SIDROPS Working Group
Internet-Draft
Intended status: Informational
Expires: 10 November 2025

Q. Li
Y. Chen
K. Xu
Z. Liu
J. Wu
Tsinghua University

9 May 2025

Risk of Stealthy BGP Hijacking under Incomplete Adoption of Route Origin Validation (ROV)
draft-li-sidrops-stealthy-hijacking-00

Abstract

This document describes how incomplete adoption of Route Origin Validation (ROV) makes certain forms of BGP hijacking less visible on the control plane while still capable of diverting traffic. We explain the underlying mechanism, define the form of the threat, analyze an real-world incident that exemplifies the issue, and discuss potential countermeasures to mitigate its impact.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 10 November 2025.

Copyright Notice

Table of Contents

1. Introduction

BGP hijacking occurs when an Autonomous System (AS), accidentally or maliciously, mis-announces an address prefix it is not authorized to originate. ASes that accept such announcement may divert traffic destined for the prefix to an incorrect AS instead of the actual prefix holder. To mitigate this risk, Route Origin Validation (ROV) [RFC6811] was introduced as part of the Resource Public Key Infrastructure (RPKI) [RFC6480]. ROV-enabled ASes validate route announcements using Route Origin Authorizations (ROAs) [RFC9582], which specify which ASes are permitted to originate specfic prefixes. The best current practice [RFC7115] suggests configuring routing policies to drop or give a very low preference to routes deemed invalid by ROV.

However, ROV adoption across the Internet is incomplete and expected to remain so for the foreseeable future. In such a state, invalid announcements may still propagate through non-ROV ASes to a certain extent, before being dropped by ROV-enabled ASes. This limited propagation creates a situation where some ASes never receive the invalid routes and are therefore unware of the ongoing incident (e.g., potential BGP hijacking). Yet they are not fully protected either, as the traffic they originate, along the data forwarding path, may traverse a non-ROV AS that has accepted the invalid route. This non-ROV AS will forward traffic towards the incorrect origin AS.

As a result, the traffic originating ASes unknowingly fall victim to BGP hijacking, unless they conduct active measurements (e.g., traceroute) or receive alerts from other network operators who spot the incident. In effect, BGP hijacking becomes stealthier in this case, due to incomplete adoption of ROV across global ASes.

The objective of this document is to highlight the side effect of incomplete ROV adoption on BGP hijacking, which results in highly stealthy BGP hijacking that is invisible to victims on the control plane. This document defines this form of BGP hijacking, explains its underlying mechanisms, analyzes a real-world incident, and discusses possible detection and mitigation approaches.

The rest of this document is structured as follows: Section 2 details the side effect of ROV in incomplete adoption. Section 3 defines the resulting stealthy BGP hijacking. Section 4 analyzes a representative real-world incident. Section 5 discusses potential detection and mitigation strategies. Finally, Section 6 concludes the document.

2. Side Effect of Incomplete ROV Adoption

This section explains how BGP hijacking can still succeed and even become stealthier under incomplete ROV adoption. Figure 1 illustrates the control-plane behavior when a malicious AS initiates a BGP hijacking attempt. In this scenario, AS G (the hijacker) announces a (sub-)prefix legitimately owned by AS E (the target). ROV-enabled ASes B and D filter out the invalid announcement, so only AS C and F may accept the hijacker's route into their routing tables, depending on their routing policies.

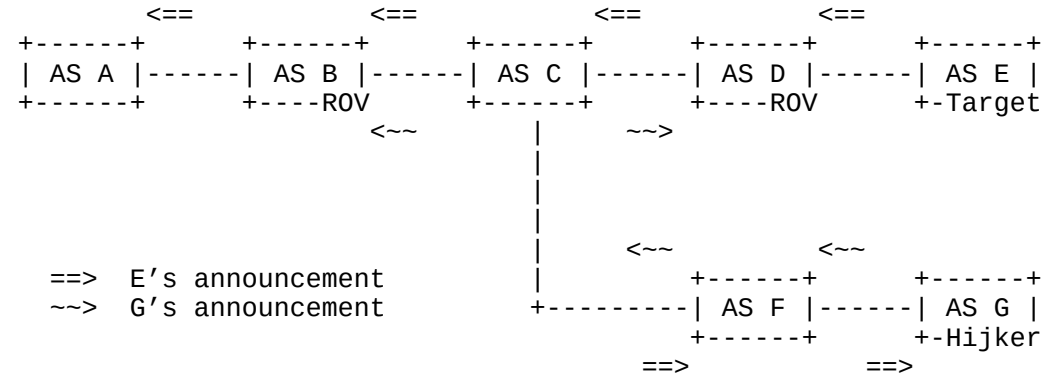

Figure 1: BGP hijacking under incomplete ROV adoption

Consider AS A as an example. AS A only receives a route to the legitimate origin (AS E), since its upstream provider AS B rejects the invalid route. As a result, from AS A's control-plane perspective, the only available route is valid, and one can expect traffic destined for the target to be correctly delivered. However, as shown in Figure 2, from a global perspective, AS A's traffic is forwarded through AS C, which accpets the hijacker's route. In this case, the traffic is silently redirected to the hijacker.

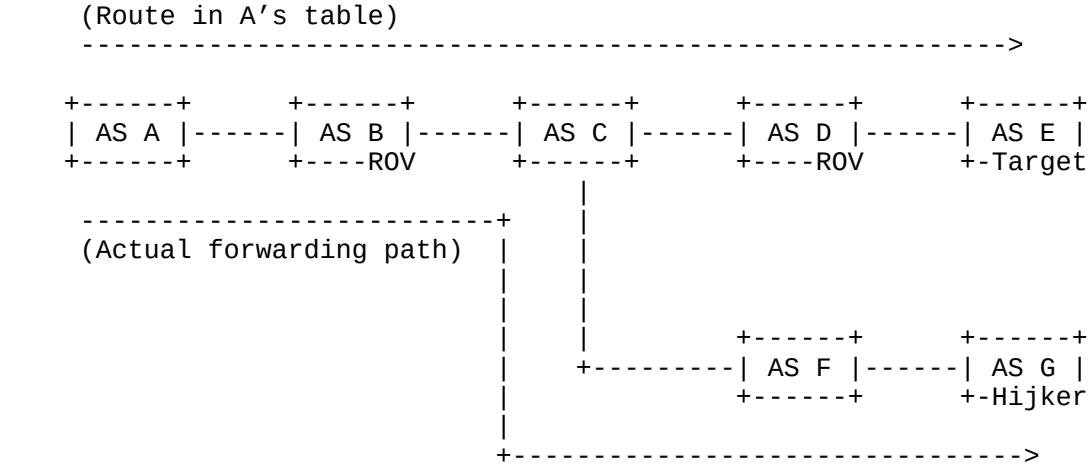

Figure 2: Discrepancy between control plane and data plane

Because AS A lacks a route to the hijacker, it remains unaware of the attack unless it conducts active measurements (e.g., traceroute) or receives external notifications. Its local control-plane protections are ineffective in detecting or responding to the hijack in this case. This highlights an unexpected side effect of incomplete ROV adoption: it prevents certain ASes from observing invalid routes, making ongoing hijacking more difficult to detect. We refer to such BGP hijacking, which compromises traffic forwarding while remaining invisible to affected ASes on the control plane, as stealthy BGP hijacking. An AS is susceptible to stealthy BGP hijacking if:

* It has no route to the hijacker due to ROV filtering, and

* At least one non-ROV AS along the legitimate path accepts the hijacker's route.

This vulnerability applies to both BGP hijacking that targets a prefix and a sub-prefix.

3. Definition of Stealthy BGP Hijacking

From a control-plane-only standpoint, this section defines stealthy BGP hijacking under incomplete ROV adoption.

3.1. Notation and Terminology

In this document, we use the following notation to describe BGP routes:

p: V ... (M) ... O

This notation represents a BGP route to prefix p as observed from a vantage point V. The sequence of ASes from V to the origin O may include one or more intermediate ASes M.

The symbols used are defined as:

p: The IP prefix being routed.

V: The vantage point, i.e., the AS from which the route is observed (typically via a BGP route collector).

M: An intermediate AS, representing any AS that appears on the path from V to the origin O. There may be multiple such ASes, or may be none.

O: The origin AS, which originates the route and claims to originate the prefix p.

We also define the following terminology for clarity in later discussions:

Conflict: Two routes are said to be in conflict if they refer to the same prefix or to overlapping prefixes (e.g., one is a more specific sub-prefix of the other), but their origin ASes differ. This indicates a potential inconsistency in prefix ownership or announcement.

RPKI-invalid: A route is considered RPKI-invalid if its prefix matches an ROA, but the origin AS does not match the AS specified, or the prefix exceeds the max length specified allowable for origination. This typically signals an unauthorized or misconfigured route announcement, which may lead to BGP hijacking.

RPKI-valid: A route is considered RPKI-valid if its origin AS matches an ROA for the prefix under RPKI, and the route is not RPKI-invalid.

Risk-critical: An AS is said to be risk-critical if it chooses to forward traffic towards an invalid route to the hijacker, while it also has route to the legitimate origin in its routing table.

3.2. Stealthy BGP Hijacking Definition

Given a pair of observed routes:

p1: V1 ... (M1) ... O1 p2: V2 ... (M2) ... O2

A stealthy BGP hijacking is said to occur when the following conditions hold:

1. The two routes conflict, i.e., p2 is equal to or a more specific sub-prefix of p1, and O2 does not equal to O1.

2. Their authorization states disagree, i.e., the prefix-origin p2-O2 is RPKI-invalid, while p1-O1 is RPKI-valid.

3. The invalid route is invisible to the victim, i.e., vantage point V1 has no observable route to prefix p2 that is originated by O2.

4. A risk-critical AS redirects traffic to the hijacker, i.e., there exists M1 such that M1 equals V2.

Under these conditions, O2 is a potential hijacker that announces the prefix p2, which is owned by O1. The invalid route does not propagate to vantage point V1. As a result, V1 observes only the legitimate route to p1 and remains unaware of the conflicting route to p2 originated by O1. However, due to the presence of a risk-critical AS M1, which appears in the legitimate path and also has a route to p2, traffic destined for p2 is silently diverted to the hijacker.

4. Real-World Incident Example

This section presents an real-world incident consistent with the definition of stealthy BGP hijacking in Section 3.2. The incident was last observed on April 24, 2025. As illustrated in Figure 3, both AS37100 (SEACOM) and AS6762 (TISparkle) observe the prefix 203.127.0.0/16 announced by its legitimate origin, AS3758 (SingNet). Meanwhile, the sub-prefix 203.127.225.0/24 is announced by an unauthorized origin, AS17894 (Innove Communications). The two origins are located in different countries and have no link between them ever observed during the most recent month. According to the APNIC’s ROV filtering measurement [APNIC], AS37100 adopts ROV with a 100% filtering rate. Therefore, it discards the RPKI-invalid /24 route. However, traffic from AS37100 (or its downstream customers)

to the /24 prefix is still hijacked when it transits through non-ROV AS6762, which accepts the /24 route.

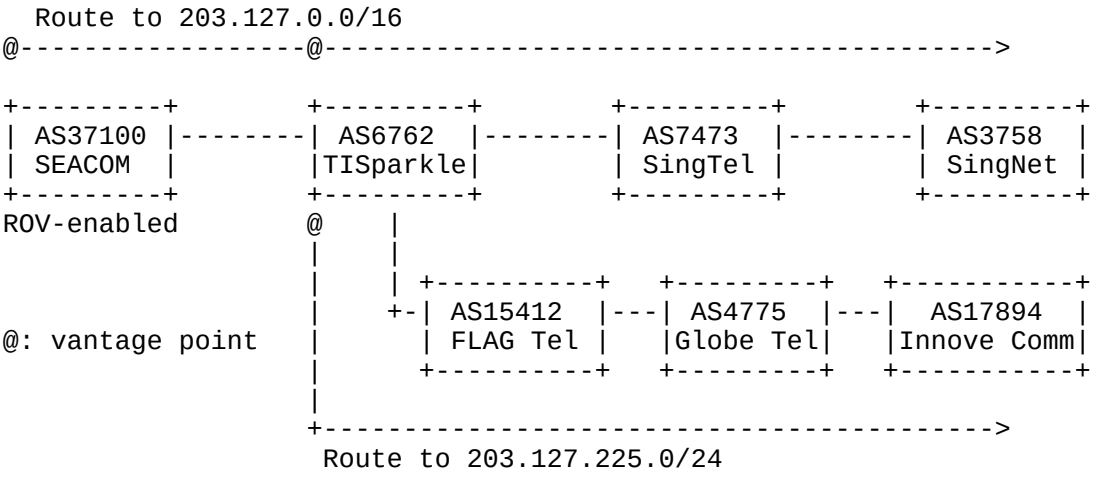

Figure 3: A real-world stealthy BGP hijacking incident

An examination using AS37100's looking glass "lg-01-ams.nl" [SEACOM] corroborates the hijack. The command "show ip bgp 203.127.0.0/16" shows a valid route via the path 37100 6762 6461 7473 3758. Meanwhile, "show ip bgp 203.127.225.0/24" returns no matching routes, confirming that AS37100 does not have visibility of the route from the unauthorized origin AS17894. However, a traceroute from AS37100 to an address within 203.127.225.0/24 shows that the final hops traverse AS17894, indicating that traffic is indeed diverted to the illegitimate origin, demonstrating a successful hijack at the data plane, even though control-plane filtering is in place.

We emphasize that the incident, while in the form of stealthy BGP hijacking, is likely caused by benign misconfigurations, given that AS17894 and AS3758 have business connections through their parent companies [SingTel] [GlobeTel], We reported the incident to AS4775 (Globe Telecoms) on February 10, 2025, and received confirmationa that it would investigate. The original looking glass output is provided in Appendix A.

5. Detection and Mitigation

The definition of stealthy BGP hijacking naturally enables a practical detection method based on inconsistencies across routing tables. By comparing routing data from multiple vantage points, one can identify route pairs that satisfy the conditions outlined in Section 3.2. Such data can be collected from self-operated ASes or public platforms, such as RouteViews [RouteViews] and RIPE RIS [RIPE_RIS]. The incident discussed in Figure 3 was discovered using this approach. In fact, an existing public monitoring service already applies this method to track stealthy BGP hijacking events in real time [Chen].

We emphasize that increasing ROV adoption across global ASes remains essential for improving BGP security. As the adoption rate increases, the feasibility and impact of stealthy BGP hijacking are expected to diminish significantly.

Meanwhile, immediate countermeasures are available. One promising approach is ROV++ [Morillo], an extension to standard ROV that enables collaboration among ROV-enabled ASes. Upon detecting RPKI-invalid routes, participating ASes can share threat intelligence, allowing for more responsive mitigation even with limited visibility. Beyond simply discarding invalid routes, ROV++ enables ROV-enabled ASes to enforce data-plane filtering or access control policies, thus effectively preventing traffic redirection to unauthorized origins.

6. Conclusion

This document formalizes stealthy BGP hijacking, a threat enabled by incomplete ROV adoption that evades control-plane detection while still diverting traffic. We define its conditions, present a real-world case, and demonstrate how it can be detected via routing table comparisons across vantage points. While broader ROV adoption remains essential, mechanisms like ROV++ offer practical mitigation by enabling coordination among ROV-enabled ASes. Addressing this risk is critical for improving the security of interdomain routing.

7. IANA Considerations

This document includes no request to IANA.

8. Security Considerations

The stealthy BGP hijacking behavior described in this document can be actively exploited by malicious ASes to divert traffic with less likelihood of being detected. While the success of such attacks depends on factors like accurate knowledge of ROV deployment, their impact can be significant, particularly in scenarios involving non-ROV transit. Detection and mitigation strategies are discussed in Section 5. Network operators are advised to adopt ROV where possible, explore collaborative defenses such as ROV++, and monitor both control- and data-plane behavior to identify and respond to suspicious routing activity.

9. References

9.1. Normative References

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/rfc/rfc6480>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/rfc/rfc9582>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/rfc/rfc6811>.

[RFC7115] Bush, R., "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)", BCP 185, RFC 7115, DOI 10.17487/RFC7115, January 2014, <https://www.rfc-editor.org/rfc/rfc7115>.

9.2. Informative References

[APNIC] Huston, G., "Measuring ROAs and ROV.", March 2025, <https://stats.labs.apnic.net/rpki>.

[SingTel] "Wikipedia - SingTel.", March 2025, <https://en.wikipedia.org/wiki/Singtel>.

[GlobeTel] "Wikipedia - Globe Telecom.", March 2025, <https://en.wikipedia.org/wiki/Globe_Telecom>.

[SEACOM] "Looking Glass lg-01-ams.nl.", February 2025, <https://lg.seacomnet.com>.

[RouteViews] University of Oregon Route Views Project, "MRT format RIBs and UPDATEs.", 2025, <http://routeviews.org/>.

[RIPE_RIS] RIPE NCC, "Routing Information Service (RIS).", 2025, <https://ris.ripe.net/docs/>.

[Morillo] Morillo, R., Furuness, J., Morris, C., Breslin, J., Herzberg, A., and B. Wang, "Routing Information Service (RIS).", DOI 10.14722/ndss.2021.24438, 2021, <https://doi.org/10.14722/ndss.2021.24438>.

[Chen] Chen, Y., "Stealthy BGP Hijakcing Incidents.", 2025, <https://yhchen.cn/stealthy-bgp-hijacking/>.

Appendix A. Looking Glass Output

All commands were executed on "lg-01-ams.nl" [SEACOM] on February 10, 2025.

Figure 4 shows the output for executing "show ip bgp 203.127.0.0/16".

Figure 5 shows the output for executing "show ip bgp 203.127.225.0/24".

Figure 6 shows the output for executing "traceroute ip 203.127.225.1".

```
######################################################################
BGP routing table entry for 203.127.0.0/16, version 3804070796
Paths: (2 available, best #2, table default)
  Not advertised to any peer
  Refresh Epoch 1
  37100 6762 6461 7473 3758
    105.26.64.17 from 105.26.64.17 (105.16.0.131)
      Origin IGP, metric 0, localpref 100, valid, external
      Commnuity: 37100:1 37100:13
      path 108E73DC RPKI State valid
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  37100 6762 6461 7473 3758
    105.26.64.1 from 105.26.64.1 (105.16.0.131)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Commnuity: 37100:1 37100:13
      path 0AB3654C RPKI State valid
      rx pathid: 0, tx pathid: 0x0
######################################################################
```

Figure 4: Output for "show ip bgp 203.127.0.0/16"

```
######################################################################
% Network not in table
######################################################################
```

Figure 5: Output for "show ip bgp 203.127.225.0/24"

```
   ######################################################################
   Tracing the route to 203.127.225.1
   VRF info: (vrf in name/id, vrf out name/id)
     1 ae-2-21.er-01-ams.nl.seacomnet.com (105.26.64.1) [AS 37100]
         0 msec 200 msec 0 msec
     2 ce-0-0-11.er-02-mrs.fr.seacomnet.com (105.16.8.209) [AS 37100]
         [MPLS: Label 2242 Exp 0] 200 msec
       ce-0-0-11.cr-01-mrs.fr.seacomnet.com (105.16.8.201) [AS 37100]
         [MPLS: Label 4474 Exp 0] 204 msec
       ce-0-0-11.cr-02-mrs.fr.seacomnet.com (105.16.8.209) [AS 37100]
         [MPLS: Label 2242 Exp 0] 20 msec
     3 ce-0-0-1.br-02-mrs.fr.seacomnet.com (105.16.33.253) [AS 37100]
         20 msec
       ce-0-0-2.br-02-mrs.fr.seacomnet.com (105.16.32.253) [AS 37100]
         24 msec
       ce-0-0-1.br-02-mrs.fr.seacomnet.com (105.16.33.253) [AS 37100]
         20 msec
     4 213.144.184.130 [AS 6762] 24 msec 20 msec 24 msec
     5 213.144.170.125 [AS 6762] 40 msec 44 msec 40 msec
     6 ae10.0.cjr01.mrs005.flagtel.com (62.216.131.154) [AS 15412]
         [MPLS: Label 7391 Exp 0] 172 msec 172 msec 168 msec
     7 ae1.0.cjr02.sin001.flagtel.com (62.216.129.181) [AS 15412]
         [MPLS: Label 3621 Exp 0] 168 msec 156 msec 156 msec
     8 ae18.0.cjr01.sin001.flagtel.com (62.216.137.165) [AS 15412]
         160 msec 160 msec 172 msec
     9 80.81.75.186 [AS 15412] 164 msec 164 msec 160 msec
    10 112.198.1.185 [AS 4775] 204 msec 216 msec 204 msec
    11  *  *  *
    12 120.28.4.38 [AS 4775] 220 msec 220 msec 216 msec
    13 202.126.45.138 [AS 17894] 224 msec
       202.126.45.134 [AS 17894] 220 msec 232 msec
    14 202.126.45.180 [AS 17894] 208 msec 216 msec 224 msec
    15  *  *  *
    16  *  *  *
   ######################################################################
```

Figure 6: Output for "traceroute ip 203.127.225.1"

Authors' Addresses

Qi Li
Tsinghua University
30 Shuangqing Road
Beijing
100084
China
Email: qli01@tsinghua.edu.cn

Yihao Chen
Tsinghua University
30 Shuangqing Road
Beijing
100084
China
Email: yh-chen21@mails.tsinghua.edu.cn

Ke Xu
Tsinghua University
30 Shuangqing Road
Beijing
100084
China
Email: xuke@tsinghua.edu.cn

Zhuotao Liu
Tsinghua University
30 Shuangqing Road
Beijing
100084
China
Email: zhuotaoliu@tsinghua.edu.cn

Jianping Wu
Tsinghua University
30 Shuangqing Road
Beijing
100084
China
Email: jianping@cernet.edu.cn