Enhanced AS-Loop Detection for BGP

draft-chen-grow-enhanced-as-loop-detection-00

Huainan Chen, China Telecom

Yunan Gu, Shunwan Zhuang, Huawei

Mar. 25, 2019
Forge AS Path Example

More forged AS paths by BackConnect

Source: https://www.nanog.org/sites/default/files/20161016_Madory_Backconnect_S_Suspicious_Bgp_v2.pdf
BGP Route Hijack and Motivation

• RFC7908
  • BGP Route Leaks Type 5: Prefix Re-origination with Data Path to Legitimate Origin

• Inbound policy for as-loop detection:
  • RFC4271, 9.1.2. Phase 2: Route Selection: “...If the AS_PATH attribute of a BGP route contains an AS loop, the BGP route should be excluded from the Phase 2 decision function...”

• Outbound policy for as-loop detection
  • Split-Horizon: Split-Horizon for EBGP is an optional function that a BGP sender will not advertise any routes that were previously received from that same AS.

• Due to misconfigurations or malicious attack, upon the detection of as loop, the current inbound/outbound check may cause:
  • Failure of route reception from certain AS
  • Failure of route advertisement to certain AS
Inbound policy enhancement

• A route advertised from AS300 to AS200
  • AS200 is added in AS-PATH by AS300 incorrectly
• Without enhancement
  • AS200 simply drops the route received from AS300
• AS200 Inbound Enhancement with AS-PATH analysis
  • ROA (already done)
  • Check local AS relationship database (with neighboring ASes)
• After enhancement
  • AS200 identifies possible hijacks

AS-Loop-Detecting at this point
Discard AS-Loop Routes directly that contains AS200

\[
\text{v}
\]
\[
x.y.z.0/24 \text{ Origin AS 600}
\]
\[
\text{AS100---AS200---AS300-----AS400-----AS500------AS600}
\]
Normal Case:
\[
\text{v}
\]
\[
x.y.z.0/24, \text{ AS-Path: 300 400 500 600}
\]
Forged Case 1:
\[
\text{v}
\]
\[
x.y.z.0/24, \text{ AS-Path: 300 200}
\]
\[
\text{Or: 300 400 200 etc.}
\]
Forged Case 2:
\[
\text{v}
\]
\[
x.y.z.0/24, \text{ AS-Path: 300 200 600}
\]
\[
\text{Or: 300 200 500 600 etc.}
\]
Outbound policy enhancement

• A route advertised from AS300 to AS200
  • AS200 is added in AS-PATH by AS300 incorrectly

• Without enhancement
  • AS300 simply drops the route to be advertised to AS200

• AS300 Outbound enhancement with AS-PATH analysis
  • Check local AS relationship database (with neighboring ASes)

• After enhancement
  • AS300 identifies possible hijacks
Summary

• Next step
  • Rename the “result type”
  • Identify “suggested actions” for each “result type”