment les préfixes d'adresses IP (comme 85.50.0.0/22 et les autres cités plus haut). Un des objets que permet la RPKI est le ROA ("*Route Origination Authorization*", RFC 6482), qui déclare quel(s) AS peuvent être à l'origine d'une annonce d'un préfixe. Il y a normalement un ROA pour les préfixes d'Orange Espagne (il se voit, ainsi que sa validité, sur le service de Hurricane Electric <https://bgp.he.net/net/85.48.0.0/12>, ou bien sur RIPE stat <https://stat.ripe.net/ui2013/widget/prefix-routing-consistency#w.resource=85.48.0.0%2F12>). Mais, pendant le problème, ce ROA avait disparu, remplacé par un autre qui donnait comme origine l'AS 49581 <https://apps.db.ripe.net/db-web-ui/lookup?source=ripe&key=AS49581&type=aut-num> (qui, j'insiste sur ce point, est apparemment totalement innocent dans cette affaire et semble avoir été choisi au hasard). Les annonces BGP d'Orange Espagne étaient donc refusés par les routeurs validants, ce qui explique les retraits de route comme celui montré plus haut, d'où l'agitation BGP, et la chute du trafic, bien des routeurs ne sachant plus comment joindre les préfixes d'Orange Espagne.

S'agissait-il d'une erreur d'Orange ? Apparemment pas. Une personne identifiée comme « Ms_Snow_OwO » s'est vantée sur Twitter d'avoir provoqué le problème. Le message a depuis disparu mais voici une copie d'écran :

Notez aussi les copies d'écran envoyées par « Ms_Snow_OwO », montrant bien l'interface du RIPE-NCC avec les ressources (notamment les préfixes IP) d'Orange Espagne :

En Europe, la très grande majorité des opérateurs qui créent des ROA ne le font pas sur une machine à eux (ce que la RPKI permet, puisqu'elle est décentralisée) mais sous-traitent cette opération au RIR, le RIPE-NCC. L'opérateur se connecte à une interface Web, le "*LIR Portal*", s'authentifie et indique les préfixes qu'il veut voir signés. On voit donc qu'un maillon nécessaire à la sécurité est l'authentification sur le portail qui sert aux opérateurs Internet. Le RIPE-NCC permet une authentification à deux facteurs, via le protocole TOTP (normalisé dans le RFC 6238), mais ce n'est pas obligatoire (ça l'est devenu le 27 mars 2024, suite à ce problème) et, selon « Ms_Snow_OwO », le mot de passe était bien trop simple. L'attaquant a pu alors s'authentifier auprès du RIPE-NCC et changer le ROA, cassant ainsi le routage.

C'est un problème courant en sécurité : toute technique qui vise à empêcher l'accès aux méchants peut être détournée pour faire un déni de service. Ainsi, par exemple, si vous bloquez un compte au bout

de N tentatives d'accès infructueuses (une très mauvaise idée, mais qu'on voit parfois), il est trivial pour un attaquant de bloquer le compte, juste en tapant n'importe quel mot de passe. Ici, on peut s'indigner de ce qu'une technique anti-usurpation mène à un déni de service mais c'est un problème bien plus vaste que la RPKI.

Comme des informations ont montré que le mot de passe d'Orange Espagne était bien trop faible (juste « ripeadmin »), beaucoup de gens ont ricané, parfois bêtement, sur cette faiblesse. En fait, comme l'attaquant a apparemment utilisé un logiciel malveillant installé sur l'ordinateur d'un employé d'Orange Espagne, il aurait pu avoir le meilleur mot de passe du monde (« 45cf*b2b44cfA7[Caractère Unicode non montré [2]]f64cccç302617F! »), cela n'aurait rien changé. Plutôt que de se focaliser sur ce mot de passe, effectivement trop faible, il vaudrait mieux insister sur l'importance d'activer l'authentification à deux facteurs, comme le recommande le RIPE <https://www.ripe.net/publications/news/ripe-ncc-access-security-breach-investigation>.

Quelques lectures sur cette attaque, presque toutes en anglais car je n'ai rien trouvé en français :

— L'article de Lawrence Abrams sur BleepingComputer <https://www.bleepingcomputer.com/news/security/hacker-hijacks-orange-spain-ripe-account-to-cause-bgp-havoc/>, le plus détaillé,
— L'analyse de HudsonRock <https://www.infostealers.com/article/infostealer-infection-of-an>, montrant comment l'attaquant a obtenu le mot de passe (pas en devinant !),
— Sur Twitter, l'analyse en temps réel de bgp.tools <https://twitter.com/bgptools/status/1742596811196436940> (excellent service <https://bgp.tools/>, d'ailleurs),
— L'annonce d'Orange sur Twitter <https://twitter.com/orange_es/status/1742616775647265035> (en espagnol).
— Bon article de l'expert Doug Madory <https://nanog.org/stories/industry-news/digging-into-the->, avec notamment des détails sur les ROA vus (idem sur le blog de Kentik <https://www.kentik.com/blog/digging-into-the-orange-espana-hack/> et sur celui de l'APNIC <https://blog.apnic.net/2024/01/26/digging-into-the-orange-espana-hack/>),
— La synthèse de Benjojo <https://blog.benjojo.co.uk/post/rpki-signed-but-not-secure>.

2. Car trop difficile à faire afficher par LaTeX