Routing Hijack - Bangladesh

Presented By:
Simon Sohel Baroi
FGL
Network Means - Problem
Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking,” is when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that a server or network is their client. This routes traffic to the wrong network operator, when another real route is available.

Example: The 2008 YouTube hijack; an attempt to block YouTube through route hijacking led to much of the traffic to YouTube being dropped around the world.

Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).
Routing Incidents are increasing (Vodafone Idea AS55410 Hijack)

Vodafone Idea (AS55410) started originating 31,000+ routes which don’t belong to them.

Prefixes belonged to Google, Microsoft, Akamai, Cloudflare, Fastly, and many others were affected.

https://www.manrs.org/2021/04/a-major-bgp-hijack-by-as55410-vodafone-idea-ltd/

https://twitter.com/DougMadory/status/1383138595112955909
Routing Incidents Cause Real World Problems

MyEtherWallet DNS Hijacked, $150,000 Worth of Eth Stolen

How Pakistan Hijacked YouTube offline (and how it never happens again)

Global Impacts of Routing Incidents

BGP routing security flaw caused Amazon Route 53 Incident

The Vast World of Fraudulent Routing

Large scale BGP hijack out of India

Routing Leak briefly takes down Google

Massive route leak causes Internet slowdown

UK traffic diverted through Ukraine

DDoS Attacks Storm Linode Servers Worldwide
# Routing Incidents (South Asia) May ~ June 2021

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event Details</th>
<th>Prefixes affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Hijack</td>
<td>Expected Origin: AS45609 BHARTI-MOBILITY-AS-AP Bharti Airtel Ltd&lt;br&gt;Detected Origin: ASN 45069 CNNIC-CTTSDNET-AP China Tietong Shandong net, CN</td>
<td>106.193.255.0/24</td>
</tr>
<tr>
<td>BGP Leak</td>
<td>Origin AS: AS 4797 Wipro Spectramind Services Pvt Ltd, IN&lt;br&gt;Leaker AS: AS4775 GLOBE-TELECOM-AS Globe Telecoms, PH&lt;br&gt;Leaked to: AS 4637 (ASN-TELSTRA-GLOBAL Telstra Global, HK)</td>
<td>112.198.30.0/24</td>
</tr>
<tr>
<td>BGP Hijack</td>
<td>Expected Origin: AS328608 Africa-on-Cloud-AS, ZA&lt;br&gt;Detected Origin: ASN 139879 GALAXY-AS-AP Galaxy Broadband, PK</td>
<td>156.241.0.0/16</td>
</tr>
<tr>
<td>BGP Hijack</td>
<td>Expected Origin: AS7018 ATT-INTERNET4, US&lt;br&gt;Detected Origin: ASN18229 CTRLS-AS-IN CtrlS Datacenters Ltd., IN</td>
<td>172.0.0.0/12</td>
</tr>
<tr>
<td>BGP Hijack</td>
<td>Expected Origin: AS33567 TELECOM-LESOTHO, LS&lt;br&gt;Detected Origin: ASN 55410 (VIL-AS-AP Vodafone Idea Ltd, IN)</td>
<td>41.203.176.0/20</td>
</tr>
<tr>
<td>BGP Leak</td>
<td>Origin AS: AS 132497 DIGITAL NETWORK ASSOCIATES, IN&lt;br&gt;Leaker AS:AS 55644 Vodafone Idea Ltd, IN (AS 55644)&lt;br&gt;Leaked to: AS3356 (LEVEL3, US)</td>
<td>103.245.69.0/24</td>
</tr>
</tbody>
</table>

Source: bgpstream.com
Lets’ Begin
AS9230
Bangladesh Online Ltd.
6th Aug, 2022 – Early Morning, NOC Found abnormalities from some clients. Some of them can’t access Google, or some random sites.

▪ The Clients are from a specific prefix
▪ They thought it’s a problem with the upstream.
▪ It might be routing issue
▪ They checked with the looking glass, found everything good.

Around 11 AM they found:
The prefix **202.84.36.0/24** is announced from Singtel AS 7473.
AS9230
Bangladesh Online Ltd.

The prefix **202.84.36.0/24** is announced from Singtel AS 7473.

- ROA Check – Found OK
- IRR Check – Found OK.
Observation from different Looking glass:

route-views.isc.routeviews.org> sh ip bgp 202.84.36.0/24 be
BGP routing table entry for 202.84.36.0/24
Paths: (5 available, best #4, table default)
   Not advertised to any peer
      19151 6461 7473
         198.32.176.164 from 198.32.176.164 (66.186.193.17)
           Origin IGP, metric 5, valid, external, best (AS Path)
           Last update: Tue Jul 26 11:43:49 2022

route-views.isc.routeviews.org>
-----------------------------------------------------------------

route-views.optus.net.au>sh ip bgp 202.84.36.0/24
BGP routing table entry for 202.84.36.0/24, version 1440601472
Paths: (2 available, best #2, table default)
   Not advertised to any peer
      7474 7473
            Origin IGP, localpref 100, valid, external, best
            Community: 7474:1202 7474:1222 7474:1403 7474:1527

route-views.optus.net.au>
AS9230
202.84.36.0/24

Observation from APNIC Portal:

Routing Status (202.84.36.0/24)

At **2022-08-06 00:00:00 UTC**, **202.84.36.0/24** was **99% visible** (by **381** of **385** RIS full peers).

First ever seen announced by AS9230, on **2001-07-20 16:00:00 UTC**.

Multi-origin prefix:
- **AS7473** - RPKI Status: 😞
- **AS9230** - RPKI Status: 😊
  - Route objects: **APNIC** and **RADB**
AS9230
202.84.36.0/24

Observation from HE Portal:

<table>
<thead>
<tr>
<th>Origin AS</th>
<th>Announcement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS9230</td>
<td>202.84.36.0/24</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>AS7473</td>
<td>202.84.36.0/24</td>
<td>Internet Service Provider</td>
</tr>
</tbody>
</table>
AS9230
202.84.36.0/24

Observation from RIPE Portal:
What to do now?
Coordination Started:

- First mail to g-stixnoc@singtel.com on 6-Aug-2022, 12:36PM local time
Coordination:

- 1\textsuperscript{st} mail to \texttt{g-stixnec@singtel.com} on 6-Aug-2022, 12:36PM local time
- 2\textsuperscript{nd} mail to \texttt{lxxxxxx@singtel.com}, cc: \texttt{g-stixnec@singtel.com} and \texttt{helpdesk@apnic.net} on 6-Aug-2022, 2:04 PM local time
- 3\textsuperscript{rd} mail to Singtel (included some more concern of Singtel) on 10 Aug-2022, 4:14PM

1\textsuperscript{st} Response from Singtel, Asking \textbf{SingTel circuit ID} for further process.
Coordination:

2nd Response from Singtel, Asking SingTel circuit ID for further process.

Global Customer Support Centre

We will check internally on your below concern.

Thank you!

Best Regards,

Singtel
Technical Assistance Centre (TAC) - Service Desk
Global Delivery - Singtel Enterprise Business
Singapore Telecommunications Limited
Dear Asim,

Thank you for your email and query.

If you find an incorrect advertisement issue of your IP address prefix by the AS7473, you are welcome to contact the network administrator of AS7473 to report the issue for their further check.

You can find their contact detail, email address and phone number, by querying the AS7473 in the APNIC Whois database below:

https://wq.apnic.net/apnic-bin/whois.pl

Regards,
Twitter and Linked-in:

Kazi Akramul Haque • 1st
IT Professional | CSO, BOL | Experienced in ISP

SingTel
STIXNOC
ST-IX
SingTel-IX
IP Network
Internet Community
IP Transit

SingTel team, please stop the unauthorized announcement of the prefix 202.84.36.0/24 from the ASN 7473, we are trying to reach you on your phone but no luck.
ASN 9230 is the only authorized to originate the prefix 202.84.36.0/24.

Foyyal Kayum • @foysal_kayum • 10 Aug

#SingTel
#STIXNOC
#ST-IX
#SingTel-IX
Internet Community
IP Transit

Please stop the unauthorized announcement of the prefix 202.84.36.0/24 from the ASN 7473, ASN 9230 is the only authorized to originate the prefix 202.84.36.0/24.
Final Result:

Problem solved from 11-Aug-2022
The ISP noticed it at around 7:00AM
<table>
<thead>
<tr>
<th>Saturday</th>
<th>Sunday</th>
<th>Monday</th>
<th>Tuesday National Day of Singapore (Holiday)</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Holiday in Singapore</td>
<td>- Holiday in Singapore</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix Hijacked</td>
<td>- Started Coordinating</td>
<td>Email + Phone</td>
<td>Email + Phone</td>
<td>Email + Phone</td>
<td>Requested through LinkedIn &amp; Twitter</td>
<td>Problem Solved</td>
<td>Surprise !!!</td>
</tr>
</tbody>
</table>
What is the Solution?
## MANRS Actions for Network Operators

<table>
<thead>
<tr>
<th>Action 1: Filtering</th>
<th>Action 2: Anti-spoofing</th>
<th>Action 3: Coordination</th>
<th>Action 4: Global Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent propagation of incorrect routing information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement filters (Inbound/Outbound) on eBGP sessions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent propagation of incorrect routing information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent traffic with spoofed source IP addresses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block traffic with spoofed source addresses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCP 38 / Unicast reverse path forwarding on interfaces</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilitate global operational communication and coordination between network operators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication between network operators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PeeringDB, route/AS objects, NOC contact details up to date</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilitate validation of routing information on a global scale</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation of routing information (IRR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Route origination authorization (ROA) and validation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Blue shading = Mandatory Action

MANRS Implementation Guide [https://www.manrs.org/isps/bcop/](https://www.manrs.org/isps/bcop/)
Why and Who will join MANRS -

CTO / CEO / network engineers !!!!
MANRS Observatory

Provide a factual state of security and resilience of the Internet routing system and track it over time

Measurements are:

- **Transparent** – using publicly accessible data
- **Passive** – no cooperation from networks required
- **Evolving** – MANRS community decide what gets measured and how
Architecture of the System
Operator Basis Report (May 2022)

MANRS Readiness

- **Filtering**: 90% (−11%)
- **Anti-spoofing**: 100%
- **Coordination**: 100% (0.0% →)
- **Global Validation IRR**: 100% (0.0% →)
- **Global Validation RPKI**: 100% (0.0% →)

Color Legend:
- Ready
- Aspiring
- Lagging
- No Data Available
Historical Incidents Data:

History

May 2021 - May 2022

Incidents

Culprits

Routing completeness (IRR)

Routing completeness (RPKI)
Incidents:

Start Date: 05-04-2022 12:25:00   End Date: 05-04-2022 12:35:00   Duration: 10m, 0s

M2C (GRIP) - Route hijack by a direct customer

Absolute: 0.5   Normalized: 90%   Incident Count: 1

<table>
<thead>
<tr>
<th>Incident Id</th>
<th>Start Time</th>
<th>End Time</th>
<th>Duration</th>
<th>Prefix</th>
<th>Paths</th>
<th>Weight</th>
<th>Source</th>
<th>Source event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2022-04-05 06:25:00</td>
<td>2022-04-05 06:35:00</td>
<td>10m, 0s</td>
<td>103.177.75.0/24</td>
<td>328474 328333 6939 132602 10075 135597</td>
<td>1</td>
<td>grip</td>
<td>moas-164913900-135597</td>
</tr>
</tbody>
</table>

Paths:

- 328474 328333 6939 132602 10075 135597
- 37468 6939 132602 10075 135597
**MANRS Conformance Report**

2022/05/01 - 2022/05/31

<table>
<thead>
<tr>
<th>MANRS Readiness Scores</th>
<th>Non-Compliance Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filtering: 90% ↓</td>
<td>AS Route Misoriginations (GRIP): 1</td>
</tr>
<tr>
<td>Anti-Spoofing: 100%</td>
<td></td>
</tr>
<tr>
<td>Coordination: 100%</td>
<td></td>
</tr>
<tr>
<td>Global Validation IRR: 100%</td>
<td></td>
</tr>
<tr>
<td>Global Validation RPKI: 100%</td>
<td></td>
</tr>
</tbody>
</table>

ASN: XXXXXXXXXXXX
Learnings:

▪ Drop the Invalids.
▪ Update Whois data periodically.
▪ Make sure the Call is picked by real person not by any Call Center or IVR.
▪ Incident/Abuse ticketing should be done for any kind of report ( internal/external ).
▪ Inform the Community about the Incident.
▪ Build secondary cordination channel/community like, MANRS, NOG.
One more thing...
Dear Team,

Please advise if you are still getting an issue on this.
Kindly provide your circuit ID so we can further check.
As of now, we checked from NTT and Singtel looking glass the subnet is no longer advertised from 7473

Have you done any changes from your end?

BGP routing table entry for 202.84.36.0/24
Versions:
  Process   dRIB/RIB   SendFlVer
  Speaker    336782605  336782605
Last Modified: Aug 12 06:25:28.715 for 1d04h
Paths: (6 available, best #4)
  Advertised IPv4 Unicast paths to update-groups (with more than one peer):
    0.2 0.3 0.4 0.14
  Advertised IPv4 Unicast paths to peers (in unique update groups):
    198.64.4.112  4.68.62.129
  Path #1: Received by speaker 0
    Not advertised to any peer
    9498 9498 17494 9230
    116.51.31.54 from 116.51.31.54 (203.101.88.34)
    Origin IGP, localpref 120, valid, external, group-best
    Received Path ID 0, Local Path ID 0, version 0
    Origin-AS validity: valid
  Path #2: Received by speaker 0
    Not advertised to any peer
    9498 9498 17494 9230, (received-only)
Thank You and also thanks to BOL Online

Acknowledgement:
Asim Bapari, Senior Manager, BOL Online,
Indra Raj Basnet, MANRS Fellow
Muhammad Yasir Shamim, MANRS Fellow