Deuxième lien Internet pour la Corée du Nord, ça se voit où ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 octobre 2017. Dernière mise à jour le 4 octobre 2017

https://www.bortzmeyer.org/star-jv-transtelecom.html

Le premier octobre 2017, le site d'information spécialisé dans la Corée du Nord, 38 North <http://www.38north.org>, a publié un excellent article <http://www.38north.org/2017/10/mwilliams100117/> sur la deuxième connexion Internet de la Corée du Nord. Où peut-on vérifier ce genre d'informations ?

L'article <http://www.38north.org/2017/10/mwilliams100117/> est un bon exemple d'OSINT (ou de ROSO ?), ne s'appuyant que sur des sources publiques, et sur l'analyse des experts de Dyn research <http://research.dyn.com/> (l'ancien Renesys, qui a publié son propre article <https://dyn.com/blog/north-korea-gets-new-internet-link-via-russia/>, une lecture très recommandée). Mais, sur le sujet de la Corée du Nord, la propagande tourne à plein régime et énormément d'informations fausses sont diffusées, d'autant plus que la dictature délirante de Kim Jong-un ne permet pas de vérifications sur place. Si les "*fake news*" ne sont pas une nouveauté (le mensonge est aussi ancien que le langage), le caractère assez technique de l'information (« la Corée du Nord a désormais un deuxième lien Internet, via la Russie ») rend les vérifications plus difficiles, pour les gens non spécialisés.

Donc, l'article de 38 North <http://www.38north.org> dit qu'un opérateur Internet russe connecte désormais la RDPC, qui n'était auparavant connectée que par la Chine. Vu le caractère…spécial de la Corée du Nord, cette connexion n'est pas une pure affaire de business et a sans doute nécessité une approbation par Moscou. Comment la vérifier ?

Car c'est tout l'intérêt de l'OSINT : le but n'est pas uniquement de faire gagner du temps aux espions (au prix d'une certaine perte de "*glamour*" : lire le Wikipédia russophone est moins spectaculaire que de pénétrer dans une chambre forte au Kremlin, après avoir séduit une belle espionne russe). L'intérêt politique de l'OSINT est de permettre des vérifications indépendantes : si on n'est pas sûr de l'information, on peut refaire une partie du travail pour la recouper.

Donc, première chose, récolter quelques informations techniques. Quelles sont les adresses IP de l'(unique) opérateur Internet nord-coréen ? On peut le savoir en partant des serveurs de noms de leur TLD, `.kp` :

```
% dig NS kp

; <<>> DiG 9.10.3-P4-Debian <<>> NS kp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44497
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;kp. IN NS

;; ANSWER SECTION:
kp. 429731 IN NS ns3.kptc.kp.
kp. 429731 IN NS ns1.kptc.kp.
kp. 429731 IN NS ns2.kptc.kp.

;; ADDITIONAL SECTION:
ns1.kptc.kp. 429731 IN A 175.45.176.15
ns2.kptc.kp. 429731 IN A 175.45.176.16

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Oct 03 11:53:28 CEST 2017
;; MSG SIZE  rcvd: 122
```

Un petit coup de whois pour vérifier :

```
% whois 175.45.176.15
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '175.45.176.0 - 175.45.179.255'

% Abuse contact for '175.45.176.0 - 175.45.179.255' is 'postmaster@star-co.net.kp'

inetnum:        175.45.176.0 - 175.45.179.255
netname:        STAR-KP
descr:          Ryugyong-dong
descr:          Potong-gang District
country:        KP
org:            ORG-SJVC1-AP
admin-c:        SJVC1-AP
tech-c:         SJVC1-AP
status:         ALLOCATED PORTABLE
mnt-by:         APNIC-HM
mnt-lower:      MAINT-STAR-KP
mnt-routes:     MAINT-STAR-KP
...
organisation:   ORG-SJVC1-AP
org-name:       Star Joint Venture Co. Ltd.
country:        KP
address:        Ryugyong-dong
address:        Potong-gang District
phone:          +850-2-3812321
fax-no:         +850-2-3812100
e-mail:         postmaster@star-co.net.kp
...
```

OK, on a bien trouvé Star JV, l'opérateur coréen. Quel est son numéro d'AS ? Il existe plein de moyens de le trouver, à partir de la base APNIC mais, ayant l'habitude du DNS, j'utilise le service DNS de RouteViews <http://www.routeviews.org/> :

```
%  dig +short TXT 0.176.45.175.aspath.routeviews.org
"54728 6939 701 4837 131279" "175.45.176.0" "24"
```

Il nous apprend que le préfixe `175.45.176.0/24` est annoncé par l'AS 131279 (rappelez-vous que les chemins d'AS se lisent de droite à gauche). Le second AS (rappelez-vous que les chemins d'AS se lisent de droite à gauche), 4837, est celui du fournisseur chinois habituel, China Unicom.

L'article de 38 North dit que cela a changé le dimanche 1 octobre. En effet, l'excellent service RIPE stat <https://stat.ripe.net/>, quand on l'interroge sur le routage de `175.45.176.0/24`, confirme une activité importante :

(Vous pouvez aussi regarder sur le site original <https://stat.ripe.net/widget/bgp-update-activity#w.starttime=2017-09-19T08%3A00%3A00&w.endtime=2017-10-03T08%3A00%3A00&w.resource=175.45.176.0%2F24>.) Cette activité indique qu'un changement a eu lieu, puis s'est propagé par BGP à tout l'Internet, déclenchant en cascade d'autres changements. (Les tables BGP sont publiques, l'Internet est très ouvert. Exercice : cherchez les autres préfixes annoncés par Star JV.)

Bon, en quoi consistait cette nouveauté BGP du dimanche matin ? On va se tourner vers le service de RouteViews <http://www.routeviews.org/> qui archive les annonces BGP et les met ensuite à la disposition du public. Les fichiers sont au format MRT (RFC 6396 [1]), qui s'analyse avec le programme bgpdump <https://bitbucket.org/ripencc/bgpdump/wiki/Home>. Et on connait l'heure approximative de l'annonce (dans l'article de 38 North et grâce à RIPE stat) donc on peut télécharger le bon fichier (il change tous les quarts d'heure, regardez le nom de fichier, au format YYYYMMDD) :

```
% wget http://archive.routeviews.org/bgpdata/2017.10/UPDATES/updates.20171001.0900.bz2
% bunzip2 updates.20171001.0900.bz2
% bgpdump updates.20171001.0900 > updates.20171001.0900.txt
2017-10-03 11:22:24 [info] logging to syslog
%
```

On charge le `updates.20171001.0900.txt` dans un éditeur, on cherche "131279" (l'AS de Star JV) et on trouve l'annonce cherchée :

```
TIME: 10/01/17 09:07:51
TYPE: BGP4MP/MESSAGE/Update
FROM: 202.73.40.45 AS18106
TO: 128.223.51.102 AS6447
ORIGIN: INCOMPLETE
ASPATH: 18106 20485 131279
NEXT_HOP: 202.73.40.45
COMMUNITY: 4635:2000
ANNOUNCE
  175.45.176.0/24
  175.45.178.0/24
  175.45.179.0/24
```

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

Ici, l'annonce BGP émise par 131279 est transmise à l'AS 20485, le nouveau transitaire de Star JV. Qui est-il ?

```
% whois AS20485
% This is the RIPE Database query service.
...
aut-num:        AS20485
as-name:        TRANSTELECOM
org:            ORG-CJSC19-RIPE
descr:          Moscow, Russia
...
organisation:   ORG-CJSC19-RIPE
org-name:       Closed Joint Stock Company TransTeleCom
org-type:       LIR
address:        Testovskayia str., 8 , enterance 3
address:        123317
address:        Moscow
address:        RUSSIAN FEDERATION
phone:          +74957846670
fax-no:         +74957846671
...
```

Il s'agit donc bien d'un russe, TransTelecom.

Maintenant, est-ce que cet opérateur russe est vraiment utilisé ? Certes, il reçoit les annonces BGP des Nord-Coréens et les relaie (c'est ainsi qu'elles sont reçues par RouteViews). Mais, comme disent les opérateurs réseaux, « "*The data plane does not always follow the control plane*" », ce qui veut dire que les paquets ne passent pas forcément par le chemin des AS qui ont relayé l'annonce. Testons depuis TransTelecom, grâce aux sondes RIPE Atlas <https://atlas.ripe.net>, en utilisant le programme atlas-traceroute <https://labs.ripe.net/Members/stephane_bortzmeyer/using-ripe-atlas-to-debug-n
On demande à trois sondes dans l'AS de TransTelecom d'aller visiter 175.45.176.15 :

```
% atlas-traceroute --format --as 20485 --requested 3 175.45.176.15

Measurement #9412526 Traceroute 175.45.176.15 from AS #20485 uses 3 probes

3 probes reported
Test #9412526 done at 2017-10-03T10:08:23Z
From:  79.140.108.66    20485    TRANSTELECOM Moscow, Russia, RU
Source address:  79.140.108.66
Probe ID:  1257
1    79.140.108.65    20485    TRANSTELECOM Moscow, Russia, RU    [8.027, 1.63, 1.634]
2    217.150.57.50    20485    TRANSTELECOM Moscow, Russia, RU    [5.27, 5.079, 5.072]
3    212.73.250.154    3356    LEVEL3 - Level 3 Communications, Inc., US    [30.465, 30.464, 31.473]
4    ['*', '*', '*']
5    ['*', '*', '*']
6    204.255.173.53    701    UUNET - MCI Communications Services, Inc. d/b/a Verizon Business, US    [132.
7    ['*', '*', '*']
8    152.63.114.26    701    UUNET - MCI Communications Services, Inc. d/b/a Verizon Business, US    [205.82
9    ['*', '*', '*']
10    219.158.101.197    4837    CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN    [380.779, 380.674,
11    219.158.3.130    4837    CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN    [385.401, 385.712, 38
12    ['*', '*', '*']
13    219.158.39.42    4837    CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN    [268.096, '*', '*']
...
```

(Vous pouvez aussi regarder une représentation graphique <https://atlas.ripe.net/measurements/9412526/#!tracemon> de cette mesure.) Et on voit bien que, même depuis TransTelecom, fournisseur de connectivité de Star JV, le trafic n'est pas envoyé via le pont de l'Amitié, mais à un opérateur

états-unien, Level 3, qui transmettra ensuite à China Unicom. (Exercice : faites pareil depuis d'autres AS, comme 18106, pour voir qu'ils envoient bien à TransTelecom - ils ont bien reçu l'annonce BGP - mais que celui-ci ne transmet pas ensuite directement aux Coréens.) Le lien tout neuf n'est donc pas utilisé pour l'instant. Ceci dit, la situation change régulièrement. Le 4 octobre, il n'y avait plus qu'un seul préfixe annoncé via TransTelecom, le `175.45.178.0/24` et lui est bien routé directement vers Star JV :

```
% atlas-traceroute --format --as 20485 --requested 3 --proto icmp 175.45.178.1

Measurement #9675151 Traceroute 175.45.178.1 from AS #20485 uses 3 probes

3 probes reported
Test #9675151 done at 2017-10-04T12:21:50Z
From:  79.140.108.66    15774    TTK-RTL Retail, RU
Source address:  79.140.108.66
Probe ID:  1257
1    79.140.108.65    15774    TTK-RTL Retail, RU    [8.441, 1.936, 1.936]
2    217.150.57.50    20485    TRANSTELECOM Moscow, Russia, RU    [5.432, 5.497, 5.441]
3    ['*', '*', '*']
4    188.43.225.153    20485    TRANSTELECOM Moscow, Russia, RU    [131.737, 132.065, 131.744]
5    ['*', '*', '*']
6    175.45.178.1    131279    STAR-KP Ryugyong-dong, KP    [130.062, 130.123, 129.827]
...
```

[Version graphique disponible en ligne <`https://atlas.ripe.net/measurements/9675151/#!tracemon`>. Notez l'utilisation du protocole ICMP, UDP étant bloqué quelque part.] Si votre FAI reçoit l'annonce via TransTelecom, vous pouvez aussi faire un traceroute depuis chez vous (ici depuis Free) (`188.43.225.153` est TransTelecom) :

```
% traceroute -I 175.45.178.1
traceroute to 175.45.178.1 (175.45.178.1), 30 hops max, 60 byte packets
...
 4  rke75-1-v900.intf.nra.proxad.net (78.254.255.42)  40.085 ms  40.079 ms  40.078 ms
 5  cev75-1-v902.intf.nra.proxad.net (78.254.255.46)  40.070 ms  40.083 ms  40.084 ms
 6  p16-6k-1-po12.intf.nra.proxad.net (78.254.255.50)  40.043 ms  25.274 ms  25.259 ms
 7  bzn-crs16-1-be1024.intf.routers.proxad.net (212.27.56.149)  29.072 ms  23.159 ms  16.617 ms
 8  194.149.165.206 (194.149.165.206)  31.358 ms  31.041 ms  31.054 ms
 9  * * *
10  tenge10-1.br01.frf06.pccwbtn.net (63.218.232.41)  30.996 ms  30.990 ms  32.615 ms
11  63-218-233-6.static.pccwglobal.net (63.218.233.6)  32.616 ms  34.156 ms  34.162 ms
12  * * *
13  188.43.225.153 (188.43.225.153)  191.185 ms  191.210 ms  180.775 ms
14  * * *
15  175.45.178.1 (175.45.178.1)  185.670 ms  185.680 ms  186.084 ms
```

Peut-être le lien vers TransTelecom est-il un lien de secours, prévu pour faire face à d'éventuelles sanctions chinoises ? Ou peut-être tout simplement le nouveau lien est en cours de configuration et que la situation n'est pas tout à fait stable ?

Notez que, si les tables et les annonces BGP sont publiques (ainsi que l'utilisation des sondes RIPE Atlas), la capacité <`https://www.bortzmeyer.org/capacite.html`> est bien plus difficile à connaitre et des affirmations comme quoi le nouveau lien représenterait « 60 % de la capacité Internet nord-coréenne » (dans cet article <`http://www.businessinsider.fr/us/north-korea-internet-transtelecom-cy`>) sont probablement de la pure spéculation.

Merci à Dyn pour des explications supplémentaires.

`https://www.bortzmeyer.org/star-jv-transtelecom.html`