

Anti-Abuse Information In RIPEstat

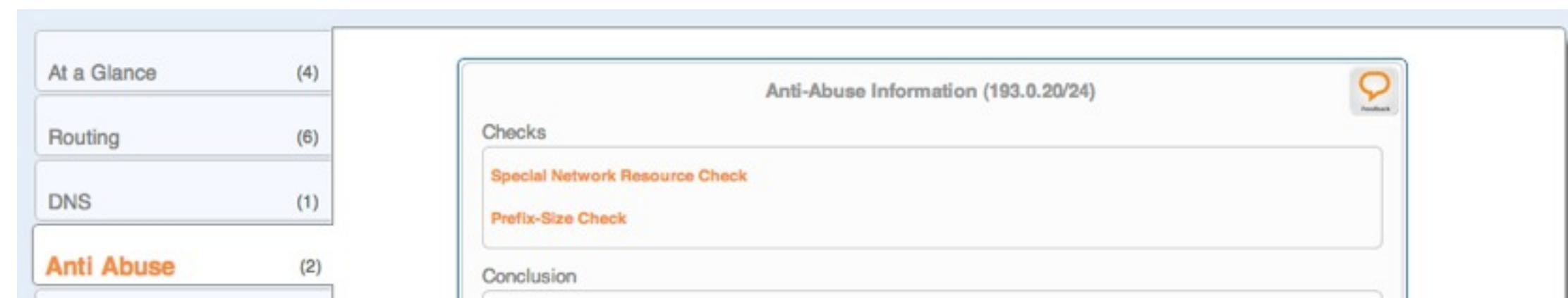
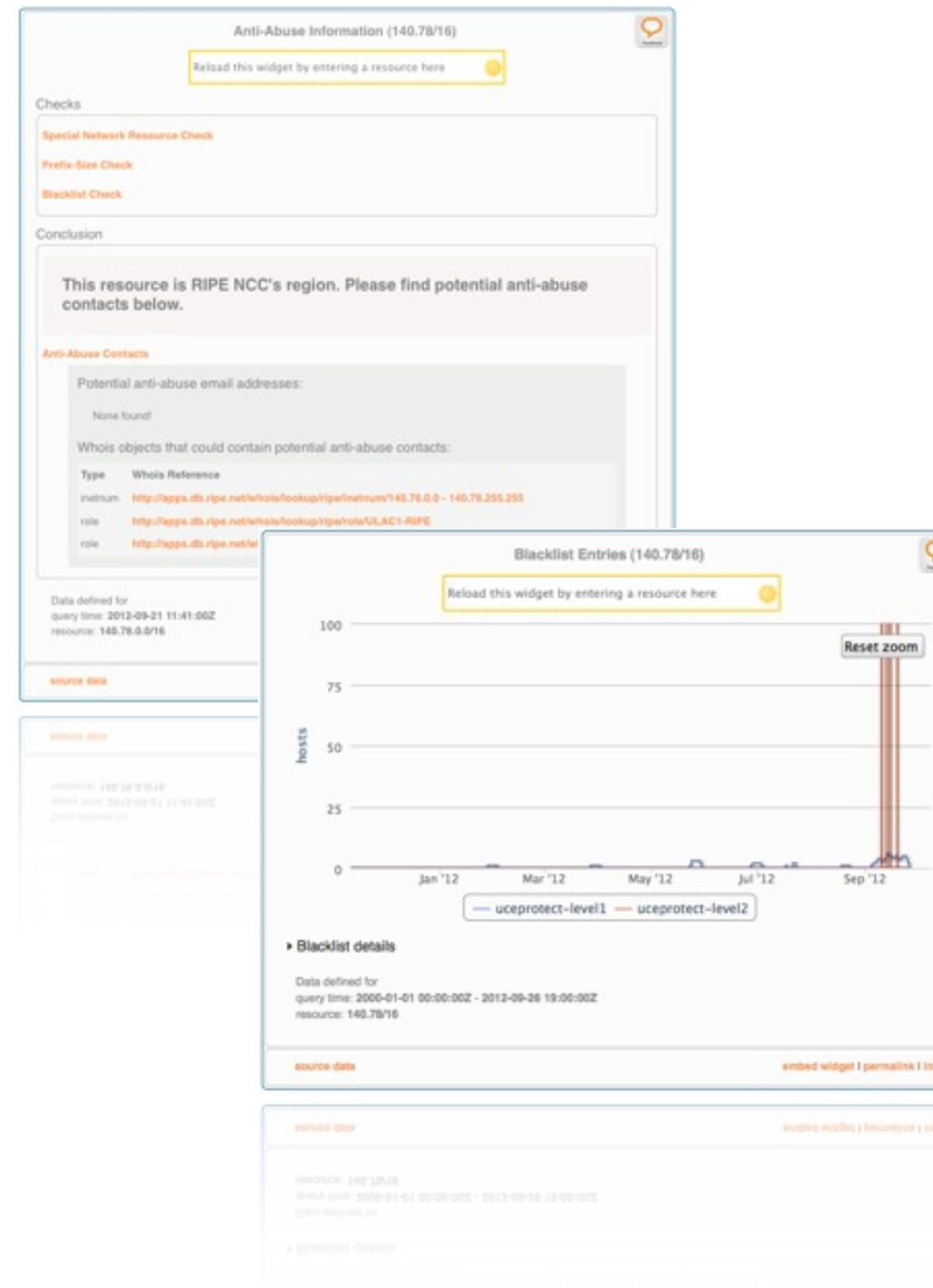
Anti-Abuse WG, RIPE65
27 September 2012

Christian Teuschel
christian.teuschel@ripe.net



Anti-Abuse on RIPEstat

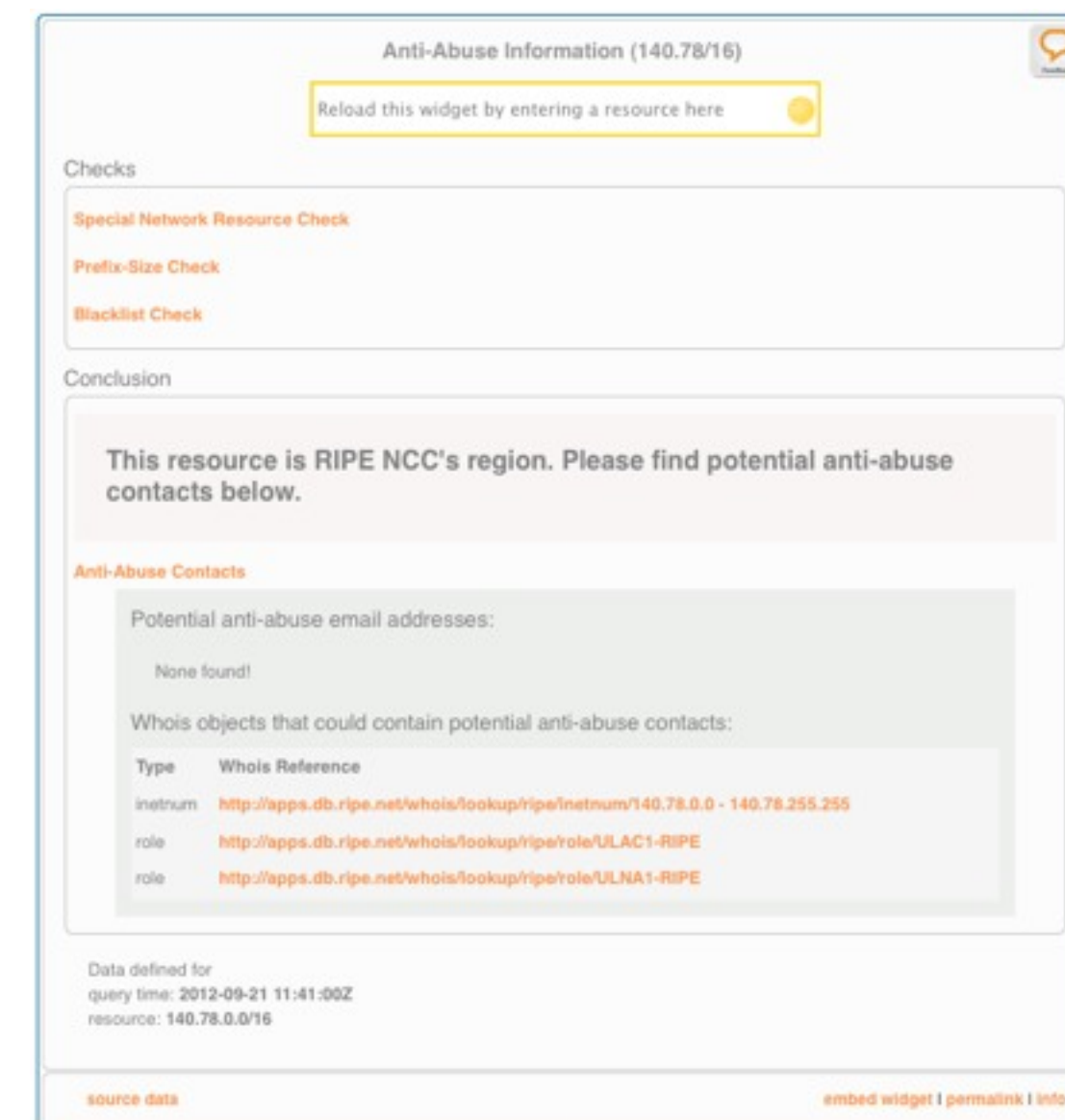
- New Anti-Abuse-Info widget
- Data sources for blacklists
- Additional anti-abuse widgets



Anti-Abuse-Info Widget - What is it?

- A lot of requests for anti-abuse information on RIPEstat's feedback channels (many users with no knowledge about anti-abuse)
- Target audience is “average” Internet user

<https://stat.ripe.net/widget/abuse-info>



The screenshot shows the 'Anti-Abuse Information (140.78/16)' widget. At the top, there is a search bar with the text 'Reload this widget by entering a resource here'. Below this, there are three check categories: 'Special Network Resource Check', 'Prefix-Size Check', and 'Blacklist Check'. A 'Conclusion' section states: 'This resource is RIPE NCC's region. Please find potential anti-abuse contacts below.' Underneath, there is a section for 'Anti-Abuse Contacts' which includes 'Potential anti-abuse email addresses: None found!' and 'Whois objects that could contain potential anti-abuse contacts:'. A table lists these objects:

Type	Whois Reference
inetnum	http://apps.db.ripe.net/whois/lookup/ripe/inetnum/140.78.0.0-140.78.255.255
role	http://apps.db.ripe.net/whois/lookup/ripe/role/ULAC1-RIPE
role	http://apps.db.ripe.net/whois/lookup/ripe/role/ULNA1-RIPE

At the bottom, it shows 'Data defined for query time: 2012-09-21 11:41:00Z resource: 140.78.0.0/16' and navigation links for 'source data', 'embed widget', 'permalink', and 'info'.

Anti-Abuse-Info Widget - What is it?

- Based on Content-Abuse-Finder

– <https://apps.db.ripe.net/search/abuse-finder.html>



Basic algorithm to extract anti-abuse info:

- IRT objects
- Abuse-mailbox attributes
- Abuse related remarks

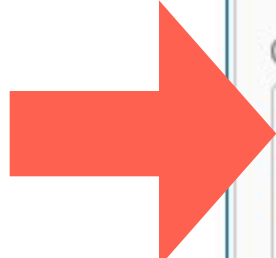
Anti-Abuse-Info Widget - There's a catch!

- Finding correct anti-abuse contacts is not trivial
 - making the extraction process too strict might result in not enough information
 - making it too moderate produces false-positives

Anti-Abuse-Info Widget - How we tried to improve it!

Checks

- Special Network e.g. RFC1918
- Blacklist results
- Prefix Size lookup for a single IP compared to e.g. /24



Anti-Abuse Information (140.78/16)

Reload this widget by entering a resource here

Checks

- Special Network Resource Check
- Prefix-Size Check
- Blacklist Check

Conclusion

This resource is RIPE NCC's region. Please find potential anti-abuse contacts below.

Anti-Abuse Contacts

Potential anti-abuse email addresses:

None found!

Whois objects that could contain potential anti-abuse contacts:

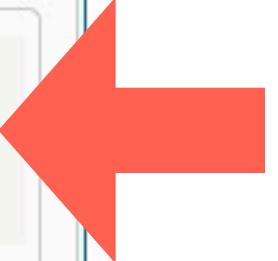
Type	Whois Reference
inetnum	http://apps.db.ripe.net/whois/lookup/ripe/inetnum/140.78.0.0 - 140.78.255.255
role	http://apps.db.ripe.net/whois/lookup/ripe/role/ULAC1-RIPE
role	http://apps.db.ripe.net/whois/lookup/ripe/role/ULNA1-RIPE

Data defined for query time: 2012-09-21 11:41:00Z resource: 140.78.0.0/16

source data embed widget | permalink | info

“Conclusion”

- No results for resources outside RIPE NCC region
- Though references to other RIR's whois DBs



Anti-Abuse-Info Widget - The solution?

- Policy proposal as the cure?
 - Abuse Contact Management in the RIPE NCC Database

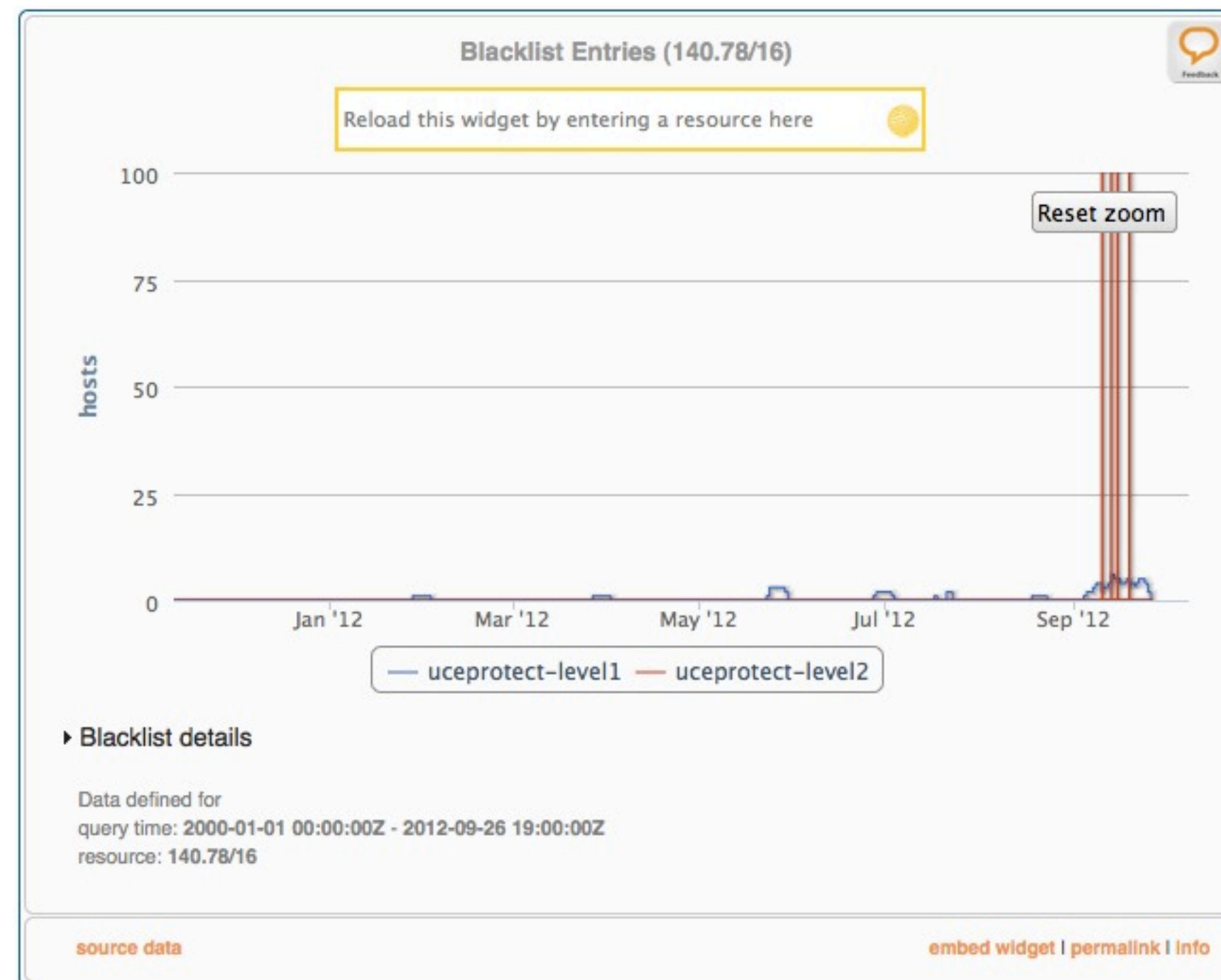
<https://www.ripe.net/ripe/policies/proposals/2011-06>

Anti-Abuse-Info Widget - How should we go on?

- Should we spend time on the Anti-Abuse-Info widget?
- What do you prefer?
 - More false-positive results or more restrictive results
 - Any more checks?
 - Geolocation
 - Distance in the RIPE DB of exact matched object and the one that carries the anti-abuse information

Blacklist Used on RIPEstat - Status quo!

- Current blacklist sources:
 - Spamhause's DROP
 - uceprotect 1-3



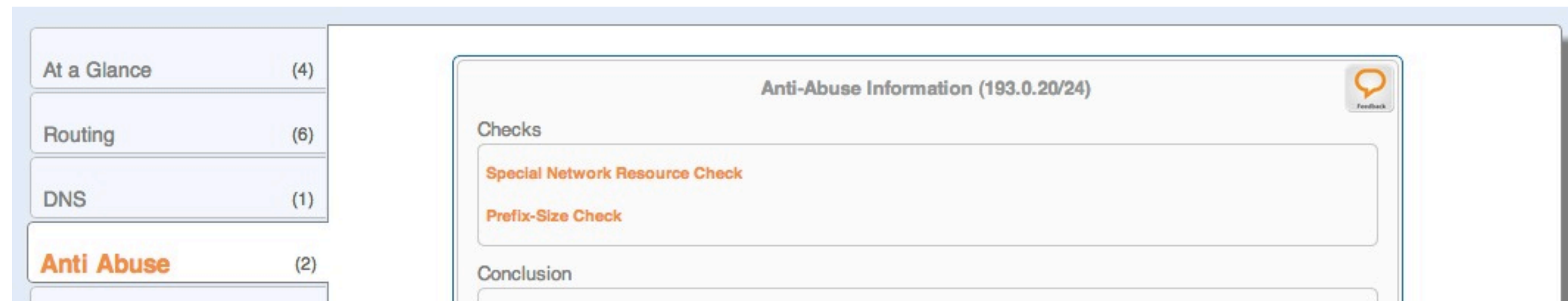
<https://stat.ripe.net/widget/blacklist>

Blacklist Used on RIPEstat - How to improve it?

- We received feedback from users that we should not use certain blacklist sources
- Is clearly marking the source of the data enough?
- What lists do you recommend? Why?

Other anti-abuse widgets - More widgets?

- RIPEstat's new UI comes with a tab for anti-abuse which currently holds:
 - Anti-Abuse-Info
 - Blacklist



- Suggestions for other widgets to add?

Feedback

- Outside this session and after RIPE65:
 - Questions
 - Recommendations
 - ...
 - and general feedback
- Reach us via: stat@ripe.net