APNIC Information Services for Network Operators

Sofía Silva Berenguer
Product Manager – Information Services
Our aim

• Provide **meaningful information services** to the communities APNIC serves

• In network operations:
  – Offer **tools** that will help you make **better-informed network decisions**, **solve routing issues** and **deal with potentially malware infected devices**

• **Listen and learn** about your most common issues so we can work together to find solutions that meet your needs
Agenda

• Update on products for network operators:
  – **NetOX** (Network Operators’ toolboX)
  – **DASH** (Dashboard for Autonomous System Health)

• APNIC **Community Insights** program

• Opportunities for you to **have a say**
NetOX

• **What is it?**
  – Set of **tools** for network operators

• **What can you do with it?**
  – Analyse your (and other) **networks** to:
    • Solve routing issues
    • Make better-informed network decisions

• **Categories:**
  – At a glance
  – Quality Check
  – Routing
  – Anti Abuse
  – Database
  – Geographic
  – Activity

• Working in collaboration with the RIPE NCC

• Available at: [https://netox.apnic.net](https://netox.apnic.net)
NetOX – Use Case

I’m considering hiring a new upstream provider. I wonder how well interconnected AS 4608 is?

They probably offer good robustness as they have three providers.

Yoshi
“I run the net”
I’m having some routing issues. AS 4608 seems to be filtering one of my prefixes. I’ve tried contacting the whois PoC but they were not very responsive. There must be a better contact for this type of issue.
I'm getting 27.100.7.0/24 transferred. I wonder if this prefix is clean.

It looks like this prefix is already in use!

And it has been routed for quite a long time!
NetOX – Use Case

Ummm, it hasn't been assigned by APNIC yet.

This prefix is a bogon!

Yoshi
“I run the net”
And it’s in a black list!

This prefix is definitely not clean!
NetOX - What are we busy with?

- **Welcome page** to clearly communicate value proposition

- Validation of **ideas for new widgets** to help network operators evaluate whether to connect to other networks
  - *We will soon run a survey! Would you like to participate?*
DASH

• **What is it?**
  – Portal for APNIC resource holders

• **What can you do with it?**
  – Be informed about **suspicious traffic seen coming from your network**
  – **Compare** suspicious activity coming from your organization’s network **against your economy or sub-region**
  – **Generate a report** summarizing your network’s situation
  – Get **additional insights** from the APNIC security team about the suspicious activities detected
  – Stay on top of relevant **security news**
Suspicious traffic
Latest 30 days

My network
- **55.0 %**
  - Current period: 01-May / 30-May
  - 447 hits
  - Previous period: 01-Apr / 30-Apr
  - 993 hits

Viet Nam
- **16.5 %**
  - Current period: 01-May / 30-May
  - 41.8K hits
  - Previous period: 01-Apr / 30-Apr
  - 50.0K hits

South East Asia
- **18.1 %**
  - Current period: 01-May / 30-May
  - 44.8K hits
  - Previous period: 01-Apr / 30-Apr
  - 54.7K hits

My network compared to Viet Nam

Daily totals of suspicious traffic seen coming from testASN compared to Viet Nam

[Graph showing daily totals of suspicious traffic]
DASH

• How does it work?
  – DASH collects data from a **distributed honeypot network** that is part of APNIC’s Community Honeynet Project
    • Read more: [https://blog.apnic.net/2019/09/17/the-apnic-community-honeynet-project/](https://blog.apnic.net/2019/09/17/the-apnic-community-honeynet-project/)

• Short video available: [https://dash.apnic.net/about](https://dash.apnic.net/about)

• It’s been a prototype for a while **BUT** DASH v1.0 will be released soon!
I've seen in DASH that some of my prefixes have been seen sending suspicious traffic!

It seems one of the networks we use for corporate customers may have devices infected with malware.

I'll download a list to talk to them and ask them to get their networks checked.
DASH – Use Case

I’ll download a PDF report to share the situation of our network with my manager and discuss it with him.
In order to solve this issue, I will need some more information about the suspicious traffic my network has been sending. I’ll request additional insights from APNIC.
DASH - What are we busy with?

• Baking DASH v1.0!

• Main features:
  – Welcome tour *(giving a few tips to start using the site)*
  – Information about suspicious traffic at the **IP level**
  – All protocols and destination ports collected by honeynet sensors now available through DASH
  – Request for additional insights from APNIC security team
APNIC Community Insights Program

• We are working hard to focus on you and your needs
• To understand your needs we are setting up a group of people who are interested in helping us create better products and services for everyone
• YOU can have an impact on the way APNIC develops products
• Let us know if you want to be heard!
• Sign up at: https://www.apnic.net/your-say
Have a say

• **NetOX**
  – Participate in a survey about *how network operators evaluate whether to connect to other networks*

• **DASH**
  – Give us your *feedback* about DASH v1.0

• Sign up to the **Community Insights** Program and you will be invited to participate in user research activities

• Use the **Feedback** button in our products to:
  – Provide suggestions
  – Report bugs

APNIC
Summary

• We are working on products to offer information to network operators
  – NetOX (Network Operators’ toolbox)
  – DASH (Dashboard for AS Health)

• We want to hear FROM YOU!
  – Do you see value in these products?
  – Do you want to provide any feedback?
  – Do you want to participate in interviews, testing sessions, and so forth?