**Anti-Abuse Working Group**

Thursday, 17 October 09:00 - 10:30

Chair: Brian Nisbet

Scribe: Ulka Athale

Co-Chair Brian Nisbet welcomed attendees, thanked the RIPE NCC staff supporting with scribing and monitoring chat, the stenographers, and stated that his co-Chair Tobias could not attend the session. The minutes from the Anti-Abuse session at RIPE 78 were approved. In his opening remarks, he mentioned the policy proposal 2019-03 that was withdrawn, and that he was surprised by the form of words of the Impact Analysis and that the Executive Board said that they were not going to do the thing that the community may or may not be asking them to do. In this case the policy proposal was withdrawn, but if it had been approved by the working group, it might have led to a constitutional crisis of sorts, and this is something that should be discussed. Brian asked the room if they had any further remarks on this issue. There were no comments.

**C.1. RIPE NCC Update on**[**2017-02**](https://www.ripe.net/participate/policies/proposals/2017-02)
Marco Schmidt - RIPE NCC

Presentation available at: <https://ripe79.ripe.net/archives/video/244>

Jordi Palet Martinez asked if the 25% was after they sent the additional emails, after the automated validation failed.

Marco clarified that there was one month in which they sent several automated emails with a stricter tone, and there was still around 20-25% who didn’t respond, requiring additional action.

Brian Nisbet asked if this now happens as a regular part of the process, once a year. Marco replied that in general it is a part of the regular process. The most important abuse mailboxes to fix were the LIR ones. If the abuse mailboxes of independent resources and more specific PA ones were not working, they would go to the sponsoring LIR to check the abuse contact.

Herve Clement, Orange, said that he was pretty happy with the proposal. He added that he had a question about the workload for the RIPE NCC, but that Marco had already partially answered it. He added that he thought that Marco now had an element to respond to the next policy proposals, proposed by Jordi perhaps, to evaluate the possible workload of the RIPE NCC and how to go a step further beyond such verification.

Rudiger Volk, Deutsche Telecom, asked Marco whether he saw any additional work to improve this process and the communications attached to it. He said that he didn’t find the information he was receiving very helpful, he would require time to work out which customers are actually the source of the problem. He suggested looking into providing mechanisms that automates the research on the RIPE NCC side and allows the recipient of the problem report to do what they are required to without additional efforts.

Marco thanked Rudiger for his feedback and said he would talk to him in more detail about how to make things clearer.

Brian also thanked Marco for his work as Policy Development Officer, in light of the announcement that Marco will be moving on to the Registration Services team at the RIPE NCC.

**C.2. Policy Proposal**[**2019-04**](https://www.ripe.net/participate/policies/proposals/2019-04)**- Validation of "abuse-mailbox"**
Jordi Palet Martinez, The IPv6 Company

Presentation available at: <https://ripe79.ripe.net/archives/video/301>

Peter Koch, DENIC, commented that when regulators, who are increasingly interested in policy making, come up with suggestions, the community usually demands that it is fact-based policy or evidence-based policy making. He asked Jordi what real world problem he was trying to solve, notwithstanding the inclusion of percentages.

Jordi replied that it was simple, the point of having a registry is to have the right registration data.

Ruediger said that he agreed with Peter. He had a slightly different angle on the same topic. In many of the policy proposals, it looks like people really want to police and it is not what RIPE is about. It is strange that Germans object to that. Peter pointed out that Jordi is creating compliance conditions, while not really spelling out what should be done. He would take that argument a step further and say that the purpose of this working group should be helping people who fail somewhere to do a better job. He didn’t see anything that tells people what is expected. If we formalize compliance criteria, evil people will construct robots and comply.

Jordi disagreed, and he tried to find the right wording, and was open to improving that. He added that someone can always trick the validation, but that doesn’t mean they are complying with the policy.

Rudiger replied that he disagreed and his point was that nothing in this process helps people set up processes respond to the real life cases, beyond the formal check.

Brian added that that there was an apt point made that part of the role of the Working Group is to educate and help. If indeed the policy was to reach consensus, there would be a work item to give more information and help. The disagreement between the Jordi and Rudiger on the policy was noted.

Carlos Friacas, FCCN, said that he thought the problem statement was pretty clear. There are people who don’t like to answer abuse checks, so this was an effective way with minimum trouble. An abuse contact is part of data if we’re trying to have a registry with the most accurate information. Something has to be done to improve the registry, it’s as though it’s ok to register abuse contacts for Donald Duck or Mickey Mouse.

Peter Koch said that the issue of accuracy has been discussed in multiple places. The bigger topic of what is the purpose of the registry will be discussed in the RIPE community plenary and be addressed by a task force. He added that we need to be careful about policy proposals concerning the jurisdiction of this community. If they want to set the business process of LIRs, ISPs or network operators, then the question is how far the community can rule those. He would rather see that in an explicit discussion rather than sliding into policy proposals that actually only define policing tests. This is a more constitutional issue – what can this community set policies or rules for and I think going to the business processes is a step too far.

Jordi replied that he agreed with Peter as far as the previous version of the policy proposal was concerned, there was too much in-depth process management, but that was no longer the case in the newer version.

Brian reminded the working group that there were roughly two weeks of the discussion period left, and asked them to share their comments on the mailing list and forum.

**E.1. "How Effective is ASN-Drop?"**
Carlos Friacas, FCCN

Presentation available at: <https://ripe79.ripe.net/archives/video/245>

Ruediger stated that he was primarily a routing person and has spent a lot of effort on routing security. Carlos was essentially suggesting taking a source of reputation classification and that is very different from security.

Carlos replied saying that reputation is a source for applying security.

Ruediger replied that he disagreed and that he was pretty sure that most routing people would disagree too. The source of information has to be understood thoroughly, and that he hadn’t made that kind of study of the Spamhaus list.

Carlos pointed out that 56% of the shortlist no longer show up on routing tables.

Ruediger said that he didn’t know why they got there. When he looks at routing tables, he sees a lot of odd stuff including faked origin ASes, AS paths that are not technically valid, in RPKI – ROAs for ASNs that should not show up for public routing. Looking at RPKI, reputation does not help because in RPKI there are authorisation forecasts that are completely invalid. It was also unclear what would be done with ROAs that are authorising bad reputation ASes.

Carlos said that this was a problem for him as well.

Ruediger stated that RPKI and reputation are separate worlds and there is no clear and useful interaction between them. Carlos replied that this indicator is possibly a sign that such a blacklist is not fully usable. Ruediger replied that mismatches can indicate problems on one side or an another. Carlos added that if 50% of the list is not announced, the value of dropping also drops. The problem with the number is that it is just a snapshot.

Ruediger said that a lot of mail only make temporary use of a lot of certain ASes, and the bad reputation might get attached to that and be marked, even if the usage occurs once in a while.

Carlos asked that if someone’s ASN got on the list, that person would try to delist it. Ruediger concluded by saying the reputation of the reputation list would go down.

**E.2. "LACNIC's WARP Centre"**
Guillermo Cicileo, LACNIC

Presentation available at: <https://ripe79.ripe.net/archives/video/247>

Carlos Friacas, FCCN said that he recognised that they had a lot of stuff provided by LACNIC that they didn’t have in the RIPE community. He hoped that the community would find the resources and will to build more and get to the point where LACNIC is. He congratulated Guillermo for all their work with regards to warning advice and reporting points.

Jordi Palet thanked him for volunteering to do the talk. The reason why he and Carlos suggested having a talk on this topic is because of their work on the BGP hijacking proposal, and this is also interesting for this community. The question is for all of us, what do we think about this. This working group is tasked to help the community, and as he found it useful, he wanted opinions on that from the group.

Brian asked how long the work has been going on for and whether it was undertaken as a LACNIC initiative or a community demand.

Guillermo replied saying the work has been ongoing for five years, and it was mainly a LACNIC initiative but based on community demand.

Brian commented that there are differences between the RIRs – why does LACNIC have this, why doesn’t RIPE? He said it was worth asking for opinions and asked whether it was something people would find useful in the RIPE region.

Ruediger said he was surprised that a member of the global CSIRT community in Europe feels that this community doesn’t provide points of contact. His impression was that the CSIRT community was quite well-organised, but that they usually don’t show up in large numbers and contribute to this working group. He said that he didn’t use their services much and would actually appreciate it if the CSIRT community interacted with them a bit more.

On the other hand, he added that a clear division of labour and clear focus of purpose for organisations makes sense. The kind of detailed incident follow-up and identification is not on the plate for the registry system. Things have worked differently in Latin America because the establishment of LACNIC took place in a very different way from how RIPE was founded 30 years ago and the demands on the people driving LACNIC are different from what is happening in Europe.

Brian said that this was a question for the community. We have done things here in a certain manner for a long time. The main activity of the NCC for a long time has been the maintaining registry, which is hugely important and still very valid. However, as the world changes and things change, the question is whether there are pieces that the community should look to, or the members should look to.

He pointed out that there are many new LIRs, many of whom are very small and do not have security people. Many of them are not large established European operators or telcos, which is something to consider. How much has the world changed? He asked how reflective the people driving RIPE, the RIPE community and membership for a long time are of the needs of the 10,000 LIRs we have gained in the last few years, or whatever the precise number was.

Carlos pointed out that that RIPE and APNIC have CSIRTs but they only account for RIR infrastructure. What WARP does goes beyond that and that’s a big added value that he saw. In the previous year there were 15 cases of reported hijacks to LACNIC. If you try to report a hijack to the RIPE NCC, nobody cares because they say RIPE NCC is a registry. Picking up on what LACNIC is doing right, there were 15 reports and they solved 14. 14 people were desperate, and their prefixes were being announced by someone else and they were helped. He would like to see the same coordination in this region, because the CSIRTs work.

Ruediger remarked that if he were to look into routing tables and browse monitoring systems, he would see multiples of 15 hijacks a day. It cannot be a task for the RIPE NCC to take care of all of them. The focus and the expertise used by the CSIRT community and routing security problems are very far apart. He could understand why when something was done successfully it clicks as a good thing, but understanding how to improve routing security is not so easy to get out of how CSIRTs work.

Carlos stated that the term is ‘routing security’ - you shouldn’t do routing security without the routing guys, or routing security without the security guys, it should be a mix.

Ruediger replied that he has worked in the IETF – there is a lot of stuff that has to be done there technically. RPKI was already created in the previous millennium, and ten years ago all the essential things were in place, we could have already deployed it. This is how slowly we are moving. He added that he was surprised that they bothered to figure out whether or not the hijacks were malicious because that doesn’t matter since you have to work on it regardless the damage is done.

Guillermo replied that he had said that it’s not easy or possible to detect whether or not it was malicious. They only process it and contact the organisation.

Ruediger commented that to actually proceed in network operation it was also irrelevant. It matters for damage claims and to the police, but it is not the first thought for network operators.

Brian asked whether Guillermo thought this could be replicated elsewhere.

Guillermo replied that in their case it was a demand from the community, so it grew naturally, from members who were sending reports and trying to contact other organisations, and asking LACNIC to do something. When they decided to build the WARP, it was LACNIC’s decision based on the community’s needs. He added that he didn’t know if it was the same in the RIPE region and it was for the RIPE community to decide.

**AOB**

Presentation available at: <https://ripe79.ripe.net/archives/video/250>

Brian opened up a discussion. He said in light of conversations around a WARP, more coordination or things like the task force in relation to the registry, it was worth asking whether the working group is doing the right thing. Are there other things they could be doing?

Ruediger asked the group an open question - lots of small entities have joined the RIPE NCC and are around. What is this working group doing to provide help to them?

Brian said that it was an excellent question. He added that it’s not on the co-chairs to do all the work, they need people to write documentation. There’s a lot of very good information and experience out there in this working group that the RIPE community could benefit from. He asked what the working group was doing to pass on information to make sure people don’t have to reinvent the wheel, as governments, regulators and LEAs look at us more closely at our operations. They need to look at how people can help – documentation, how-to guides, etc.

He asked the group to please think about these questions and actions, and to think about what they would like on the agenda for RIPE 80 in Berlin. He reminded them to participate in the Community Plenary and the PC elections.