A2B Internet

Moving to default Routeserver IRR filtering …

Moving to a more secure peering via the IXP routeservers …

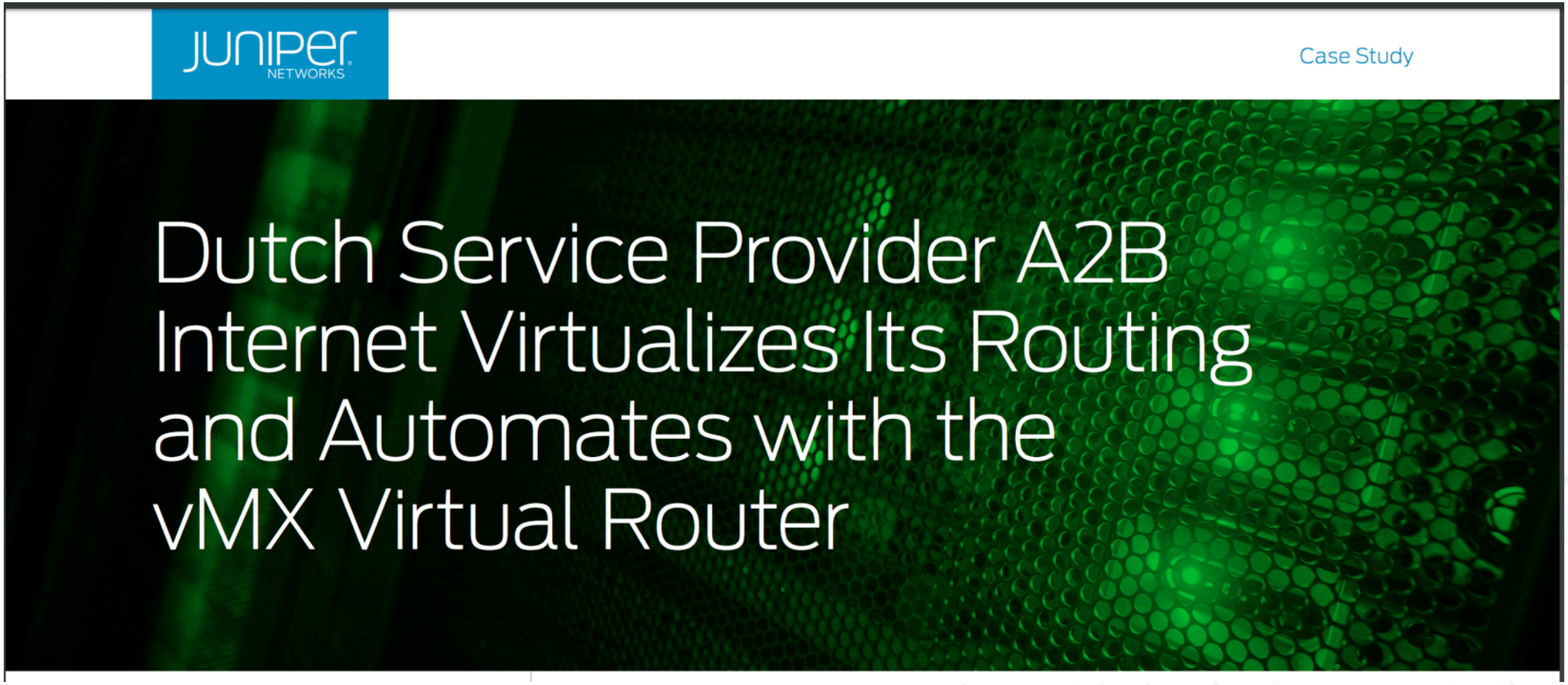
Short intro

- A2B Internet is a Dutch network provider.
  - Providing datacenter connectivity and internet access on fiber.

- We implemented the Juniper Networks vMX solution recently
  - http://newsroom.juniper.net/press-releases/a2b-internet-deploys-juniper-networks-vmx-as-the-first-virtual-network-function--nyse-jnpr-11g134000-001

- New kit, means new things to try out … ;-)

New kit to play with …



Current status is a mix and match

- Some IXP's are still offering a no-filter policy… by default
- Some IXP's are offering IRR based filtering by default and RPKI optional..
- Overview on your local IXP status : https://peering.exposed/
  - The IXP Spreadsheet is maintained by Job Snijders (NTT) & Samer Abdel-Hafez (Netflix)

Let’s seek community agreement on:

- The new default for IXP routeservers should be based on IRR data minimal … and RPKI valid data ..

- There should be a normalized configured max-prefixes per peer (into the Route Server)
- Delete small prefixes .. (0.0.0.0/0 prefix-length-range /25-/32 reject) (after IRR check)
- No Default Accept (0.0.0.0/0 exact)
- No Private ASn’s. Such as (as-path private 64512-65534) and ..
  - as-path private 4200000000 – 4294967294 (https://tools.ietf.org/html/rfc6996)

- RPKI Strict … meaning .. Drop RPKI invalid announcements … especially via the routeservers …

Verifying your peers info

- All most of the data is already public ...
  - ./peeringdb.sh 51088

```
Network AS51088
name: A2B Internet
info_prefixes4: 100
info_prefixes6: 25
ipaddr4: 80.249.208.209
ipaddr6: 2001:7f8:1::a505:1088:1
```

- This info comes directly from the peeringdb.net API

What can you do on your side ?

- Do some basic filtering on every peer that you have .. For both v4 and v6 …
- Keep the filtering generic, but effective …
- At minimum … use max-prefix filters … and
  - no-small-prefixes
  - no-private-asn
  - No-Known-Transit-ASN-in-Path

Apply simple filters yourself … (1)

- Juniper Networks syntax :

- as-path no-transit-import-in ".* (174|209|701|702|1239|1299|2914|3257|3320|3356|3549|3561|4134|5511|6453|6461|6762|7018) .*";

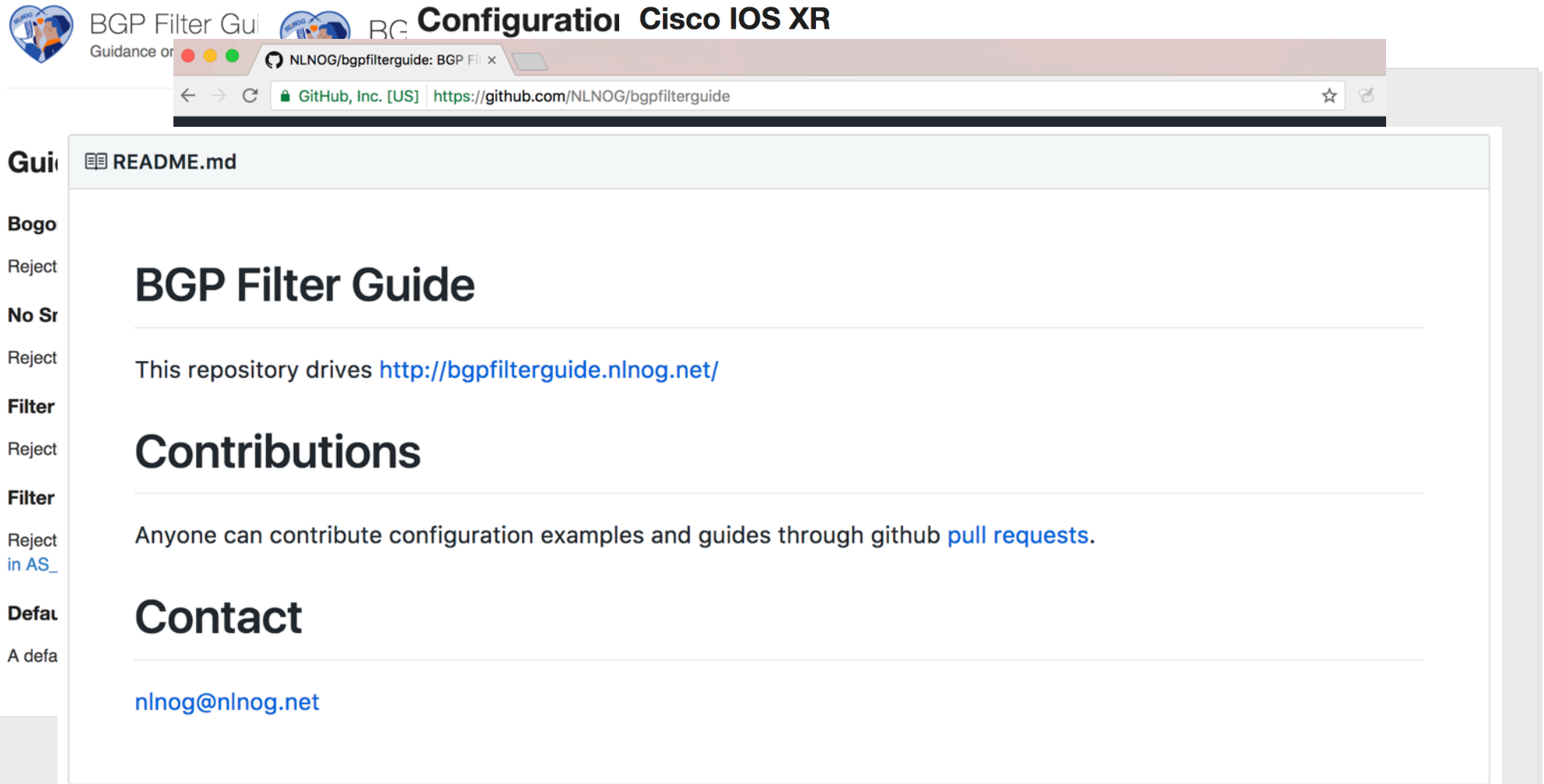
- as-path-group bogon-asns {
- as-path zero ".* 0 .*";
- as-path as_trans ".* 23456 .*";
- as-path reserved1 ".* [64496-131071] .*";
- as-path reserved2 ".* [4200000000-4294967295] .*"; }

- 0.0.0.0/0 prefix-length-range /25-/32 reject

Apply simple filters yourself … (2)

- Juniper Networks syntax :
- as-path too-many-hops ".{100,}";
- community delete own-community members ”<your ASN> : *";
  - term *delete-own-community* {
  - then community delete own-community ;

https://BGPFilterGuide.NLNOG.NET



A2B Internet

Verifying the no-transit catch … (32 hidden entries)

```
inet.0: 630929 destinations, 967236 routes (630926 active, 1 holddown, 32 hidden)
  Prefix   Nexthop       MED     Lclpref    AS path
  37.18.122.0/23          80.249.212.148                  58291 174 42755 58272 I
  62.93.195.0/24          80.249.208.212                  13237 200093 1299 174 20756 I
  81.24.160.0/20          80.249.212.81                   15704 12321 3356 6739 20973 24799 I
  81.85.218.0/24          80.249.208.189      201         20562 24753 3356 5511 15808 38056 I
  89.105.216.0/23         80.249.213.35                   206676 24875 24875 174 174 21159 21159 I
  91.204.76.0/22          80.249.211.147                  197426 3257 2914 202786 I
  125.253.143.0/24        80.249.208.189      201         20562 24753 3257 4134 4809 38056 I
  145.90.8.0/24           80.249.208.200      25          12859 1140 1140 6461 10886 1972 1133 I
  206.202.0.0/18          80.249.211.147                  197426 3257 174 393545 I
  213.195.64.0/19         80.249.212.81                   15704 12321 3356 174 15915 I
```

A2B Internet

Proper peer filtering

- Resulting in peer - leak protection :

```
inet.0: 630829 destinations, 967198 routes (630822 active, 5 holddown, 36 hidden)
  Prefix   Nexthop       MED     Lclpref    AS path
  81.85.218.0/24          80.249.208.189       201                20562 24753 3356 5511 15808 38056 I
  125.253.143.0/24        80.249.208.189       201                20562 24753 3257 4134 4809 38056 I
```

- Even if it is intentional leaking …

More specifics in sight ..

```
213.137.128.0/21   *[BGP/170] 2w4d 17:13:44, MED 0, localpref 140
                      AS path: 6774 I, validation-state: unverified
                    > to 80.249.209.76 via xe-0/0/2.602
                    [BGP/170] 2w6d 14:02:40, MED 0, localpref 100
                      AS path: 6774 I, validation-state: unverified
                    > to 80.249.208.87 via xe-0/0/2.602
213.137.134.0/24   *[BGP/170] 2w4d 17:13:44, MED 0, localpref 140
                      AS path: 6774 I, validation-state: unverified
                    > to 80.249.209.76 via xe-0/0/2.602
                    [BGP/170] 2w6d 14:02:40, MED 0, localpref 100
                      AS path: 6774 I, validation-state: unverified
                    > to 80.249.208.87 via xe-0/0/2.602
213.137.135.0/28   *[BGP/170] 2w4d 17:08:09, MED 0, localpref 140
                      AS path: 6774 I, validation-state: unverified
                    > to 80.249.209.76 via xe-0/0/2.602
213.137.135.16/28  *[BGP/170] 2w4d 17:09:34, MED 0, localpref 140
                      AS path: 6774 I, validation-state: unverified
                    > to 80.249.209.76 via xe-0/0/2.602
```

Strict peering …

- You could create per peer route filters …

- cmd: bgpq3 -EJ AS1200 -R 24
  Output :

```
policy-options {
 policy-statement NN {
replace:
  from {
    route-filter 80.249.208.0/21 upto /24;
    route-filter 91.200.16.0/22 upto /24;
    route-filter 185.55.136.0/22 upto /24;
    route-filter 195.69.144.0/22 upto /24;
  }
 }
}
```

Strict peering … Pro's and cons

- It is a lot more 'work' if you don't automate this …
- Especially if you only update the peers, if they notify you …
- But it is not the holy grale … because sometimes you still get weird stuff.. Some peers even create /30 route objects …
- Just because they can …

Accept or drop on matching Route Object ?

- So if you see a match on a route object but it is a small prefix..
  - Let’s say a /28 .. But with a valid Route Object in one of the DB’s ..
  - Accept or drop ?

IRR filter sanitized ??

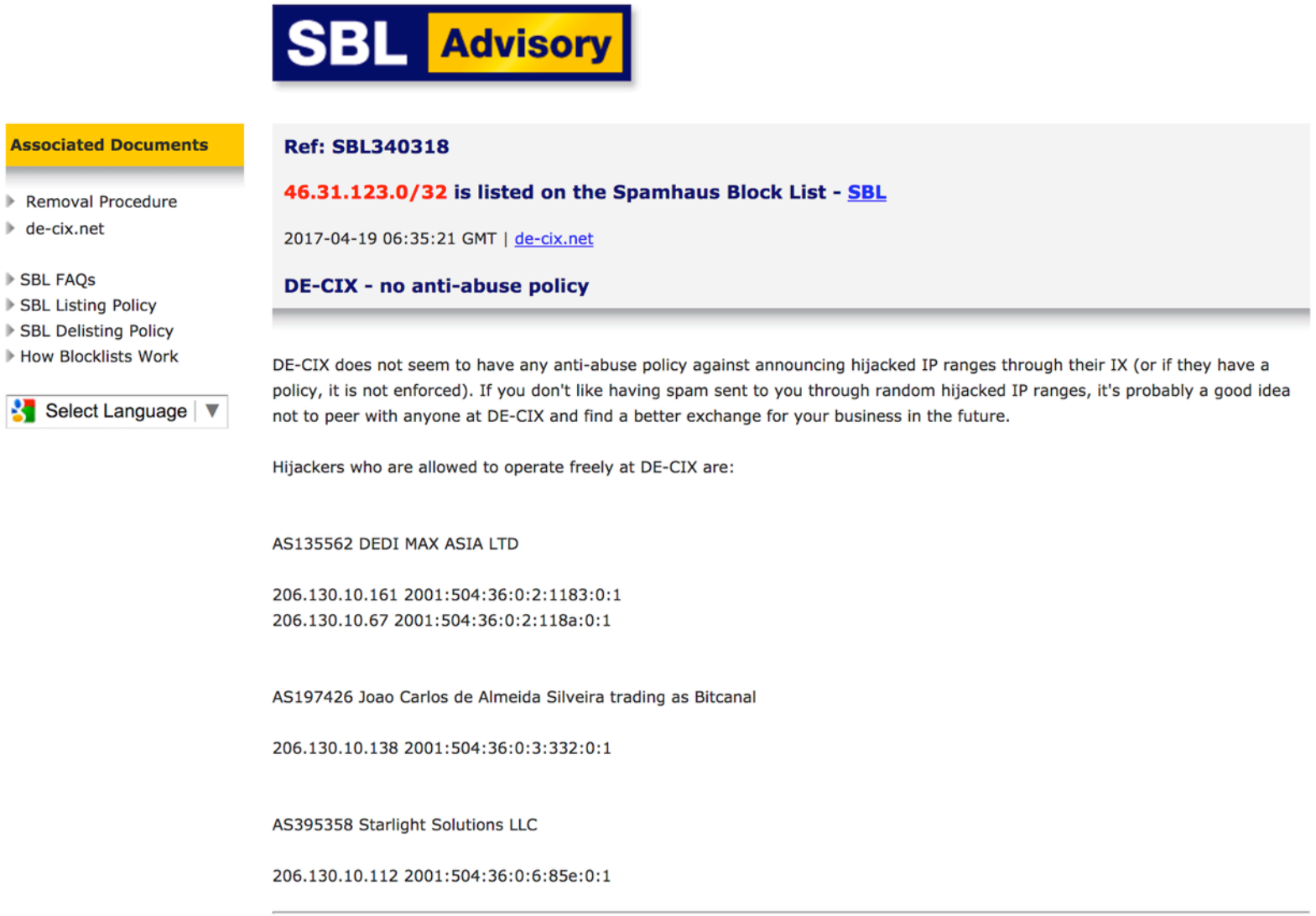
bgpq3 -R 24 -EJ AS-AMS-IX-RS | grep "/30"

route-filter 1.55.48.0/30 exact;
route-filter 41.181.72.112/30 exact;
route-filter 61.213.191.8/30 exact;
route-filter 173.192.67.144/30 exact;

route-filter 210.18.22.0/30 exact;
route-filter 223.118.2.24/30 exact;
route-filter 223.118.2.28/30 exact;

/32‘s … /29‘s …
Etc etc …

We should do better …



SBL Advisory

Associated Documents

- Removal Procedure
- de-cix.net

- SBL FAQs
- SBL Listing Policy
- SBL Delisting Policy
- How Blocklists Work

Select Language

Ref: SBL340318

46.31.123.0/32 is listed on the Spamhaus Block List - SBL

2017-04-19 06:35:21 GMT | de-cix.net

DE-CIX - no anti-abuse policy

DE-CIX does not seem to have any anti-abuse policy against announcing hijacked IP ranges through their IX (or if they have a policy, it is not enforced). If you don't like having spam sent to you through random hijacked IP ranges, it's probably a good idea not to peer with anyone at DE-CIX and find a better exchange for your business in the future.

Hijackers who are allowed to operate freely at DE-CIX are:

AS135562 DEDI MAX ASIA LTD

206.130.10.161 2001:504:36:0:2:1183:0:1
206.130.10.67 2001:504:36:0:2:118a:0:1

AS197426 Joao Carlos de Almeida Silveira trading as Bitcanal

206.130.10.138 2001:504:36:0:3:332:0:1

AS395358 Starlight Solutions LLC

206.130.10.112 2001:504:36:0:6:85e:0:1

bgpstream
@bgpstream

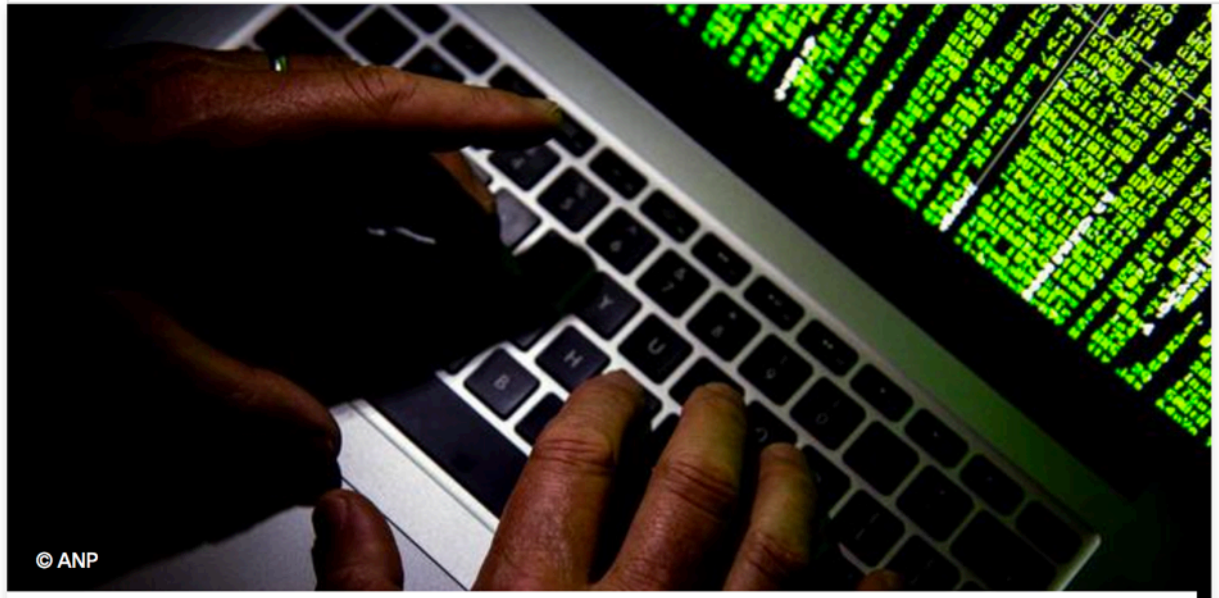
BGP,HJ,hijacke
104.37.44.0/2
unknown, bgp

8:03 PM - 13 May 2016

BANEN DIGITALE KRANT SERVICE WI

Nieuws Cultuur & Leven **deVolkskrant**

Tech



IP-adressen ministerie gekaapt door Bulgaren

IP-adressen van het ministerie van Buitenlandse Zaken zijn vorig jaar in handen gekomen van Bulgaarse criminelen. Tussen 19 november en 26 november 2014 had een Bulgaarse bende Nederlandse overheidsadressen in bezit.

Door: Huib Modderkolk 25 juli 2015, 02:00

...

the conduct

Following

26615
ular S.A.,-,By
Security,
62

A2B Internet

The new IXP Routeserver Default Policy

- By default :
  - IRR-data as the absolute minimal default filter
  - No default accept ..
  - Filter on private (Bogon) AS'n, RFC1918 and small (more-specific) prefixes
  - Max-prefix limit per peer (ingress) !!
  - Filter known transit AS's ingress per peer into the RS. (avoiding table leaking..)
  - Filter all RPKI invalid announcements (especially via the route servers!)
  - Filter on small prefixes, after accepting on IRR data filter

- Lock down "outed" spam/hijack operating AS's with fixed (manual) ingress filters, if you intent to keep taking their money …

Questions?

Or by email to: ebais@a2b-internet.com

A2B Internet