APNIC Policy Proposal

Title: Resource Hijacking is an APNIC Policy Violation

Version: 1

Name: Carlos Friacas
Jordi Palet Martínez

Email: cfriacas@fccn.pt
jordi.palet@theipv6company.com

Problem Statement:

This proposal aims to clarify that resource hijacking is not accepted as normal practice within APNIC service region, primarily because it negates the core purpose of running a (Regional Internet) Registry. The proposal is not concerned with simple operational mistakes – it is intended to address deliberate hijacking events.

A "hijack" is defined as announcing a prefix to another network without the resource holder's consent, or the act of leasing or selling numbering resources which have exclusive rights of use by third parties (again, without their consent). Hijacking is not an acceptable behaviour and there must be consequences for resource hijacking for those that have a service agreement (either directly or indirectly) with APNIC. This proposal aims to clarify that an intentional hijack is indeed a policy violation.

Resource hijacking (while not limited to the below) is commonly observed to have several objectives:

- Diverting law enforcement from the real origin of packets tied with illegal activities;
- Temporarily making use of address space without any maintenance cost associated (i.e. RIR membership);
- Impersonating third party networks and services;
- Eavesdropping on the traffic of third-party networks (i.e. man-in-the-middle attacks);
- Disrupting IP communications between two or more third party networks.

a. Arguments Supporting the Proposal

- Resource hijacking completely invalidates the purpose of a Regional Internet Registry;
- There is a gap in APNIC policies, which allows the support of hijacking operations with a set of legitimate obtained resources;
- The legitimate resource holders need to see their exclusive rights of usage better defended at registry level;
- Having a rule/policy in place at APNIC against resource hijacking might prevent some actors to engage in such abusive practices;
- If nothing changes in this field, the reputation of APNIC and APNIC service region will continue to be affected from a cybersecurity perspective due to hijacking events.

b. Arguments Opposing the Proposal

- Neither APNIC community or APNIC are the “Routing Police”.

Mitigation/counter-argument: Nobody will try to dictate to anyone how their routing policy should be at any given moment. However, APNIC needs to be able to choose not to enter into (or maintain) a contractual relationship with people/companies that are performing resource hijacks. There are already enough sources of historic and almost real-time routing data, which function as a worldwide observatory. From these sources, it is possible in some circumstances to accurately evaluate who is performing resource hijacks and harming (or trying to harm) third party networks by doing so. The external experts proposed in this framework are mere evaluators, who can use available sets of routing data to determine whether resource hijacking events have taken place, and whether were intentional or not.

- A policy violation can be determined following a simple mistake done during BGP operation.

  Mitigation/counter-argument: Firstly, initiating a process relies on a report. Then the expert analysis will determine if BGP hijacking is a common action from APNIC member that the report was issued about, or if they only happen to have made an operational error. Data about the BGP protocol is massive, and if the experts do not find enough related evidence, then the report will be dismissed.

- This proposal places APNIC in a difficult legal territory.

  Mitigation/counter-argument: APNIC follows the rules/policies issued by the community. However, if a suspected hijacker issues a lawsuit against APNIC, legal insurance can be a possibility (even if there is an associated cost).

- A single innocent party wrongly accused is worse than one hundred resource hijackers stopped.

  Mitigation/counter-argument: While this is valid within almost all law jurisdictions, it does not prevent the existence of rules or laws. The proposal is simply trying to end a clear gap in APNIC region ruleset.

- Acknowledging more policy violations, will not improve global routing security. Tools such as RPKI, MANRS or other should still be used instead.

  Mitigation/counter-argument: The degree of RPKI or MANRS deployment is still very low, and this policy is needed to address this lack of deployment. The need for this policy should be reviewed in a few years when different stages of deployment are reached by RPKI, MANRS and other tools.

Objective of policy change:

To ensure that there is an explicit policy about this problem and the community can tackle it.

Situation in other regions:

The policy proposal has already been submitted to RIPE, LACNIC, ARIN and AfriNIC.

Proposed policy solution:

Proposed Text

1.0 Introduction

Hijacks happen on an almost daily basis. Resource hijacking happens mostly but not exclusively through the use of eBGP. In the rest of this document, "BGP hijacks" must be interpreted as the announcement of any kind of resource (IPv4, IPv6, ASN) through BGP, without the consent of the legitimate resource holder, including unallocated/unassigned ones.

Hijacks have different visibility characteristics. They can be on a global scale (propagated to all networks) or restricted (only one or some networks). Their impacts can also vary, and it is not only resource holders who are affected, but also networks (and end users) who receive illegitimate/hijacked routes and suffer the indirect consequences of this.

There are already initiatives and technologies such as MANRS and RPKI, which unfortunately are not enough to significantly reduce hijacks. While MANRS and RPKI are strongly encouraged, policy should address the lack of community rules about hijacking. Through this document, APNIC community clarifies that hijacking is not an acceptable practice.

APNIC is not a mere “virtual land registry”, due to the fact it also has a role in the distribution of resources and is a membership-based organisation with a charter to support a larger community of users. Any persistent hijack can be understood as undermining APNIC credibility as a registry, thus policy is needed as a form of industry self-regulation.

This policy does not try to address problems caused by operational errors or occasional hijacks, but instead tries to create a way for victims to report persistent intentional hijacks. By making more of these cases public and searchable, each Autonomous System will have additional information to inform its decisions about interconnection.

2.0 Resource Hijacking is a Policy Violation

A hijack is generally understood to be the announcement of routes to third parties without the consent of the resource holder. This is considered to be a violation of APNIC policy.

A hijack of numbering resources or the announcement of unallocated or unassigned IP addressing space or Autonomous System Numbers to third parties are also considered a policy violation. The victim of a hijack is not only the legitimate owner of the hijacked resources, but also those who receive announcements of hijacked prefixes. On a sale or lease context, both the legitimate owner as the party paying for the resource usage are victims.

Only reports in which the suspected hijacker is subject to APNIC policies can be investigated.

3.0 Scope: Accidental vs. Deliberate

A distinction can be made between accidental or deliberate hijacks from available routing datasets, looking at parameters such as duration, recurrence, possible goals, and the size of hijacked blocks. Other parameters may also be considered in the future.

Accidental events usually emerge from situations where a hijacked prefix or ASN is very similar to other resources held by the source of the hijack.

4.0 Lines of Action

APNIC is not able to monitor the occurrence of resource hijacks or assess whether they are policy violations. It must therefore rely on external parties, both to report hijacks and to determine whether they are deliberate.

Reports sent to APNIC need to include a minimum set of details, such as: “Networks Affected”, “Offender ASN”, “Why am I reporting this Hijack? (Holder or Receiving Party)”, “Hijacked Prefixes/ASNs” and “Timespan”. This is not a definitive list and other details may also be required.

APNIC will provide a web-based form (or equivalent alternatives) to submit reports. Information regarding the hijacked routes/ASNs reported will be made publicly available to limit the risk of duplicate reports being submitted.

The involved parties will be notified as soon as they are identified. This will allow them to provide any relevant information and mitigate the hijack, avoiding further damages and possibly false claims.

APNIC will define a pool of worldwide experts who can assess whether reported hijacks constitute policy violations. Experts from this pool will provide a judgement regarding each reported case, no later than six weeks from the moment the report was received. If this judgement report is not completed within six weeks, the case will be dismissed.

Direct upstream or transit providers of a suspected hijacker that facilitate a hijack through their networks should be notified about the publication of a judgement report. This is not to be considered a formal warning and a response is not required. However, the notification will ask if they can provide further information or identify anything odd.

The expert investigation could suggest other related organisations (such as multiple LIRs from a single business group), which may be considered by APNIC in the event of a future closure process. This possibility aims to prevent hijackers from continuing their activities from a simulated customer's network. The expert investigation could also identify relationships between LIRs/End Users within the same business groups.

If an alleged hijacker can demonstrate that their infrastructure was improperly manipulated by third parties (for example, compromised routers), then the hijack cannot be considered intentional.

5.0 Experts: Definition

An expert is an external party to APNIC, ideally with at least five years' experience with eBGP from dealing with configurations related to peering and transit providers. Experts should be familiar with the common forms of interconnection agreements, both within and outside of APNIC's service region.

6.0 Pool of Experts

The selection procedure for the pool of experts should be open and managed by APNIC, possibly in collaboration with other RIRs:

1. Every two years, a call for applications to the expert panel will be made to the global community, noting the experience and knowledge required. Additional calls will be made if/when the pool needs to be expanded.
2. To join the pool of experts, a candidate will need a statement of support from three different networks (ASes) from three different countries within the APNIC service region, which are within different LIR sponsorships.
3. The authors of this proposal and active APNIC WG Chairs are not eligible to become experts. If an expert is selected as APNIC WG Chair, they will need to step down from expert duties, after completing their participation in any ongoing cases.
4. The same number of experts must participate in each phase (initial and appeal, if applicable).
5. The minimum number of experts per case and phase will be three. If a larger number is necessary, it must be odd, and the community will be informed of the reasons for the change. Cases involving Internet Exchange Points or transit providers with significant customer bases accused of hijacking should have two additional experts per set.
6. The experts for each case/phase will be chosen at random, to ensure a balanced sharing of cases.
7. The identity of the experts chosen for a particular case will be kept confidential to avoid bribery attempts or reprisal actions against them.
8. Before accepting a case, experts must sign a document that confirms their impartiality and states that they have no direct or indirect relationship with the involved parties.
9. Experts must sign a non-disclosure agreement with APNIC that covers any information provided by an accused party as part of their appeal.
10. Cases must be completed by the experts that were initially assigned to them, even if they are replaced in a selection process while a case is ongoing. If there is a justified cause, one expert (only) may be replaced by another; this must be communicated to APNIC community.

11. Experts will be replaced if they are unresponsive to either their fellow experts on a case or APNIC. Experts will also be replaced if they fail to comply with the defined time frames in three separate cases.
12. A person can only serve as an expert for four consecutive years (two terms). They must then stand down for at least two years before they are eligible to apply for selection again.
13. APNIC will need to provide legal insurance for all experts, exclusively covering investigations/cases where they were involved.
14. The assignment of cases to experts will follow a programmed process (a draw from a minimum number of experts currently handling no cases, or a minimum of cases).
15. New cases cannot be investigated until the pool of available experts is at least twice the minimum number that can be assigned to a single case.

7.0 Procedure

The procedure must incorporate at least the following elements:

1. APNIC will verify that a report contains sufficient information before assigning it to a group of experts. If this is not the case, the report will be dismissed.
2. If a report is accepted, the suspected hijacker will be notified and given an opportunity to respond, providing evidence as they see fit.
3. Experts assigned to a case will verify the reported information regarding historical BGP data and will review any evidence provided by the suspected hijacker.
4. The group of experts assigned to a case will publish a joint report with their conclusions.
5. The experts will dismiss any cases that are clearly accidental, though they must indicate this in their report. APNIC can share this report with the responsible party to avoid future reoccurrences.
6. For an event to be identified as an intentional hijack, there must be unanimity between all experts on the case.
7. Experts cannot add accused parties to a case.
8. A suspected hijacker must be given the opportunity to appeal a report. In this case, a different group of experts will review the case. Again, there must be unanimity between all experts or the case will be dismissed.
9. APNIC staff (or staff from other RIRs) cannot be part of an expert group, though they may provide administrative assistance. This does not include contacting the people which originally filed a report to request more information or providing any non-public APNIC membership information.
10. Neither APNIC nor the claimant(s) can appeal expert decisions.

8.0 Retroactivity

Only hijacking events that occur after this policy has been implemented may be considered.

9.0 Report and Evidence Eligibility

Only networks directly affected by a hijack may file a report.

A report can only be filed:

If the victim is the legitimate holder of a hijacked IP address prefix or Autonomous System;

If the victim has received a hijacked IP address prefix through BGP or a route with an AS-PATH that includes a hijacked Autonomous System.

A report is not admissible if the person reporting it was not affected in any way by the hijack.

Evidence older than six months, counted from the time a report is submitted, cannot be considered or included in any expert report.

10.0 Sources of Information for Expers: Examples

The following is only a reference, not an exhaustive list:

- stat.ripe.net and stat.ripe.net APIs
- bgpmon.net and bgpstream.com
- irrexplorer.nlnog.net
- routeviews
- caida openBMP
- www.team-cymru.com/bogon-reference.html
- cidr report
  - www.potaroo.net/cgi-bin/as-report?as=<asn>
  - www.potaroo.net/cgi-bin/per-prefix?prefix=<prefix>
- bgp.he.net
- ixpdb.euro-ix.net/en/ixpdb/asns/
- atlas.ripe.net
- traceroute.org

11.0 Guidelines for Experts

All non-private information disclosed by accused parties when objecting to a specific report should be included in the expert report (at least in an appendix).

Company registries (www.ebr.org and similar) can be useful in determining if different companies can be associated with the same actor.

Special care must be given to situations where a hijacked prefix is very similar to a prefix legitimately held by an accused party. In these cases, checking to see if the legitimate prefix was announced within the same period may shed some light on the case.

BGP leaks are outside the scope of this policy. Any case strictly related to BGP leaks should be dismissed.

12.0 Possible Objections

A report containing an expert judgement on the case will be sent to the suspected hijacker. This party will then have a maximum of four weeks to object to any conclusions included in the report. Any objections are then assessed and ruled as admissible/non-admissible by the experts, during a maximum two-week review period. Following this, the report is finalised and published.

13.0 Appeals

Following publication of the final expert report, the suspected hijacker has a maximum of two weeks in which they can file an appeal. If an appeal is filed, an alternative set of experts (a minimum of three) will review the report for a maximum of four weeks. In order to maintain a ruling of “intentional hijack”, all experts involved in the review need to agree that this has occurred. The results of this review are final and cannot be further appealed.

14.0 Ratification

Once the report has been published, any policy violation will need to be ratified by all experts involved in the case, following a two-week public consultation on the report. If ratification is not declared unanimously, the report will be dismissed. Ratification will be delayed in case of an appeal, until the second set of experts has published its review. Experts can refuse to ratify a report based on undisclosed information sources or input from the public consultation.

15.0 Transition Period

As soon as the policy implementation is completed, a transition period of six months will be established. This will allow organisations that announce unassigned address space or Autonomous System Numbers (due to operational errors or other non-malicious reasons) to receive only a warning.

Existing “Bogons” at the time of policy implementation should be treated as exclusions and cases where they are referenced should be dismissed before awarding a case to experts.

16.0 Holders of Legacy or Provider Independent Resources

If an accused party is a Legacy Resource Holder (either with a direct or indirect relation to APNIC), the registration of their legacy resources will not be affected, as APNIC policies are not applicable to these resources. However, if a policy violation is ratified, what is described in section 17.0 will apply, in which case other APNIC services such as reverse DNS or Resource Certification (RPKI) could be denied to the accused party.

Holders of Provider Independent resources that are sponsored by an LIR that is found have committed a deliberate hijack will not have their resources de-registered and will be able to find a new sponsoring LIR (provided they were not involved). In the same way, a sponsoring LIR is not responsible if its customer is found to have committed a hijack.

17.0 Continued violations regarding Hijacking of Resources from the same party

In instances where a resource holder has regularly and repeatedly hijacked network resources, not allocated or authorised for their use, procedures defined in the membership agreement and policies may apply. This policy does not endorse the initiation of a LIR closure procedure on the basis of a single policy violation.

Advantages of the proposal:
Fulfilling the objectives above indicated.

Disadvantages of the proposal:
None foreseen.

Impact on resource holders:
None.

Additional Information:
This policy is relevant as well to NIR members, as usual with all APNIC policies.

References:

- RIPE: https://www.ripe.net/participate/policies/proposals/2019-03
- LACNIC: https://politicas.lacnic.net/politicas/detail/id/LAC-2019-5
- ARIN: https://www.arin.net/participate/policy/proposals/2019/ARIN_prop_266_v2/
- AFRINIC: https://www.afrinic.net/policy/proposals/provisions-for-resource-hijacking