**Anti-Abuse Working Group Minutes RIPE 78**

23 May 2019, 09:00-10:30
WG Co-Chairs: Alireza Vaziri, Brian Nisbet, Tobias Knecht

Scribe: Antony Gollan
Status: Draft

**A. Administrative Matters**

The scribe and chat monitor were thanked and the draft minutes from RIPE 77 were approved without comment.

Brian Nisbet, Anti-Abuse WG Co-chair, noted there was one change to the agenda: they would talk about 2019-04, “Validation of “abuse-mailbox”” after the update on the implementation of the previous abuse-c proposal (2017-02), as it made sense to keep these topics together.

**B. Update**

**B1. Recent List Discussion**

The video archive is available online at:

<https://ripe78.ripe.net/archives/video/83/>

Brian said he understood that the topics the WG discussed were dear to people’s hearts and they were all passionate about dealing with abuse. However, the community had a code of conduct and they were adults. He wanted to remind people to consider whether their contribution helped the discussion or just added heat. He also reminded people to focus on the proposal being discussed. There had been some people sending snarky comments off-list, which also was not helpful.

Michele Neylon, Blacknight, said he had huge issues with the mailing list and wondered if it was fit-for-purpose. It had become hard for people to engage constructively and if it was merely a place to trade insults, he did not think people like himself could continue to participate.

Brian said this was why he had raised this. People needed to think about how they were interacting on the list. They did not have an alternative to the mailing list at the moment, as the RIPE community required all decisions to happen on the mailing list. While he accepted Michele’s point, given the topic, he thought the discussion might have gone similarly in other WGs.

Rüdiger Volk, Deutsche Telekom, said if the mailing list was largely going to be noise then it was not appropriate to consider it as a working tool for getting consensus and keeping stakeholders engaged. They should consider instituting checkpoints where people with only limited time could read a summary of the discussion and the status of the proposal.

Alexander Isavnin, Internet Protection Society, said there had been a lot of anonymous “security experts” in this discussion. This was different from the traditional approach of RIPE, where they knew who they were talking to, which supported a kind of academic trust. Unlike in other WGs, these discussions were crowded by people they had never met in person and who claimed they were experts.

Brian said unfortunately that was the nature of the beast - they did not scan passports and real names were not required. He could not see that they would be changing this.

**C. Policies**

**C1. RIPE NCC Update on 2017-02**

**Angela Dall'Ara, RIPE NCC**

The video archive is available online at:
<https://ripe78.ripe.net/archives/video/86/>

Hervé Clément, Orange (and co-author of the policy proposal), said he wanted to thank Angela for her efforts, and he was very happy with how the implementation was going. He asked if she could expand on the workload in terms of FTEs.

Angela said they had hired three temporary colleagues, who had been calling people, sending emails and helping with database updates. They had started with them on 11 March and they were still busy.

Piotr Strzyżewski, RIPE NCC Executive Board, referred to slide 9. He said he represented a moderate-sized LIR and he was responsible for abuse contacts – all of them had failed the initial validation. He referred to Jordi’s upcoming proposal and cautioned him to keep this in mind when proposing things that would be much heavier and create more work for members. He said he would provide Angela with some use cases to improve the tool for future releases.

Jori Palet Martinez, The IPv6 Company, asked if Angela had a feel for how many validated abuse contacts were actually for relevant abuse contacts in an organisation.

Angela said the policy had not requested them to verify if the contact was the right one.

Jordi said he could set abuse@ripe.net as their contact and pass the validation that way.

Angela said people should check in the full text search to see where their email was registered. This was something they could all do in the RIPE Database.

Rüdiger said Angela had mentioned that they put some effort into shaping the communication in good ways. They did not see this within his company – it had been reported to him that the verification emails looked suspicious – asking people to click on a link but not explaining why or for what purpose. He also asked what percentage of new abuse contacts entered into the database (that were validated within the first 24 hours) failed the initial validation.

Angela said about 10% of these new contacts failed.

Rüdiger said this was quite high. He thought they should be looking at what these people’s perceptions were in terms of their responsibilities and what further support or information the RIPE NCC could provide to help them set up their initial contacts.

Angela agreed that the first validation email might have been a bit bold in the sense of “please click here.” They had updated the email since then to include more information and a link to the policy. For new LIRs that were creating their abuse contact, this was done via a field in the membership form that included wording that they should check this was a working email. She thought it was helpful that a ticket was created immediately when this failed the validation, to show that they were being helpful rather than punitive and simply wanted to get the contact updated.

Rüdiger suggested they could send an example of the email to the WG mailing list.

Angela said they could do this.

Rüdiger asked if they were providing new information for new LIR to clarify what the RIPE NCC considered a “valid” email.

Angela said they were not and possibly they could clarify in the description that a valid email was one that was able to accept email. She added that it was difficult to give a clear message in a single email - people often had poor English or were not reading the emails.

**C2. Policy Proposal 2019-04 - Validation of "abuse-mailbox"**

**Jordi Palet Martinez, The IPv6 Company**

Hervé noted that 2017-02 had only been accepted back in June. Personally, he would have waited a little longer to see the impact of the first policy proposal in terms of the RIPE NCC’s workload. If they decided not to go into the details he had provided last time, he thought the RIPE NCC had a large number of members and so it was not so easy to check. He also noted that while 2017-02 had added only one line to the policy, Jordi’s proposal added four paragraphs and he was not sure if this was a good thing.

Jordi said he had discussed this with the chairs and the RIPE NCC for about one year before submitting the proposal. They agreed that they needed to wait for some results from the previous policy proposal. However, the results of the last proposal were not telling them how many contacts were really valid.

Piotr said he was thinking of the boiling frog. He had seen a comment from Carlos saying they should wait a year or so after the policy was accepted. Jordi was taking small steps that extended the burden on the members. In the previous presentation, Jordi had said they could not be sure if an abuse contact that passed validation was legitimate, because someone could add the RIPE NCC’s (for example). However, Piotr did nott think that Jordi’s proposal solved this either – he did not imagine the RIPE NCC would send one email for every individual database reference.

Jordi replied that he had included a solution for this in the proposal but had been told by the RIPE NCC not to put so many details and instead just to tell them what he wanted to be validated.

Michele said he hated the proposal and did not know what it was trying to solve. He thought Jordi was covertly trying to get to something else that he had not proposed. Instead, he was proposing something that gave anyone a headache but did not actually solve anything. Saying it was not appropriate to wait for the results of the other policy changes was disingenuous. Because if the other proposal, which was to do with the basic technical validation of abuse contacts, were to show that there was a very large percentage of abuse contacts that did not work technically, he would be getting to the same place. Jordi’s proposal was creating a lot of work for the RIPE NCC but did not move the needle towards what he was trying to achieve - which was to enforce some kind of responsiveness. If that was what he wanted, he should create a new proposal.

Nick agreed with Michele’s comment and said they were all interested in combating abuse in their region, but this proposal did not achieve this. He said the proposal effectively said that there must be an abuse contact that was reachable by a human and if there was not, the RIPE NCC would close them down. The rest of the proposal was micromanaging of the RIPE NCC staff and telling them how to do their jobs, which he found somewhat demeaning. It was not their business as a WG to tell the RIPE NCC what to do in this level of detail. A policy proposal should include a broad outline of what they wanted to achieve. If Jordi’s proposal was that they must have abuse contacts and these must be reachable by email and if registries would be closed if they did not – this was fundamentally an unfair and inappropriate policy to have. He said on the mailing list the point had already been made that, if you had a policy like this, it could be taken to the courts and if it could be found as disproportionate under law and any members that were closed down could have this decision overturned.

Jordi said he had mentioned this in his slides (relating to due diligence).

Nick said this referred to acts of dishonesty in cases where organisations had a direct relationship to the RIPE NCC rather than micromanaging the operations of organisations.

Hans Petter, speaking as Chief Security Officer at Visma, said he agreed with the big picture goal that they needed to handle abuse in a responsible and efficient manner. Today, and in the future, this did not necessarily mean a human response. His people worked with automation and machine learning and so on. If they put requirements like this on them and it became a nuisance, it would be automated. He asked why they needed a policy to tell the RIPE NCC to implement what was in its mission and in their contract. This was their responsibility to implement this. What Jordi was describing was technical implementation details rather than policy.

Peter Koch, DENIC, said this was not a policy proposal – it had no clarity about what he wanted to achieve and lacked precision. He considered this an abuse of the policy process, because the bigger picture was that he was trying to re-purpose the database and as a community they needed to stop this on higher grounds. He agreed with Piotr’s comment about the boiling frog. They could have a discussion about the purpose of the database, but changing it slice-by-slice was not the way to go. What they were missing was a common-sense understanding of what the database was and what the PDP was for. Regarding what was on Jordi’s slides, the RIPE NCC had no obligation or power for the RIPE NCC to enforce random policies. He had no interest in Jordi’s stories of “forum shopping” either – a chain was only as strong as its weakest link and he hoped RIPE would remain strong and could retain its sense.

Martin Levy, Cloudflare, said as interesting as it was, in a world of automation Jordi’s proposal went nowhere. His company dealt with an enormous amount of abuse email that was handled through automation. This policy did not handle this. He also noted that when he reviewed his abuse contact, he removed the phone and fax number, because it was not needed based on where this was going. He said Jordi’s proposal did not work and they should deal with it via automation.

Rüdiger said he could see the value of improving abuse processing as it was available in the wild. Abuse-c was an attempt to support this, but it was not the goal that they were all after. What Jordi was actually proposing was that they would depend on a Turing Test implementation, which could be defeated even with this proposal, simply buy hiring one of Amazon’s Mechanical Turks.

**C.3. Policy Proposal 2019-03 - BGP Hijacking is a RIPE Policy Violation (Preliminary Analysis by the RIPE NCC)
Marco Schmidt, RIPE NCC**

The video archive is available at:

<https://ripe78.ripe.net/archives/video/90/>

There were no questions.

**C.4. Policy Proposal 2019-03 - BGP Hijacking is a RIPE Policy Violation**

**Carlos Friacas, FCT|FCCN and Jordi Palet Martinez, The IPv6 Company**

The video archive is available at:

<https://ripe78.ripe.net/archives/video/91/>

Daniel Karrenberg, RIPE NCC, said they did not have enough time in the agenda to discuss this. This was about the fundamental distinction between top-down and bottom-up regulation. When the RIPE NCC was new, they had talked with a lot of governments who had a very top-down attitude. They had said: “You get your authority from IANA and you can turn off the Internet and we are very concerned about this.” He had replied that this was one way of seeing it – another way was that the real power was with the operators because they agreed to use these particular number pools, and they decided how to exchange traffic. If they decided that they did not like what the RIPE NCC was doing, they could move to a different system. What they were seeing here was a fundamental shift from the model where the operators were responsible for what they were doing and agreed on norms that allowed the Internet was operated responsibly. With this proposal they were seeing a shift from that approach to a top-down one that would break down. Rather than trying to use their self-regulation as a crowbar for their particular interest, the responsible parts of the community should think about how they could use their individual actions to eliminate or suppress the ill-intentioned part of the community. They would not have this problem if people would do basic route filtering and use RPKI. If they did not want this routing police stuff to happen as operators, they had to make some investments there. If they did not do this, the future looked very black.

Rüdiger said he had several thoughts that the proposal was insane as Jordi went through his presentation. It was not reasonable to do a proposal that assumed some process would work 100% of the time. Instead of investing in strange processes, more investment in actual routing security, implementation and work was needed. Other insanity points - he did not understand why they could not change a proposal’s title. If the process did not allow it, they could just withdraw the old proposal and submit a new version. One point where he wondered if their PDP had insanity in it was if it was true that changing the proposal text required the RIPE NCC to put a lot of work into the impact analysis before they community could have a consensus discussion.

Brian said it was possible to change text in the PDP, but there was a level of change that meant a completely different version was required.

Michele said he had originally supported the proposal, but he now had to withdraw all support for it. This was because if someone was unable to articulate what was in a proposal, then that proposal was flawed and needed to be withdrawn. He agreed with others that at a higher/meta-level, there were issues that operators needed to address and agree on. From an ethical standpoint, what Jordi was proposing was not a bad idea. However, the way he had gone about it, as per his other proposal, was fundamentally flawed. They agreed that hijacking resources was bad, but if he could not articulate this narrowly enough, then the proposal was flawed. He suggested re-framing the proposal more narrowly or else withdrawing it entirely. An alternative might be to have this as some kind of charter that they could agree on.

Jordi asked if Michele was willing to co-author a new proposal if he withdrew this one.

Michele clarified that he was not.

Piotr, speaking for himself, said Daniel had made a false distinction between government and self-regulation. Comparing RIPE to government or a regulatory body did not make sense as RIPE was super-inclusive and governments participated as part of the community. As a side-note, he suggested they look at the RIPE NCC’s arbiters panel for analogies about how the process worked that could be applied to the panel of experts.

Ana Wilson, HEAnet, thanked Jordi for bringing this forward. She did disagree to the slide from the RIPE NCC Services WG (on due diligence). Businesses needed to do to know who they were dealing with and this did not necessarily apply to the situation.

Peter Koch said it was not clear which version of the proposal was the subject of the impact analysis [the Chair clarified that it was the current version two]. He thought it was a failure of the process if the latest version of the proposal could not be made available to the community in the right place.

Brian said it had been sent to the mailing list and they were working to get it up in the correct place as soon as possible.

In addition to what Piotr had said about regulation, just because RIPE “self-regulated” (maybe of its own scope), this did not make it better than something that governments could come up with. That said, attribution at the international level had been subject to a number of failed attempts in UN and other fora. He found it very brave that this could be done in passing through a policy proposal in the RIPE region without the necessary involvement of experts in international law and international treaties.

Nick Hilliard, INEX, said the RIPE NCC was a registry and it should steer clear of attempting to dictate what the address resources were used for. If it became a stick with which to beat people, control of that stick would be taken away from the RIPE community and put into the hands of law enforcement authorities; they did not want to do this. In a more practical sense, Jordi was creating a sledgehammer to chase mosquitos. Someone could create a company for 50 euros, get resources for hijacking, and then disappear. You could do this hundreds of times per day by API. By the time the policy would be implemented, it would not be able to solve the problem. If someone was criminal enough to hijack resources, then they would be criminal enough to avoid the policy.

Owen DeLong, Great Home Technologies, said there was a fundamental misunderstanding about the registry in the policy proposal. Registries did not grant rights but rather rights were granted by the community on the basis of that registry. This distinction lay under most of the problems with this proposal and it was not understood by a large part of the community. Once this was understood, it became clear how impossible implementation of the policy would be and how harmful it could become.

Randy Bush, IIJ, said he would underline a point Daniel made – if you want to fix routing problems, you had to work with network operators.

Brian noted that they had MANRS and other people who were working on these things.

**E. Presentations**

**E1. The Curious Case of Fake UK LIRs**

**Gaith Taha**

The video archive is available at:

<https://ripe78.ripe.net/archives/video/95/>

Alexander said yesterday there had been some emotional discussion about the closure of Russian LIRs in the RIPE NCC Services WG. In Gaith’s presentation, he saw maintainer objects from those LIRs. He felt that they could find those people who were preparing malicious things, as the RIPE NCC had made some Russian LIRs responsible for that. He felt they should continue to discuss this.

**E2. Domain Abuse Activity Reporting**

**Samaneh Tajalizadehkhoob**

The video archive is available at:

<https://ripe78.ripe.net/archives/video/96/>

Brian apologised that there was no time for comments as they were already running into the break.

**X. AOB**

Brain thanked everyone for the robust discussion and reminded them to bring things to the mailing list.