**Anti-Abuse Working Group Minutes RIPE 84**

Markus de Brün, Co-Chair of the working group, introduced the session and went through the opening administrative matters. He noted that minutes from the last meeting had been sent to the list and, with no further comments, he declared the minutes approved.

Markus noted recent discussions on abuse handling training (see D.1) and on abuse-c: and inbound spam filtering, but there had been relatively little discussion on the list recently. He also noted that there were no recent policy changes to discuss.

D. Interactions
D.1. RIPE NCC Abuse Handling Training

The presentation is available at:
<https://ripe84.ripe.net/wp-content/uploads/presentations/42-Anti-Abuse-Training-update-RIPE-84-Final.pdf>

Gerardo Viviers presented on the RIPE NCC’s Abuse Handling training, noting some of the improvements made based on feedback received after earlier presentations. He noted the goals of the webinar, to motivate people to care about abuse handling, while providing some useful tools to manage it. The first iteration of the course is expected to be ready before the end of Q2/2022, at which point it will be opened for further feedback.

Markus asked the working group how best to proceed; Gerardo noted that a Zoom meeting was better attended than an asynchronous presentation and confirmed that the RIPE NCC will organise a further Zoom session to present the new iteration.

D.2. DNS Abuse Institute Reporting Tool
Graeme Bunton gave an update on the work of the DNS Abuse Institute, an organisation created in 2021 by the Public Internet Registry (PIR) to coordinate an industry-wide effort to tackle DNS abuse. The institute has created a tool called Net Beacon ([www.netbeacon.org](http://www.netbeacon.org)). Launching in the first week of June, it will provide a website for reporting, standardised forms, and “enrichment” (various kinds of analysis, correlation with other sources etc.). This is not a commercial endeavour (it is part of PIR’s not-for-profit mission) and will distribute the collected reporting to gTLD registries and registrars (they are still working to integrate with ccTLDs). Graeme noted that the forms provided by Net Beacon will be embeddable on your own websites, while the reports can be tailored for specific users. Net Beacon is not an abuse management tool, however; it’s about getting abuse reports into the abuse management system you may already be using. It does not identify abuse, and the information will not be retained long-term.

Graeme noted that he is keen to hear back from the community on how people deal with abuse reports, what information they look for, how escalation is managed.

Patrick Tarpey of OFCOM noted that the EU recently made an announcement about handling CSAM and terrorism-related content (the UK also has regulation in this space); he asked how the tool can deal with different regulatory regimes and asks. Graeme noted that this tool is not trying to fit into any particular regulatory regime, and specific needs for specific laws will be addressed by other tools. The legal “floor” tends to be higher than what Net Beacon would capture.

Daniel Mahony (ISC) asked about a spam source that refuses to respond to any reporting or complaint. Graeme noted that a centralised reporting function can be useful in providing a record that complaints have been filed with the provider; this can be helpful with escalating action against the spam source.

D.3. RIPE Database Requirements Task Force Report
Markus noted that the task force had presented recommendations to various RIPE working groups based on its report. One point, regarding publishing the legal address of resource holders in the RIPE Database, was pushed to the Anti-Abuse Working Group for further discussion. The task force could not reach consensus on a recommendation on this matter, and Markus noted that the working group needs to consider how to reach a position. The matter will be taken to the mailing list.

E. Presentations
E.1. Countering DDoS Attacks with Comprehensive ACLs learnt from Blackholing Traffic - Matthias Wichtlhuber, DE-CIX

The presentation is available at:
<https://ripe84.ripe.net/wp-content/uploads/presentations/22-ddos_acls.pdf>

Matthias looked at the methods for countering DDoS attacks, from remote-triggered blackholing to more costly DDoS mitigation techniques (which are more effective); between those extremes are Access Control Lists (ACLs), but there is no centralised collection of good ACLs. He described an approach developed based on IXPs’ visibility of RTBH traffic and announced that they will be providing open access to the list of ACLs they have compiled. The approach leverages “association rule mining” (as used in e-commerce platforms) to identify traffic to be blackholed. The ACLs are hosted on Github (link in slides).

Praveen Puvvadi from Twitch asked whether the model works fast enough to react during an ongoing DDoS attack. Matthias noted that this is not an online model - that might be possible, but it would be a lot more work. He also clarified that they are not open sourcing the model, only the results.

Steven Bakker from AMS-IX asked about how often the ACLs are updated. Matthias noted they will likely update but was unsure as to the frequency (perhaps quarterly or half-yearly). Steven suggested that it would be interesting to see how much difference there would be between updates.

Praveen asked whether IPv6 or IPv4 makes any difference. Matthias confirmed that since they’re only looking at the header data, it doesn’t make much difference.

E.2. Pro-active blocking reduces "unwanted traffic" to a bare minimum > 99% - Jeroen Leendertz, Hackers Bescherming B.V.

The presentation is available at:
https://ripe84.ripe.net/wp-content/uploads/presentations/111-RIPE-84-19-5-22-Anti-Abuse-E2.pdf

Jeroen presented on a new approach to reducing ”unwanted/bad” traffic using blocklists. He sought to open a community discussion of this kind of solution, which is blocking around 50% of traffic even for small websites. He noted that he would share further information on the mailing list.

There was no other business, and Markus closed the meeting at 10:14.