Basics - Routing Security

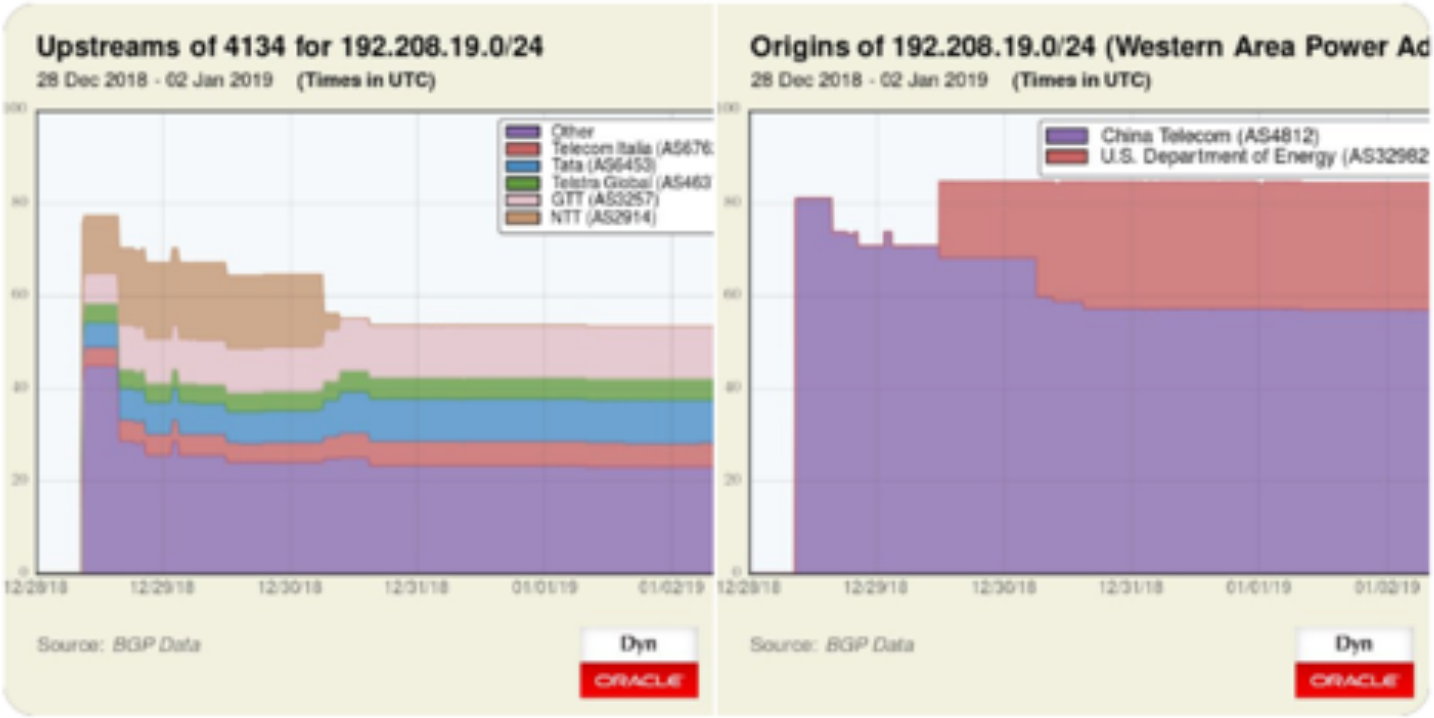
You must filter your peers.

InternetIntelligence
@InternetIntel

Following

Replying to @InternetIntel @bad_packets

China Telecom hijack of US Dept of Energy route continuing into 6th day. Both entities are presently announcing the same Dept of Energy prefix (192.208.19.0/24).

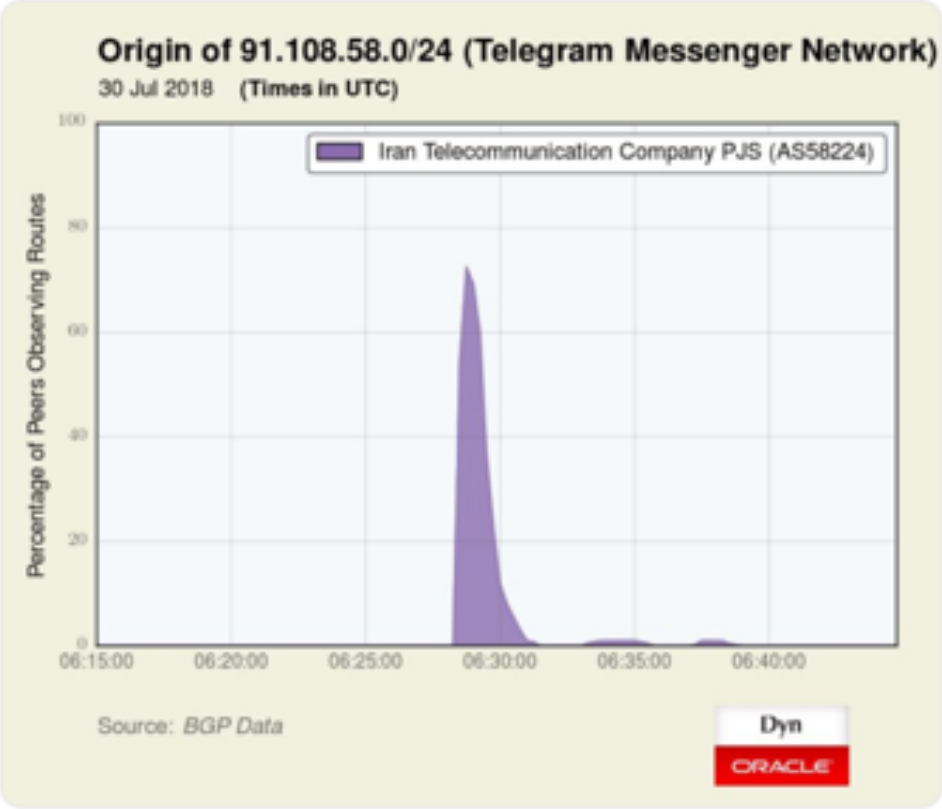


6:11 AM - 2 Jan 2019

InternetIntelligence
@InternetIntel

Follow

At 06:28 UTC earlier today (30-Jul), an Iranian state telecom network briefly leaked over 100 prefixes. Most were Iranian networks, but the leak also included 10 prefixes of popular messaging app @telegram (8 were more-specifics).



7:45 AM - 30 Jul 2018

Basics - Routing Security

- Routing security is important in two directions:
  - The routes you receive
  - The routes you announce

- Starting with the routes you receive...

Basics - Routing Security

- Most networks won't/don't filter their peers.
- This is negligent behavior
- The routes you receive should be filtered in three ways:
  - Prefix Count
  - AS-Path
  - Prefix list

http://routing.he.net

HURRICANE ELECTRIC
INTERNET SERVICES

Submit

OUTE FILTERING HOME ALGORITHM

AS13335

ASN	STATUS	PEERINGDB_IRR	EXTRACTED_V4	EXTRACTED_V6	OK_V4	OK_V6	SOURCE
13335	explicit	AS-CLOUDFLARE			AS-CLOUDFLARE	AS-CLOUDFLARE	peeringdb

ILTERS

AF	AS-SET NAME	IRR STATUS	IRR BUILT	IRR LINES	PREFIXES RECEIVED	FILTER BUILT	FILTER LINES	POLICY	REASONS	FILTE
4	AS-CLOUDFLARE	good	October 18 2018 13:18:53	1203	522	October 19 2018 13:18:44	522	DISPLAY	DISPLAY	DISPLA
6	AS-CLOUDFLARE	good	October 18 2018 13:19:08	553	108	October 19 2018 13:18:47	108	DISPLAY	DISPLAY	DISPLA

REFIX LISTS

AF	ROUTER	NAME	STATUS	CHECKED	EXISTING_LINES	VERIFIED	EXISTING	DELTA	LOG
4	core1.ams1.he.net	prefix-filter-as13335	verified	July 02 2018 15:23:00	522	July 02 2018 15:23:01	DISPLAY	DISPLAY	DISPLA

HURRICANE ELECTRIC
INTERNET SERVICES

Submit

ROUTE FILTERING HOME ALGORITHM

AS13335

ASN	STATUS	PEERINGDB_IRR	EXTRACTED_V4	EXTRACTED_V6	OK_V4	OK_V6	SOURCE
13335	explicit	AS-CLOUDFLARE			AS-CLOUDFLARE	AS-CLOUDFLARE	peeringdb

FILTERS

AF	AS-SET NAME	IRR STATUS	IRR BUILT	IRR LINES	PREFIXES RECEIVED	FILTER BUILT	FILTER LINES	POLICY	REASONS	FILTER
4	AS-CLOUDFLARE	good	October 18 2018 13:18:53	1203	522	October 19 2018 13:18:44	522	DISPLAY	DISPLAY	DISPLAY
6	AS-CLOUDFLARE	good	October 18 2018 13:19:08	553	108	October 19 2018 13:18:47	108	DISPLAY	DISPLAY	DISPLAY

PREFIX LISTS

AF	ROUTER	NAME	STATUS	CHECKED	EXISTING_LINES	VERIFIED	EXISTING	DELTA	LOG
4	core1.ams1.he.net	prefix-filter-as13335	verified	July 02 2018 15:23:00	522	July 02 2018 15:23:01	DISPLAY	DISPLAY	DISPLAY

HURRICANE ELECTRIC
INTERNET SERVICES

Submit

ROUTE FILTERING HOME ALGORITHM

AS13335

ASN	STATUS	PEERINGDB_IRR	EXTRACTED_V4	EXTRACTED_V6	OK_V4	OK_V6	SOURCE
13335	explicit	AS-CLOUDFLARE			AS-CLOUDFLARE	AS-CLOUDFLARE	peeringdb

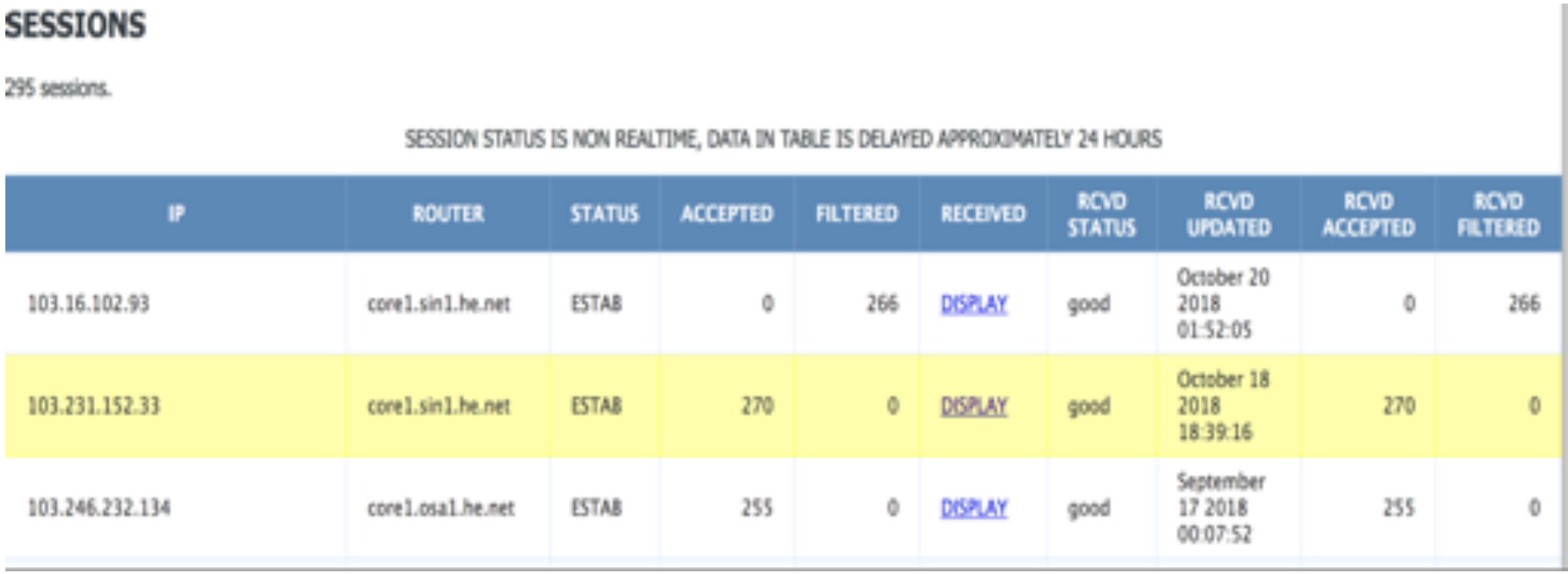
FILTERS

AF	AS-SET NAME	IRR STATUS	IRR BUILT	IRR LINES	PREFIXES RECEIVED	FILTER BUILT	FILTER LINES	POLICY	REASONS	FILTER
4	AS-CLOUDFLARE	good	October 18 2018 13:18:53	1203	522	October 19 2018 13:18:44	522	DISPLAY	DISPLAY	DISPLAY
6	AS-CLOUDFLARE	good	October 18 2018 13:19:08	553	108	October 19 2018 13:18:47	108	DISPLAY	DISPLAY	DISPLAY

PREFIX LISTS

AF	ROUTER	NAME	STATUS	CHECKED	EXISTING_LINES	VERIFIED	EXISTING	DELTA	LOG
4	core1.ams1.he.net	prefix-filter-as13335	verified	July 02 2018 15:23:00	522	July 02 2018 15:23:01	DISPLAY	DISPLAY	DISPLAY

http://routing.he.net



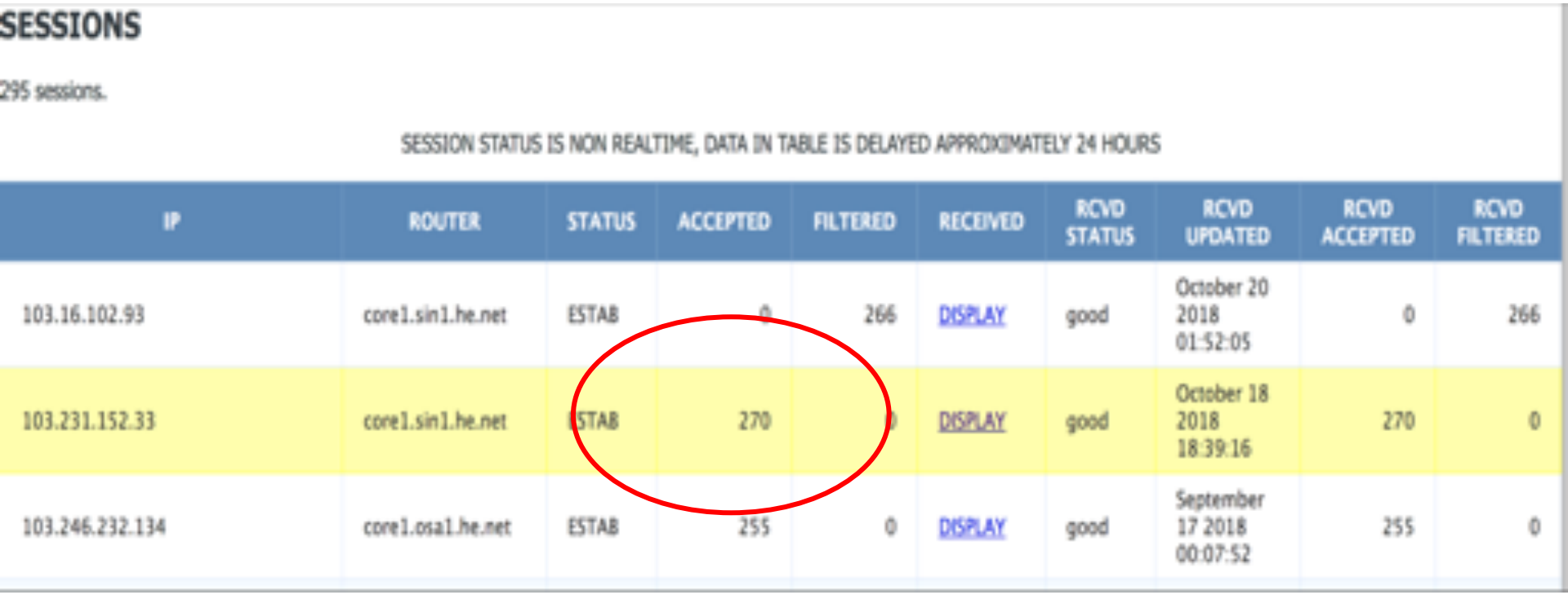
SESSIONS

295 sessions.

SESSION STATUS IS NON REALTIME, DATA IN TABLE IS DELAYED APPROXIMATELY 24 HOURS

IP	ROUTER	STATUS	ACCEPTED	FILTERED	RECEIVED	RCVD STATUS	RCVD UPDATED	RCVD ACCEPTED	RCVD FILTERED
103.16.102.93	core1.sin1.he.net	ESTAB	0	266	DISPLAY	good	October 20 2018 01:52:05	0	266
103.231.152.33	core1.sin1.he.net	ESTAB	270	0	DISPLAY	good	October 18 2018 18:39:16	270	0
103.246.232.134	core1.osa1.he.net	ESTAB	255	0	DISPLAY	good	September 17 2018 00:07:52	255	0

http://routing.he.net



SESSIONS

295 sessions.

SESSION STATUS IS NON REALTIME, DATA IN TABLE IS DELAYED APPROXIMATELY 24 HOURS

IP	ROUTER	STATUS	ACCEPTED	FILTERED	RECEIVED	RCVD STATUS	RCVD UPDATED	RCVD ACCEPTED	RCVD FILTERED
103.16.102.93	core1.sin1.he.net	ESTAB	0	266	DISPLAY	good	October 20 2018 01:52:05	0	266
103.231.152.33	core1.sin1.he.net	ESTAB	270	0	DISPLAY	good	October 18 2018 18:39:16	270	0
103.246.232.134	core1.osa1.he.net	ESTAB	255	0	DISPLAY	good	September 17 2018 00:07:52	255	0

```
SSH@core1.ams1.he.net>terminal length 0
sh ip bgp nei 185.1.32.22 received-routes
       There are 262 received routes from neighbor 185.1.32.22
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      1.0.0.0/24          185.1.32.22                100        0      ME
         AS_PATH: 13335
2      1.1.1.0/24          185.1.32.22                100        0      ME
         AS_PATH: 13335
3      23.227.63.0/24      185.1.32.22                100        0      ME
         AS_PATH: 13335
4      64.68.192.0/24      185.1.32.22                100        0      ME
         AS_PATH: 13335
5      66.235.200.0/24     185.1.32.22                100        0      EF
         AS_PATH: 13335
6      104.16.0.0/12       185.1.32.22                100        0      ME
         AS_PATH: 13335
7      104.16.0.0/20       185.1.32.22                100        0      ME
```

```
SSH@core1.ams1.he.net>terminal length 0
sh ip bgp nei 185.1.32.22 received-routes
       There are 262 received routes from neighbor 185.1.32.22
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      1.0.0.0/24          185.1.32.22                100        0      ME
         AS_PATH: 13335
2      1.1.1.0/24          185.1.32.22                100        0      ME
         AS_PATH: 13335
3      23.227.63.0/24      185.1.32.22                100        0      ME
         AS_PATH: 13335
4      64.68.192.0/24      185.1.32.22                100        0      ME
         AS_PATH: 13335
5      66.235.200.0/24     185.1.32.22                100        0      EF
         AS_PATH: 13335
6      104.16.0.0/12       185.1.32.22                100        0      ME
         AS_PATH: 13335
7      104.16.0.0/20       185.1.32.22                100        0      ME
```

```
Toms-MacBook-Pro-38:Downloads tom$ whois -h whois.radb.net 66.235.200.0
route:      66.235.200.0/24
descr:      CMI  (Customer Route)
origin:     AS38082
mnt-by:     MAINT-AS58453
changed:    qas_support@cmi.chinamobile.com 20180906
source:     RADB

route:      66.235.200.0/24
descr:      CMI IP Transit
origin:     AS38082
admin-c:    MAINT-CMI-INT-HK
tech-c:     MAINT-CMI-INT-HK
mnt-by:     MAINT-CMI-INT-HK
changed:    qas_support@cmi.chinamobile.com 20180906
source:     NTTCOM
```

Hurricane Electric Route Filtering Algorithm

- Read more here
- http://routing.he.net/algorithm.html

- Example:
- xx.7.224.0/24,rejected,does not strictly match IRR policy or RIR handles
- xx.10.254.0/23,accepted,strictly matched IRR policy
- xx.17.248.0/24,accepted,strictly matched IRR policy
- xx.26.36.0/22,rejected,does not strictly match IRR policy or RIR handles
- xx.26.39.0/24,rejected,does not strictly match IRR policy or RIR handles

Hurricane Electric Route Filtering

- Please check and update your IRR or RIR handles

- Check your routing here:
- http://routing.he.net/

- We at now filtering ~90% of all our peers
- Rolling it out slowly over the last six months

Resources

- Seattle SIX
- Tom Paseka tom@cloudflare.com
- BGP.HE.NET
- https://bgpmon.net/
- https://twitter.com/InternetIntel
- DYN

HURRICANE ELECTRIC
INTERNET SERVICES

Thanks!

Walt Wollny, Director Interconnection Strategy
Hurricane Electric AS6939
walt@he.net