NDSS
Symposium 2026

Understanding the Stealthy BGP Hijacking Risk in the ROV Era

Yihao Chen, Qi Li, Ke Xu, Zhuotao Liu, Jianping Wu

清華大學
Tsinghua University

中关村实验室
ZGC Laboratory

北京信息科学与技术
国家研究中心
BEIJING NATIONAL RESEARCH CENTER
FOR INFORMATION SCIENCE AND TECHNOLOGY

2026/02/26

Content

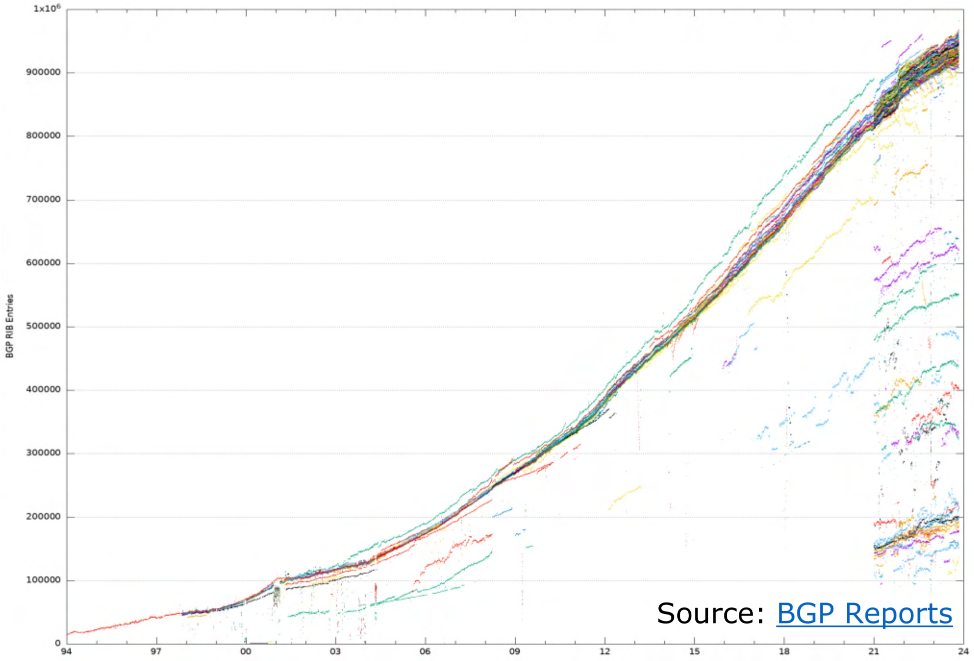
1. Background on BGP (In)security
2. BGP Hijacking in the ROV Era: A Real Case
3. Is BGP Hijacking Becoming More Elusive?
4. Real-World Observations & Insights
5. Towards Analytical Risk Assessment
6. Discussions & Future Work

Content

1. Background on BGP (In)security
2. BGP Hijacking in the ROV Era: A Real Case
3. Is BGP Hijacking Becoming More Elusive?
4. Real-World Observations & Insights
5. Towards Analytical Risk Assessment
6. Discussions & Future Work

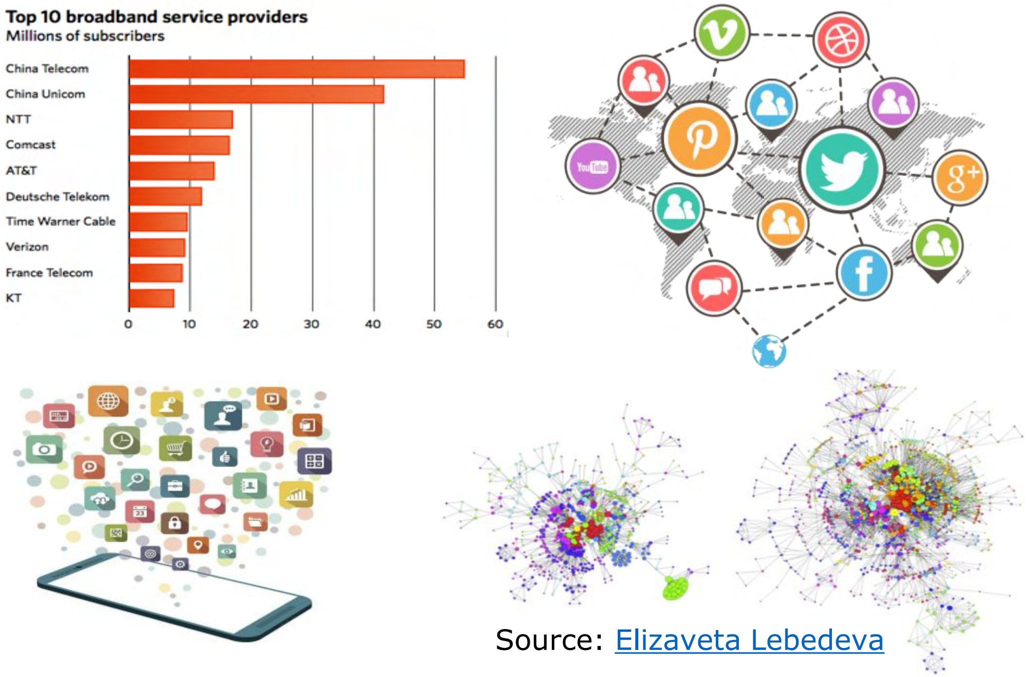
BGP in Today’s Internet

- The foundational routing protocol maintaining **global Internet connectivity**.
- Over **960k interdomain routes** in operation, supporting more than **75k ASes**.



Source: BGP Reports

Rapid Growth of the BGP Table



Source: Elizaveta Lebedeva

Vast Applications and Services over BGP

BGP Hijacking and RPKI/ROV

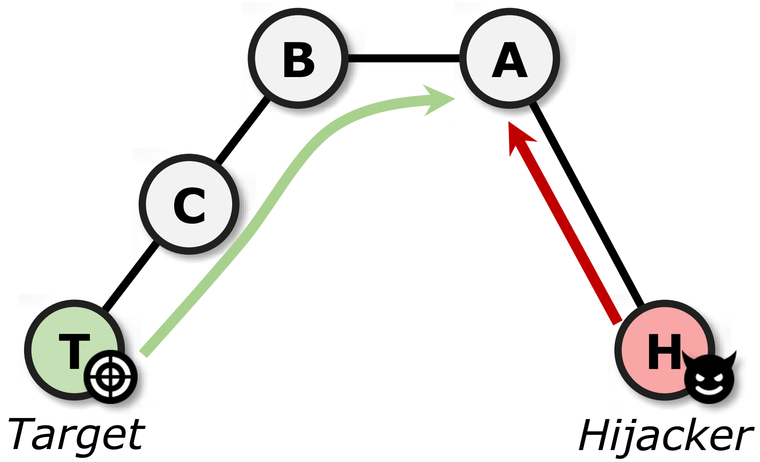
- BGP does not guarantee **prefix-origin authenticity**.

  …… RPKI/ROV does, in an **incremental** manner.

BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

  …… RPKI/ROV does, in an **incremental** manner.

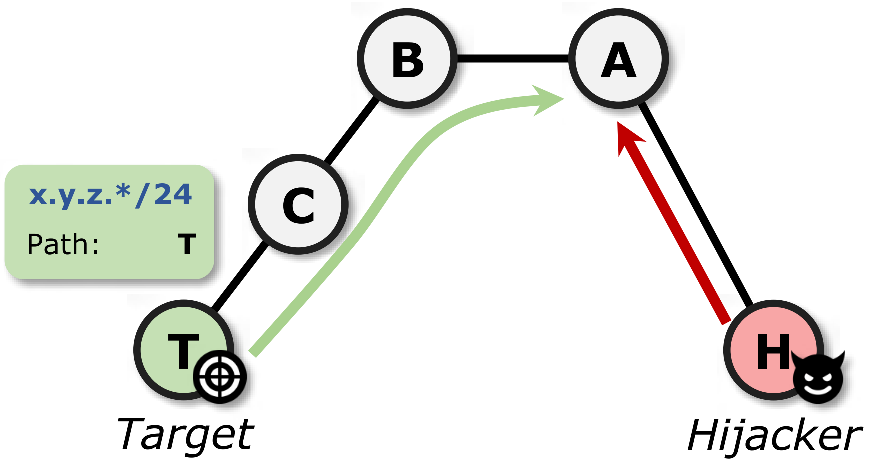


BGP Hijacking Illustration

BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

…… RPKI/ROV does, in an **incremental** manner.

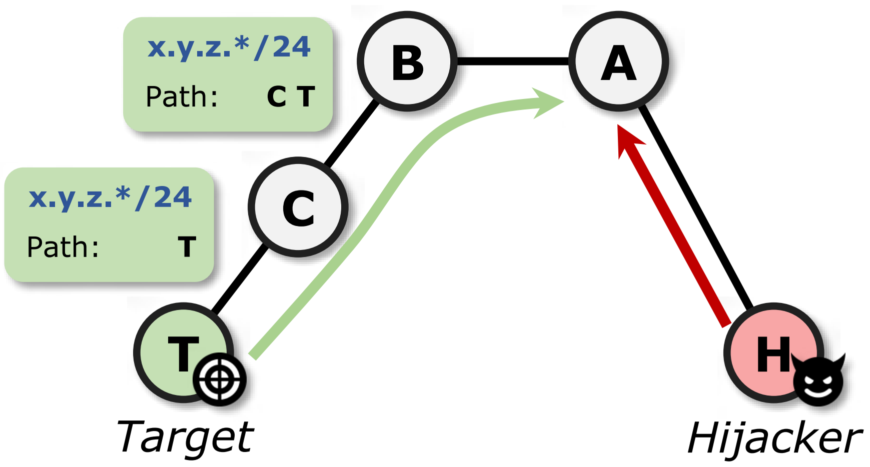


BGP Hijacking Illustration

BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

  ⋯⋯ RPKI/ROV does, in an **incremental** manner.

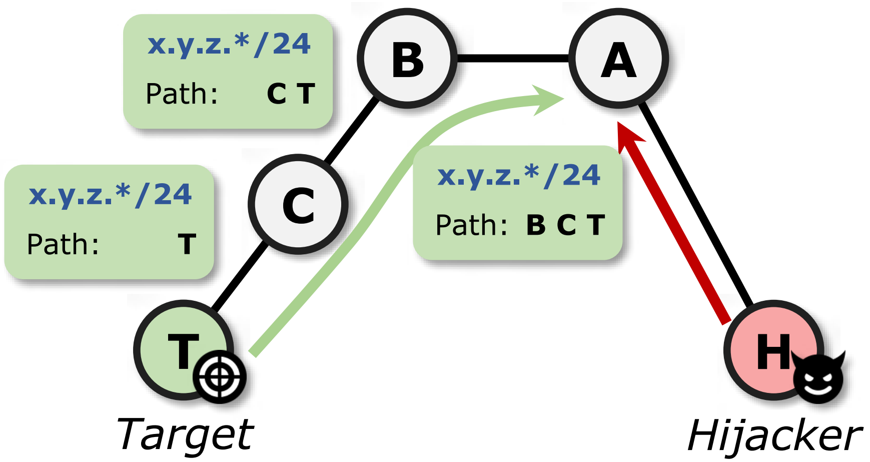


BGP Hijacking Illustration

BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

…… RPKI/ROV does, in an **incremental** manner.

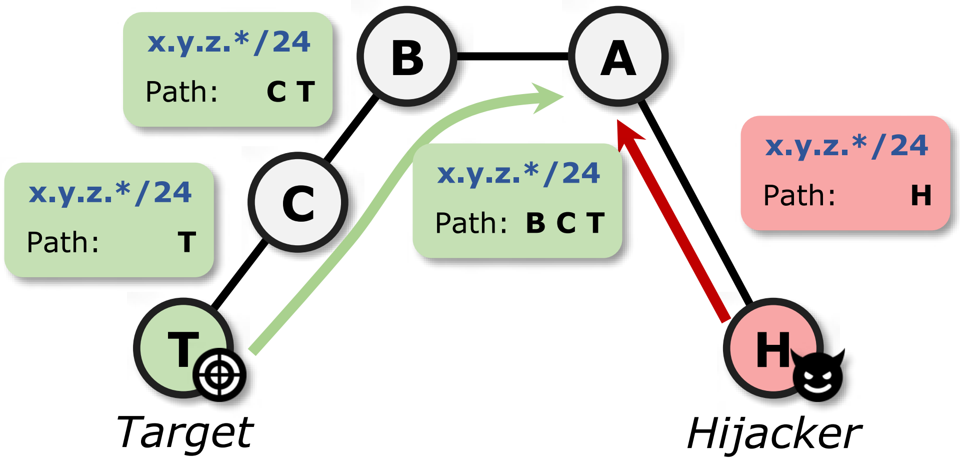


BGP Hijacking Illustration

BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

  …… RPKI/ROV does, in an **incremental** manner.

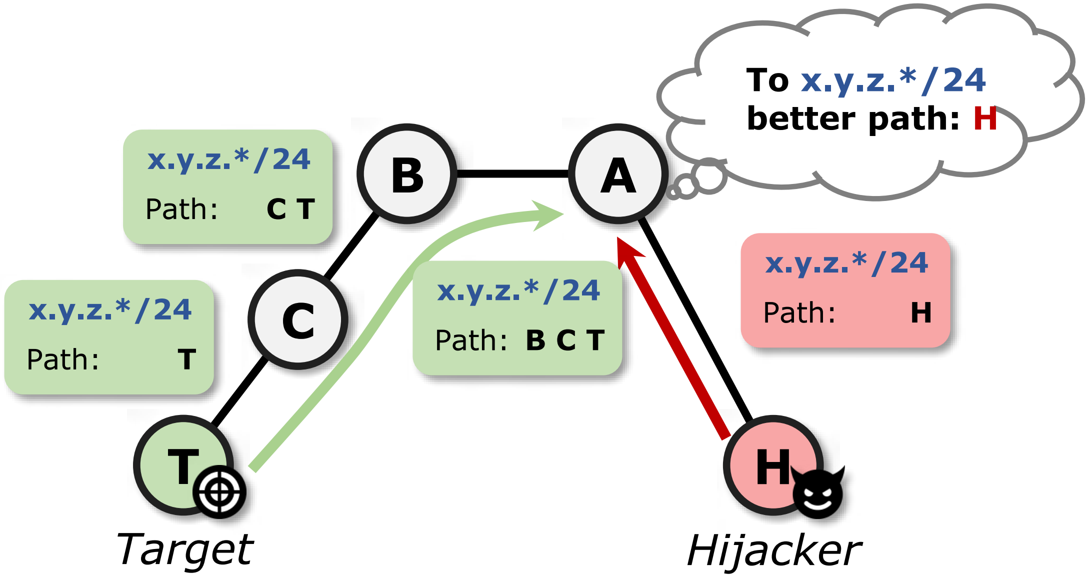


BGP Hijacking Illustration

BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

  …… RPKI/ROV does, in an **incremental** manner.

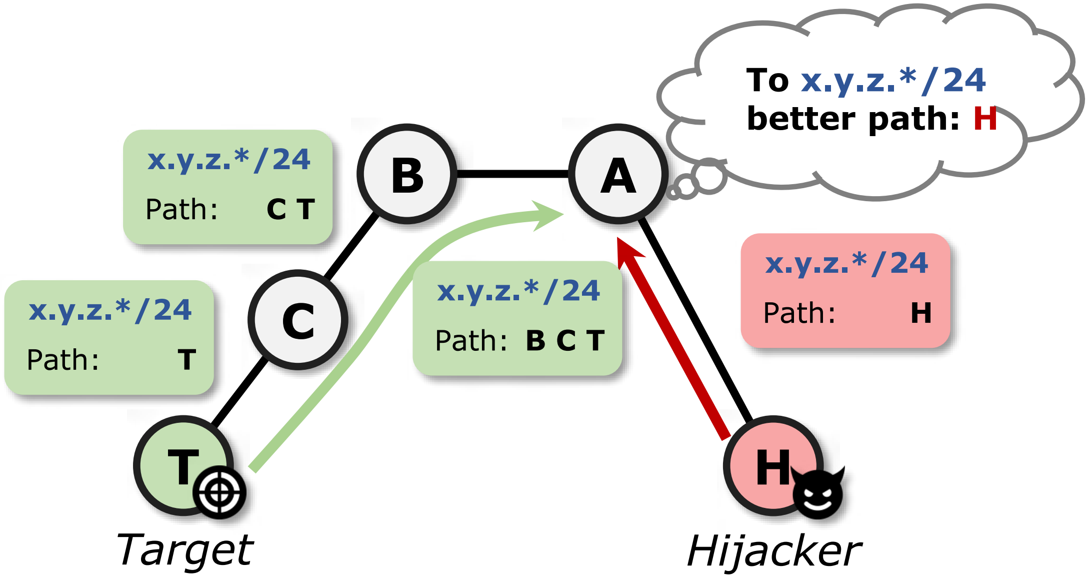


BGP Hijacking Illustration

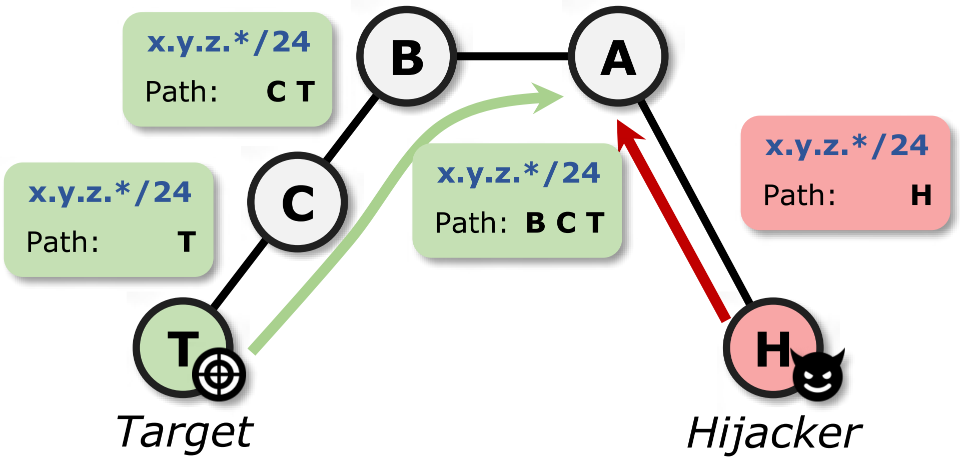
BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

  …… RPKI/ROV does, in an **incremental** manner.



BGP Hijacking Illustration

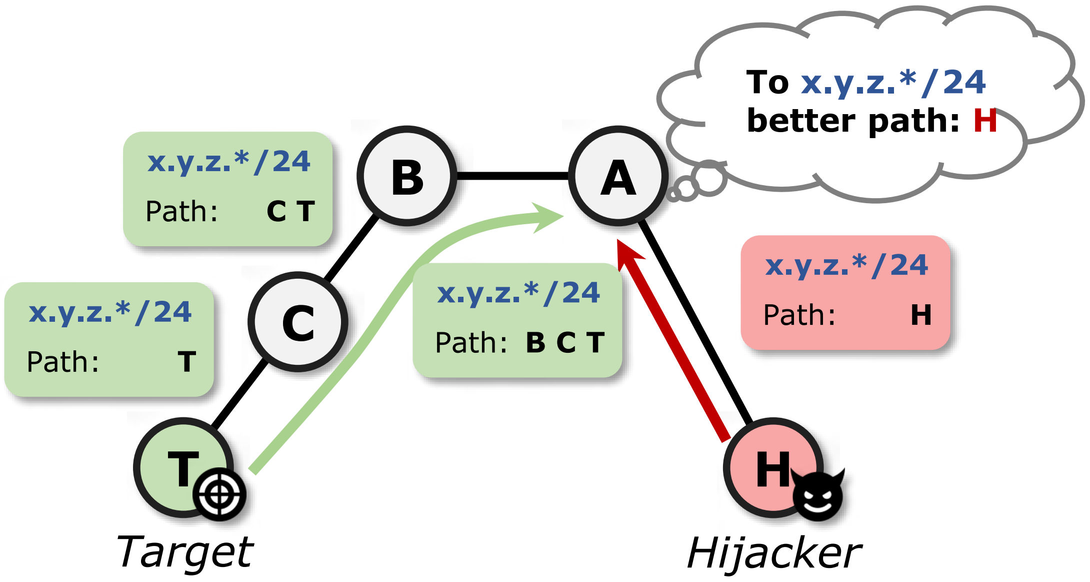


How RPKI/ROV Mitigates BGP Hijacking

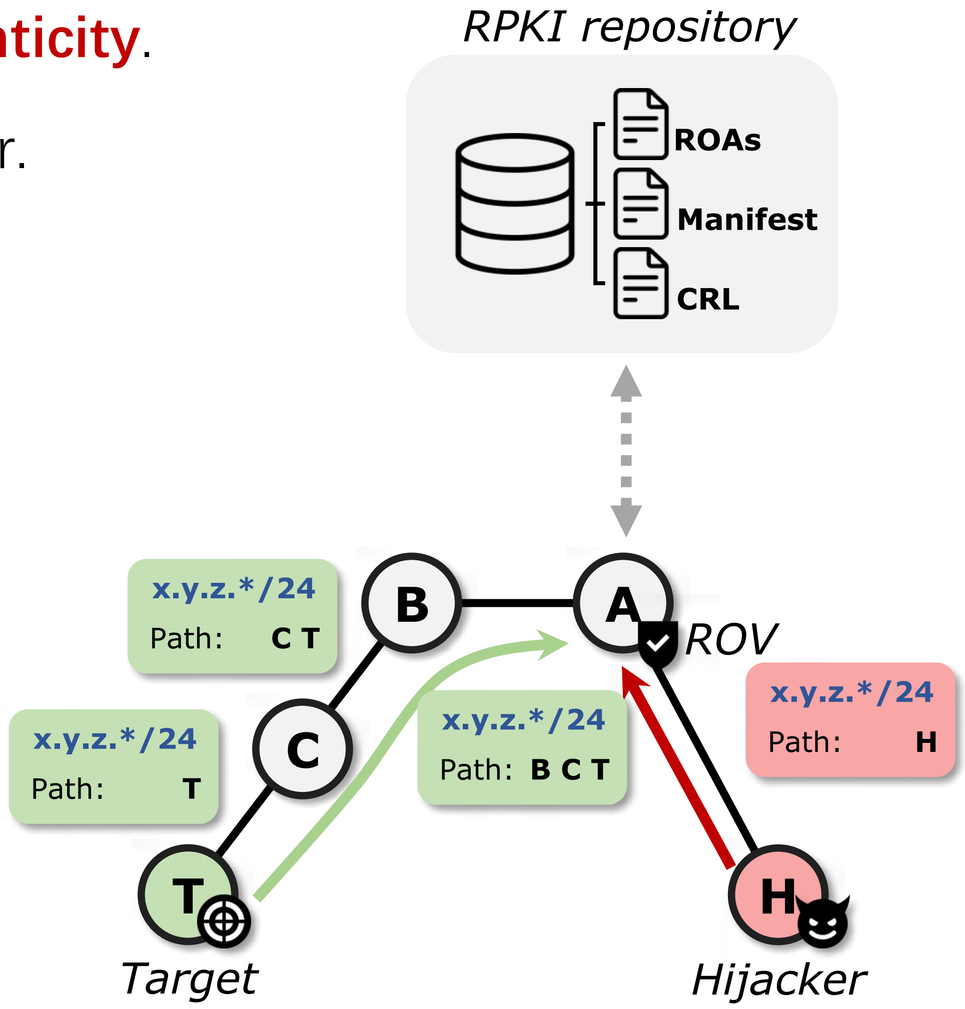
BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

  …… RPKI/ROV does, in an **incremental** manner.



BGP Hijacking Illustration

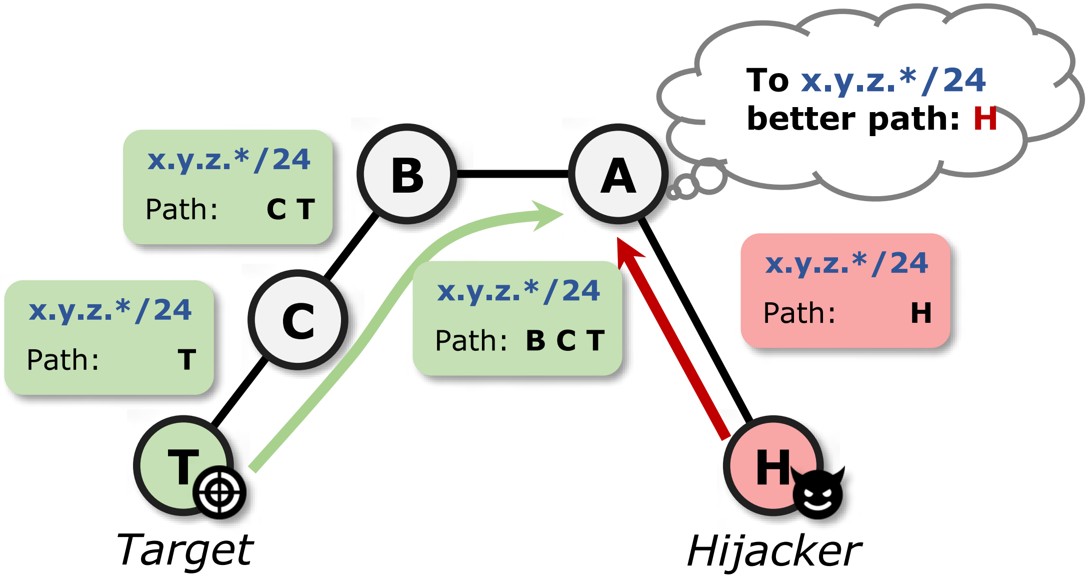


How RPKI/ROV Mitigates BGP Hijacking

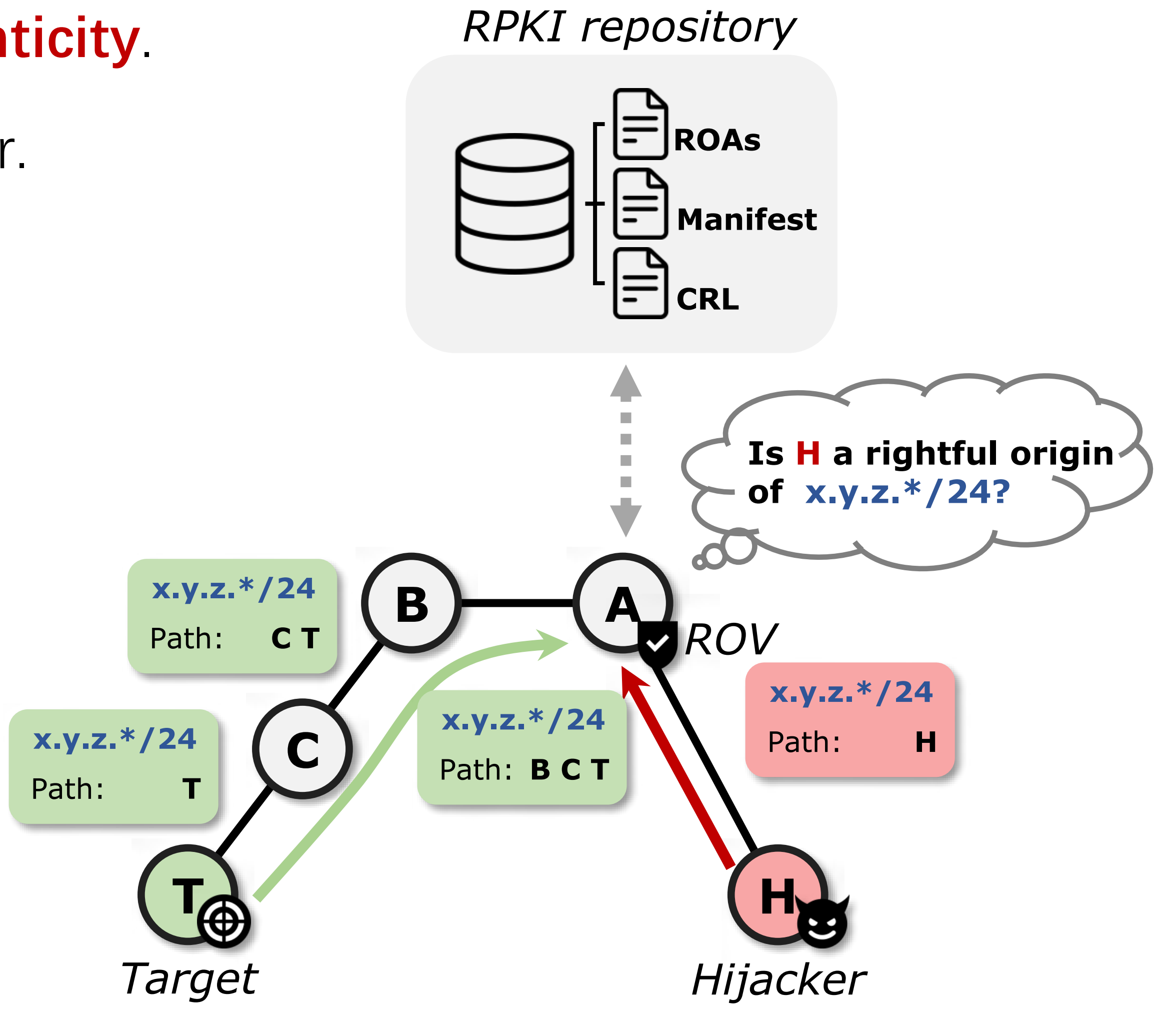
BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

  …… RPKI/ROV does, in an **incremental** manner.



BGP Hijacking Illustration

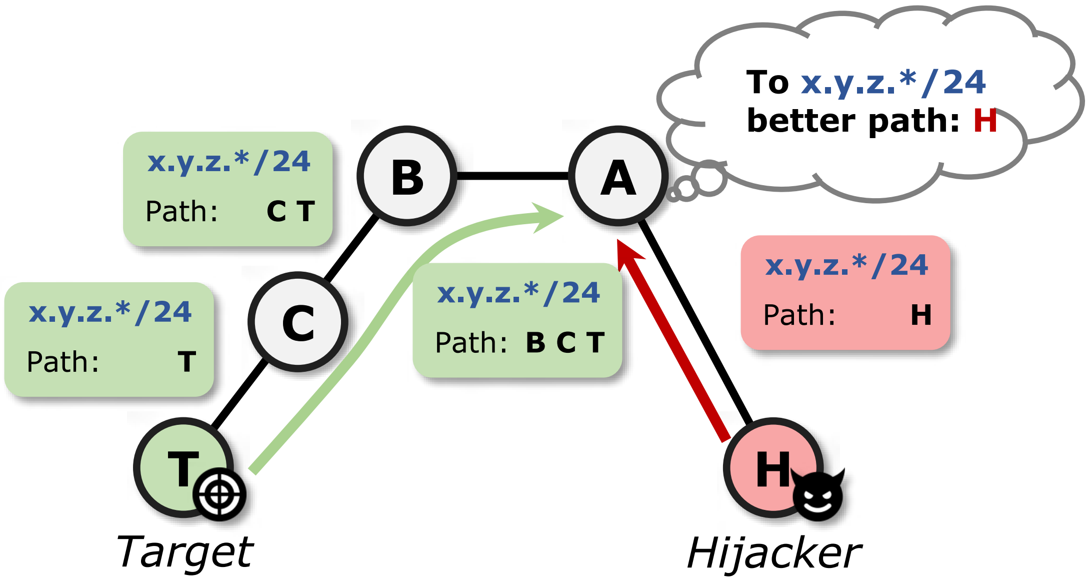


How RPKI/ROV Mitigates BGP Hijacking

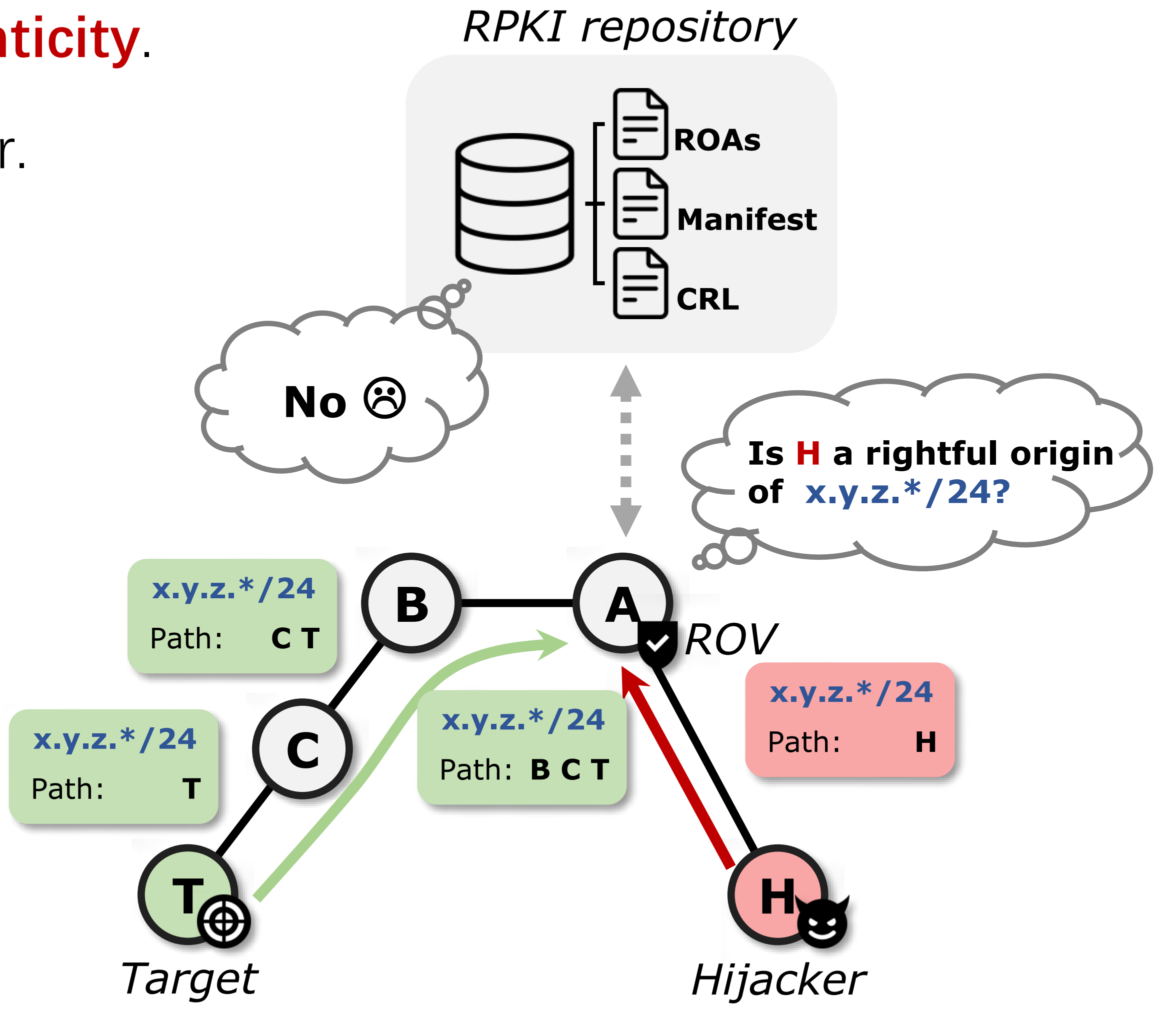
BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

  …… RPKI/ROV does, in an **incremental** manner.



BGP Hijacking Illustration

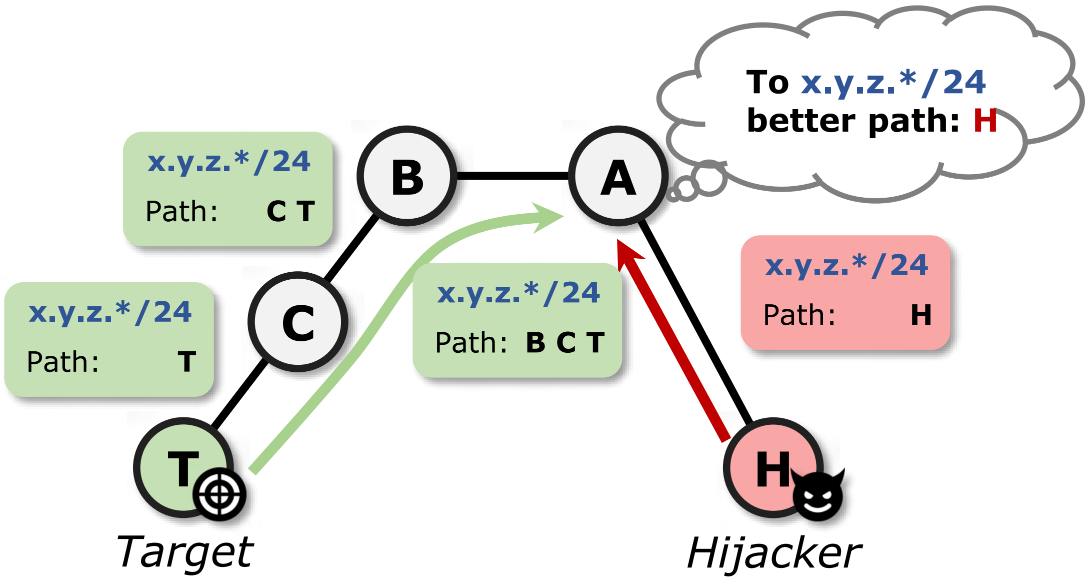


How RPKI/ROV Mitigates BGP Hijacking

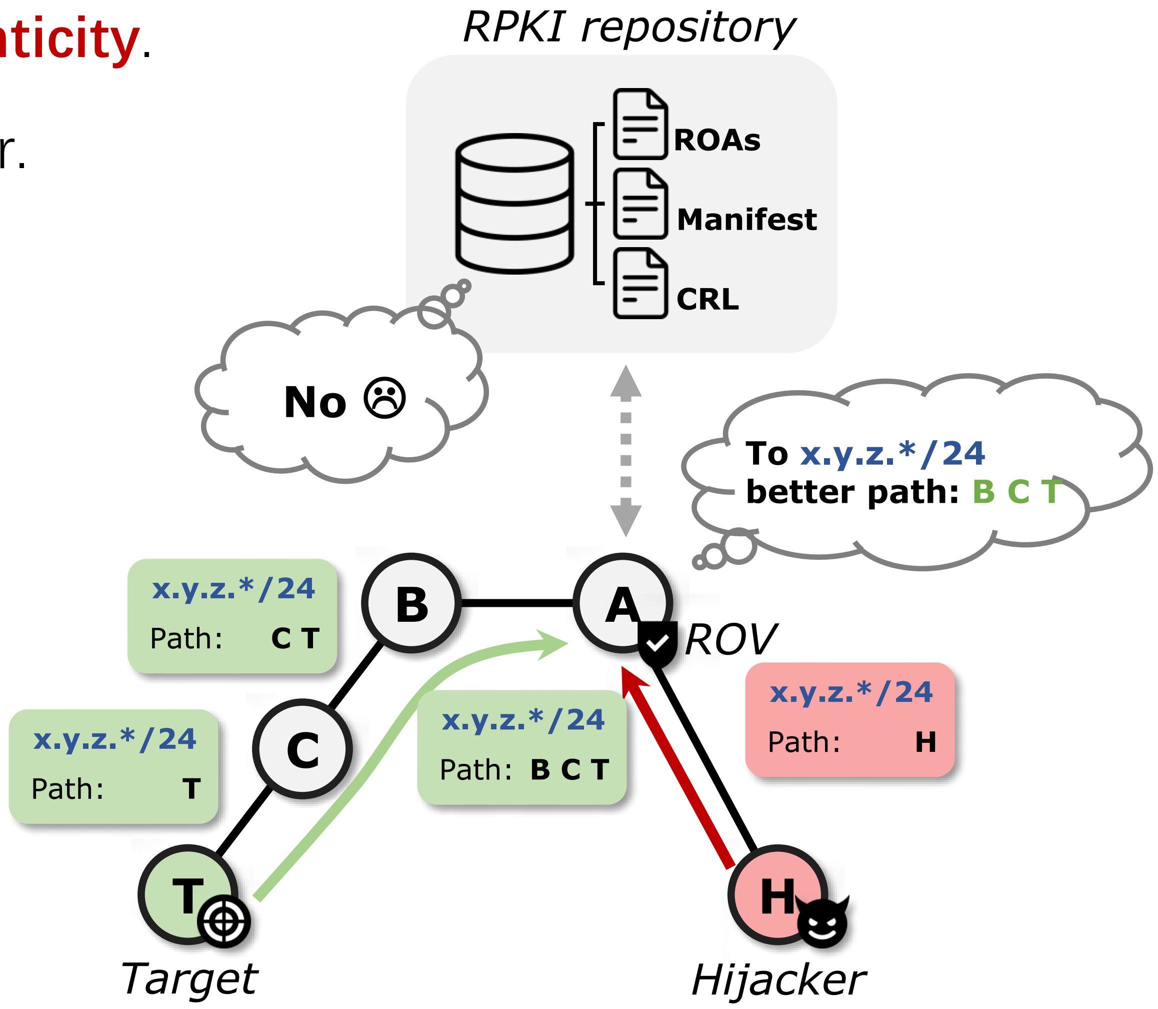
BGP Hijacking and RPKI/ROV

- BGP does not guarantee **prefix-origin authenticity**.

  …… RPKI/ROV does, in an **incremental** manner.



BGP Hijacking Illustration

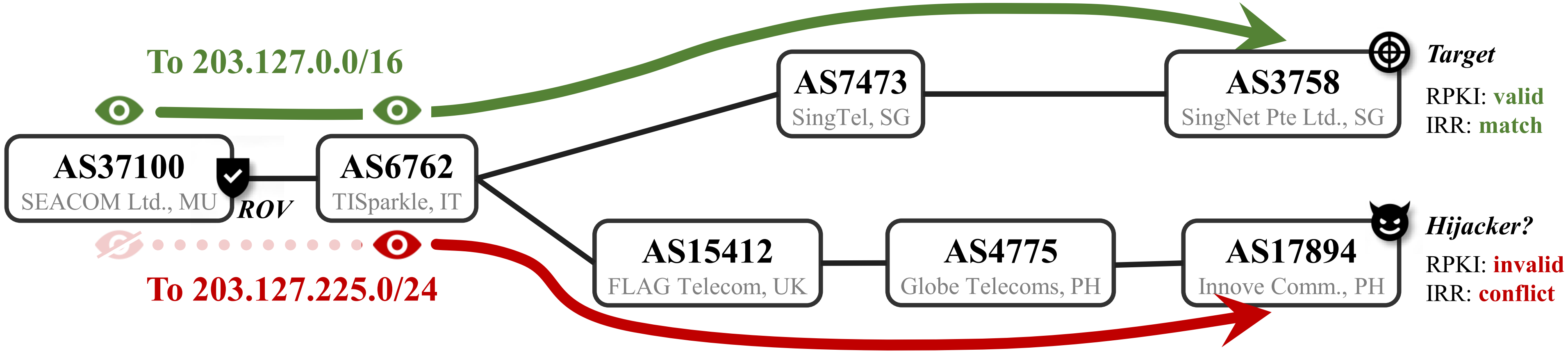


How RPKI/ROV Mitigates BGP Hijacking

Content

1. Background on BGP (In)security
2. BGP Hijacking in the ROV Era: A Real Case
3. Is BGP Hijacking Becoming More Elusive?
4. Real-World Observations & Insights
5. Towards Analytical Risk Assessment
6. Discussions & Future Work

Case Study: Hijacking on 203.127.225.0/24

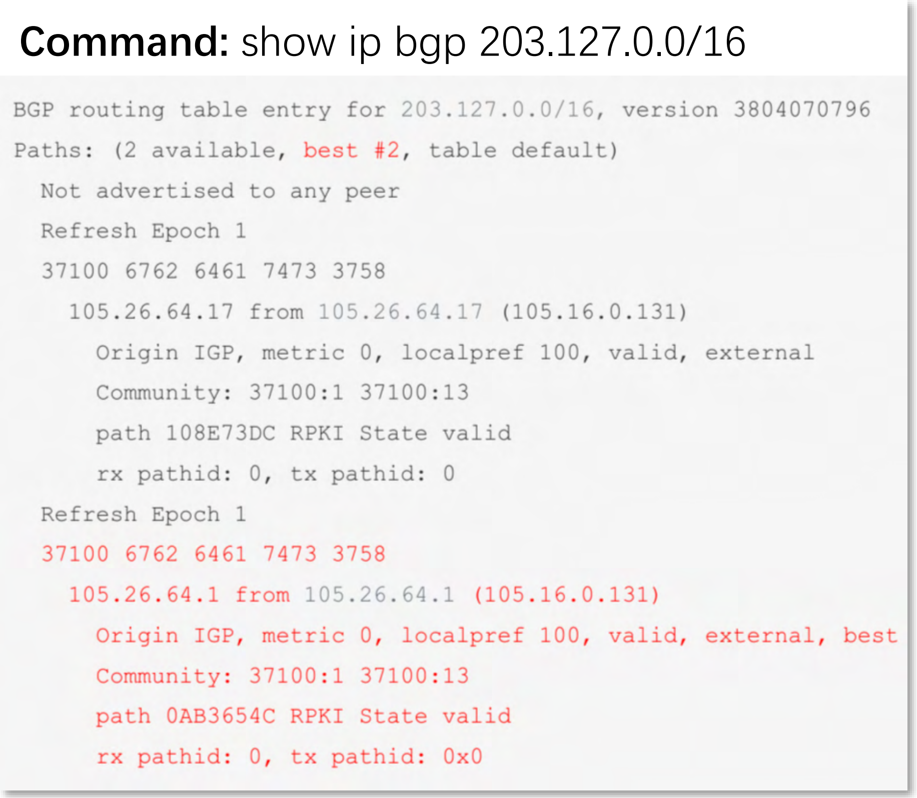


⋆ First observed: 2023-10-01 Last observed: 2025-04-24

⋆ While in the form of BGP hijacking, this case is very likely to be caused by misconfiguration; we awaiting response from relevant operators.

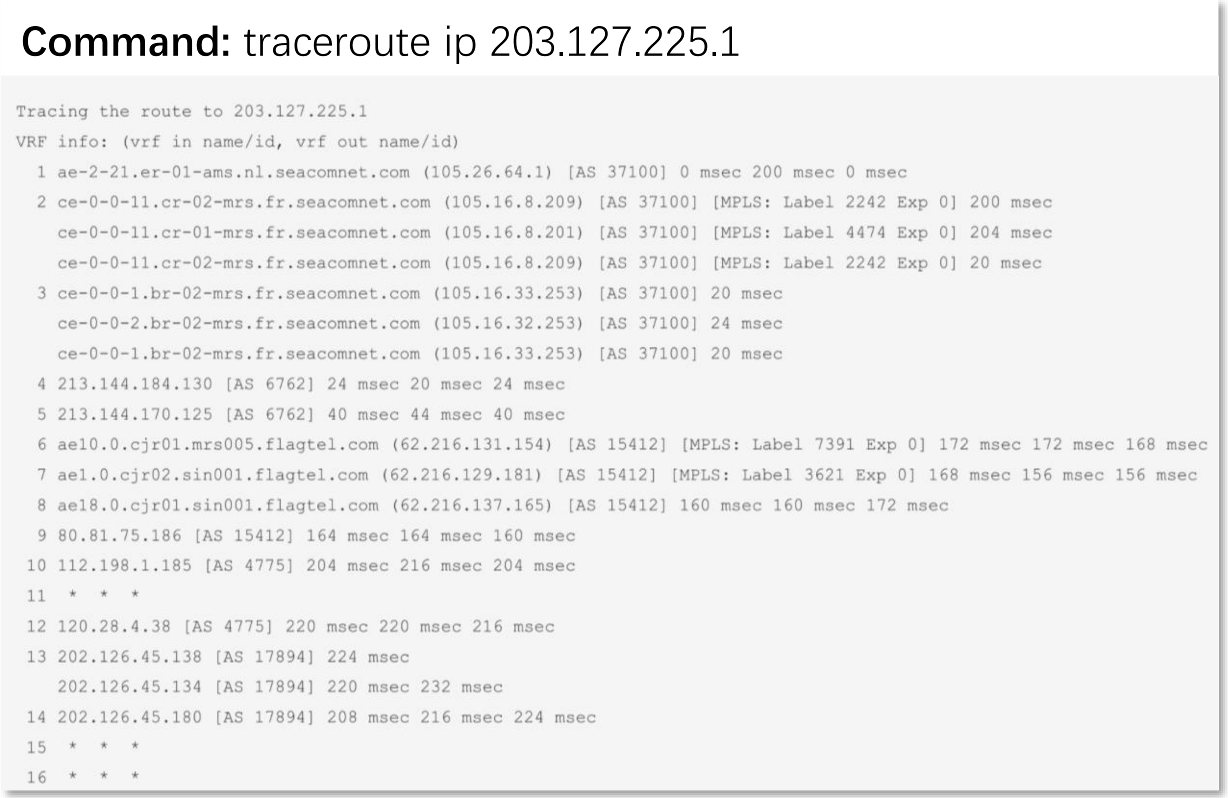
- AS17894 mis-announces a /24 without RPKI or IRR authorization, while AS3758 is the legitimate origin.
- ROV-enabled AS37100 discards the invalid route, and thus **has the legitimate /16 route only.**
- Consequently, just by looking the routing table, AS37100 (and its customers) remains **unaware of the ongoing hijacking**, and tends to believe their traffic be forwarded correctly.
- However, **legacy AS6762 accepts the illegitimate route**, actually forwarding /24 traffic to AS17894.

Evidence from AS37100’s Looking Glass



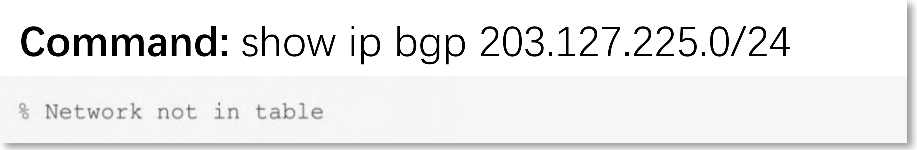
Command: show ip bgp 203.127.0.0/16

```
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
      Community: 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
      Community: 37100:1 37100:13
      path 0AB3654C RPKI State valid
      rx pathid: 0, tx pathid: 0x0
```



Command: traceroute ip 203.127.225.1

```
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.cr-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  *  *  *
```



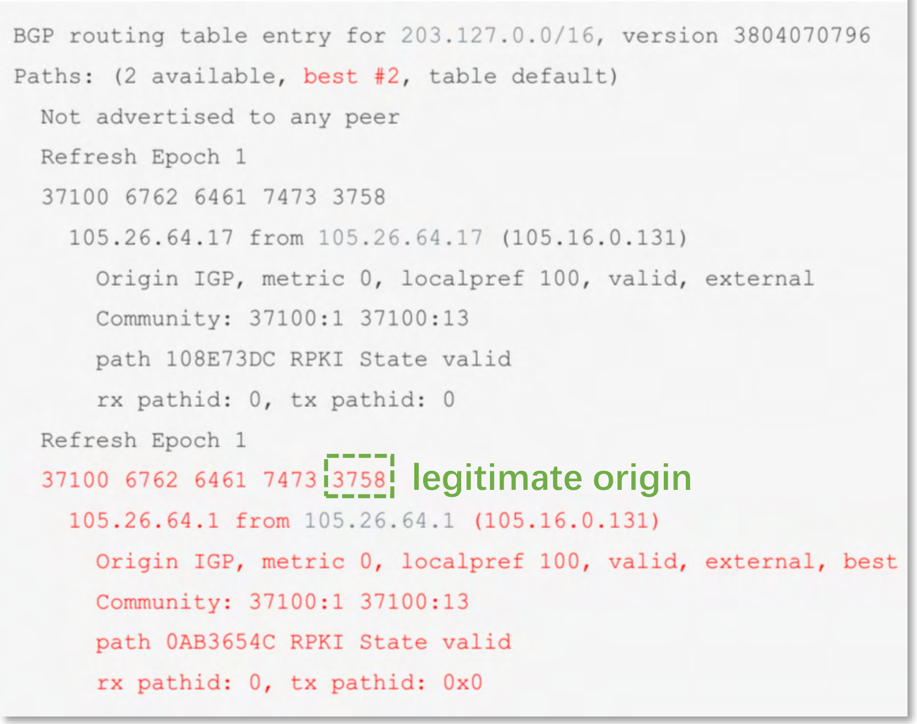
Command: show ip bgp 203.127.225.0/24

```
% Network not in table
```

* All commands were performed on “lg-01-ams.nl” on Feb 10, 2025.

Evidence from AS37100’s Looking Glass

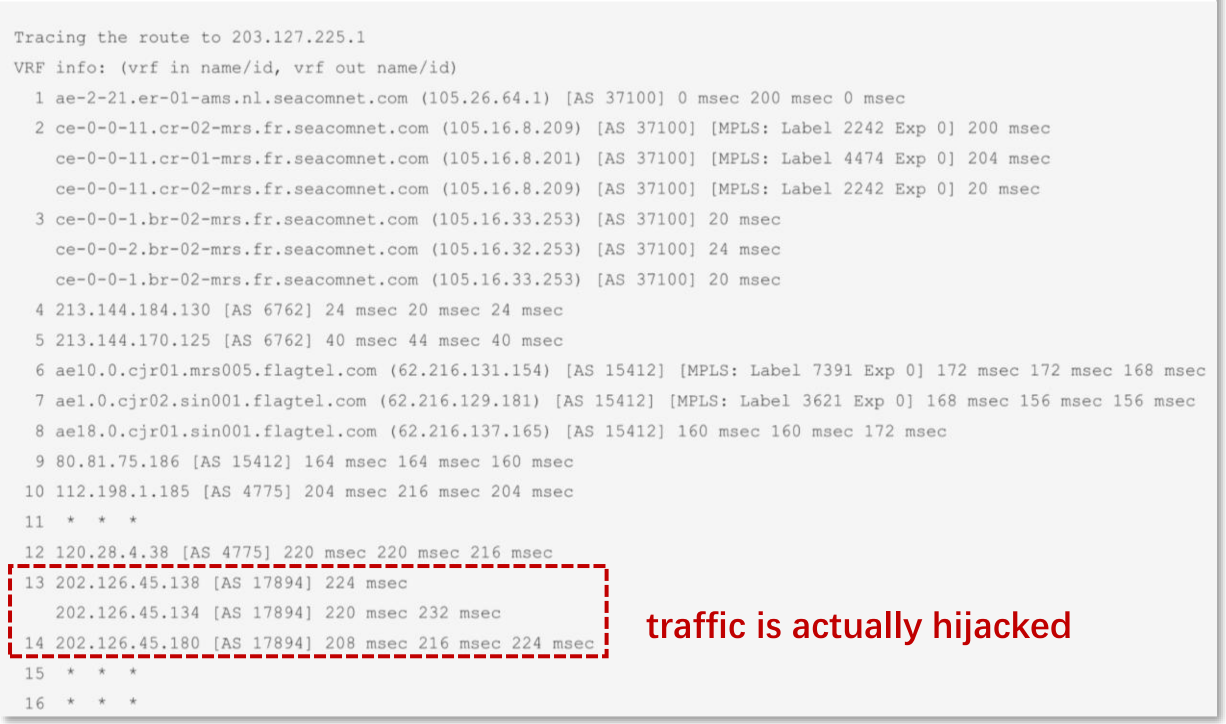
Command: show ip bgp 203.127.0.0/16



```
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
      Community: 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
      Community: 37100:1 37100:13
      path 0AB3654C RPKI State valid
      rx pathid: 0, tx pathid: 0x0
```

legitimate origin

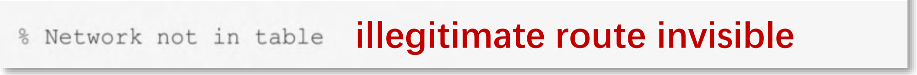
Command: traceroute ip 203.127.225.1



```
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.cr-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  *  *  *
```

traffic is actually hijacked

Command: show ip bgp 203.127.225.0/24



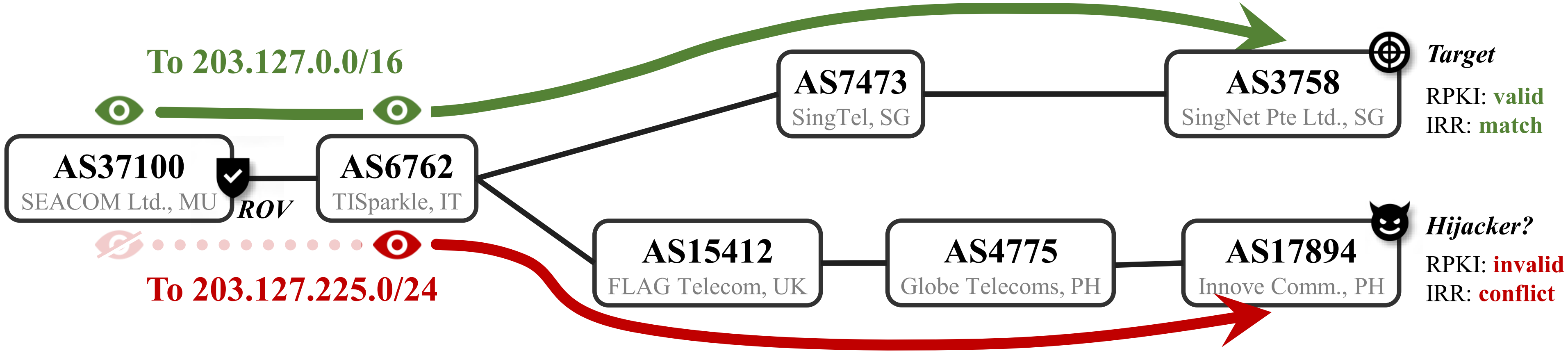
```
% Network not in table
```

illegitimate route invisible

Traffic to 203.127.225.0/24 is hijacked, but the misbehavior is invisible from AS37100’s routing table

* All commands were performed on “lg-01-ams.nl” on Feb 10, 2025.

What Remains Alarming in this Case?



⋆ First observed: 2023-10-01 Last observed: 2025-04-24

⋆ While in the form of BGP hijacking, this case is very likely to be caused by misconfiguration; we awaiting response from relevant operators.

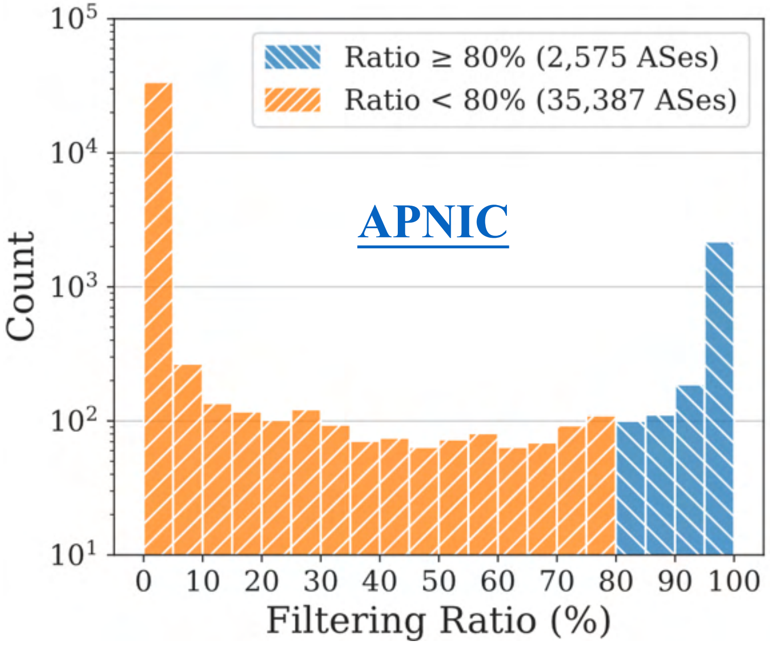
BGP hijacking (intentional or not) still succeeds, and becomes less spotted (stealthier), due to the incomplete ROV deployment in the current Internet.

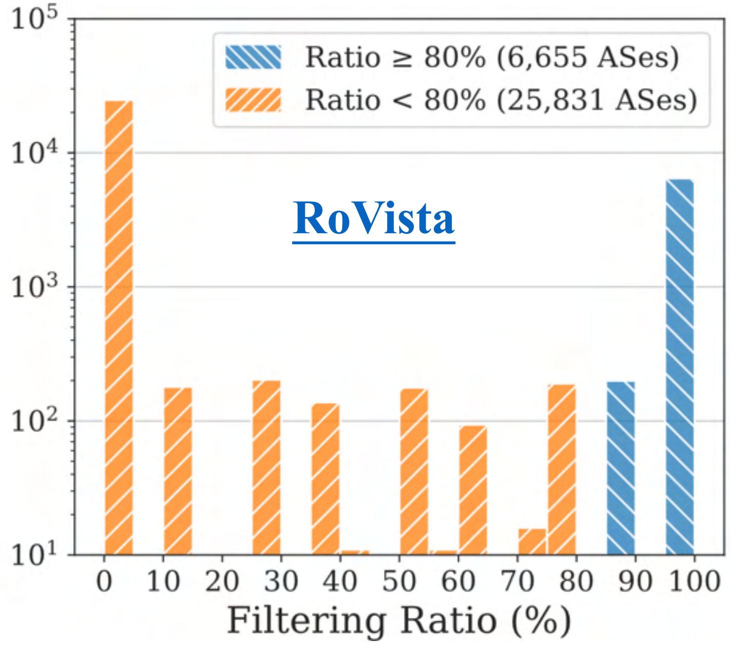
Content

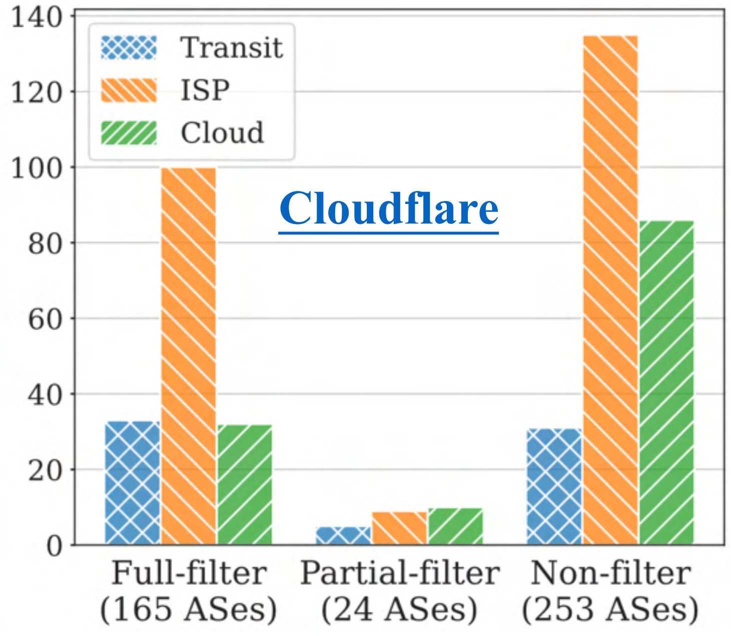
1. Background on BGP (In)security
2. BGP Hijacking in the ROV Era: A Real Case
3. Is BGP Hijacking Becoming More Elusive?
4. Real-World Observations & Insights
5. Towards Analytical Risk Assessment
6. Discussions & Future Work

RPKI/ROV in Today's Internet

- ROAs have covered **55.9% IPv4 prefixes** and **56.9% IPv6 prefixes***
- Yet ROV deployment is **presumably limited**

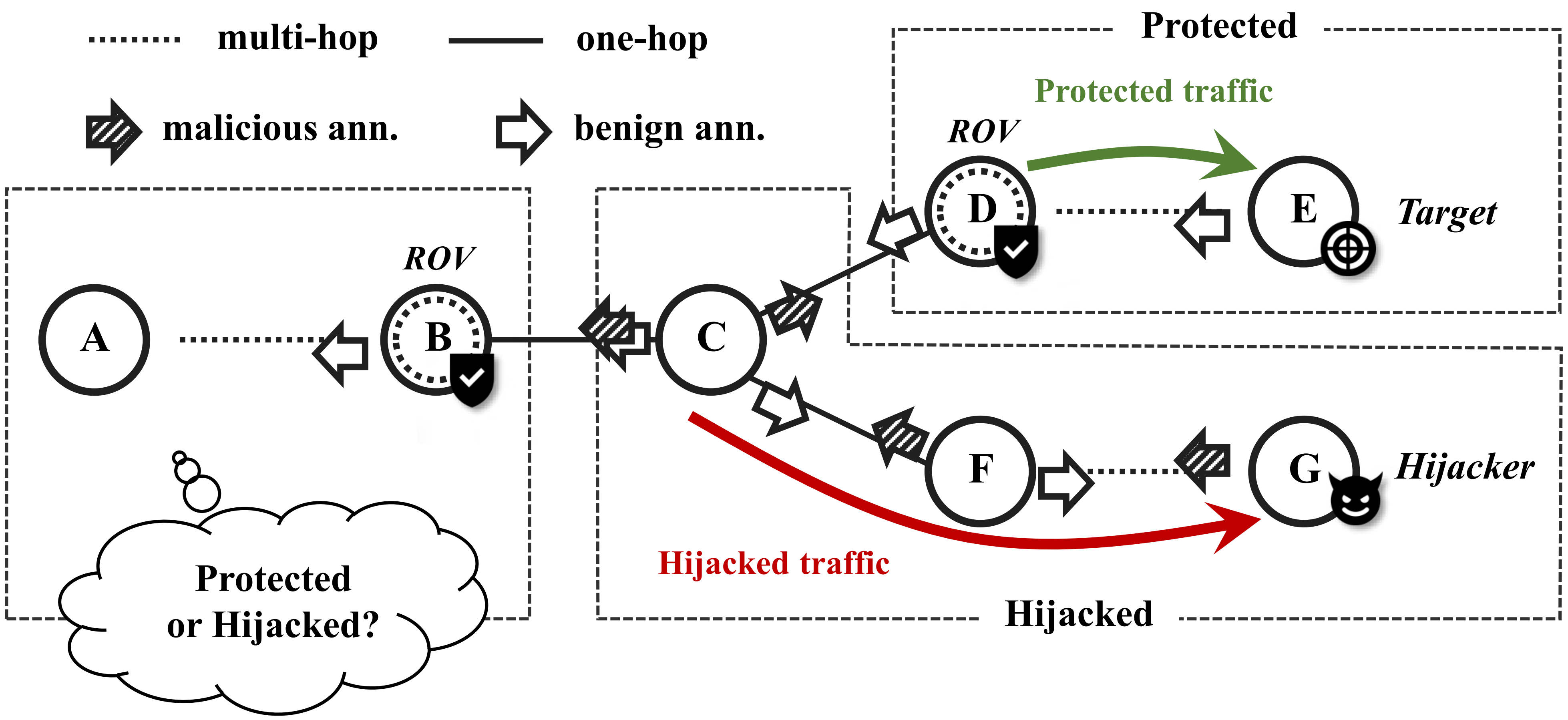






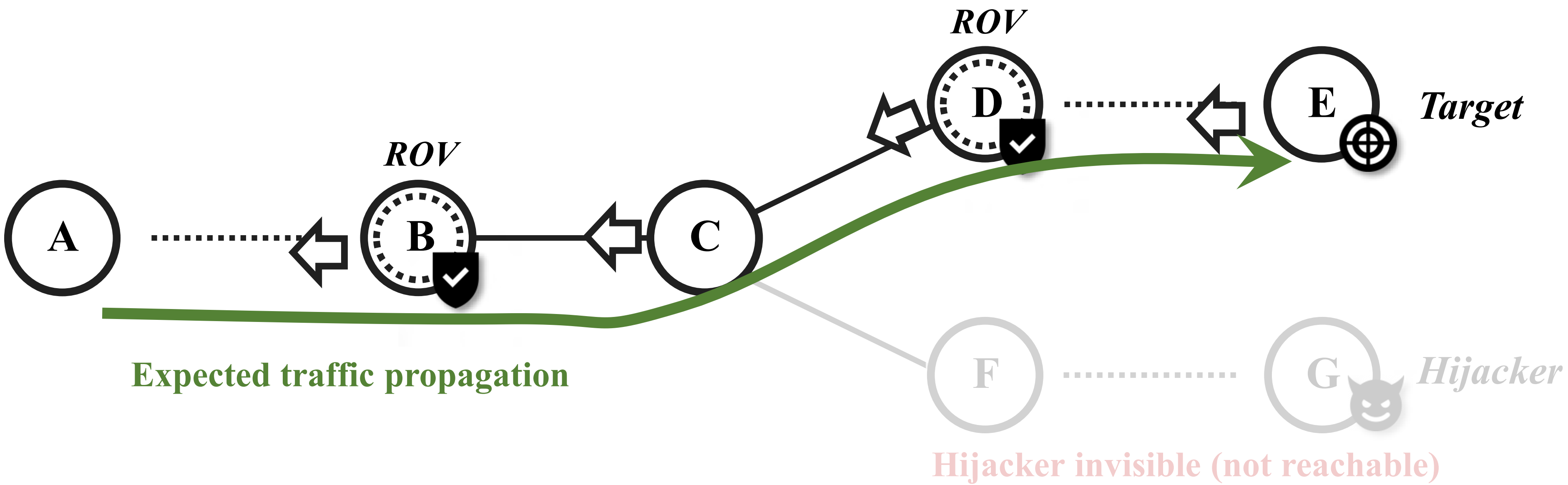
* Source: https://rpki-monitor.antd.nist.gov/ROV (2025/4/27)

BGP Hijacking Under Partial ROV deployment



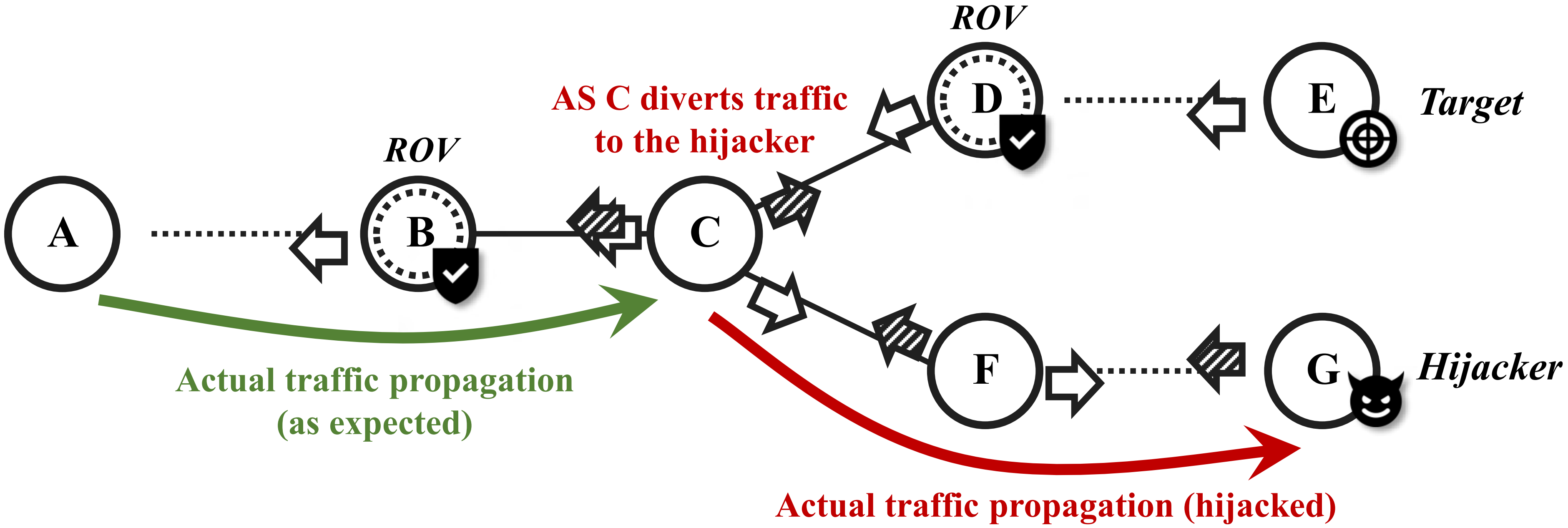
⁎ This is the general topology structure that illustrates how BGP hijacking can succeed despite partial ROV deployment. It does not reflect the whole Inter-AS topology, but only the part that makes the stealthy hijacking scenario possible.

AS A's Perspective


ROV
ROV
A
B
C
D
E
Target
F
G
Hijacker
Expected traffic propagation
Hijacker invisible (not reachable)

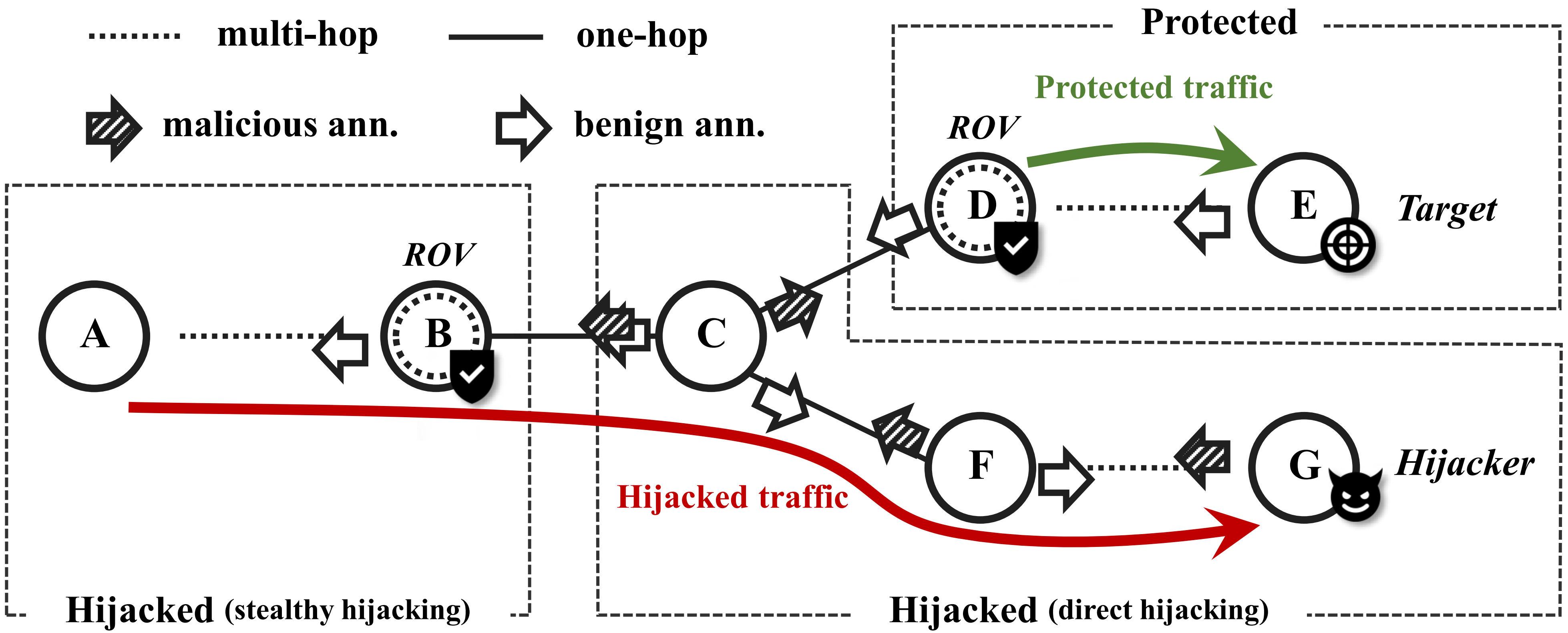
- The hijacker is invisible to AS A on the control plane, due to the ROV filtering of AS B
- AS A would expect its traffic safely forwarded along the correct path (green)

Global Perspective


ROV
ROV
AS C diverts traffic to the hijacker
A
B
C
D
E
F
G
Target
Hijacker
Actual traffic propagation (as expected)
Actual traffic propagation (hijacked)

- AS C, however, is not protected by ROV, and diverts traffic to the hijacker, as long as it accepts the prefix (either the target prefix or a subprefix of it) announced by the hijacker.
- AS A falls victim to hijacking unknowingly.

Stealthy Hijacking: An Unexpected Downside of ROV



Stealthy hijacking can evade all self-operated control-plane detections.

Content

1. Background on BGP (In)security
2. BGP Hijacking in the ROV Era: A Real Case
3. Is BGP Hijacking Becoming More Elusive?
4. Real-World Observations & Insights
5. Towards Analytical Risk Assessment
6. Discussions & Future Work

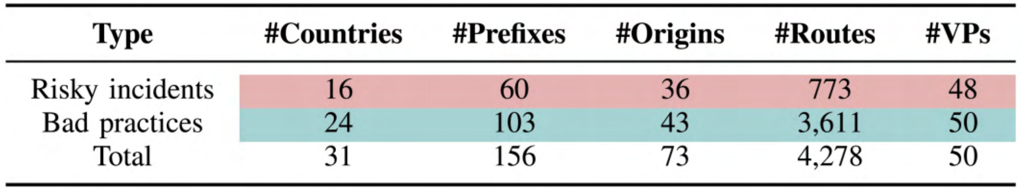
Stealthy Hijacking in the Wild

Data Sources

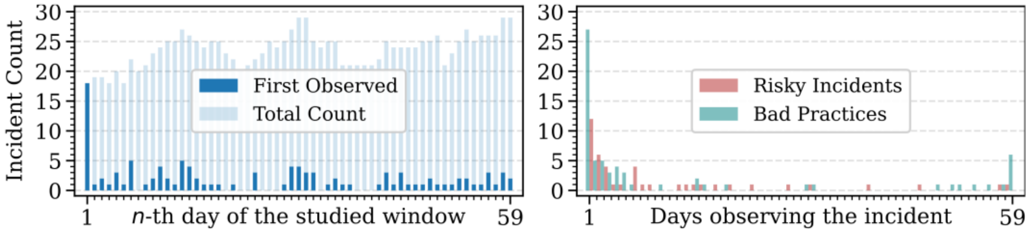
- Routing data: Daily RIB from RouteViews collectors (route-views2, amsix, wide) since Jan 1, 2025.
- Prefix-origin legitimacy: RIPE NCC’s RPKI archives, RADb IRR database, the 5 RIRs’ WHOIS.
- Behaviors: CAIDA’s AS Relationship and Organization data, IANA’s ASN allocation status.

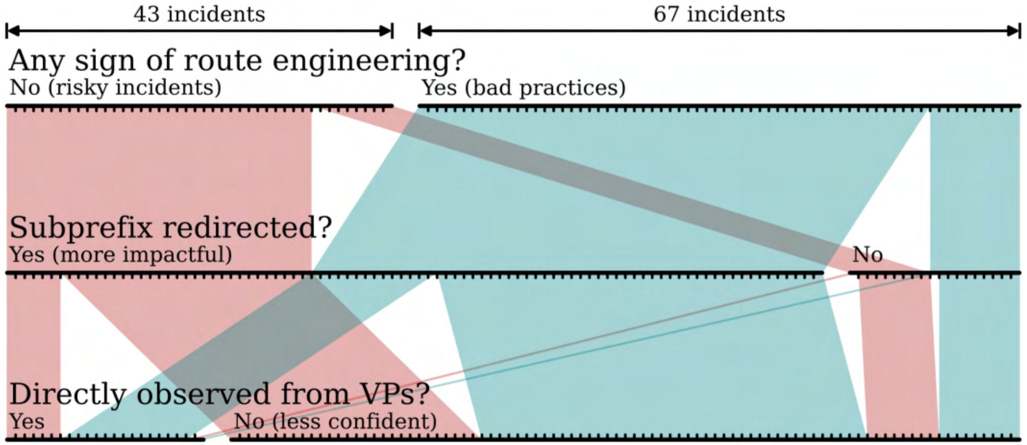
Results (first two months)

- **1,394 observations**
  - 18-29 per day, 0-5 newly discovered daily
- **110 unique incidents**
  - 69.1% last within 7 days, 12.7% over 30 days
  - 67 linked to poor route engineering
  - 91 involving sub-prefix hijacking
  - 22 directly observed from vantage points
- **Impact:**



Type	#Countries	#Prefixes	#Origins	#Routes	#VPs
Risky incidents	16	60	36	773	48
Bad practices	24	103	43	3,611	50
Total	31	156	73	4,278	50





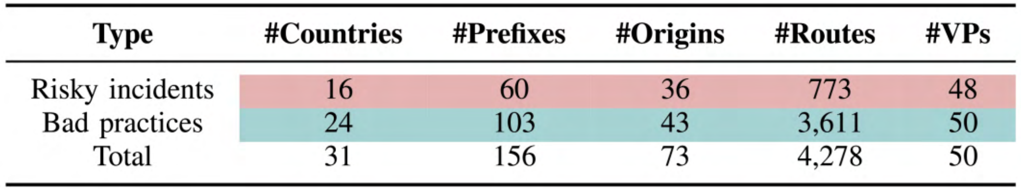
Stealthy Hijacking in the Wild

Data Sources

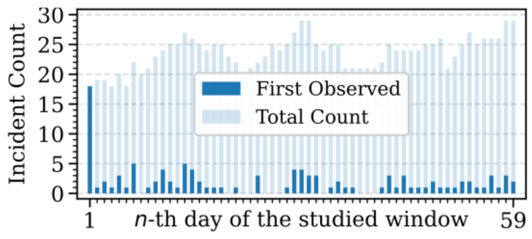
- Routing data: Daily RIB from RouteViews collectors (route-views2, amsix, wide) since Jan 1, 2025.
- Prefix-origin legitimacy: RIPE NCC’s RPKI archives, RADb IRR database, the 5 RIRs’ WHOIS.
- Behaviors: CAIDA’s AS Relationship and Organization data, IANA’s ASN allocation status.

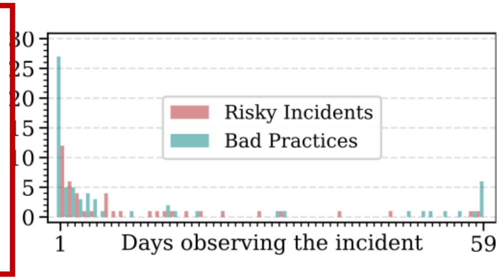
Results (first two months)

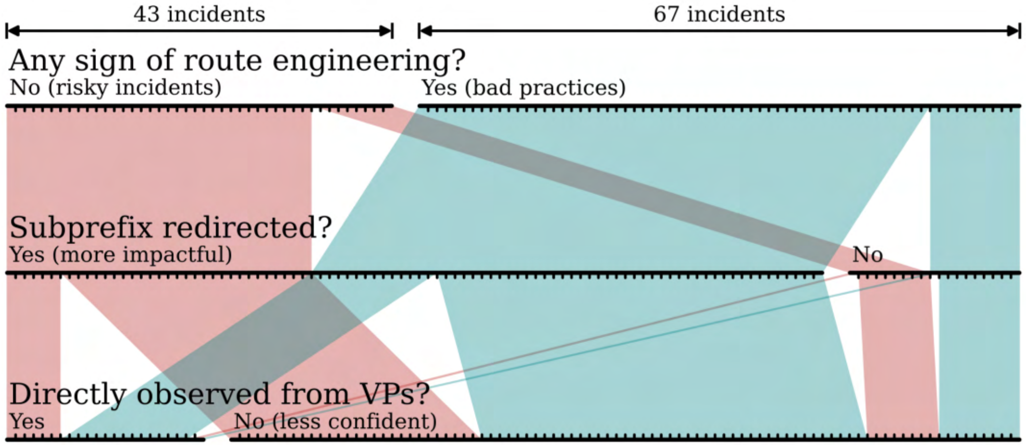
- **1,394 observations**
  - 18-29 per day, 0-5 newly discovered daily
- **110 unique incidents**
  - 69.1% last within 7 days, 12.7% over 30 days
  - 67 linked to poor route engineering
  - 91 involving sub-prefix hijacking
  - 22 directly observed from vantage points
- **Impact:**



Type	#Countries	#Prefixes	#Origins	#Routes	#VPs
Risky incidents	16	60	36	773	48
Bad practices	24	103	43	3,611	50
Total	31	156	73	4,278	50







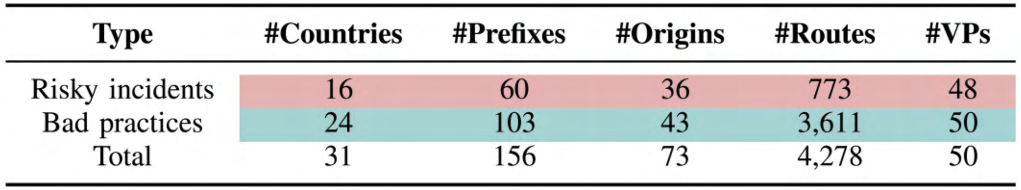
Stealthy Hijacking in the Wild

Data Sources

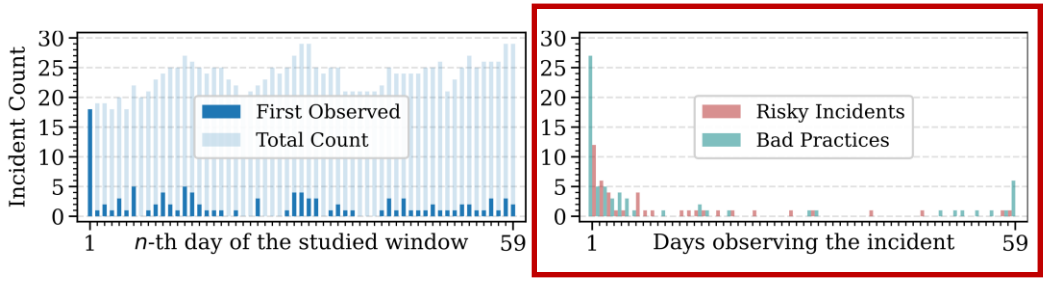
- Routing data: Daily RIB from RouteViews collectors (route-views2, amsix, wide) since Jan 1, 2025.
- Prefix-origin legitimacy: RIPE NCC's RPKI archives, RADb IRR database, the 5 RIRs' WHOIS.
- Behaviors: CAIDA's AS Relationship and Organization data, IANA's ASN allocation status.

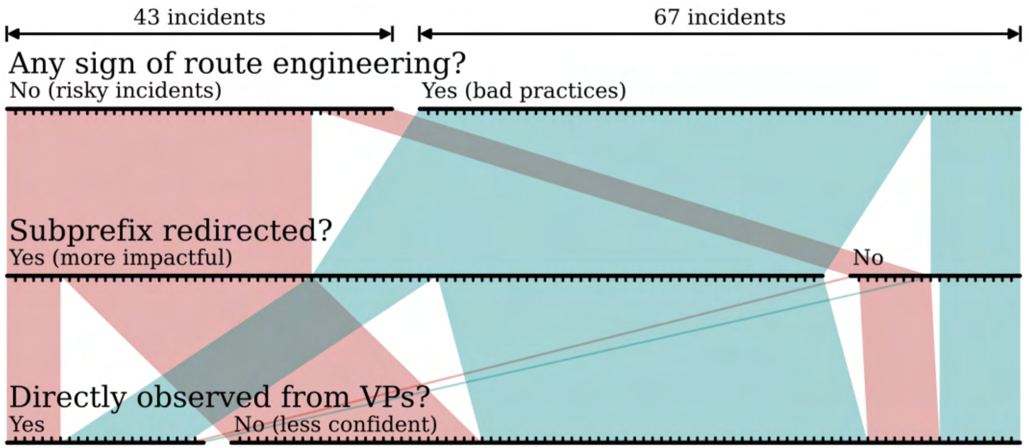
Results (first two months)

- **1,394 observations**
  - 18-29 per day, 0-5 newly discovered daily
- **110 unique incidents**
  - 69.1% last within 7 days, 12.7% over 30 days
  - 67 linked to poor route engineering
  - 91 involving sub-prefix hijacking
  - 22 directly observed from vantage points
- **Impact:**



Type	#Countries	#Prefixes	#Origins	#Routes	#VPs
Risky incidents	16	60	36	773	48
Bad practices	24	103	43	3,611	50
Total	31	156	73	4,278	50





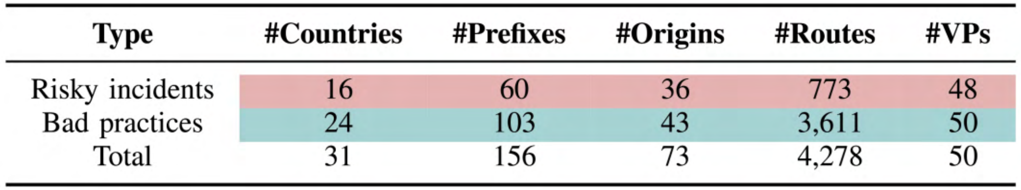
Stealthy Hijacking in the Wild

Data Sources

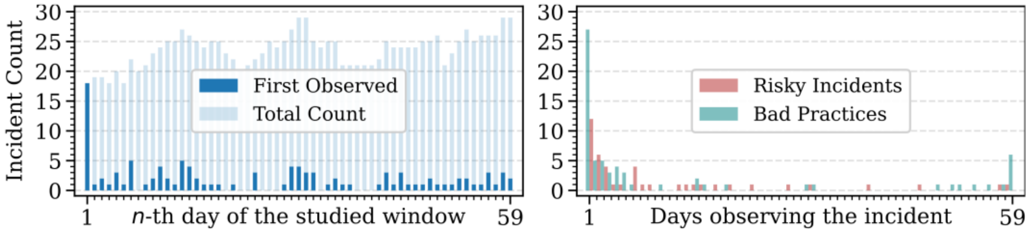
- Routing data: Daily RIB from RouteViews collectors (route-views2, amsix, wide) since Jan 1, 2025.
- Prefix-origin legitimacy: RIPE NCC's RPKI archives, RADb IRR database, the 5 RIRs' WHOIS.
- Behaviors: CAIDA's AS Relationship and Organization data, IANA's ASN allocation status.

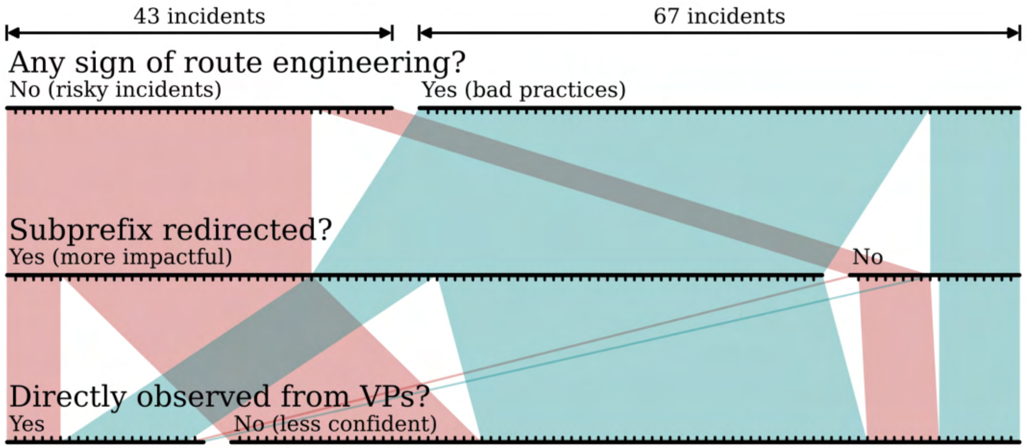
Results (first two months)

- **1,394 observations**
  - 18-29 per day, 0-5 newly discovered daily
- **110 unique incidents**
  - 69.1% last within 7 days, 12.7% over 30 days
  - 67 linked to poor route engineering
  - 91 involving sub-prefix hijacking
  - 22 directly observed from vantage points
- **Impact:**



Type	#Countries	#Prefixes	#Origins	#Routes	#VPs
Risky incidents	16	60	36	773	48
Bad practices	24	103	43	3,611	50
Total	31	156	73	4,278	50





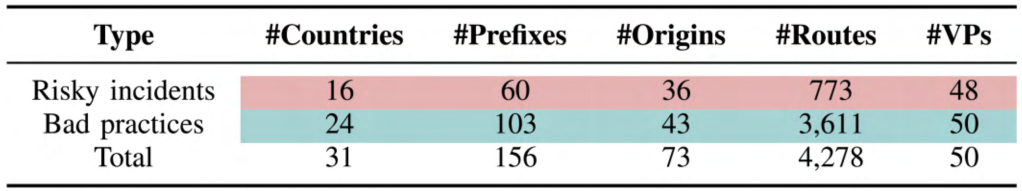
Stealthy Hijacking in the Wild

Data Sources

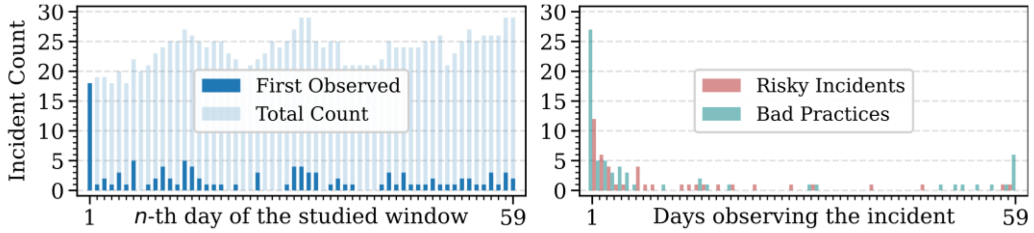
- Routing data: Daily RIB from RouteViews collectors (route-views2, amsix, wide) since Jan 1, 2025.
- Prefix-origin legitimacy: RIPE NCC's RPKI archives, RADb IRR database, the 5 RIRs' WHOIS.
- Behaviors: CAIDA's AS Relationship and Organization data, IANA's ASN allocation status.

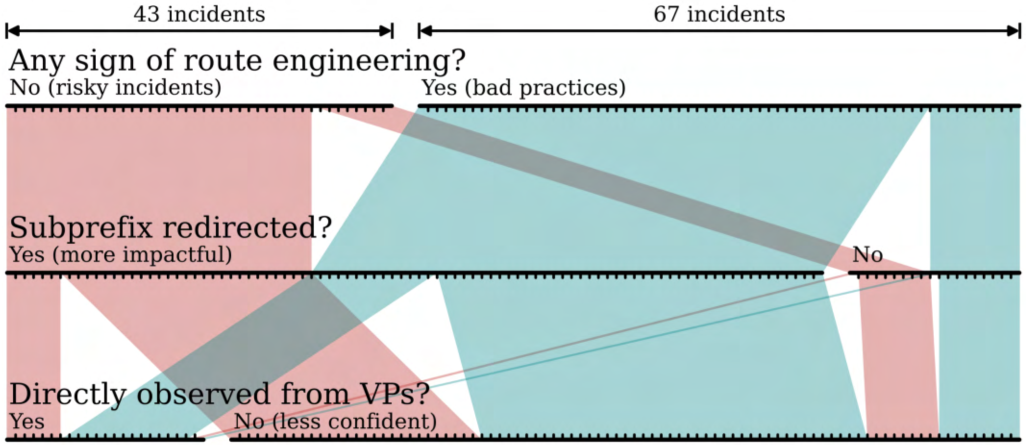
Results (first two months)

- **1,394 observations**
  - 18-29 per day, 0-5 newly discovered daily
- **110 unique incidents**
  - 69.1% last within 7 days, 12.7% over 30 days
  - 67 linked to poor route engineering
  - 91 involving sub-prefix hijacking
  - 22 directly observed from vantage points
- **Impact:**



Type	#Countries	#Prefixes	#Origins	#Routes	#VPs
Risky incidents	16	60	36	773	48
Bad practices	24	103	43	3,611	50
Total	31	156	73	4,278	50





43 incidents

67 incidents

Any sign of route engineering?

No (risky incidents)

Yes (bad practices)

Subprefix redirected?

Yes (more impactful)

No

Directly observed from VPs?

Yes

No (less confident)

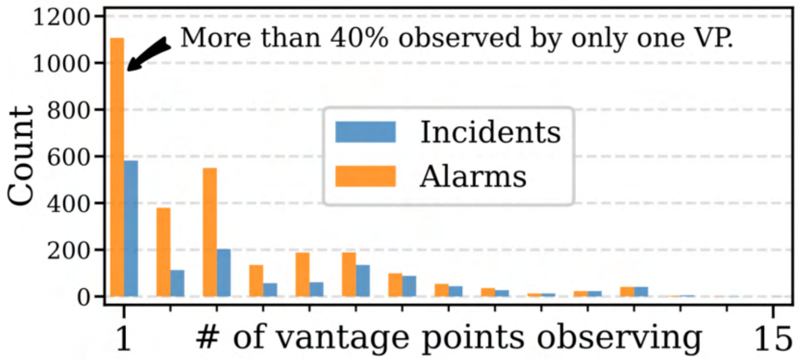
Stealthy Hijacking in the Wild

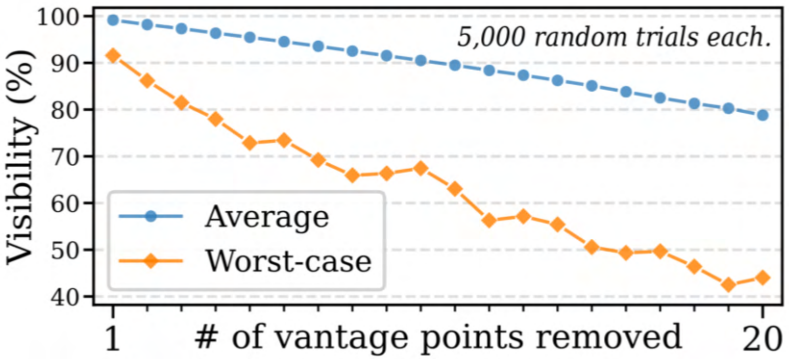
Number of VPs observing each incident

- Most incidents are seen by three or fewer VPs, with over 40% visible to only one VP.

Incident visibility w/ random VP removal

- Removing 20 VPs: 22% average drop in observable incidents, and up to 55% drop in the worst case.





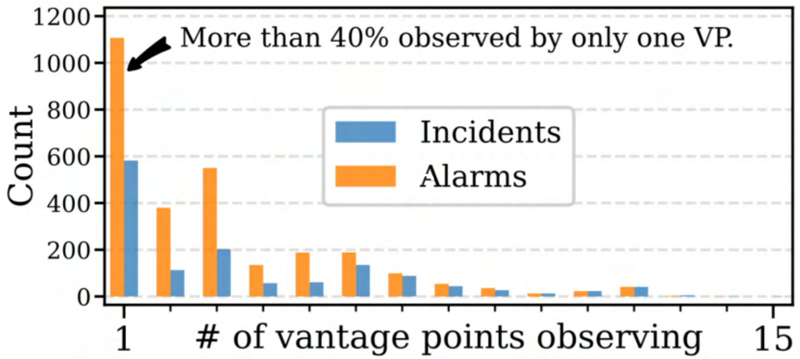
Stealthy Hijacking in the Wild

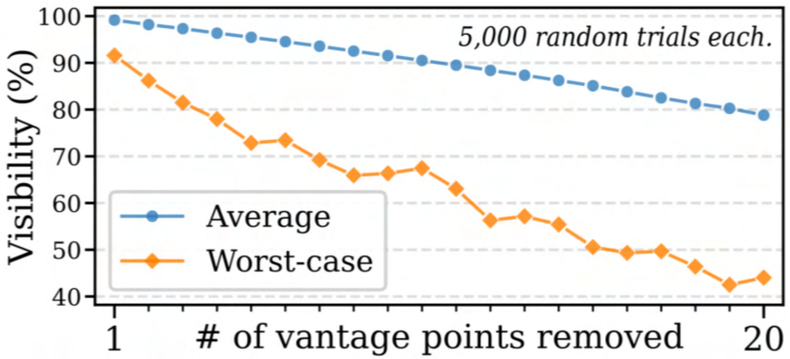
Number of VPs observing each incident

- Most incidents are seen by three or fewer VPs, with over 40% visible to only one VP.

Incident visibility w/ random VP removal

- Removing 20 VPs: 22% average drop in observable incidents, and up to 55% drop in the worst case.





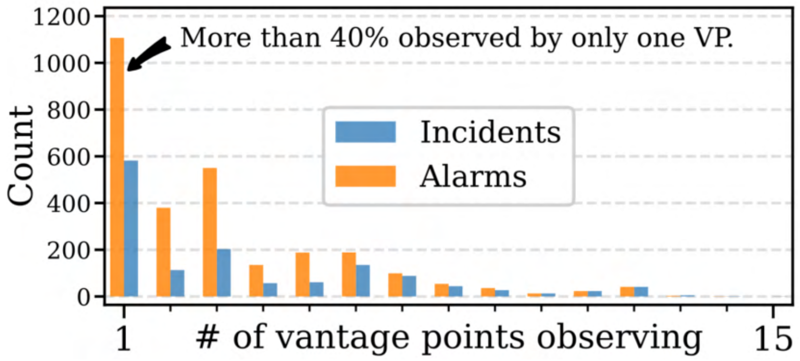
Stealthy Hijacking in the Wild

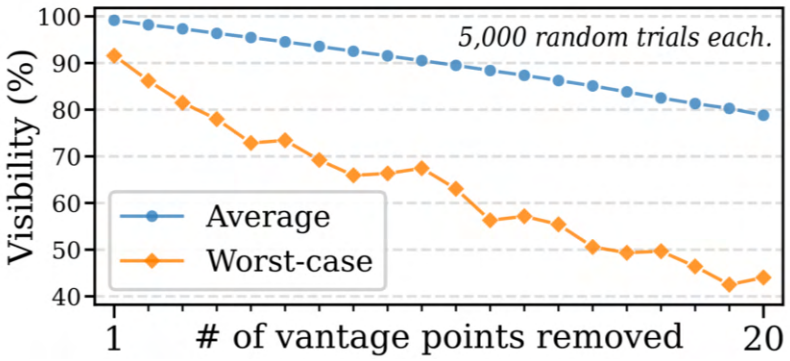
Number of VPs observing each incident

- Most incidents are seen by three or fewer VPs, with over 40% visible to only one VP.

Incident visibility w/ random VP removal

- Removing 20 VPs: 22% average drop in observable incidents, and up to 55% drop in the worst case.





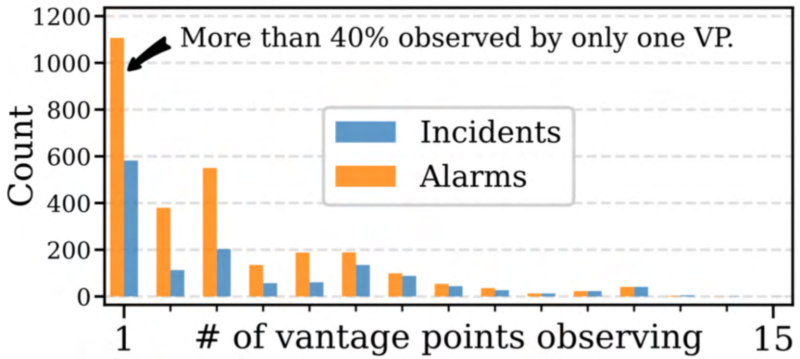
Stealthy Hijacking in the Wild

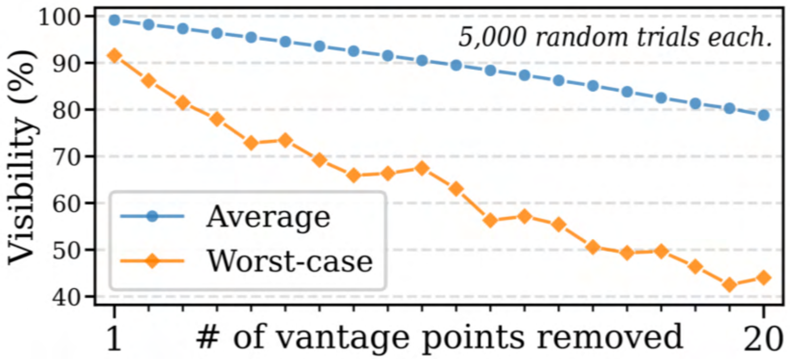
Number of VPs observing each incident

- Most incidents are seen by three or fewer VPs, with over 40% visible to only one VP.

Incident visibility w/ random VP removal

- Removing 20 VPs: 22% average drop in observable incidents, and up to 55% drop in the worst case.



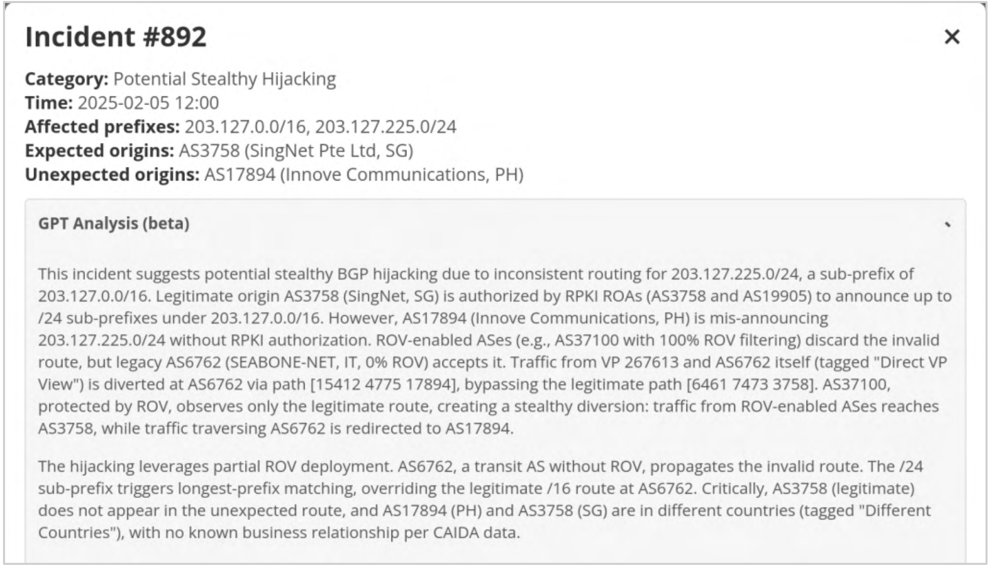


Takeaway#0 Stealthy hijacking in the wild is mostly short-lived and targets sub-prefixes, with new cases emerging almost daily and some persisting long-term, likely due to overlooked misconfigurations. Its exposure is sensitive to vantage points.

Public Monitoring Service

Our website to publish stealthy hijacking incidents in the wild: https://yhchen.cn/stealthy-bgp-hijacking/

- Set up search options and date range
- Search your interested ASN/prefix/organization
- Review the results and feedback
- Beta feature: GPT analysis with routing knowledge augmentation



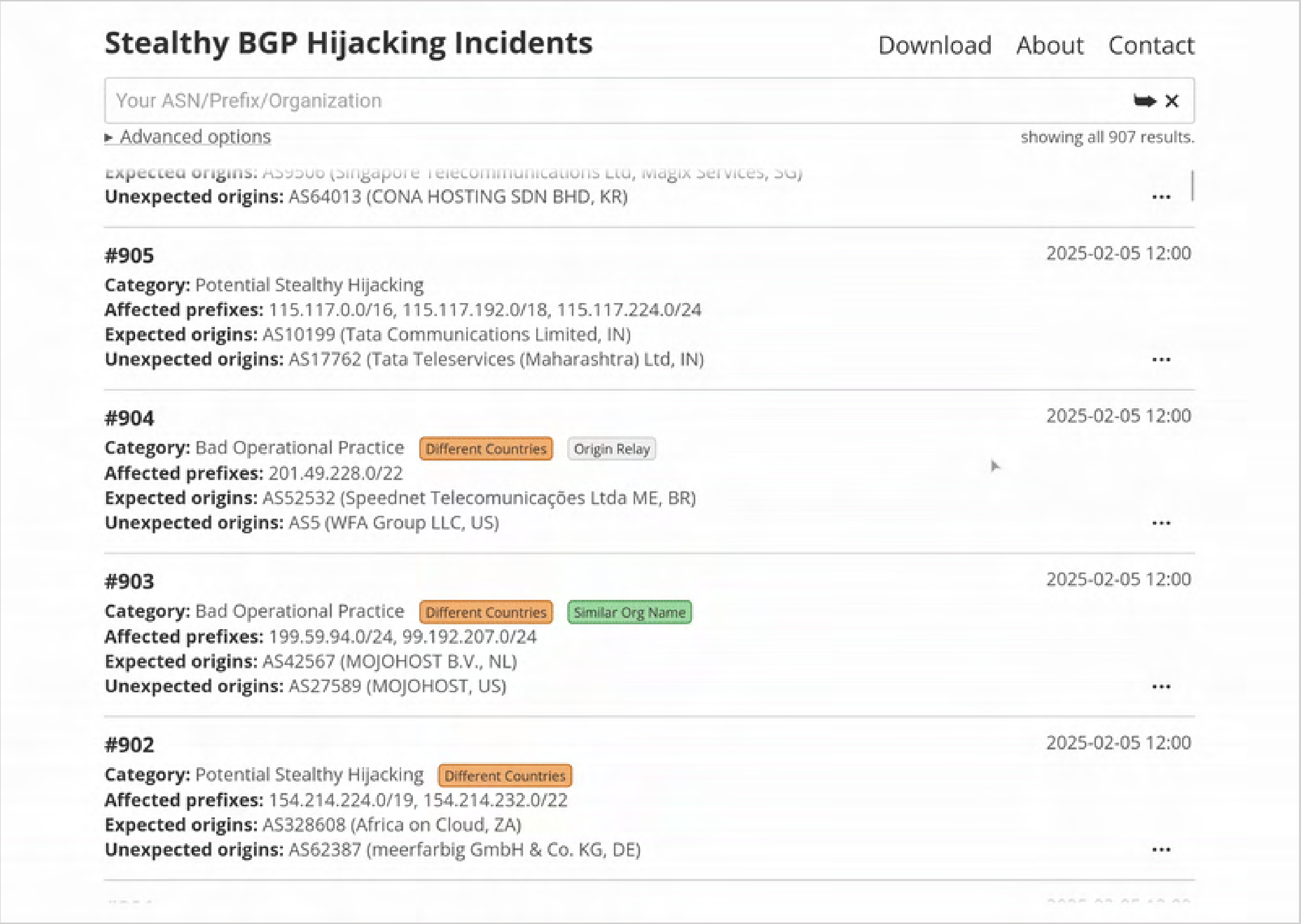
Incident #892

Category: Potential Stealthy Hijacking
Time: 2025-02-05 12:00
Affected prefixes: 203.127.0.0/16, 203.127.225.0/24
Expected origins: AS3758 (SingNet Pte Ltd, SG)
Unexpected origins: AS17894 (Innove Communications, PH)

GPT Analysis (beta)

This incident suggests potential stealthy BGP hijacking due to inconsistent routing for 203.127.225.0/24, a sub-prefix of 203.127.0.0/16. Legitimate origin AS3758 (SingNet, SG) is authorized by RPKI ROAs (AS3758 and AS19905) to announce up to /24 sub-prefixes under 203.127.0.0/16. However, AS17894 (Innove Communications, PH) is mis-announcing 203.127.225.0/24 without RPKI authorization. ROV-enabled ASes (e.g., AS37100 with 100% ROV filtering) discard the invalid route, but legacy AS6762 (SEABONE-NET, IT, 0% ROV) accepts it. Traffic from VP 267613 and AS6762 itself (tagged "Direct VP View") is diverted at AS6762 via path [15412 4775 17894], bypassing the legitimate path [6461 7473 3758]. AS37100, protected by ROV, observes only the legitimate route, creating a stealthy diversion: traffic from ROV-enabled ASes reaches AS3758, while traffic traversing AS6762 is redirected to AS17894.

The hijacking leverages partial ROV deployment. AS6762, a transit AS without ROV, propagates the invalid route. The /24 sub-prefix triggers longest-prefix matching, overriding the legitimate /16 route at AS6762. Critically, AS3758 (legitimate) does not appear in the unexpected route, and AS17894 (PH) and AS3758 (SG) are in different countries (tagged "Different Countries"), with no known business relationship per CAIDA data.



Stealthy BGP Hijacking Incidents

showing all 907 results.

Expected origins: AS9506 (Singapore Telecommunications Ltd, Magix Services, SG)
Unexpected origins: AS64013 (CONA HOSTING SDN BHD, KR) ...

#905 2025-02-05 12:00
Category: Potential Stealthy Hijacking
Affected prefixes: 115.117.0.0/16, 115.117.192.0/18, 115.117.224.0/24
Expected origins: AS10199 (Tata Communications Limited, IN)
Unexpected origins: AS17762 (Tata Teleservices (Maharashtra) Ltd, IN) ...

#904 2025-02-05 12:00
Category: Bad Operational Practice Different Countries Origin Relay
Affected prefixes: 201.49.228.0/22
Expected origins: AS52532 (Speednet Telecomunicações Ltda ME, BR)
Unexpected origins: AS5 (WFA Group LLC, US) ...

#903 2025-02-05 12:00
Category: Bad Operational Practice Different Countries Similar Org Name
Affected prefixes: 199.59.94.0/24, 99.192.207.0/24
Expected origins: AS42567 (MOJOHOST B.V., NL)
Unexpected origins: AS27589 (MOJOHOST, US) ...

#902 2025-02-05 12:00
Category: Potential Stealthy Hijacking Different Countries
Affected prefixes: 154.214.224.0/19, 154.214.232.0/22
Expected origins: AS328608 (Africa on Cloud, ZA)
Unexpected origins: AS62387 (meerfarbig GmbH & Co. KG, DE) ...

* Daily analysis results since 2025-01-01

Content

1. Background on BGP (In)security
2. BGP Hijacking in the ROV Era: A Real Case
3. Is BGP Hijacking Becoming More Elusive?
4. Real-World Observations & Insights
5. Towards Analytical Risk Assessment
6. Discussions & Future Work

Why Analytical Risk Assessment?

Questions unanswered:

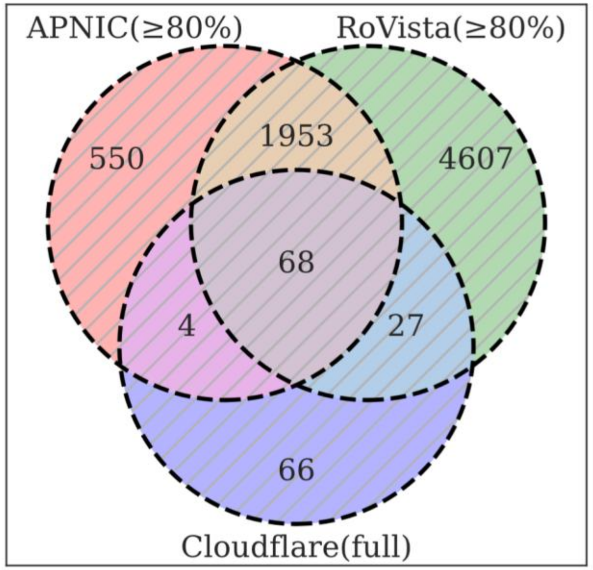
The prevalence, extent, distribution, influencing factors, etc. of the risk within our real-world Internet.

- Use **CAIDA AS relationships** to reconstruct Internet topology
- Use **APNIC, RoVista, Cloudflare** measurement to gain ROV deployment status
- Perform BGP route inference on the topology and generate **all Internet-scale routes**
- Thoroughly analyze **all possible "victim-target-hijacker" 3-tuple** to determine those at risk of stealthy BGP hijacking.

Is it possible to **comprehensively** assess the stealthy hijacking risk introduced by the **current** ROV deployment?

Challenges: Criteria to identify risk? Knowledge of routes? Measurement of ROV deployment? ......

Results: Overall Risk Level



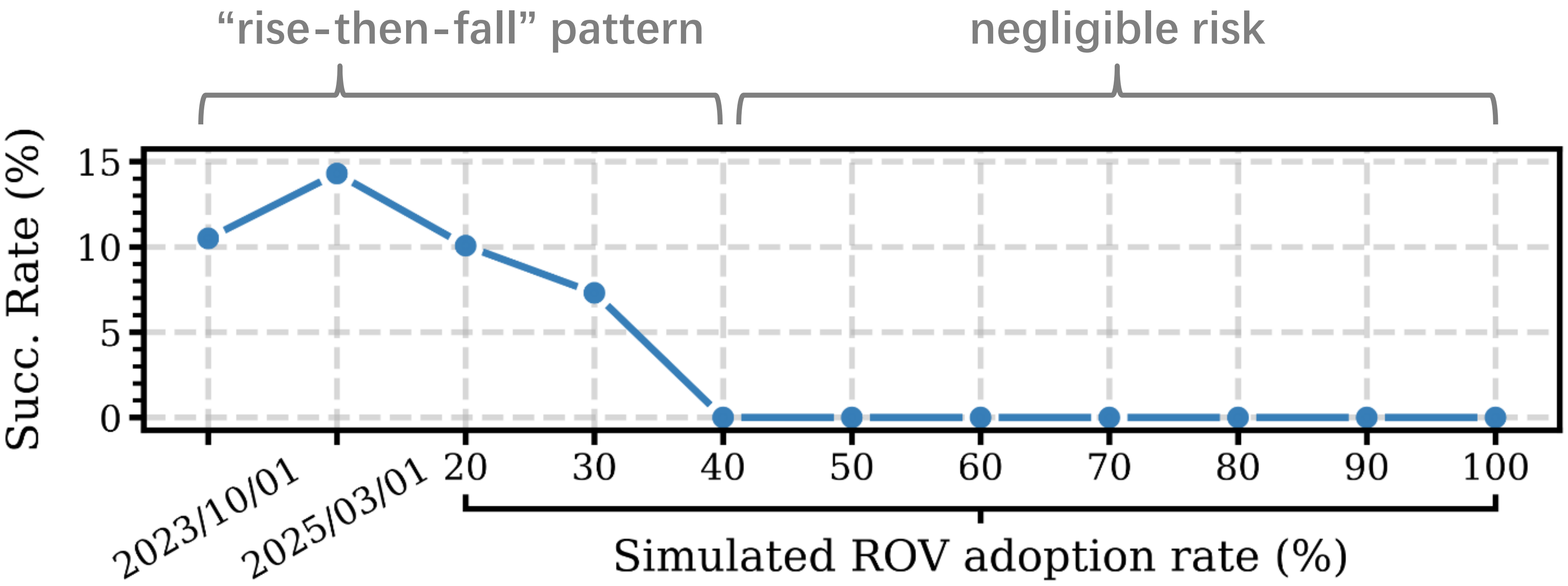
7,275 ASes identified ROV-enabled by three sources collectively

Stealthy Hijacking	Sub-Prefix	Exact-Prefix
w/ ROV	0.141 ▲0.141	0.002 ▲0.002
w/o ROV	0.000	0.000

Direct Hijacking	Sub-Prefix	Exact-Prefix
w/ ROV	0.419 ▼0.567	0.106 ▼0.248
w/o ROV	0.986	0.354

Takeaway#1 While effectively mitigating direct hijacking risk, the current partial ROV deployment significantly amplifies stealthy hijacking risk from 0 to a 14.1% overall success probability. This risk arises solely due to ROV deployment.

Results: Risk Evolution Pattern



Takeaway#7 Stealthy BGP hijacking risk initially rises as ROV deployment increases but eventually declines once deployment exceeds a threshold, i.e., a "rise-then-decline" pattern. Current data suggest we may now be entering the declining phase.

Content

1. Background on BGP (In)security
2. BGP Hijacking in the ROV Era: A Real Case
3. Is BGP Hijacking Becoming More Elusive?
4. Real-World Observations & Insights
5. Towards Analytical Risk Assessment
6. Discussions & Future Work

Discussions & Future Work

Limitations of the approach

- Not including complex routing policies for now
- False positives due to route filtering (not so much)

Operational insights

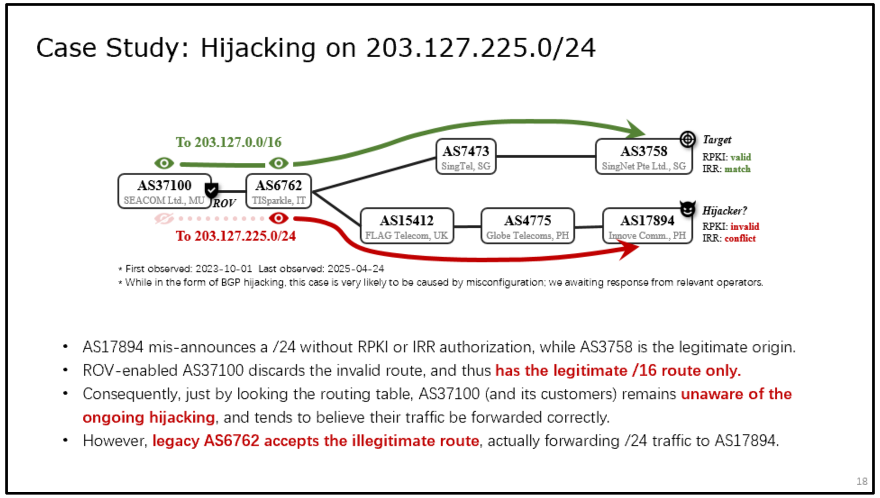
- For network operators: stay alert about discarded routes
- Route collector platforms and probing facilities help a lot
- Docs & community: IETF drafts, RFC work, and open discussions

Risk countermeasures

- Keep increasing RPKI/ROV deployment (according to Takeaway#2)
- Co-analyzing routing data from multiple VP to identify inconsistencies
- Collaboration among ROV-enabled ASes to share threat information
- Select routes without ASes that appear on the dropped invalid routes

Summary

Motivation: a real-world case

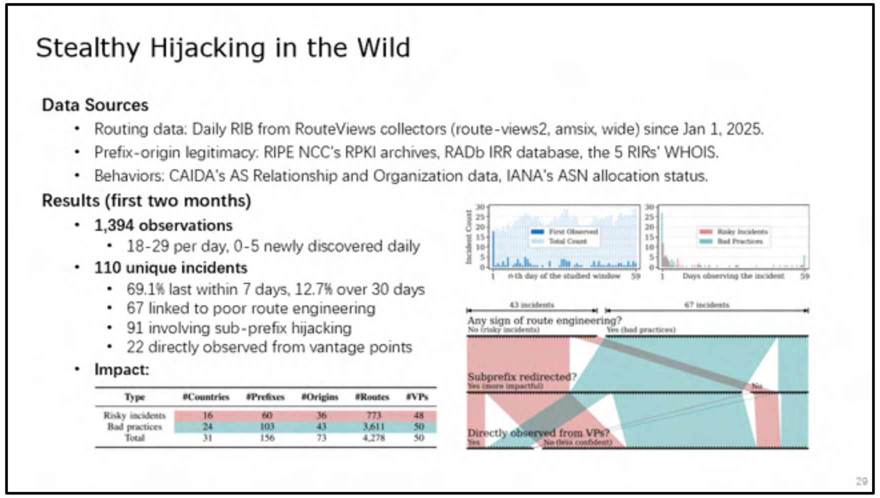


Case Study: Hijacking on 203.127.225.0/24

* First observed: 2023-10-01 Last observed: 2025-04-24
* While in the form of BGP hijacking, this case is very likely to be caused by misconfiguration; we awaiting response from relevant operators.

- AS17894 mis-announces a /24 without RPKI or IRR authorization, while AS3758 is the legitimate origin.
- ROV-enabled AS37100 discards the invalid route, and thus **has the legitimate /16 route only**.
- Consequently, just by looking the routing table, AS37100 (and its customers) remains **unaware of the ongoing hijacking**, and tends to believe their traffic be forwarded correctly.
- However, **legacy AS6762 accepts the illegitimate route**, actually forwarding /24 traffic to AS17894.

Approach: empirical + analytical



Stealthy Hijacking in the Wild

Data Sources

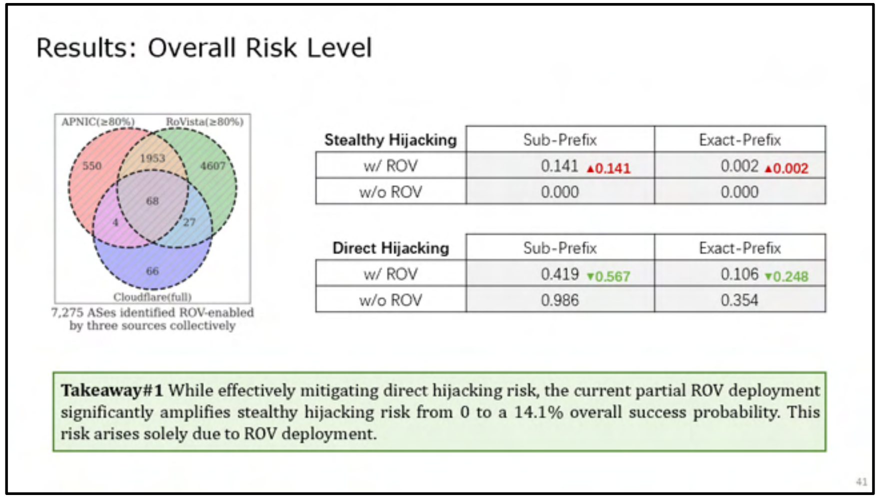
- Routing data: Daily RIB from RouteViews collectors (route-views2, amsix, wide) since Jan 1, 2025.
- Prefix-origin legitimacy: RIPE NCC's RPKI archives, RADb IRR database, the 5 RIRs' WHOIS.
- Behaviors: CAIDA's AS Relationship and Organization data, IANA's ASN allocation status.

Results (first two months)

- **1,394 observations**
  - 18-29 per day, 0-5 newly discovered daily
- **110 unique incidents**
  - 69.1% last within 7 days, 12.7% over 30 days
  - 67 linked to poor route engineering
  - 91 involving sub-prefix hijacking
  - 22 directly observed from vantage points
- **Impact:**

Type	#Countries	#Prefixes	#Origins	#Routes	#VPs
Risky incidents	16	60	36	773	48
Bad practices	24	103	43	3,611	50
Total	31	156	73	4,278	50

Evaluation: eight takeaways



Results: Overall Risk Level

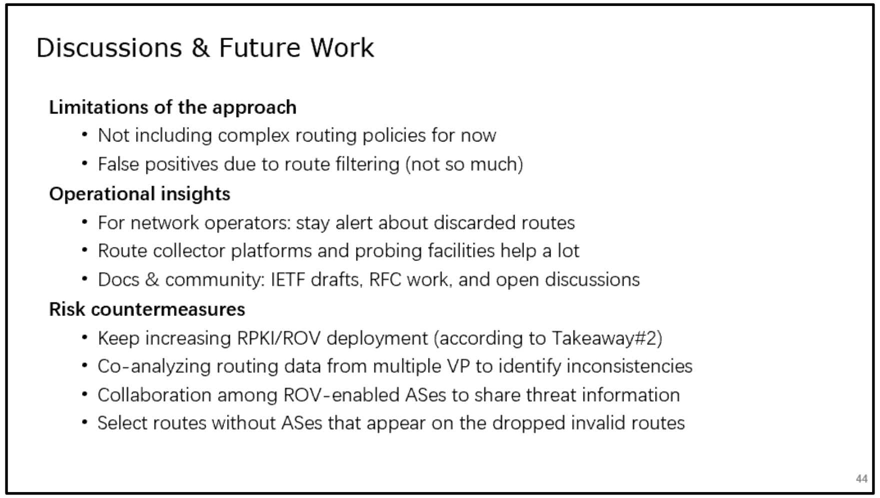
7,275 ASes identified ROV-enabled by three sources collectively

Stealthy Hijacking	Sub-Prefix	Exact-Prefix
w/ ROV	0.141 ▲0.141	0.002 ▲0.002
w/o ROV	0.000	0.000

Direct Hijacking	Sub-Prefix	Exact-Prefix
w/ ROV	0.419 ▼0.567	0.106 ▼0.248
w/o ROV	0.986	0.354

Takeaway#1 While effectively mitigating direct hijacking risk, the current partial ROV deployment significantly amplifies stealthy hijacking risk from 0 to a 14.1% overall success probability. This risk arises solely due to ROV deployment.

Discussion: limitations & future work



Discussions & Future Work

Limitations of the approach

- Not including complex routing policies for now
- False positives due to route filtering (not so much)

Operational insights

- For network operators: stay alert about discarded routes
- Route collector platforms and probing facilities help a lot
- Docs & community: IETF drafts, RFC work, and open discussions

Risk countermeasures

- Keep increasing RPKI/ROV deployment (according to Takeaway#2)
- Co-analyzing routing data from multiple VP to identify inconsistencies
- Collaboration among ROV-enabled ASes to share threat information
- Select routes without ASes that appear on the dropped invalid routes

Q&A

Artifact Evaluated
NDSS
SYMPOSIUM
Available
Functional
Reproduced

Thank you!

Key Takeaways

- Partial ROV deployment introduces stealthy hijacking risks to the current Internet.
- Risk assessment is viable based on complete knowledge of routes and ROV deployment.
- We seek insights from both real-world observations and analytical analysis.
- A 14.1% success rate of stealthy hijacking is introduced by the current ROV deployment.

Contact: yh-chen21@mails.tsinghua.edu.cn (Yihao Chen)

Online Service: https://yhchen.cn/stealthy-bgp-hijacking

BGP Simulator: https://github.com/yhchen-tsinghua/matrix-bgpsim

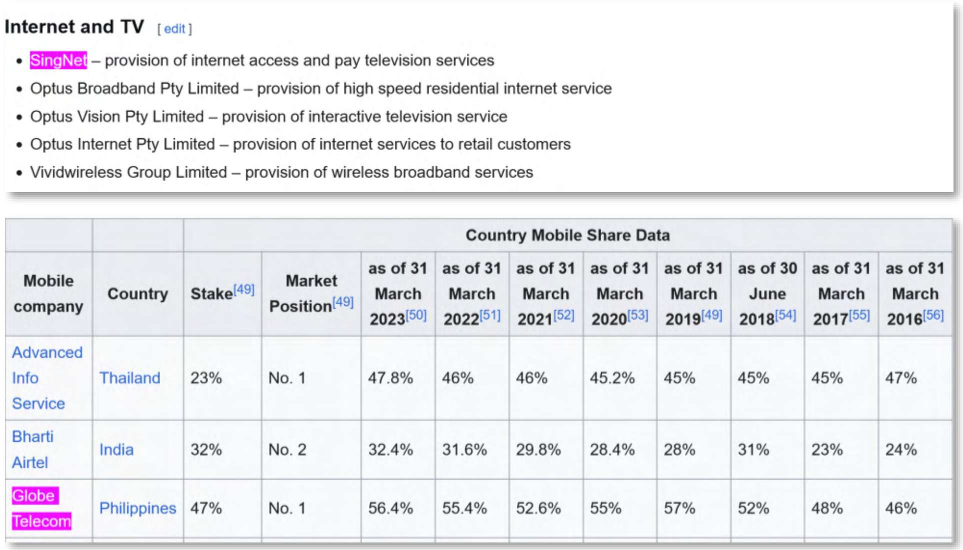
Artifact: https://github.com/yhchen-tsinghua/stealthy-bgp-hijacking

Appendix: Intent behind the Example Incident?

The incident is likely caused by benign misconfiguration, given that:

1. AS17894’s parent organization, **Innove Communications**, is a subsidiary of **Globe Telecom**
2. AS3758’s parent organization, **SingNet**, is operated by **SingTel**
3. **SingTel** is the principal shareholder of **Globe Telecom**

We informed Global Telecom about the incident and received promise to investigate.

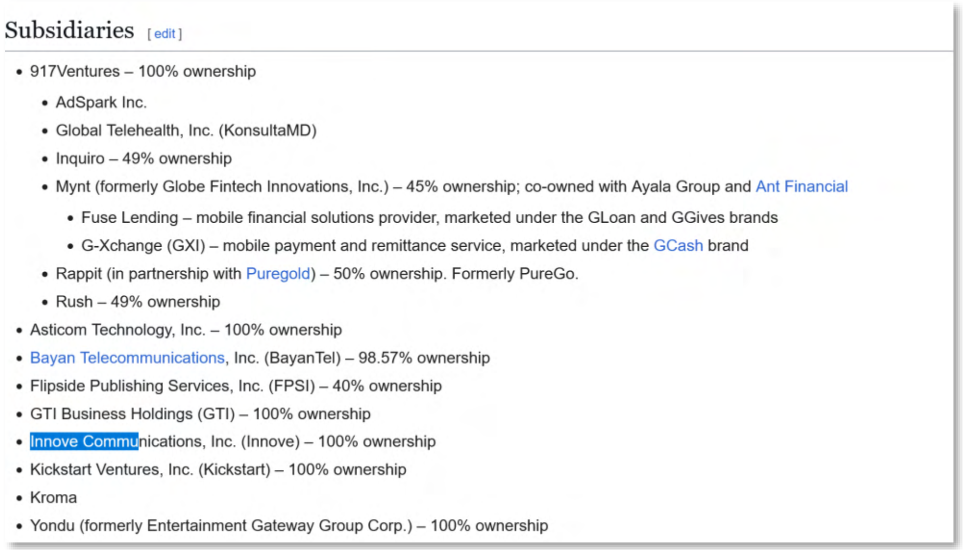


Internet and TV [edit]

- SingNet – provision of internet access and pay television services
- Optus Broadband Pty Limited – provision of high speed residential internet service
- Optus Vision Pty Limited – provision of interactive television service
- Optus Internet Pty Limited – provision of internet services to retail customers
- Vividwireless Group Limited – provision of wireless broadband services

		Country Mobile Share Data									
Mobile company	Country	Stake[49]	Market Position[49]	as of 31 March 2023[50]	as of 31 March 2022[51]	as of 31 March 2021[52]	as of 31 March 2020[53]	as of 31 March 2019[49]	as of 30 June 2018[54]	as of 31 March 2017[55]	as of 31 March 2016[56]
Advanced Info Service	Thailand	23%	No. 1	47.8%	46%	46%	45.2%	45%	45%	45%	47%
Bharti Airtel	India	32%	No. 2	32.4%	31.6%	29.8%	28.4%	28%	31%	23%	24%
Globe Telecom	Philippines	47%	No. 1	56.4%	55.4%	52.6%	55%	57%	52%	48%	46%

Wikipedia snippet of “SingTel”



Subsidiaries [edit]

- 917Ventures – 100% ownership
  - AdSpark Inc.
  - Global Telehealth, Inc. (KonsultaMD)
  - Inquiro – 49% ownership
  - Mynt (formerly Globe Fintech Innovations, Inc.) – 45% ownership; co-owned with Ayala Group and Ant Financial
    - Fuse Lending – mobile financial solutions provider, marketed under the GLoan and GGives brands
    - G-Xchange (GXI) – mobile payment and remittance service, marketed under the GCash brand
  - Rappit (in partnership with Puregold) – 50% ownership. Formerly PureGo.
  - Rush – 49% ownership
- Asticom Technology, Inc. – 100% ownership
- Bayan Telecommunications, Inc. (BayanTel) – 98.57% ownership
- Flipside Publishing Services, Inc. (FPSI) – 40% ownership
- GTI Business Holdings (GTI) – 100% ownership
- Innove Communications, Inc. (Innove) – 100% ownership
- Kickstart Ventures, Inc. (Kickstart) – 100% ownership
- Kroma
- Yondu (formerly Entertainment Gateway Group Corp.) – 100% ownership

Wikipedia snippet of “Globe Telecom”

Appendix: Heuristics for Stealthy Hijacking Discovery

Data Sources

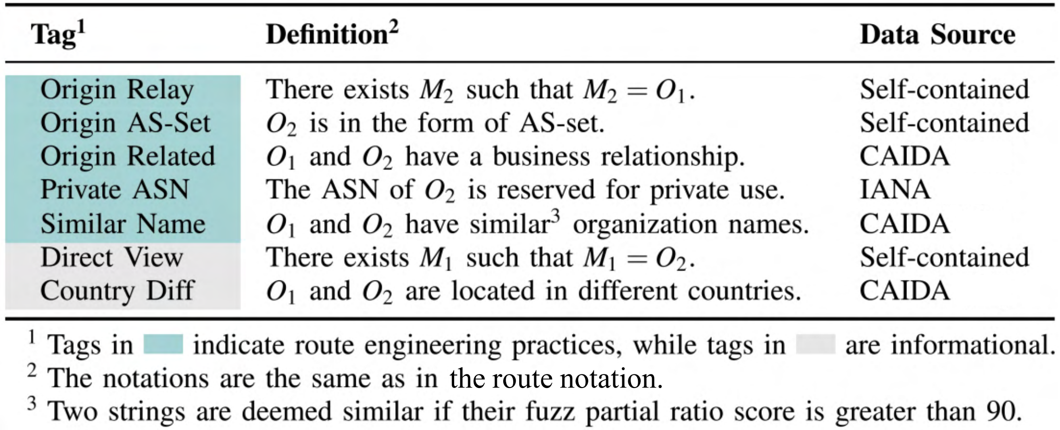
- Routing data: Daily RIB from RouteViews collectors (route-views2, amsix, wide) since Jan 1, 2025.
- Prefix-origin legitimacy: RIPE NCC’s RPKI archives, RADb IRR database, the 5 RIRs’ WHOIS.
- Tagging: CAIDA’s AS Relationship and Organization data, IANA’s ASN allocation status.

Heuristics

- Given two routes $p_1 \colon V_1 \cdots (M_1) \cdots O_1$ and $p_2 \colon V_2 \cdots (M_2) \cdots O_2$, examine the following conditions:
  a) Conflict: p_2 equals or is a sub-prefix of p_1, and $O_2 \neq O_1$.
  b) Unauthorized: p_2/O_2 is RPKI-invalid, IRR-conflicting, and WHOIS-mismatching, while p_1/O_1 is all good.
  c) Stealthiness: V_1 has no route to p_2 originated by O_2.
  d) Risk-critical AS: There exist M_1 and M_2, with $M_1 = M_2$.
  e) Risk-critical VP: There exists M_1, such that $M_1 = V_2$.
- **Loose Heuristics:** conditions (a)-(d) hold.
- **Strict Heuristics:** conditions (a)-(c) and (e) hold.

Tags

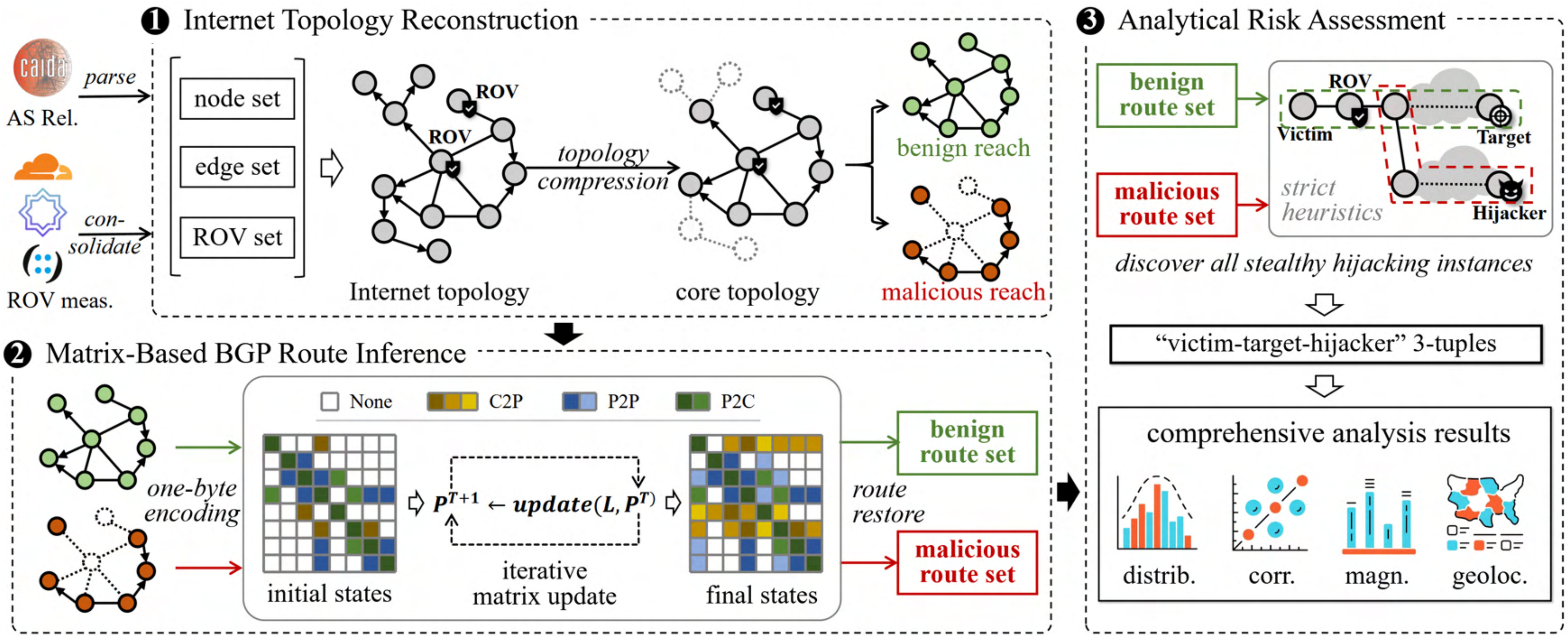
- Incidents w/o any signs of route engineering is **risky**
- Otherwise, it is considered **benign misconfiguration**



Tag[1]	Definition[2]	Data Source
Origin Relay	There exists M_2 such that $M_2 = O_1$.	Self-contained
Origin AS-Set	O_2 is in the form of AS-set.	Self-contained
Origin Related	O_1 and O_2 have a business relationship.	CAIDA
Private ASN	The ASN of O_2 is reserved for private use.	IANA
Similar Name	O_1 and O_2 have similar[3] organization names.	CAIDA
Direct View	There exists M_1 such that $M_1 = O_2$.	Self-contained
Country Diff	O_1 and O_2 are located in different countries.	CAIDA

[1] Tags in 🟦 indicate route engineering practices, while tags in ⬜ are informational.
[2] The notations are the same as in the route notation.
[3] Two strings are deemed similar if their fuzz partial ratio score is greater than 90.

Appendix: Analytical Risk Assessment Workflow



Appendix: Gap in Existing Studies

- ROV++ [Morillo et al, NDSS'21]
  - ➢ Assume **unrealistic ROV deployment** for experiments.
  - ➢ Evaluate with **limited stealthy hijacking samples**.
  - ➢ Present **overall hijacking rate** only.

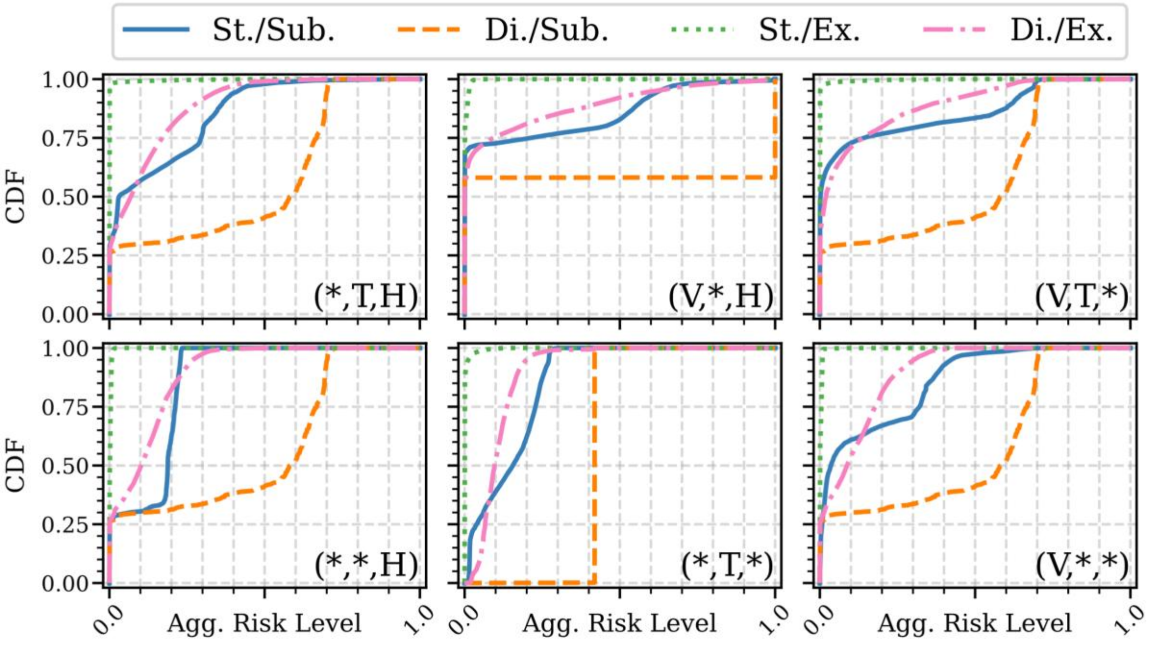
Questions unanswered:

The prevalence, extent, distribution, influencing factors, etc. of the risk within our real-world Internet.

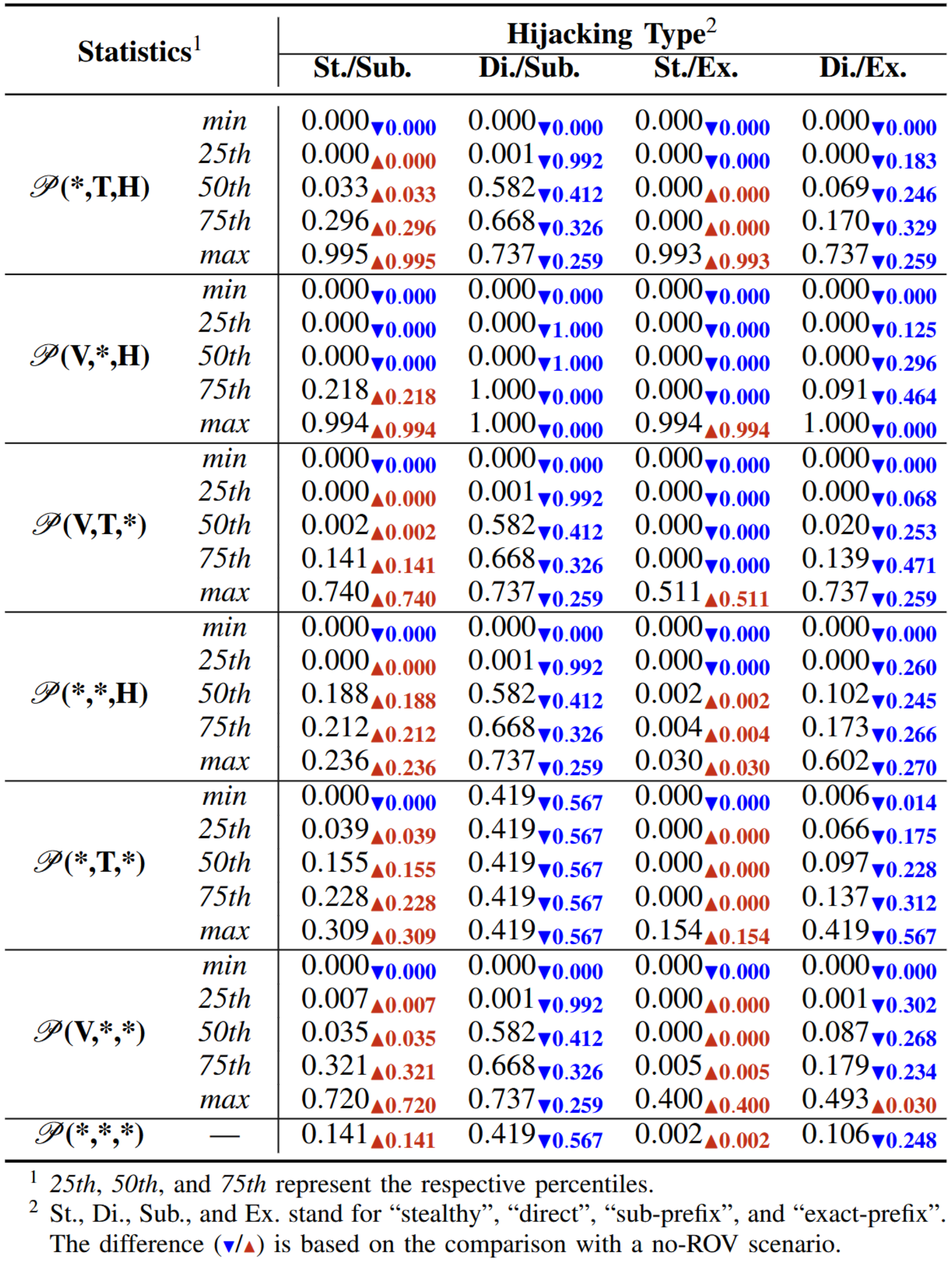
Is it possible to **comprehensively** evaluate the stealthy hijacking risk introduced by the **current** ROV deployment?

Challenges: Criteria to identify risk? Knowledge of routes? Measurement of ROV deployment? ……

Appendix: Aggregated Risk Level



Takeaway#2 Targeted stealthy hijacking achieves near-certain success on specific AS pairs (up to 99.5%), while non-targeted stealthy hijacking distributes risk more evenly across Ases (with a maximum of 23.6%). In contrast, direct hijacking does not exhibit these patterns.

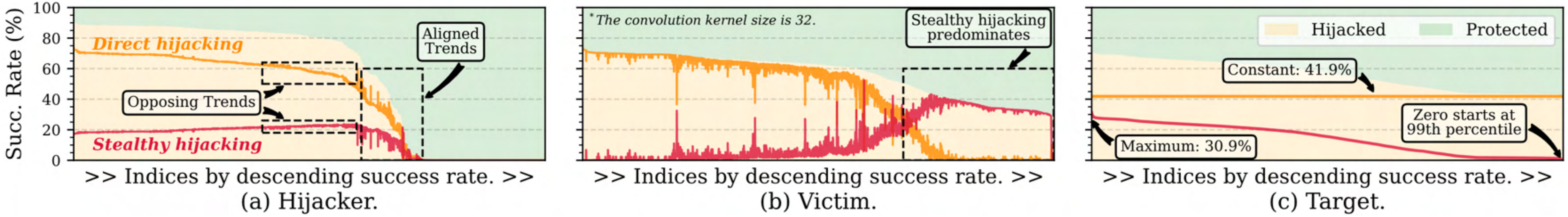


Statistics[1]		**Hijacking Type**[2]			
		St./Sub.	**Di./Sub.**	**St./Ex.**	**Di./Ex.**
𝒫(*,T,H)	*min*	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000
	25th	0.000 ▲0.000	0.001 ▼0.992	0.000 ▼0.000	0.000 ▼0.183
	50th	0.033 ▲0.033	0.582 ▼0.412	0.000 ▲0.000	0.069 ▼0.246
	75th	0.296 ▲0.296	0.668 ▼0.326	0.000 ▲0.000	0.170 ▼0.329
	max	0.995 ▲0.995	0.737 ▼0.259	0.993 ▲0.993	0.737 ▼0.259
𝒫(V,*,H)	*min*	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000
	25th	0.000 ▼0.000	0.000 ▼1.000	0.000 ▼0.000	0.000 ▼0.125
	50th	0.000 ▼0.000	0.000 ▼1.000	0.000 ▼0.000	0.000 ▼0.296
	75th	0.218 ▲0.218	1.000 ▼0.000	0.000 ▼0.000	0.091 ▼0.464
	max	0.994 ▲0.994	1.000 ▼0.000	0.994 ▲0.994	1.000 ▼0.000
𝒫(V,T,*)	*min*	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000
	25th	0.000 ▲0.000	0.001 ▼0.992	0.000 ▼0.000	0.000 ▼0.068
	50th	0.002 ▲0.002	0.582 ▼0.412	0.000 ▼0.000	0.020 ▼0.253
	75th	0.141 ▲0.141	0.668 ▼0.326	0.000 ▼0.000	0.139 ▼0.471
	max	0.740 ▲0.740	0.737 ▼0.259	0.511 ▲0.511	0.737 ▼0.259
𝒫(*,*,H)	*min*	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000
	25th	0.000 ▲0.000	0.001 ▼0.992	0.000 ▼0.000	0.000 ▼0.260
	50th	0.188 ▲0.188	0.582 ▼0.412	0.002 ▲0.002	0.102 ▼0.245
	75th	0.212 ▲0.212	0.668 ▼0.326	0.004 ▲0.004	0.173 ▼0.266
	max	0.236 ▲0.236	0.737 ▼0.259	0.030 ▲0.030	0.602 ▼0.270
𝒫(*,T,*)	*min*	0.000 ▼0.000	0.419 ▼0.567	0.000 ▼0.000	0.006 ▼0.014
	25th	0.039 ▲0.039	0.419 ▼0.567	0.000 ▲0.000	0.066 ▼0.175
	50th	0.155 ▲0.155	0.419 ▼0.567	0.000 ▲0.000	0.097 ▼0.228
	75th	0.228 ▲0.228	0.419 ▼0.567	0.000 ▲0.000	0.137 ▼0.312
	max	0.309 ▲0.309	0.419 ▼0.567	0.154 ▲0.154	0.419 ▼0.567
𝒫(V,*,*)	*min*	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000	0.000 ▼0.000
	25th	0.007 ▲0.007	0.001 ▼0.992	0.000 ▲0.000	0.001 ▼0.302
	50th	0.035 ▲0.035	0.582 ▼0.412	0.000 ▲0.000	0.087 ▼0.268
	75th	0.321 ▲0.321	0.668 ▼0.326	0.005 ▲0.005	0.179 ▼0.234
	max	0.720 ▲0.720	0.737 ▼0.259	0.400 ▲0.400	0.493 ▲0.030
𝒫(*,*,*)	—	0.141 ▲0.141	0.419 ▼0.567	0.002 ▲0.002	0.106 ▼0.248

[1] *25th*, *50th*, and *75th* represent the respective percentiles.

[2] St., Di., Sub., and Ex. stand for “stealthy”, “direct”, “sub-prefix”, and “exact-prefix”. The difference (▼/▲) is based on the comparison with a no-ROV scenario.

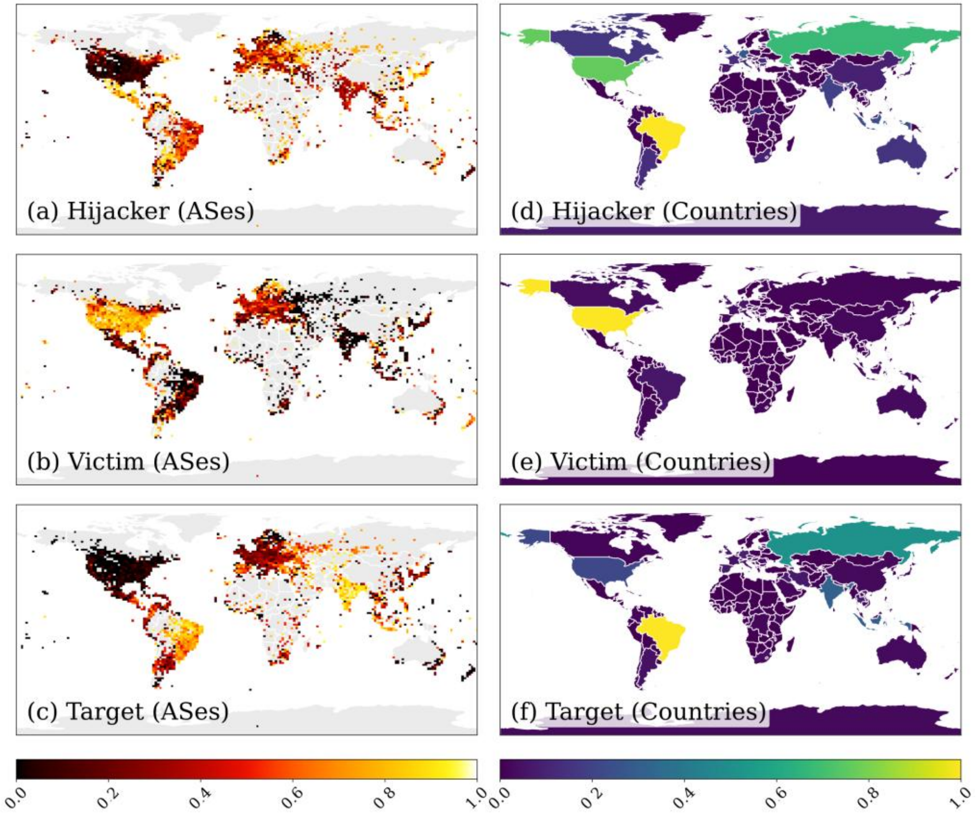
Appendix: Risk Distribution



(a) Hijacker.

(b) Victim.

(c) Target.



(a) Hijacker (ASes)

(d) Hijacker (Countries)

(b) Victim (ASes)

(e) Victim (Countries)

(c) Target (ASes)

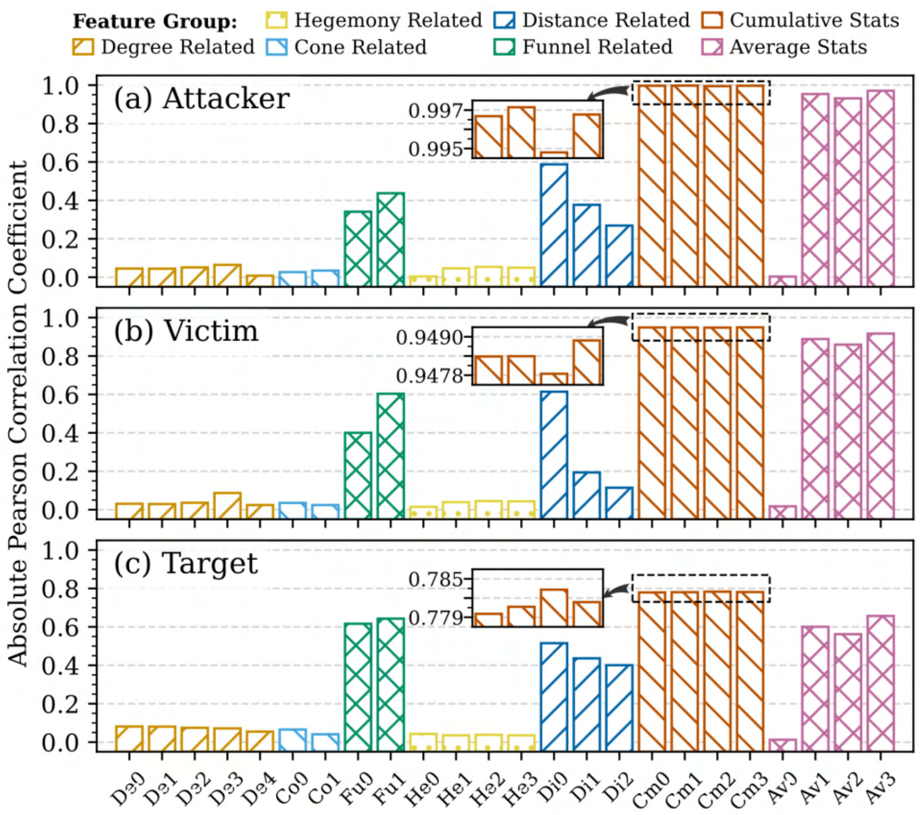
(f) Target (Countries)

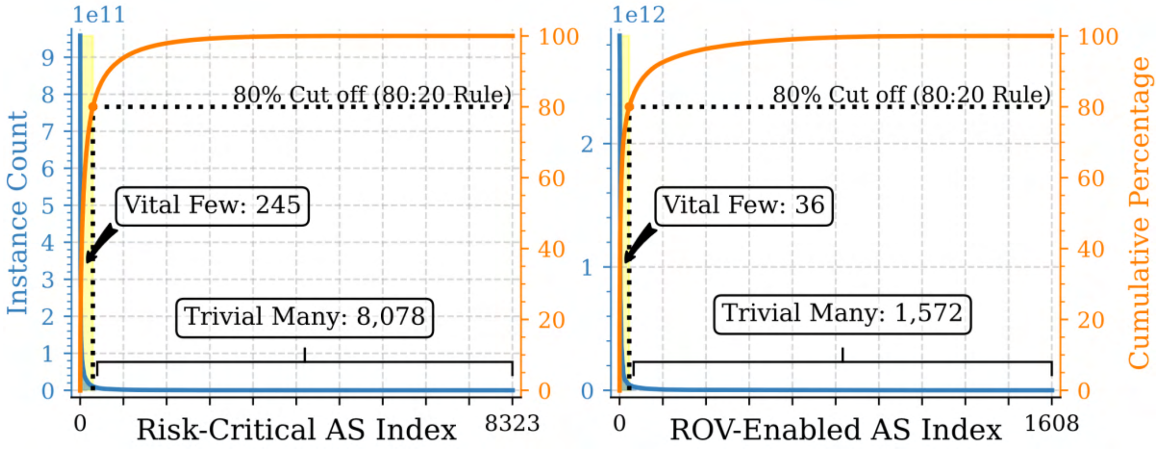
Takeaway#3 While stealthy hijacking risk mostly opposes the overall risk trend across ASes, its diminishing gain is eventually suppressed as ROV's restrictions on attackers prevail.

Takeaway#4 ASes most effective in launching stealthy hijacking concentrate in Europe, South America, and North America; victim-prone ASes are primarily in North America; and target-prone ASes are mainly in South America and South Asia.

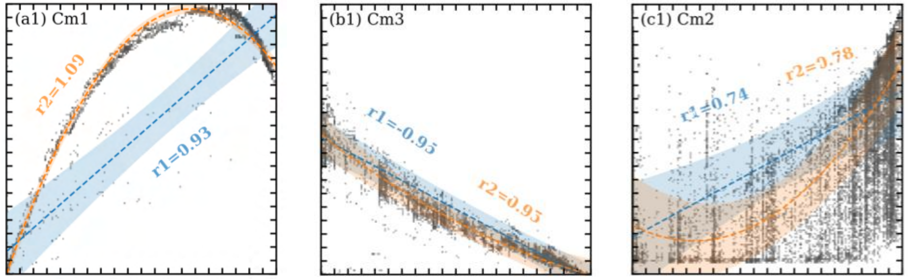
* By statistical role-country correlation, rather than actual or intentional behavior of any country.

Appendix: Influencing Factors





Takeaway#5 Cumulative statistics of AS hegemony show the strongest quadratic correlation with stealthy hijacking risk, making them powerful indicators for predicting risk levels.



Takeaway#6 A small fraction of risk-critical and ROV-enabled ASes account for the majority of stealthy hijacking risk, calling for focused risk mitigation efforts on these key ASes.

Appendix: Performance Evaluation

Accuracy

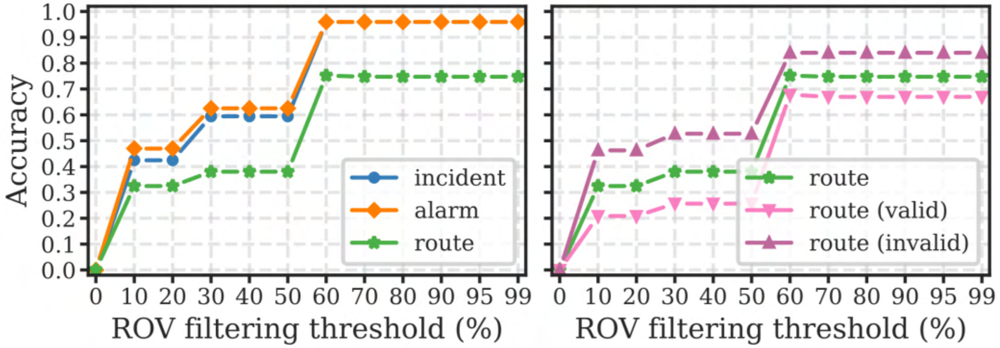
- How analytical risk assessment results align with real-world stealthy hijacking incidents, over varying ROV filtering thresholds.

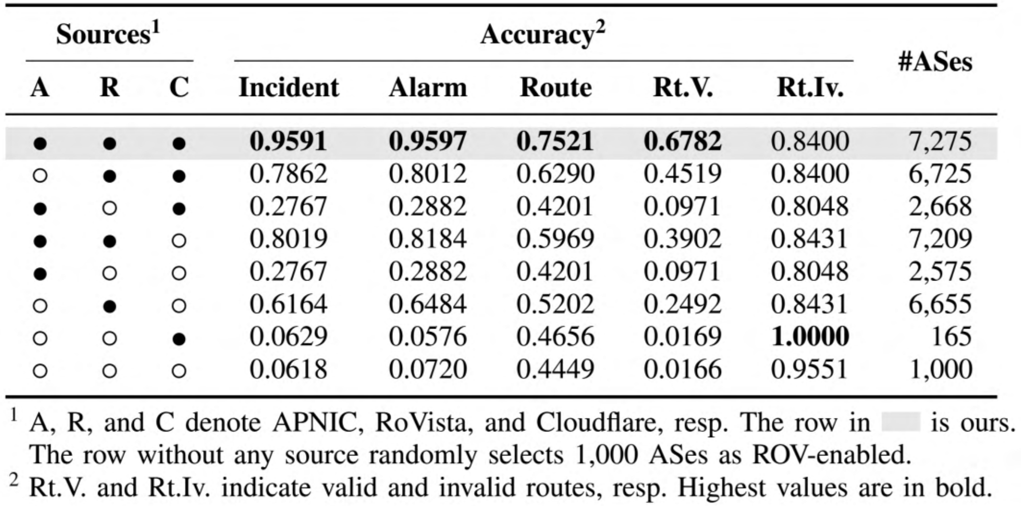
Input Ablation

- Accuracy after removing any ROV input source.

Robustness

- Resistance against random mislabels in ROV input.

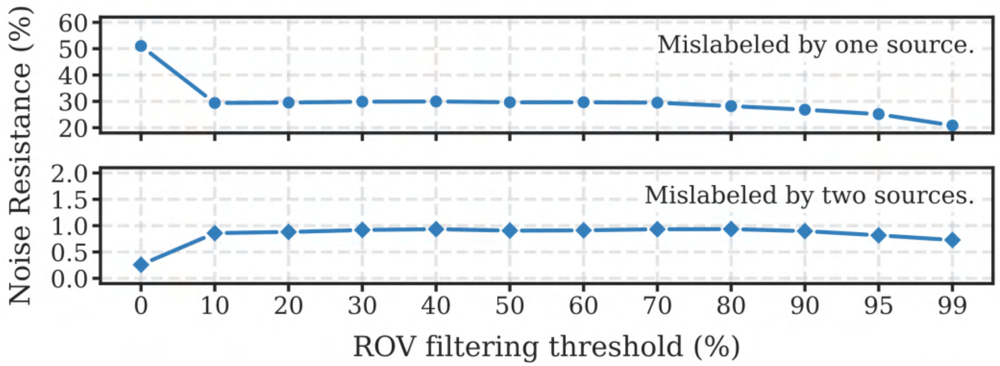




Sources[1]			Accuracy[2]					#ASes
A	R	C	Incident	Alarm	Route	Rt.V.	Rt.Iv.	
●	●	●	**0.9591**	**0.9597**	**0.7521**	**0.6782**	0.8400	7,275
○	●	●	0.7862	0.8012	0.6290	0.4519	0.8400	6,725
●	○	●	0.2767	0.2882	0.4201	0.0971	0.8048	2,668
●	●	○	0.8019	0.8184	0.5969	0.3902	0.8431	7,209
●	○	○	0.2767	0.2882	0.4201	0.0971	0.8048	2,575
○	●	○	0.6164	0.6484	0.5202	0.2492	0.8431	6,655
○	○	●	0.0629	0.0576	0.4656	0.0169	**1.0000**	165
○	○	○	0.0618	0.0720	0.4449	0.0166	0.9551	1,000

[1] A, R, and C denote APNIC, RoVista, and Cloudflare, resp. The row in ░ is ours. The row without any source randomly selects 1,000 ASes as ROV-enabled.

[2] Rt.V. and Rt.Iv. indicate valid and invalid routes, resp. Highest values are in bold.


Noise Resistance (%)
Mislabeled by one source.
Mislabeled by two sources.
ROV filtering threshold (%)