RPKI vs Social Engineering Attack

Security Routing SIG – 10 Feb 2026

Sanjaya – APNIC
Carlos Martinez – LACNIC

Overview

- The incident
- Investigations
- Findings
- Resolution
- Lessons learned

The incident

- LACNIC helpdesk received complaints about email messages not being delivered
- Part of address space assigned to LACNIC was hijacked by a rogue AS
  - Advertised by spoofing LACNIC’s AS
  - Transited through the rogue AS’s upstream

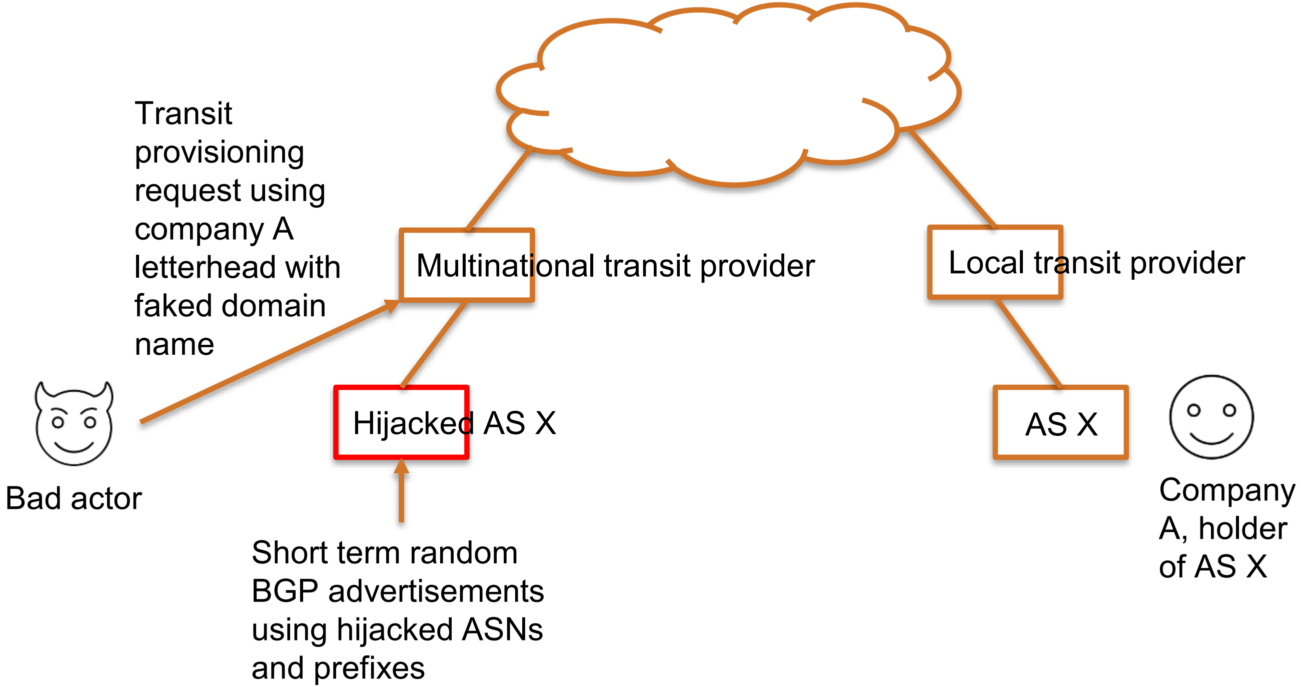
Investigation (LACNIC)

- LACNIC's space was hijacked intermittently
  - 9 July at 19:47 (GMT-3) for 20 minutes
  - 10 July at 20:34 (GMT-3) for 15 minutes
  - 12 July at 10:13 (GMT-3) for 5 minutes
  - No further events occurred
- The rogue AS has been involved in repeated hijacking events affecting address space in AFRINIC, ARIN, LACNIC and APNIC

Investigation (APNIC)

- LACNIC escalated the incident to APNIC
- APNIC contacted APJII/IDNIC (the Indonesian ISP association and National Internet Registry) to investigate and stop the hijacking activities
- Key finding:
  - The hijack wasn’t done by the rogue ASN’s owner. It was done by a bad actor that hijacked the ASN and managed to convince a multinational transit provider to propagate the hijacked prefixes

Findings

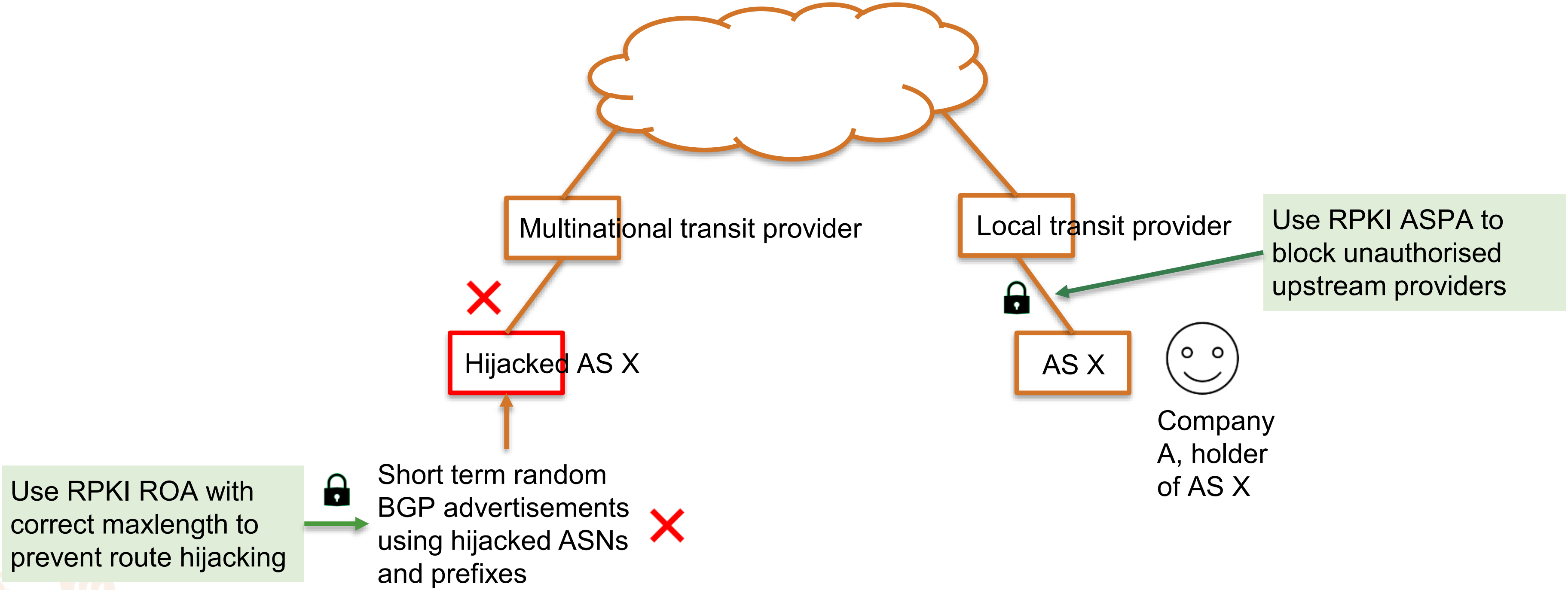


Transit provisioning request using company A letterhead with faked domain name
Multinational transit provider
Local transit provider
Hijacked AS X
AS X
Bad actor
Company A, holder of AS X
Short term random BGP advertisements using hijacked ASNs and prefixes

Resolution

- The multinational transit provider terminated the service to the bad actor upon receiving report from the hijacked ASN holder
- A final investigation and resolution report submitted by APJII/IDNIC and the hijacked ASN owner and shared with APNIC and LACNIC. They agreed to use this incident as a case study in routing security discussions

Lessons Learned



Multinational transit provider

Local transit provider

Use RPKI ASPA to block unauthorised upstream providers

Hijacked AS X

AS X

Company A, holder of AS X

Use RPKI ROA with correct maxlength to prevent route hijacking

Short term random BGP advertisements using hijacked ASNs and prefixes

2026 APRICOT APNIC 61

JAKARTA, INDONESIA
4 – 12 February 2026

#apricot2026