draft-ietf-grow-filtering-threats-02

Camilo Cardona, IMDEA Networks Institute

Pierre Francois, IMDEA Networks Institute

Paolo Lucente, Cisco

Executive summary

- If you
  - – filter more specific BGP prefixes of others, or
  - – use communities to trigger selective propagation of your BGP paths to more specific prefixes,
- the transit policy of someone in your AS neighborhood may get violated,
  - – without black-holing of traffic
  - – Someone ends up offering free rides through his infrastructure without anyone complaining

So what can we do?

- Technically enforce the respect of your policies
  - Analyzed to be difficult
  - Leads to black-holing when facing the situation

- Carefully filter / tag paths
  - Need to be aware of the risks
- Monitor your network
  - Let the policy violation happen, react to it

History

- Presented at IETF a long time ago,
    - Advised to present to operators
- Presented at RIPE, got hallway feedback
    - "It happened to me" / "I did it"
    - "I do filtering and tag my paths with communities to do TE, I'd be ashamed if it would lead to policy violation at my peers"
    - Met Paolo
        - Provided a tool to detect policy violations in your network
- Working Group doc at GROW

Status

- In last call but no more comments received
- Added Paolo as a co-author
  (He should have been from day one :-S)

- Let’s try to close this?

Comments or questions?

On the grow mailing list!

Thank you