# Technical Report
## STEALTHY HIJACKING DISCOVERY AS A SERVICE

We develop and maintain an automated service that discovers and presents stealthy hijacking incidents in the wild. This service includes a backend for data processing and a frontend to provide structured reports and interactive features. Starting on June 10, 2025, we further integrate an on-demand data-plane validation feature into the service using RIPE Atlas [1].

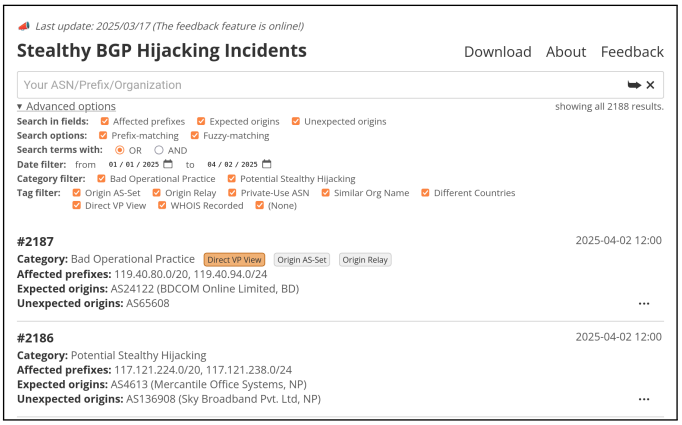
**Backend.** The backend executes the discovery pipeline described in §IV as a cron job on a daily basis. This pipeline consists of four steps: (i) fetching RouteViews RIB snapshots to obtain the latest global routing tables across different vantage points, (ii) organizing all routes in a Trie structure to discover potential stealthy hijacking instances based on the heuristics in §IV-A, (iii) validating against the latest RIPE NCC's RPKI database, the RADb IRR database, and the five RIR's WHOIS databases, (iv) aggregating the remaining instances to generate structured incident reports in JSON format, and (v) pushing reports to the frontend hosting platform.

**Frontend.** As shown in Figure 1, the frontend is designed with the following features.

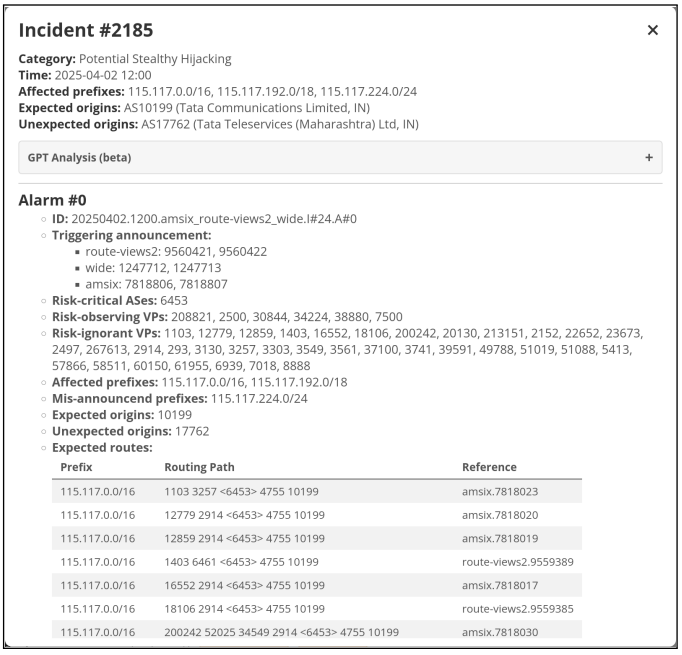
- Display: Each reported incident is displayed in a structured format, allowing users to examine important details such as affected prefixes, origin ASes, timestamps, and linked tags.
- Search: A lightweight search engine, MiniSearch[1], powers efficient lookup based on ASNs, prefixes, and organization names, allowing users to quickly find incidents of interest.
- Filter: Users can refine their search queries through flexible filters, including the time range, the incident category, and the set of incident tags to include.
- Download: To support further studies, all incident reports are available for direct download in JSON format.
- Feedback: An embedded Google Form allows users to provide feedback on specific incidents for the continuous refinement and validation of our service.

**Validation.** To complement the control-plane incident discovery, we incorporate an on-demand data-plane validation mechanism using RIPE Atlas. Specifically, for an incident to validate, we issue traceroute measurements from probes located in the victim AS to the target prefix, aiming to verify whether traffic is diverted to the suspected hijacker. In a recent validation run on June 16, 2025, we examined all 26 incidents of the day, where 24 had probe coverage and 10 yielded usable destination information via traceroute. Among these, 9 were confirmed true, including all high-confidence cases. The one false case likely stemmed from route engineering, indicated by AS prepending. These results demonstrate the reliability of our stealthy hijacking discovery from a data-plane perspective.

[1]https://github.com/lucaong/minisearch




(a) The search-and-index page.




(b) An example incident detail page.

Fig. 1: The frontend design of our online service.

## REFERENCES

[1] RIPE NCC, "Ripe atlas," 2025. [Online]. Available: https://atlas.ripe.net/